

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/327282017>

# FUNDAMENTALS OF INFORMATION SECURITY

Book · April 2017

CITATIONS

0

READS

13,383

1 author:



**Bosubabu Sambana**

Raghu Engineering College

104 PUBLICATIONS 26 CITATIONS

SEE PROFILE

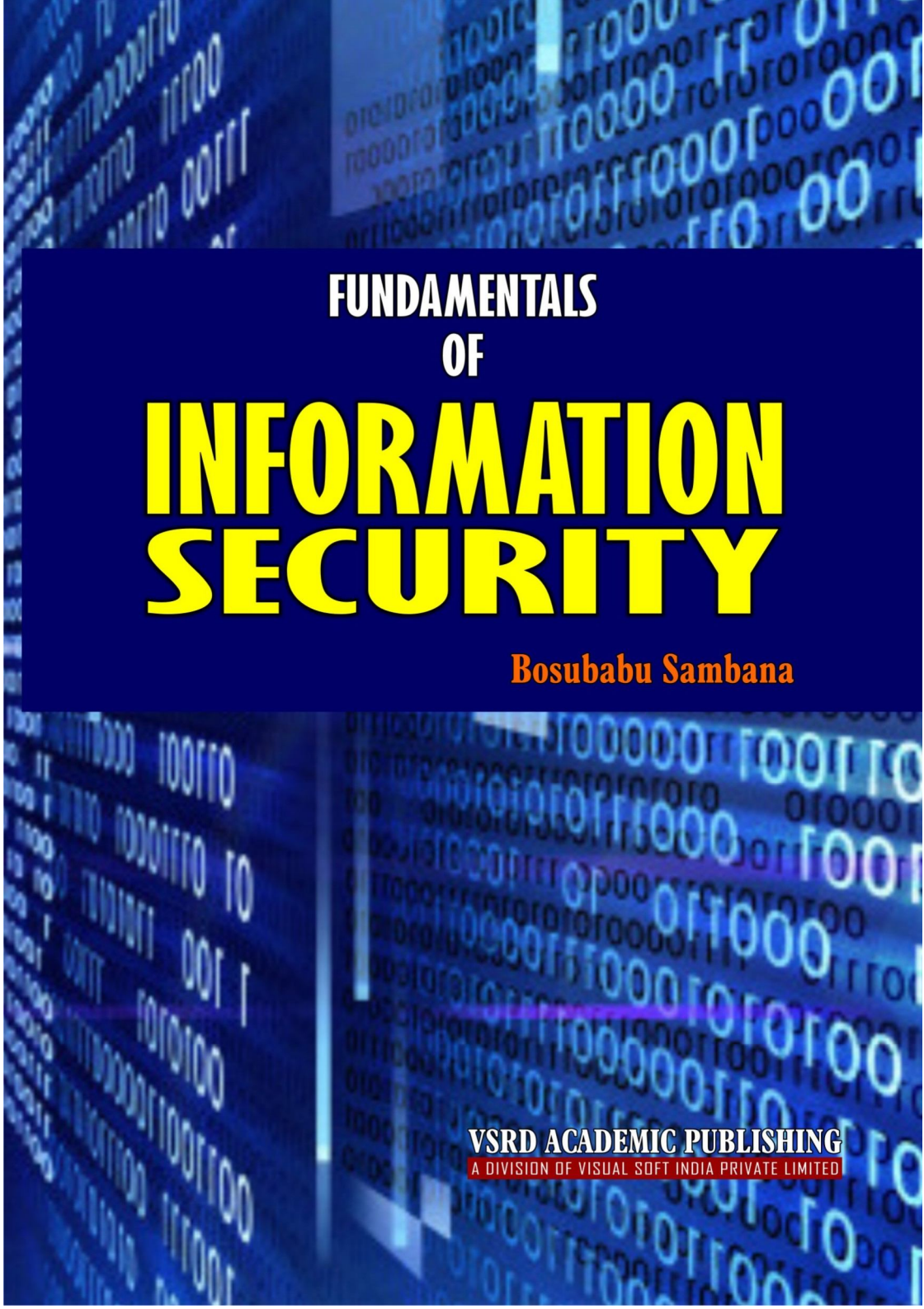
Some of the authors of this publication are also working on these related projects:



