A Survey on Security Threats in Cloud Computing Technology

Harpinder Singh^1, Sheetal Kalra^2

1(Department of Computer Sciences and Engineering, Guru Nanak Dev University, RC, Jalandhar, Punjab, India
harpinder2065@gmail.com)
2(Assistant Professor, Department of Computer Sciences and Engineering, Guru Nanak Dev, University, RC, Jalandhar, Punjab, India
sheetal.kalara@gmail.com)

ABSTRACT

This manuscript introduces the characteristics, deployment and service models of cloud computing technology. Secondly, an analysis of the security threats in cloud computing under various areas of cloud has been done. The main aim of this manuscript is to understand the security risks and challenges which are currently security threats under the cloud models as well as network concerns to stagnate the threats within cloud environment

Keywords: Cloud computing, Security, Network threats

faced in the cloud computing scenario. This paper also provided reveals different

According to the U.S. NIST (National Institute of Standards and Technology) [2] Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing is the use of cloud resources (hardware and software) that are delivered as a service over a network (typically the Internet). A cloud service is generally used by the clients as and when needed, normally on the hourly basis. This "on-demand" or "pay as you go" approach makes the cloud service flexible. NIST further differentiates cloud as having five essential characteristics, three service models, and four deployment models.

1.1 Characteristics of Cloud Computing

Cloud computing differs from local computing in many ways. NIST has identified five characteristics in particular:

- On-Demand Self-Service: A user can request one or more services whenever he needs them and can pay using a ‘‘pay-and-go’’ method without having to interact with humans using an online control panel [1].
- Broad Network Access: A user is not tied to one location but can access resources from anywhere the network (typically the Internet) is available.
- Resource Pooling (Multi-tenancy): Cloud computing utilizes a multitenant model which allows

multiple users/customers to share resources from a large resource pool [8]. The resources are dynamically assigned and reassigned to facilitate each customer’s needs and includes processing, storage, memory, network bandwidth, and virtual machines

- Rapid Elasticity: Elasticity is another name for scalability; elasticity means the ability to increase or decrease resources whenever required. Users can request different services and resources as much as they need at any time. This characteristic is so admirable that Amazon, as a well-known cloud service vendor, has named one of its most popular and commonly used services the Elastic Compute Cloud (EC2) [1].
- Measured Service (Pay-Per-Use): The amount of usage by a customer is monitored by the provider and can be used for billing or other purposes. Any resources that are used are carefully monitored, controlled and recorded which allows the cloud service provider to be completely transparent with the consumer of the resources and facilities. The user only pays for the amount of resources they consume and are always made aware of any discrepancies, spikes or abnormal behavior regarding resources.

1.2 Deployment Models

There are four standard models, or types, of cloud computing that can be implemented to satisfy varying needs of users or providers.

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

Public Cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider [1]. One of the advantages of a Public cloud is that they may be larger than an enterprises cloud, thus providing the ability to scale seamlessly, on demand.

Private Cloud**:** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider [2]. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud [3].

Community Cloud**:** Based on their similar requirements, concerns, and policies, a number of organizations establish a community and share cloud computing to be used by their community member’s consumers. A third-party service provider or a series of community members can be responsible for providing the required infrastructure of the cloud computing. Lowering costs and dividing expenses between community members along with supporting high security are the most important advantages of a community cloud

Hybrid Cloud**:** A combination of two or more different public, private, or community clouds led to the creation of a different cloud model called hybrid cloud, in which constitutive infrastructures not only keep their specific properties but also require standardized or agreed functionalities to enable them to communicate with each other with respect to interoperability and portability on applications and data [1].

1.3 Service Models

Cloud computing can refer to several different service types, these services are described below:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Software as a Service: SaaS is software offered by a third party provider, available on demand, usually via the Internet configurable remotely. Examples include online Word Processing, Google Docs, and Spreadsheet tools. [35]. There is no need to install and run the special software on your computer if you use the SaaS. Instead of buying the software at a relative higher price, user just follows the pay-per-use pattern, which can reduce total cost of software. This allows businesses to save money, as it removes licensing fees and they only pay for what they use and when they use. It also removes the need to upgrade software packages as the cloud service provider does this automatically so the end user will always be up-to-date. One of the greatest benefits of SaaS is that the user can access their work and services from anywhere in the world where they can connect to the Internet.

