A Survey on Security Threats for Cloud Computing

Nagaraju Kilari,
Selection Grade Lecturer (SGL),
Department of Computer Science,
Garden City College,
Bangalore, Karnataka, India.

Dr. R. Sridaran,
Dean, Faculty of Computer Applications,
Marwadi Education Foundation's Group of Institutions,
Rajkot, Gujarat, India.

Abstract

Cloud Computing provides an efficient and flexible way for services to meet escalating business needs. Cloud-shared infrastructure and associated services make it cost effective alternative to traditional approaches. However, they may also introduce security breaches and privacy issues. As more cloud based applications keep evolving, the associated security threats are also growing. Many research works on cloud security exist in partial forms of either specifically on cloud issues or virtualization-related security issues. In this paper, an attempt has been made to consolidate the various security threats in a classified manner and to illustrate how cloud and virtualization vulnerabilities affect the different cloud service models.

1. Introduction

Most of the organizations are shifting their approach from traditional computing to Cloud Computing (CC) in order to reduce the operational and maintenance costs. In this paradigm shift, customers need not invest more on hardware, software or services. Instead, they rely upon clouds [29]. The US National Institute of Standards and Technology (NIST) defines the key characteristics of cloud as on-demand self-service, rapid elasticity and pay as per the usage of business models [25]. In this regard, customers only have to pay for what they use, because cloud services and their resources are delivered over the internet on-demand basis [19]. As such, CC is changing the way in which computing services were traditionally being delivered.

CC has emerged from the technologies including grid computing, distributed computing, parallel computing, virtualization technology and utility computing [23]. In practice, cloud services heavily depend upon virtualization and its software, which is usually known as Virtual Machine Monitor (VMM) or Hypervisor [21]. It allows a single physical server to host many guest virtual machines (VM), operating systems and applications without the cost and complexity of running multiple machines [33]. At present popular VMMs are classified into Type 1 and Type 2 [4]. The comparative analysis between Type1 and Type 2 is presented in Appendix 1.

According to Amarnath Jasti et al. [4], virtualization optimizes the application performance in a cost effective manner, but it can also introduce a few security risks. In cloud, security plays a major role due to the fact that customers outsource their data and computation tasks on cloud servers, which are controlled and managed by potentially untrustworthy cloud providers [15]. The following section provides the significance of cloud security in detail.

1.1 Significance of Security in Cloud Computing

The popularity of CC is mainly due to the fact that many enterprise applications and data are moving into cloud platforms; however, lack of security is the major barrier for cloud adoption [6]. According to a recent survey by International Data Corporation (IDC), 87.5% of the masses belonging to varied levels starting from IT executives to CEOs have said that security is the top most challenge to be dealt with in every cloud service [10]. Many of the threats found in existing platforms. Out of them, the Security Threat is considered to be of High Risk [3]. Figure 1 shown below illustrates this fact via the pyramid diagram.