Automated Wheel Chair for Physically Challenged [View project](#)



Copyrights [View project](#)



# **FUNDAMENTALS OF INFORMATION SECURITY**

**Bosubabu Sambana**

**VSRD ACADEMIC PUBLISHING**  
A DIVISION OF VISUAL SOFT INDIA PRIVATE LIMITED



**FUNDAMENTALS**  
**OF**  
**INFORMATION SECURITY**

**Bosubabu Sambana**  
*Assistant Professor – CSE Dept.*  
**Avanthi Research & Technological Academy, Bhogapuram**  
**Jawaharlal Nehru Technological University**  
**Kakinada, Andhra Pradesh, INDIA.**

# FUNDAMENTALS OF INFORMATION SECURITY

Copyright © : Bosubabu Sambana  
Publishing Rights © : VSRD Academic Publishing  
*A Division of Visual Soft India Pvt. Ltd.*

**ISBN-13: 978-93-86258-38-0**

**FIRST EDITION, APRIL 2017, INDIA**

*Typeset, Printed & Published by:*  
**VSRD Academic Publishing**  
*(A Division of Visual Soft India Pvt. Ltd.)*

**Disclaimer:** The author(s) are solely responsible for the contents of the papers compiled in this book. The publishers or its staff do not take any responsibility for the same in any manner. Errors, if any, are purely unintentional and readers are requested to communicate such errors to the Editors or Publishers to avoid discrepancies in future.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the Publishers & Author.

*Printed & Bound in India*

## **VSRD ACADEMIC PUBLISHING**

*A Division of Visual Soft India Pvt. Ltd.*

### **REGISTERED OFFICE**

154, Tezabmill Campus, Anwarganj, KANPUR–208003 (UP) (IN)  
Mb: 99561 27040, Web: [www.vsrdpublishing.com](http://www.vsrdpublishing.com), Email: [vsrdpublishing@gmail.com](mailto:vsrdpublishing@gmail.com)

### **MARKETING OFFICE (NORTH INDIA)**

Basement-2, Villa-10, Block-V, Charmwood Village, FARIDABAD–121009 (HY)(IN)  
Mb: 98999 36803, Web: [www.vsrdpublishing.com](http://www.vsrdpublishing.com), Email: [vsrdpublishing@gmail.com](mailto:vsrdpublishing@gmail.com)


### **MARKETING OFFICE (SOUTH INDIA)**

340, FF, Adarsh Nagar, Oshiwara, Andheri(W), MUMBAI–400053 (MH)(IN)  
Mb: 99561 27040, Web: [www.vsrdpublishing.com](http://www.vsrdpublishing.com), Email: [vsrdpublishing@gmail.com](mailto:vsrdpublishing@gmail.com)

# P R E F A C E

Now a day's Information Security is plays vital role in our technical world, everyone must need to know about it, in this way this book fully supports and doubt clearances of various fields.

In this book we learn need for Security through various strategies, planning for security, design principles of network architecture, how to information security provides more ways during transmission in safely manner without any consumptions, other chapters we learn briefly on IP security, Web security, Data communication system, Information Security and Cyber security. In this way detailed elaborates every concepts with valid examples and its applications.

 *Mr. Bosubabu Sambana*

# ACKNOWLEDGEMENT

This Book is heartily dedicated to beloved

my Father and God

**Sri.S. DANDASI**

He completely scarifies entire his life for me.  
Thanking you for giving birth from your soul.

AND

My Life inspirer **Sri.Dr.A.P.J.Abdul Kalam**



# **About the Book**

This book on Fundamentals of Information Security is designed to focus on the basics of information transmitted in various fields, in during transmission protect more security through layer by layer, and knowledge seeker much understand various security platforms during data transmission. It may be helpful for various universities prescribed syllabus covered in existing streams.