Platform as a Service: The capability provided to the consumer is to deploy onto the cloud infrastructure his own applications without installing any platform or tools on their local machines. PaaS refers to providing platform layer resources, including operating system support and software development frameworks that can be used to build higher-level services. There are many examples of PaaS today such as Google's App Engine, Amazon's EC2 and Microsoft's Azure platform.

Infrastructure as a Service: The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. Some of the most popular examples of IaaS today include Amazon's Elastic Compute Cloud (EC2), Go Grid's Server Path, and Rackspace.

1. RELATED WORK

This section presents the related works on cloud computing security threats from different authors. There are several cloud computing threats related to either service models. But, as cloud computing technology totally depends on network or internet, various threats related to network security have been accounted in this paper.

Kui Ren et al. [4] have investigated various security challenges for the public cloud without considering the threats in service models

Kresimir Popovic et al. [5] in their research work have provided a generic overview of the security issues, the requirements and the challenges that many cloud service providers encounter.

Christos Kalloniatis [6] provided clear linkage among cloud computing areas, threats within the areas and security and privacy properties. The author also provide set of requirements for analysis and design methodologies that are developed in order to consider cloud security and privacy as part of their development process.

Keiko Hashizume [7] presented security issues for cloud three service models: SaaS, PaaS, and IaaS. As described in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing.

S. Subashini [9] in this paper, there are extreme advantages in using a cloud-based system, there are yet many practical problems which have to be solved. Cloud computing is a disruptive technology with profound implications not only for Internet services but also for the IT sector as a whole. Still, several outstanding issues exist, particularly related to service-level agreements (SLA), security and privacy, and power efficiency.

Gurdev Singh [10] in this paper, author discusses the most common unaddressed security areas in the cloud computing. Also provide some authentication mechanism for accessing the information as well as accessing the resources and also there should be system that monitor whole process and save the log files in that system.

Hassan Rasheed [13] in this paper author look at the issue of cloud computing security auditing from three perspectives: user auditing requirements, technical approaches for (data) security auditing and current cloud service provider capabilities for meeting audit requirements. There also divided specific auditing issues into two categories: infrastructure security auditing and data security auditing.

A.V. Uznov, [24] studies the incorporation of security features during the development of a distributed system which requires a sound analysis of potential attacks or threats in various contexts, a process that is often termed as “threat modeling”. The authors combine the values of threat libraries and taxonomies and propose an extensible, two-level “pattern based taxonomy” for distributed systems.

S. Moral-García et al [25] presents various instances of the solution models for the Secure SaaS enterprise security pattern in an attempt to discover the risks that an organization would incur if each of the instances was to be deployed.

Sadhana Rana [29] this paper allows an informed assessment of the security risks and benefits of using cloud computing. The author have also provided security guidance for potential and existing users of cloud computing**.**

2. CLOUD SECURITY CHALLENGES

In this section first analyzed security threats in the cloud service model and also analyzed network security threats in next half

2.1 Service Model Challenges: The various security challenges with the service models are discussed below:

- **Data Leakage and Consequent Problems**: Data insertion or deletion without the backup leads to certain drastic data related problems like security, integrity, locality, segregation and breaches. This would lead to sensitive data being accessed by the unauthorized users. One solution to this data leakage problem, as provided by Danny Harnik [17], is de-duplication with allowing a limitation on number of user uploads per time window. The term de-duplication means storing only a single copy of redundant data and providing just a link to this copy rather than storing actual copies of this data. Second solution is Fragmentation-redundancy-scattering

(FRS) technique [7]. FRS aims to provide intrusion tolerance and, in consequence, secure storage.