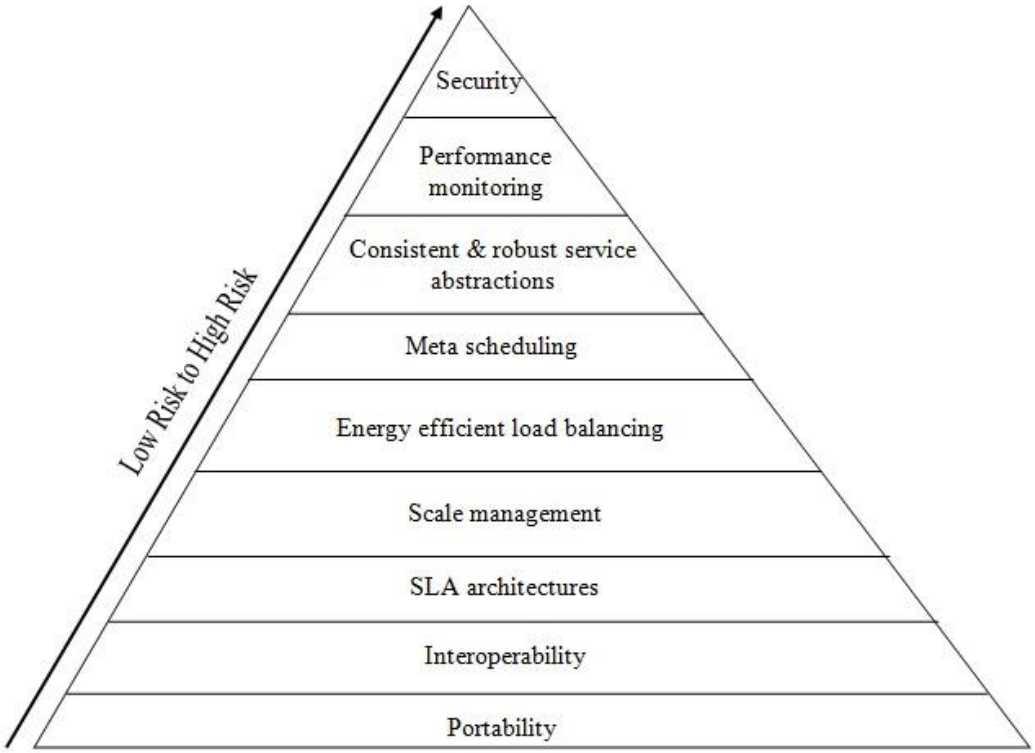

Figure 1. Classification of threats based on risk factor

These threats can be avoided in an application by introducing some suitable elements. Such an approach has been suggested by Ramgovind [28] and Nitin Singh Chauhan [24] in terms of six major security elements. They are respectively Confidentiality, Integrity, Authentication, Authorization, Non-repudiation and Availability which are further explained below:

- **Confidentiality** is the process of making sure that the data remains private, confidential and restricted from unauthorized users [28]. Data encryption is one of the most popular options of security before pushing the data into cloud.

- **Integrity** is the guarantee by which the data is protected from accidental or deliberate (malicious) modification. Hashing techniques, digital signatures and message authentication codes are used to preserve data integrity [35]. Integrity problems are in big scale due to the multi-tenancy characteristic of cloud [24].

- **Authentication** is the mechanism by which the systems may securely identify their users.

- **Authorization** determines the level of access to system resources attributed to a particular authenticated user [29].

- **Non-repudiation** is an extension to the identification and authentication service. It is used to ensure that the messages sent are properly received and acknowledgements are sent back to the sender [7]. In other words, establishing a two way communication between a sender and a receiver.

- **Availability** ensures that an organization has its full set of computing resources available and usable at all times for its real users [37].

Out of these major principles in cloud security, availability is the area where cloud based infrastructure appears to be in its greatest challenge [1]. CC provides on-demand services to customers who expect minimum or no down time. Breaching such expectation would be detrimental to the future of cloud [23].

The remaining parts of this paper are organized as follows: Section 2 discusses some of the similar surveys. Section 3 provides the categorization of the security risks associated with the cloud. The effects of various security threats on cloud service models are also highlighted.

2. Related Work

Many researchers have investigated on cloud security. In 2010, Amarnath et al. [4], stated that

the VMs across a shared physical infrastructure will be rapidly grown in a cloud platform. However, this would also introduce new vulnerabilities such as VM-Hopping and VM-Escape. In this literature, the authors have emphasized the importance of virtualization in the context of CC security. The study is limited to the threats resulting from virtualization techniques only.

Wayne et al. [34], have listed the benefits of CC along with the basic security issues. This research brings out the primary problems in terms of cloud security and privacy. The limitation of this work is that it focuses only on public clouds. Moreover, the authors have not proposed any tool or framework to address the identified issues.

In 2010, Kresimir Popovic et al [19] surveyed security in CC, which was elaborated in a way that covers security issues and challenges. However, the research analyses cloud security from a generic viewpoint outside cloud virtualization and was not able to demonstrate the effects of different threats on cloud service models.