Apart from course specific learning, this book is meant for a wide range of readers who intend to learn the basics of Information Security and its applications. This book lays emphasis on various security development strategies, and fully clarification about web and IP security through cyber security awareness helpful of Real time applications.

## **Organization of the Book**

This book consists of Six (6) chapters. It starts with the Planning for security and end with Cyber security.

Chapter 1 gives an introduction to planning for security, the basic building blocks Fundamentals of Information Security, Information Security policies, Cryptography analysis through proven one algorithm and attacks, Public key management and S/MIME etc.

Chapter 2 enhances the basic concepts studied in chapter 1 and gives an introduction to IP Security. It covers the aspects of IP Security and detailed explains IP Security Architecture, and domain of inter connections.

Chapter 3 is dedicated to Web Security development environment and explains the issues faced by an unauthorized owner/user access to developing methods in the existing resources.

Chapter 4 introduces the basic concepts of Data



communication system and its Network Architecture, various types of computer Networks and its topologies. Discussed in detailed for ease in application approach on digital transmission, wireless communication system and transmission media.


Chapter 5 discusses on the various requirements and procedure to develop few applications of information security with protection methods and cryptography aligned various topics, Email security, The SDLC.

Chapter 6 enhances the basic concepts studied in cyber security with digital forensics related concepts, cyber crimes and its categories with problem solving issues, cyber law, E-Governances.

### **Salient Features of the Book**

The salient features of the book include:

- Detailed explanation on the basics of Information security
- Study on various building blocks of an information security applications.
- Description of computer networking concepts.
- Detailed study on the models of data transmission and transmission media with suitable examples.
- Introduction to Real time operation in information systems and Cryptography algorithms with related concepts.
- Study on Data communication system and used in Real- time platform.
- Implementation of Information security to real life applications.
- Easy to understand Public key algorithm and Email Security.
- Basic concepts of Cyber security with related issues.
- Description of Cyber Law, Intellectual Property Rights and Information Security Act.

 *Bosubabu Sambana*

# CONTENTS

<b>CHAPTER 1 : PLANNING FOR SECURITY .....</b>	<b>1</b>
1.1. INTRODUCTION .....	3
1.2. INFORMATION SECURITY POLICY, STANDARDS AND PRACTICES.....	3
1.3. INFORMATION SECURITY BLUEPRINTS .....	7
1.4. PRINCIPLES OF CRYPTOGRAPHY .....	9
1.5. ADVANCED ENCRYPTION STANDARD (AES).....	12
1.6. CRYPTOGRAPHY TOOLS.....	15
1.7. ATTACKS ON CRYPTOSYSTEMS.....	17
1.8. PUBLIC-KEY MANAGEMENT .....	20
1.9. S/MIME (SECURE/ MULTIPURPOSE INTERNET MAIL EXTENSION).....	21
1.10. MULTIPURPOSE INTERNET MAIL EXTENSIONS (MIME) .....	22
1.11. MIME .....	25
 <b>CHAPTER 2 : IP SECURITY .....</b>	<b>27</b>
2.1. INTRODUCTION .....	29
2.2. UNDERSTANDING IPSEC .....	29
2.3. IP SECURITY OVERVIEW.....	31
2.3.1. BENEFITS OF IPSEC.....	33
2.4. IP SECURITY ARCHITECTURE .....	35
2.4.1. IPSEC DOCUMENTS .....	36
2.5. DOMAIN OF INTERPRETATION (DOI) .....	38
2.6. IP VERSIONS .....	39
2.6.1. INTERNET PROTOCOL V4 (IPV4).....	40
2.6.2. INTERNET PROTOCOL V6 (IPV6).....	44
 <b>CHAPTER 3 : WEB SECURITY .....</b>	<b>49</b>
3.1. INTRODUCTION .....	51
3.2. WEB SECURITY CONSIDERATIONS .....	51
3.3. DIGITAL SIGNATURE .....	52
3.4. SECURE SOCKETS LAYER .....	58
3.5. TRANSPORT LAYER SECURITY .....	60
3.6. HOW TO WORKS .....	61