- **Malicious Attacks**: The threat of malicious attackers is augmented for customers of the cloud services by the use of various IT services which lacks the lucidity between the procedure and process relating to the service providers. Malicious users may gain access to certain confidential data and thus leading to data breaches. Farzad Sabahi [11] has described malicious attacks by the unauthorized users on the victim's IP address and physical server. An access control mechanism tool can be thought of to control unauthorized user in accessing secured data. Peter Mell [27] has shown Infrastructure as a Service as one of the service that exposes challenges with using virtualization as a frontier security protection to defend against malicious cloud users.
- **Backup and Storage**: The cloud vendor must ensure that regular backup of data is implemented that even ensure security with all measures. But this backup data is generally found in unencrypted form leading to misuse of the data by unauthorized parties. Thus data backups lead to various security threats. As per the study carried by Intel IT center [26], more the server virtualization increases, a very difficult problem with backup and storage is created. Danny Harnik et al. [17], have shown that de-duplication in cloud storage is carried out with the misuse of data backup. Data de-duplication is listed as one of the solution to reduce backup and offline storage volumes.
- **Shared Technological Issues**: IaaS vendors transport their services in a scalable way by contributing infrastructure. But this structure does not offer strong isolation properties for a multi-tenant architecture. Hence in order to address this gap, virtualization hypervisor intercede the access between guest operating system and the physical compute resources. As discussed by Perez R [12], in spite of several advantages, these hypervisors have exhibited flaws that have permitted guest operating systems to expand inappropriate levels of control or authority on the underlying platform. This certainly led to security issues on the cloud. Lori M. Kaufman [15] has shown the implementation of IaaS by the customer to facilitate the infrastructure or hardware usage.
- **Service or Account Hijacking:** Service hijacking is considered as one of the top most threat. Service hijacking associated with gaining an illegal control on certain authorized services by various unauthorized users. It accounts for various techniques like phishing, exploitation of software and frauds. According to Rajnish Choubey [28], account hijacking has been pointed as the severe threats. The chances of hijacking ones account increases considerably as no native API's (Application Program Interface) are used for registering various cloud services. The Countermeasure provided on Hijacking by a non-profit

organization Cloud Security Alliance (CSA) [7] that promotes the use of best practices in order to provide security in cloud environments. CSA has issued an Identity and Access Management Guidance which provides a list of recommended best practiced to assure identities and secure access management.

- **Malicious VM Creation**: An attacker who creates a valid account can create a VM image containing malicious code such as a Trojan horse and store it in the provider repository. The one solution for malicious virtual machine creation is MIRAGE [7] the author proposes a virtual machine image management system in a cloud computing environments. This approach includes the following security features: access control framework, image filtering, a provenance tracking, and repository maintenance services. However, one limitation of this approach is that filters may not be able to scan all malware or remove all the sensitive data from the images. Also, running these filters may raise privacy concerns because they have access to the content of the images which can contain customer's confidential data.
- **VM Hopping**: K. Owens [30] have concluded that with VM hopping, an attacker on one VM gains rights to use another victim VM. The attacker can check the victim VM's resource procedure, alter its configurations and can even delete stored data, thus, putting it in danger the VM's confidentiality, integrity, and availability. A requirement for this attack is that the two VMs must be operating on the same host, and the attacker must recognize the victim VM's IP address. Although PaaS and IaaS users have partial authority, Thomas Ristenpart et al. [14] have shown that an attacker can get hold of or decide the IP address using benchmark customer capabilities on the basis of various tricks and combinational inputs to fetch user's IP. Thus it can be inferred that VM hopping is a rational threat in cloud computing. Additionally, multi-tenancy makes the impact of a VM hopping attack larger than in a conventional IT environment. Because quite a few VMs can run at the same time and on the same host there is a possibility of all of them becoming a victim VMs. VM hopping is thus a critical vulnerability for IaaS and PaaS infrastructures.
- **VM Mobility**: The content of VM virtual disks are saved as files such that VMs can be copied from one host to another host over the system or via moveable storage devices with no physically pilfering hard drive. VM mobility might offer quick use but could show the way to security problems likewise, the rapid spread of susceptible configurations that an attacker could make use of to endanger the security of a novel host. Several types of attacks might take advantage of weaknesses in VM mobility which includes man in-the-middle attacks. The severity of the attacks ranges from leaking perceptive information, to completely compromising the guest OS.