In 2011 Shengmei Luo et al [31] provided a generic overview of the security issues, requirements and challenges related to cloud virtualization. The authors also suggested various security frame works to avoid some of the threats related to virtualization. However, these authors have not discussed in detail the implications of virtualization technology on different cloud service models.

The work of Hsin-Yi Tsai et al [11], considers security issues in different service models based on some of the security benchmarks (Integrity, Availability and Confidentiality) , but it is limited to only cloud virtualization.

Akhil Behl [2] investigated the security issues related to the cloud in 2011. The author discusses the existing security approaches to secure the cloud infrastructure, applications and their drawbacks. But this work did not discuss in detail on threats related to virtualization and the service models.

In 2012, S.U.Muthunagai et al. [30], surveyed the security threats related to virtualization and proposed an efficient cloud protection system architecture, intends to provide security to the guest VM from the other guest VM. However, the primary aim is limited to focus on the security vulnerabilities in cloud infrastructure.

Although there is a considerable amount of ongoing research for developing security tools; there is a need to consider the specific challenges faced by CC. Since virtualization plays a major role in CC, it is essential to consider the additional threats introduced by virtualization. Providing such a kind of complete survey becomes the motivation for us to present our survey.

3. Categorization of Security Threats

Cloud security threats are identified and classified into different categories as shown in the schematic diagram below.

The efficiency of cloud services can be thought of a double-edged sword [8] providing equal opportunities for advantages as well as threats. The structure of a cloud application has much more points of failure than traditional IT options [14], [16] like Abuse and Nefarious use of cloud services, interfaces and unknown risks.

The schematic diagram depicted in Figure 2 gives the security threats at various levels. The diagram further reveals that Virtualization may attract additional four important security threats namely, Isolation Failure, Service Disruption, Dependency on Hypervisor and Shared Technology. This classification also lists some of the new-age threats including VM -Hopping and VM- Escape, where VM-Hopping is a threat by which an attacker can make use of his VM(s) to spy another user's VM(s) and in VM Escape an attacker gets control over the host machine and gain access to all the VMs. The survey also presents different possible vulnerabilities which would exist in networks by augmenting the hypervisor together with consequences like Cloud Service Downtime and Data Loss or Data Theft which are due to poor cloud infrastructure. This section will start by discussing these issues and examine other risks related to virtualization. Few cases of Malevolence and Multi-Tenancy caused by security issues illustrate possibility of compromising an entire cloud network.