## **CHAPTER 4 : DATA COMMUNICATION SYSTEM..... 63**

<b>4.1. INTRODUCTION.....</b>	<b>65</b>
<b>4.2. NETWORK ARCHITECTURE .....</b>	<b>66</b>
<b>4.3. TYPES OF COMPUTER NETWORKS.....</b>	<b>69</b>
4.3.1. PERSONAL AREA NETWORK.....	70
4.3.2. LOCAL AREA NETWORK.....	71
4.3.3. METROPOLITAN AREA NETWORK.....	72
4.3.4. WIDE AREA NETWORK .....	72
4.3.5. PRIVATE NETWORKS .....	73
4.3.6. INTERNETWORK.....	73
<b>4.4. NETWORK TOPOLOGIES .....</b>	<b>74</b>
4.4.1. BUS TOPOLOGY .....	75
4.4.2. RING TOPOLOGY .....	77
4.4.3. STAR TOPOLOGY .....	78
4.4.4. MESH TOPOLOGY.....	80
4.4.5. TREE TOPOLOGY .....	82
4.4.6. HYBRID TOPOLOGY .....	83
4.4.7. POINT-TO-POINT .....	84
4.4.8. DAISY CHAIN .....	84
<b>4.5. DIGITAL TRANSMISSION.....</b>	<b>85</b>
<b>4.6. WIRELESS COMMUNICATION SYSTEM .....</b>	<b>93</b>
4.6.1. TYPES OF WIRELESS COMMUNICATION .....	94
<b>4.7. TRANSMISSION MEDIA .....</b>	<b>103</b>

## **CHAPTER 5 : INFORMATION SECURITY .....107**

<b>5.1. INTRODUCTION.....</b>	<b>109</b>
<b>5.2. CRITICAL CHARACTERISTICS OF INFORMATION .....</b>	<b>110</b>
<b>5.3. THE SDLC.....</b>	<b>111</b>
<b>5.4. SECURITY ATTACKS .....</b>	<b>117</b>
<b>5.5. FIREWALL DESIGN PRINCIPLES .....</b>	<b>118</b>
5.5.1. FIREWALL CHARACTERISTICS .....	119
5.5.2. LIMITATIONS OF FIREWALLS.....	121
<b>5.6. PUBLIC KEY CRYPTOGRAPHY ALGORITHMS.....</b>	<b>121</b>
5.6.1. WORKING MECHANISM .....	122
<b>5.7. E-MAIL SECURITY .....</b>	<b>126</b>
5.7.1. PRIVACY ENHANCED MAIL (PEM) .....	127
5.7.2. PRETTY GOOD PRIVACY (PGP).....	128
5.7.3. SECURE MULTIPURPOSE INTERNET MAIL EXTENSIONS (S/MIME).....	129

<b>5.8. WHY IS INFORMATION SECURITY IMPORTANT.....</b>	<b>130</b>
<b>5.9. INFORMATION SECURITY AND PROTECTION .....</b>	<b>132</b>

## **CHAPTER 6 : CYBER SECURITY ..... 137**

<b>6.1. OBJECTIVES .....</b>	<b>139</b>
6.1.1. CREATE AWARENESS .....	140
6.1.2. INTERNATIONAL NETWORK ON CYBER SECURITY .....	142
<b>6.2. NEED FOR CYBER LAW.....</b>	<b>143</b>
<b>6.3. THE INFORMATION TECHNOLOGY ACT.....</b>	<b>144</b>
<b>6.4. CYBER SECURITY VARIOUS STRATEGIES.....</b>	<b>146</b>
<b>6.5. CYBER FORENSICS .....</b>	<b>156</b>
<b>6.6. CYBER CRIMES.....</b>	<b>156</b>
6.6.1. HISTORY OF CYBER CRIME .....	157
6.6.2. TYPES OF CYBER CRIMES.....	157
6.6.3. CYBER CRIME IN MODERN SOCIETY.....	160
6.6.4. CATEGORIES OF CYBER CRIME .....	160
6.6.5. HOW TO TACKLE CYBER CRIME .....	161
<b>6.7. E-GOVERNANCE .....</b>	<b>163</b>
<b>6.8. CYBER SECURITY.....</b>	<b>165</b>
<b>6.9. DIGITAL FORENSICS .....</b>	<b>171</b>
6.9.1. FORENSICS BRANCHES .....	172
6.9.2. APPLICATIONS.....	174
<b>6.10. CYBER LAWS IN INDIA .....</b>	<b>176</b>
6.10.1.NEED FOR CYBER LAW IN INDIA .....	176
<b>6.11. INTELLECTUAL PROPERTY RIGHTS .....</b>	<b>178</b>