According to B. Grobauer [21], a PaaS provider offers a variety of pre-configured computing platform and solution stacks to the service users. The users take advantage of the libraries and APIs (Application Program Interface) to build up their individual applications on permanent computing platform by importing their VM images.

- **VM Denial of Service**: Virtualization lets numerous VMs split physical resources like CPU, network bandwidth and memory or disk. A Denial-of-Service or DoS attack in virtualization takes place when one VM occupies all the obtainable physical resources such that the hypervisor cannot hold up more VMs and accessibility is endangered. The most excellent move towards preventing a DoS attack is to bound resource allocation using correct configurations. In cloud computing, DoS attacks could still happen as discussed by Jianyong Chen [23], but having service providers place sufficient configurations to put a ceiling on the resources owed to the VMs decreases their probability. Additionally, it is advisable to have the Service Level Agreement (SLA). This legally identifies responsibilities of the service provider and the user.

2.2 **Network Issues on Cloud:** Several cloud computing threats related to service models have been noticed. But, as cloud computing technology totally depends on network or internet, various threats related to network security have been accounted in this section. H.B. Tabakki et al. [33] have stated security issues with network on cloud. It provides virtual resources, high bandwidth and software to the consumers on demand. But in reality, the network structure of this cloud faces various attacks and security issues like cloud malware injection attack, browser security issues, flooding attacks, MITM, locks-in, incomplete data deletion, data protection and XML signature element wrapping, Port Scanning, which are explained further below.

- **Browser Security (Sniffing/Spoofing virtual networks):** IP Spoofing is a technique of hijacking browsers by redirecting the Internet user to a falsified website [10]. Every client uses browser to send the information on the network. The browser uses SSL technology to encrypt user's identity and credentials. But hackers from the intermediary host may acquire these credentials by the use of sniffing packages installed on intermediary host. Steve Kirsch [16] states that in order to overcome this problem, one should have a single identity but this credential must allow various levels of assurance which can be achieved by obtaining approvals digitally. M. Jensen [31] has shown that Web Services security (WS-security) concept on browsers work with XML encrypted a message which does not need to be decrypted at intermediated hosts.
- **MITM (Man-In-The-Middle)** attacks In cloud computing, the improper configuration of SSL (Secure Socket Layer) which is a commonly used protocol for

managing the security of a message transmission on the Internet will create a security problem known as "Man in the Middle Attack". If there is a problem with SSL, it gives a chance to the hacker to launch an attack on the data of both the parties and in an environment like cloud computing it can create disasters [34]

- **SQL Injection Attack**: These attacks are malicious act on the cloud in which a spiteful code is inserted into a model SQL code. This allows the invader to gain unauthorized access to database and eventually to other confidential information. Further, SQL injection attacks as described by Sara Qaisar et al. [19], uses the special characters to return the data for example in SQL scripting the query usually ends up with where clause which again may be modified by adding more rows and information in it. The information entered by the hacker are misread by the website as that of the user's data and this will then allow the hacker to access the SQL server leading the invader to easily access and modify the functioning of a website.
- **Flooding Attacks**: In this attack, the invader sends the request for resources on the cloud rapidly so that the cloud gets flooded with the ample requests. As per the study carried out by IBM [20], cloud has a property to expand on the basis of large amount of request. It will expand in order to fulfill the requests of invader making resources inaccessible for the normal users.
- **XML Signature Element Wrapping**: It is found to be a very renowned web service attack. According to Jamil [18], it protects identity value and host name from illegal party but cannot protect the position in the documents. The attacker simply targets the host computer by sending the SOAP messages and putting scrambled data which the user of the host computers cannot understand. As per the studies by researchers at Ruhr University, and mentioned by the editor Lee Garber [22], the XML Signature wrapping attack changes simply the content of the signed part of a message without tampering the signature. This would not let the user to understand the twisted data, thus misguiding and misleading the user. [32]The best countermeasure approach would be to enhance the interface between the signature verification function and the business logic. In this approach, the signature verification returns some sort position description of the signed data, next to a Boolean value. The business logic may then decide if data about to be processed has been signed or not.
- **Data Scavenging (Incomplete Data Deletion)**: Incomplete data deletion is treated as hazardous in cloud computing. Since data cannot be completely removed from unless the device is destroyed, attackers may be able to recover this data. According to Sara Qaisar et al. [19], when data is deleted, it does not remove replicated data placed on dedicated backup server. The operating system of that server will not delete data unless it is

specifically commanded by the network service provider. Precise data deletion is majorly impossible because copies of the data are saved in replica but are not available for usage.