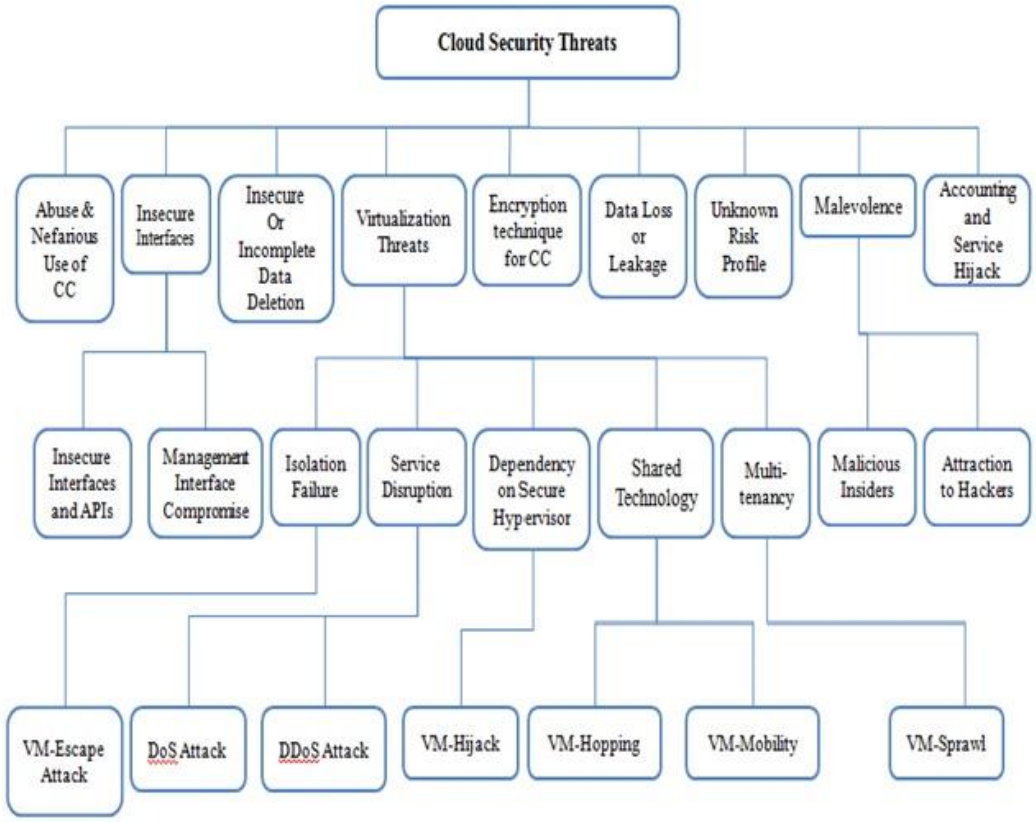

Figure 2: Various categories of cloud security threats

CC belongs to Internet-based technologies and it offers three types of services, namely, Infrastructure as a service (IAAS), Platform as a service (PAAS) and Software as a service (SAAS) [22] , [35]. Next section deals with a threat associated with IAAS and PAAS services.

3.1 Abuse and Nefarious Use of CC

This threat is relating to the shortcomings of registration process associated with cloud. Cloud Service Providers offer IAAS and PAAS to their customers with a minimum requirement of a credit card. By taking advantage of this registration process, hackers may be able to conduct susceptible activities like Spamming and Phishing [26]. Initially, PAAS providers have suffered from this attack. However, recent evidence shows that hackers have begun to target IAAS vendors as well (CSA-Cloud Security Alliance). The next section explains the use and security of these service interfaces.

3.2 Insecure Interfaces & Data Deletion Activity

Cloud providers supply a set of software interfaces or APIs that customers use to manage and interact with the cloud services. The security and availability of cloud services depend upon the security of these basic APIs [27]. Without proper management of authentication, it leads to Insecure Interfaces. To maintain the secrecy of cloud data, the interfaces must be designed to protect against both accidental and malicious attacks.

In cloud, it is impossible to delete an information to its full since a storage media such as an hard disk might be shared by multiple organizations. The information that is not completely deleted could still reside in insecure locations [37] which may cause inconsistency.

3.3 Virtualization Threats

Virtualization is yet another important technology for the realization of CC; but the services offered by Virtualization may also introduce some forms of risks to its applications [33] as explained below:

- **Isolation Failure**: One of the primary benefits of Virtualization is known as Isolation [31]. This benefit, if not deployed properly will generate a threat to the environment [18]. Poor isolation or inappropriate access control policy will cause the inter-attack between two VMs or between VMs and its associated VMM. For instance, VM Escape is one of the worst cases happening if the Isolation between the host and

the VMs is compromised. In case of VM Escape, the program running in a VM is able to bypass the VMM layer and get access to the host machine. Since the host machine is the root of security of a virtual system, the program which gains access to the host machine can also gains the root privileges.