Book Matter

Book Matter





## ABOUT THE AUTHOR



**Bosubabu Sambana** working with Assistant Professor, Department of CSE, Avanathi's Research and Technological Academy, Vizianagaram. Affiliated to Jawaharlal Nehru Technological University-Kakinada. He is completed Bachelor of Science from Andhra University. He is completed Master of Computer Applications and Master of Technology in Computer Science & Engineering from Jawaharlal Nehru Technological University – Kakinada, Pursing Master of Science in Mathematics, Andhra University - Andhra Pradesh, India. He has 4 years good teaching experience and having a good Knowledge on Space Research, Future Internet Architecture, Cloud Computing, Internet of Things/Services/Data, Data Analytics, Computer Network and Hacking along with Computer Science Subjects. He has guided 12 B.Tech Students. He is Published 18 Research Papers in various reputed SCI /Scopus Indexed International and National Journals, Magazines and Conferences. He is participated 4 International and 3 National Conferences. He is Participated 2 National / International Workshop and 2 FDP. He is filling and processing 1 Patent application in Patent Office, Chennai and wrote 2 Textbook in Computer Science stream and have 2 Copyright and Secured 6 Certifications from NPTEL-IIT's various specifications like Algorithms for BigData, C++ Programming, Introduction to Research, Wireless Sensor Adhoc Networks, Internet Architecture, Internetwork Security, and Computer Architecture, Cloud computing etc. He is the member of SERB, Indian Science Congress, W3C, INTERNET SOCIETY, W3C, NASA (Student), Springer, Elsevier, Science Alert, IET, Editorial Manager, MECS-PRESS-IJMECS/ IJCSIT, W3C, Manuscriptcentral, TUBITAK-GIRIS, Internet Society, IAENG, IAAET, IJMETMR, IJECSE, IJCST, IJECSE and editorial / review member in ACM, IJMETMR, and Springer- Journal of Big Data.

### VSRD ACADEMIC PUBLISHING

A DIVISION OF VISUAL SOFT INDIA PRIVATE LIMITED

#### HEAD OFFICE

154, Tezabmill Campus, Anwarganj, KANPUR - 208 003 (UP) (INDIA)

Mb.: +91 99561 27040 || Web.: [www.vsrdpublishing.com](http://www.vsrdpublishing.com) || Email: [vsrdpublishing@gmail.com](mailto:vsrdpublishing@gmail.com)

#### MARKETING OFFICE (NORTH INDIA)

Basement-2, Villa-10, Block-V, Park Avenue, Charmwood Village, FARIDABAD - 121 009 (HY) (INDIA)

Mb.: +91 98999 36803 || Web.: [www.vsrdpublishing.com](http://www.vsrdpublishing.com) || Email: [vsrdpublishing@gmail.com](mailto:vsrdpublishing@gmail.com)

#### MARKETING OFFICE (SOUTH INDIA)

340, First Floor, Adarsh Nagar, Oshiwara, Andheri (W), MUMBAI -400 053 (MH) (INDIA)

Mb.: +91 99561 27040 || Web.: [www.vsrdpublishing.com](http://www.vsrdpublishing.com) || Email: [vsrdpublishing@gmail.com](mailto:vsrdpublishing@gmail.com)

FIRST EDITION, APRIL 2017

ISBN-13: 978-93-86258-38-0

Code No. : VSRDAP20170406

PRINTED IN SINGLE COLOUR

Size : A5

Pages : x+180

Price : ₹ 190.00

Export Price : US \$ 19.00

ISBN 978-93-86258-38-0



9 789386 258380