- **Locks In**: Locks in is a small tender in the manner of tools, standard data format or procedures, services edge that could embark on the data, application and service portability, not leading to facilitate the customer in transferring from the one cloud provider to another or transferring the services back to home IT locations [34]
- **Port Scanning**: Port scanning is the act of scanning a computer's ports. Port scanning identifies open doors to a computer since it is a place where information goes into and out of the computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer. The security groups are usually configured to allow traffic from any source to specific port of the computer and then the port responds to the signal. Both TCP and UDP employ port numbers to identify the higher layer applications at hosts that are communicating with each other. End-to-end data communications on the Internet, in fact, are uniquely identified by the source and destination host IP addresses and the source and destination TCP/UDP port numbers. In cloud computing, where there will be interaction of the third party servers and systems, the port scanners may provide an opportunity for attackers when the subscriber configures the security group to allow traffic from any source to a specific port, then that specific port will be vulnerable to a port scan.[34]

3. CONCLUSION

There are many advantages using cloud computing model but despite these advantages there are also many security challenges in the cloud computing. This paper analysis every security threat found across both the cloud models and the networks and also reveals solutions. The paper shall look at ways in which security threats can be a danger to cloud computing and how they can be provided countermeasures on the attacks. It is no secret that cloud computing is becoming more and more popular today and is ever increasing in popularity with large companies as they share valuable resources in a cost effective way. Due to this increasing demand for more clouds there is an ever growing threat of security becoming a major issue.

REFERENCES

[1] Amin Jula, Elankovan Sundararajan, Zalinda Othman"Cloud computing service composition: A systematic literature review" Elsevier,– Expert Systems with Applications 41 (2014) 38093824

[2] Mell P, Grance T. The NIST definition of cloud computing draft, 800145, January2011. <http://www.nist.gov/itl/cloud/index.cfm>

[3] Kuyoro S. O. Ibikunle F. Awodele O. "Cloud Computing Security Issues and Challenges" International Journal of

Computer Networks (IJCN), Volume (3) : Issue (5) : 2011

[4] Kui Ren, Cong Wang, and Qian Wang, llinois Institute of Technology, “Security Challenges for the Public Cloud”, IEEE Press, 2012, pp. 69 – 73.

[5] Kresimir Popovic and Zeljko Hocenski, “Cloud Computing Security Issues and Challenges,” Proc. 33rd Int’l Convention on Information and Comm. Technology, Electronics and Microelectronics (MIPRO 10), IEEE Press, 2010, pp. 344–349.

[6] Christos Kalloniatis, Haralambos Mouratidis, Manousakis Vassilis, Shareeful Islam” Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts” Elsevier, Computer Standards & Interfaces 36 (2014) 759–775

[7] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez” An analysis of security issues for cloud computing” Springer,Journal of Internet Services and Applications 2013,

[8] Sean Carlin, Kevin Curran” Cloud Computing Technologies “International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.1, No.2, June 2012, pp. 59~65 ISSN: 2089-3337

[9] S. Subashini n, V. Kavitha Anna UniversityTirunelveli,Tirunelveli,TN62 7007,“A survey on security issues in service delivery models of cloud computing” Journal of Network and Computer Applications 34(2011).

[10] Gurdev Singh, Amit Sharma, Manpreet Singh Lehal “Security Apprehensions in Different Regions of cloud Captious Grounds” International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011

[11] Farzad Sabahi, “Cloud Computing Security Threats and Responses”, 978-1-61284-486-2, IEEE, 2011, pp: 245 – 249.