- **Service Disruption**: This threat may occur when an attacker gains access to an organization's login credentials which may lead to further vulnerable activities such as Denial-of-Service (DoS) or Distributed-Denial-of-Service (DDoS) attacks where a DoS attack is an attempt to make a computer resource unavailable to its intended users [32]. One common method of this type of attack involves saturating the target machine with bogus requests such that it cannot respond to the legitimate requests in a timely manner [9]. An attacker typically uses multiple computers to launch an assault. Eradication of the DoS attacks using IDS (Intrusion Detection Systems) over the cloud will solve most of these problems [36]. Another excellent approach is to limit the resource allocation using proper configurations. On the other hand, a DDoS attack aims to make services or resources unavailable for indefinite amount of time by flooding it with useless traffic [13]. The two main objectives of these attacks are, to exhaust computer resources (CPU time and Network bandwidth) so that it makes services unavailable to legitimate users [17]. The second objective is, imitating pragmatic web service traffic, in order to create a large group of agents to launch an attack [6]. Thus, DDoS attack is a major threat to Availability. The solution for this event is to increase number of such critical resources.

- **Dependency on Secure Hypervisor**: The security of a computer system depends on the quality of the underlying software kernel that controls the execution of several processes. In case of multi-tenant architecture, a single server can host several VMs on it and thus would have the respective configuration file of all VMs. The security could be a main aspect since all these information will be stored with a common storage system. By gaining access to this information, an attacker can launch VM Hijack attack on the VMs which are hosted on the same server [10].

- **Shared Technology Issues**: These issues arise when IAAS vendors deliver their services in sharing infrastructure [4]. These infrastructures were not designed to offer strong isolation. For example, VM Hopping is an attack which happens, when two VMs are deployed over the same host. An attacker on first VM can gain access over the second VM by knowing the IP address or gaining access over the host. If the attacker gains access over the host, he can monitor the traffic going over the second VM. Hence he can attack the second VM by changing the flow of traffic or manipulate the traffic itself. Strong compartmentalization is required to ensure that users do not interfere with other tenants running on the same cloud provider. Thus, compromise on Confidentiality is a serious security issue.

- **Multi-tenancy**: During execution of multiple VMs on the same host, different users can share both the application and physical hardware [10]. This may lead to information leakage and other exploitations. For instance, in a virtual system, inappropriate VM management policy will cause VM sprawling [31], a case where number of VMs rapidly growing while most of them are idle or never be back from sleep, which may cause resource of host machine being largely wasted.

3.4 Encryption Technique for CC

Encrypting data is one of the solutions to secure cloud data [20], but it limits the efficiency of the cloud. This is because encrypted documents must first be decrypted before they can be searched or manipulated. Furthermore, cloud data must be encrypted before storing. Performing encryption and decryption on large data sets can be prohibitively expensive and time consuming. The following section gives a brief idea about how the data loss will violate the data integrity in cloud.

3.5 Data Loss or Leakage

Top threats for Cloud Computing like Data loss or Data leakage may due to how the data is structured. Firstly, data of an organization must be stored in servers of other nations. This is a significant concern for some organizations. Secondly, the duration of data retained by the Cloud provider, may continue to remain on the provider's servers, even after it has been deleted by the client [10]. Thirdly, improper deletion of data records and alteration of data without proper backup can result in permanent loss of data. Last but not the least, insufficient authentication, authorization and audit control, allows unauthorized parties to gain access into sensitive data. Therefore, Data Integrity must be upheld if CC is to be secured. The following section explains the possible implications if there is a breach in the trust between the cloud providers and its users.

3.6 Unknown Risk Profile

Few of the key objectives of CC is the reduction of hardware, software ownership and maintenance [12]. The financial and operational benefits must be weighed carefully against the security concerns. A cloud provider may not disclose a security threat even if it occurs. Hence, the client is exposed to unknown risk profile arising out of the situation. Versions of software, security practices, vulnerability profiles and security design are some of the important factors, for estimating any company's security position. The next section describes how un-authorized users can influence the authorization.

3.7 Malevolence

Malevolence is defined as, malicious insider, working as a cloud employee, harvesting confidential data or taking complete control of the cloud services with minimal or no possibility of detection [2]. Therefore it is a major challenge as to how an organization can restrict its internal employees, contractors, vendors and other trusted people who have access to critical resources from within the network. This key challenge can be addressed to a certain degree by enforcing strict supply chain management and conducting a comprehensive supplier assessment [38]. Authorization plays a vital role in securing the cloud.

Transparency is very important in the overall information security and management practices. When a cloud provider hires their cloud employees, certain factors such as hiring standards, policies regarding how their employees can access to virtual & physical assets and how the employees are being monitored in their work are to be clarified. If the cloud provider does not consider the significance of the above factors, this situation may create more opportunities to the hackers [35].

3.8 Accounting and Service Hijack

Typically, a cloud is accessed by a web interface using authentication in the form of passwords. In this scenario, the possibilities of an account being hacked are very high. The security policy control may not be effective in the case of a Malicious Insider colluding with the attackers. If an attacker gains access to any client's credentials, thereby gaining access to the entire sensitive data, and causing disaster to the whole secrecy [33]. The summary of impacts of these security threats on different cloud service models are presented in the following section.

4. Summary

Table 1 of Appendix shows the vulnerability of IAAS, PAAS and SAAS model in various threat categories. It can be observed that IAAS is the most affected among the three domains, especially in the area of isolation failures, dependency on hypervisors, shared technology and multi-tenancy.

Complications with data privacy and data protection continue to down grade the market [5]. In the case of Virtualization Security, one of the most important considerations is Hypervisor [33]. Knowledge about various hypervisor attacks would help the design of Virtualization Security Vulnerabilities that do exist for infrastructure. The hypervisors are classified into two categories: Type 1 and Type 2 [32], [36] where Type 1 hypervisors run directly on the system hardware and the Type 2 on a host operating system that provides Virtualization Services [39].

Table 2 of Appendix provides the consolidation of various features supported by both Type 1 and Type 2 hypervisors. From this table, it is evident that Type 1 Hypervisors are typically the most preferred approach, because they can achieve higher virtualization efficiency by dealing directly with the hardware and provide higher performance efficiency, availability and security than type 2 hypervisors. Type 2 hypervisors are used mainly on systems where support for a broad range of I/O devices is important.

5. Conclusion and Future Work

Any application relying upon an emerging technology should also consider the different possible threats as well. Such an application with an inability to anticipate or handle the threats may probably lead to failures. The classification of various security threats presented in this paper would definitely benefit the cloud users to make out proper choice and cloud service providers to handle such threats efficiently. The future work of the authors would involve developing a model to detect and prevent the most common Virtualization related threats.

References

[1] Ajay Gupta, "Introduction to Cloud Computing", IISC, 2010, pp. 1-7.
[2] Akhil Behl, "Emerging Security Challenges in Cloud computing, an insight to Cloud security challenges and their mitigation", IEEE, 2011, pp. 217-221.

[3] Aman Bakshi and Yogesh B, "Securing cloud from DDOS Attacks using Intrusion Detection System in VM", IEEE, 2010, pp. 260-264.
[4] Amarnath jasti, "Security in Multi-tenancy Cloud", IEEE, 2010.
[5] Artem Volokyta, Igor Kokhanevych and Dmytro Ivanov, "Secure Virtualization in Cloud Computing", IEEE, 2012, pp. 395.
[6] Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi, "Securing Cloud computing Environment against DDoS Attacks", IEEE, 2011, pp. 1-5.
[7] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Zhenghu Gong, "The Characteristics of Cloud Computing", IEEE, 2010, pp. 275-279.
[8] Farhan Bashir Shaikh and Sajjad Haider, "Security in Cloud Computing", IEEE, 2010, pp. 214-219.
[9] Farzad Sabahi, Iran Farzad Sabahi, Iran, " Virtualization-Level Security in Cloud computing", IEEE, 2011, pp. 250-254.
[10] Haoyong Lv and Yin Hu, "Analysis and Research about Cloud Computing Security Protect Policy", IEEE, 2011, pp. 214-216.
[11] HsinYi Tsai, "Threat as a Service? Virtualization's impact on Cloud Security", IEEE, 2012, pp. 32-37.
[12] http://www.cloudalliance.org/topthreats, "Top threats to Cloud computing", pp. 8-14.
[13] Irfan Gul, Atiq ur Rehman and M Hasan Islam, "Cloud Computing Security Auditing", IEEE, pp. 143-148.
[14] Jakub Szefer and Ruby B. Lee, "A Case for Hardware Protection of Guest VMs from Compromised hypervisors in Cloud computing", IEEE, 2011, pp. 248-252.
[15] Jen-Sheng Wang, Che-Hung Liu and Grace TR Lin, "How to Manage Information Security in Cloud Computing", IEEE, 2011, pp. 1405-1410.