[12] [12] Perez R, van Doorn L, Sailer R. “Virtualization and hardware-based security”. IEEE Security and Privacy 2008;6(5):24–31.

[13] [13] Hassan Rasheed “Data and infrastructure security auditing in cloud computing environments” International Journal of Information Management 34 (2014) 364–368.

[14] Thomas Ristenpart et al., “Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds,” Proc. 16th ACM Conf. Computer and Communications Security (CCS09), ACM Press, 2009, pp. 199–212.

[15] Lori M. Kaufman, Bruce Potter, “Monitoring Cloud Computing by Layer, Part 1”, 1540-7993/11, IEEE, pp: 66 – 68.

[16] Steve Kirsch et al., “The Future of Authentication”, 1540-7993/12, IEEE, January-February 2012, pp: 22 – 27.

[17] Danny Harnik, Benny Pinkas, Alexandra Shulman-Peleg, “Side Channels in Cloud Services: Deduplication in Cloud Storage”, 540-7993/10, IEEE, 2010, pp: 40 – 47.

[18] Jamil, D., Zaki, H. “Security issues in cloud computing and counter measures”, International Journal of Engineering Science and Technology (IJEST) , Vol. 3 No. 4, pp: 2672-2676.

[19] Sara Qaisar, Kausar Fiaz Khawaja, “Cloud Computing: Network/Security Threats and counter measures”, Interdisciplinary Journal of Contemporary Research in Business, ijcrb.webs.com, January 2012, Vol 3, N0 9, pp: 1323 – 1329.

[20] Web 2.0/SaaS Security, Tokyo Research Laboratory,

IBM.Research.http://www.trl.ibm.com /projects/web20sec/web20sec_e.html

[21] Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker, "Understanding Cloud Computing Vulnerabilities", IEEE, 1540-7993/11, 2011, pp: 50-57.

[22] Lee Garber, "Serious Security Flaws identified in Cloud Systems", News Briefs, IEEE, December, 2011, pp: 21 – 23.

[23] Jianyong Chen, Yang Wang, Xiaomin Wang, "On demand security architecture for Cloud Computing, IEEE 2011, pp: 1 – 12.

[24] A.V. Uznov and E.B. Fernandez, "An Extensible Pattern-based Library and Taxonomy of Security Threats for Distributed Systems"

[25] S. Moral-García et al., "Enterprise Security Pattern: A Model-Driven Architecture Instance",

[26] Intel IT Center, "Preparing your Virtualized Data Center for the Cloud", pp: 1 – 20.

[27] Peter Mell, "What's Special about Cloud Security?" , IEEE, IT Pro July/August 2012, pp: 6 – 8.

[28] Rajnish Choubey, Rajshree Dubey, Joy Bhattacharjee, "A Survey on Cloud Computing Security, Challenges and Threats", International Journal on Computer Science and Engineering, ISSN: 0975-3397, Vol. 3 No. 3 March 2011, pp: 1227 – 1231.

[29] Sadhana Rana; Pramod kumar joshi "risk analysis in web applications by using cloud computing"International Journal of Multidisciplinary Research Vol.2 Issue 1, January 2012, ISSN 2231 5780.

[30] K. Owens, "Securing Virtual Computer Infrastructure in the Cloud," white paper, Savvis Communications Corp., 2009.

[31] M. Jensen, "On Technical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing, pp: 109 – 116.

[32] Juraj Somorovsky, Mario Heiderich,Meiko Jensen, Jörg Schwenk "All Your Clouds are Belong to us–Security Analysis of Cloud Management Interfaces"http://csrc.nist.gov/publications/drafts/800-145/Draft- SP-800-145 cloud-de_nition.pdf.

[33] H. Takabi, J.B.D. Joshi, and G.-J. Ahn, "Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," Proc. 1st IEEE Int'l Workshop Emerging Applications for Cloud Computing, 2010, pp. 393–398.

[34] Mr. D. Kishore Kumar, Dr. G. Venkatewara Rao, Dr. G. Srinivasa Rao "Cloud Computing: An Analysis of Its Challenges & Security Issues" International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 5, October 2012