[16] Jinzhu Kong, "A practical approach to improve the data privacy of virtual machines", IEEE, 2010, pp. 936-941.
[17] Junya Sawazaki, Toshiyuki Maeda, Akinori Yonezawa, "Implementing a Hybrid VM Monitor for Flexible and Efficient Security Mechanisms", IEEE, 2010, pp. 37-45.
[18] Jyotiprakash Sahoo, Mohapatra and Lath R, "Virtualization: A Survey on Concepts, Taxonomy and Associated Security Issues", IEEE, 2010, pp. 222-226.
[19] Kresimir Poovic Zeljko Hocenski, "Cloud computing security issues and challenges", IEEE, 2010, pp. 344-349.
[20] M. Yasin Akhtar Raja AND Shaftab Ahmed, "Tackling Cloud Security Issues and Forensics Model", IEEE, 2010, pp. 190-196.
[21] Manabu Hirano, Takahiro Shinagawa, Hideki Eiraku, Shoichi Hasegawa, Kazumasa Omote, Takeshi Okuda, Eiji Kawai, and Suguru Yamaguchi, "A Two-step Execution Mechanism for Thin Secure Hypervisors", Third International Conference on Emerging Security Information, Systems and Technologies, IEEE, 2009, pp. 129-134.
[22] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", IEEE, 2012, pp. 5490 – 5499.
[23] Murat Kantarcioglu, Alain Bensoussan and SingRu, "Impact of Security Risks on Cloud Computing Adoption", IEEE, 2011, pp. 670-674.
[24] Nitin Singh Chauhan and Ashutosh Saxena, "Energy Analysis of Security for Cloud Application".
[25] Panagiotis Kalagiakos and Panagiotis Karampelas, "Cloud Computing Learning", IEEE, 2011.
[26] Prashant Srivastava, Satyam Singh, Ashwin Alfred Pinto, Shvetank Verma, Vijay K. Chaurasiya and Rahul Gupta, "An architecture based on proactive model for security in cloud computing", IEEE, 2011, pp. 661-667.
[27] Qinbo Xu, Cuixia Ni, Guang Jin, and Xian Liang, "Improve the information security practice Instruction with VM techniques", IEEE, 2010, pp. 285-288.
[28] Ramgovind S, Eloff MM and Smith E, "The Management of Security in Cloud Computing", IEEE, 2010.
[29] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki and Sugata Sanyal, "A Survey on Security Issues in Cloud Computing", IEEE.
[30] S.U.Muthunagai, C.D. Karthic and S. Sujatha, "Efficient Access of Cloud Resources through Virtualization Techniques, IEEE, 2012, pp. 174-178.
[31] Shengmei Luo, Zhaoji Lin, Xiaohua Chen, "Virtualization security for Cloud computing service", IEEE, 2011, pp. 174-178.
[32] Shubhashis Sengupta, Vikrant Kaulgud and Vibhu Saujanya Sharma, "Cloud computing Security - Trends and Research Directions", IEEE, 2011, pp. 524-531.
[33] Udaya Tupakula and Vijay Varadharajan, "TVDSEC: Trusted Virtual Domain Security", IEEE, 2011, pp. 57-63.
[34] Wayne A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud computing", NIST, IEEE, 2011, pp. 1-8.
[35] Wentao Liu, "Research on Cloud Computing Security Problem and Strategy", IEEE, 2012, pp. 1216-1219.
[36] Xiangyang Luo, Lin Yang, Linru Ma, Shanming Chu and Hao Dai, "Virtualization Security Risks and Solutions of Cloud computing Via Divide-Conquer Strategy", IEEE, 2011, pp. 637-641.

[37] Xiaojun Yu and Qiaoyan Wen, "A view about cloud data security from data life cycle", IEEE, 2010.
[38] Yoshiaki Hori, Takashi Nishide and Kouichi Sakurai, "Towards Countermeasure of Insider Threat in Network Security", IEEE, 2011, pp. 633-636.
[39] Zhi Wang and Xu xian Jiang, "Hyper Safe: A Lightweight Approach to Provide Lifetime Hypervisor Control Flow", IEEE, 2010, pp. 380-393.

Author's Profile

Mr. Nagaraju Kilari, M.Sc. (Information System), M.Phil., is presently a Selection Grade Lecturer, Department of Computer Science, **Garden City College**, Bangalore. He has done M.Sc. Information System from Andhra University, and M.Phil., Computer Science from Global University, Nagaland. He has participated and presented various papers in National Conferences. His areas of interest are object oriented languages and web technologies.

Dr R. Sridaran has done his post graduation in Computer Applications, Management and a Doctoral degree in Computer Science. As an Entrepreneur, he has offered his consultancy services to various service sectors. He is having 17 years of academic experience and currently associated with Marwadi Education Foundation's Group of Institutions, Rajkot, Gujarat as Dean. His research interests include Design Pattern, Cloud Computing, HCI & Business Intelligence.

Appendix

Table 1: Impacts of threats in service models

Sl. No.	Threat Name	Cloud Domain		
		IAAS	PAAS	SAAS
1	Abuse and Nefarious Use of CC	✓	✓	×
2	Insecure Interfaces and APIs	✓	✓	✓
3	Management Interface Compromise	✓	✓	✓
4	Insecure or Incomplete Data Deletion	✓	×	×
5	Isolation Failure	✓	×	×
6	Dependency on Secure Hypervisor	✓	×	×
7	Multi-tenancy	✓	×	×
8	Shared Technology Issues	✓	✓	✓
9	Data Loss or Leakage	✓	✓	✓
10	Unknown Risk Profile	✓	✓	✓
11	Malicious Insiders	✓	✓	✓
12	Attraction to Hackers	✓	✓	✓
13	Account or Service Hijacking	✓	✓	✓

Table 2: Type 1 and Type 2 Hypervisors

Sl.No	Feature	Type 1	Type 2
1.	**Definition**	Hypervisors run directly on the system hardware.	Hypervisors run on a host operating system.
2.	**Support**	Hardware virtualization.	Operating system virtualization.
3.	**Examples**	VMware ESXi and Citrix XEN Server.	KVM, Virtual Box, VMware Server and Microsoft Virtual PC.
4.	**Efficiency, Availability and Security**	Comparatively better than Type 2.	Though inferior, it is used mainly on systems where support for a broad range of I/O devices is important.
5.	**Performance**	Very high. Resources are not being consumed by a bloated parent operating system.	Steep resource-overhead penalties reduce performance.
6.	**Ease of use**	Fairly easy to install but complicated to configure.	Easy to install, use and maintain.
7.	**High availability**	Yes.	No.
8.	**Reliability**	Yes.	Moderate.
9.	**Virtualization hypervisor management**	More options for management and automation. Centralized consoles to manage large number of hosts and VMs.	Fewer options for management and automation as well as limited VMs can be managed.
10.	**Cost**	Very costly.	Moderate.
11.	**Scalability**	Very high (easily run hundreds of VMs on a single host).	Very limited scalability (in the size of the VMs and the number of VMs that can run on a single host).
12.	**Resource control**	It offers the least amount of resource overhead and advanced resource controls that allow you to guarantee, prioritize and limit VM resource usage.	It has no or limited resource controls, so VMs have to fight each other for resources.
13.	**Size OR Complexity**	Smaller.	Bigger and more complex.