A Survey on Cloud Based Security Issues

Mr. Mahesh Kharde
Department of Computer Engineering.
G.H.Raisoni College of Engineering and Management, Ahmednagar.

Abstract

Cloud Computing plays an important role in eliminating the requirement of infrastructure in IT industries. It provides the flexible way to meet business needs. We can avoid cost of infrastructure at user side by using cloud computing technologies. While Cloud plays an important role, we should also note the security threats which gets born due to cloud computing. Many surveys done shows partial security exist, but can be disastrous when not applied correctly. Cloud introduces many new issues which should be cleared so that cloud infrastructure can increase. In this paper, we survey all existing issue in cloud, making a review of the literature on the subject. Here we show how cloud and virtualization affects in cloud service models

1. Introduction

From many years internet is a driving power towards the various technologies that have been come in existence. Over few year's cloud has witnessed an enormous shift towards cloud infrastructure. Many organization are moving towards cloud computing from traditional computing. Instead of investing more cost on infrastructure such as hardware, cloud, service they rely on cloud. Now consumer has to only pay for amount they used. Cloud is Internet of things, there are many advantages of using cloud computing including i) accessible over globe and automated process ii) less cost of maintenances and hardware iii) flexible. In clod environment we need not required to own infrastructure. Cloud integrates supporting high scalability and multi-tenancy, offeringenhanced flexibility if compared with existing technologies.

Cloud computing has been derived for technologies like virtualization technology and utility computing[23],disturbed computing, grid computing, Cloud depends upon virtualization, parallel computing and its software called virtual machine monitor (VMM) or hypervisor [21]. There is one physical server and many host get connected to it.

As per Amarnath Jasti et al. [4], virtualization increase application performance and optimized it but there might be concern of security risk we should be considering security at higher level, since in cloud we have data of customers. The following are the importance of cloud security

1.1 Importance of Security in Cloud Computing

Since Enterprise application systems are moving into cloud platform, so lack of security can cause breach of security to customer's data. As per recent international data corporation (IDC), 875 of total belonging at varied level said that they prefer security at highest level than any other criteria. Following is the level of security risks

According to Ramgovind [28] and Nitin Singh Chauhan [24] we can minimize threats by 6 elements respectively Confidentiality, Integrity,Authentication, Authorization, Non-repudiation and Availability. They are which are further explained below:

ISSN:2278 – 7798

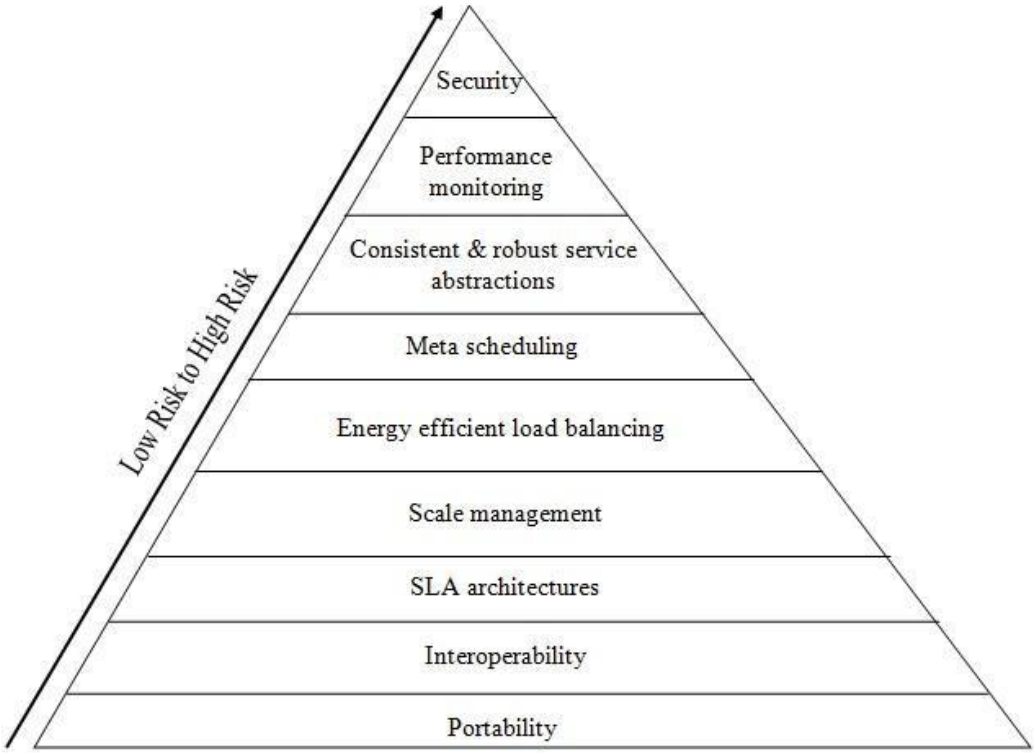

Figure 1: Classification of threatsrisk factor

- **Confidentiality** It is the process of making sure that the data remains secrete, confidential and not available to from unauthorized users [28]. Confidentiality can be implemented using Data encryption. It Data Encryption we change it to different format which is difficult for human to read

- **Integrity**It is the guarantee which states that data is not modified or changed accidently. Different Techniques such as message authentication codes, Hashing techniques, and digital signatures can be used to preserve data integrity [35]. Integrity problems are in big scale due to the multi user characteristic of cloud [24].

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

- **Authorization**It states the access control to the system resources. It is generally handled by User Id and password. It states that only particular authenticated user [29] is allowed to access the system.

- **Non-repudiation** It is extension to the authentication service and identification. It states that whether message is send correctly and acknowledge us back to its sender [7]. Its states two communication between receivers and sender.

- **Availability** It states that resources should not underflow and it ensures that all user gets access to the system [37]. Cloud security mainly appears in the availability which is greatest challenge [1]. Customer expects no down time in cloud computing. Attaches such as DOS (Denial of service) can affect the availability of the system or infrastructure. The remaining paper is categorized as section. Some other survey done by other authors. Section 3 gives the classification of the risks present in cloud.

2. Related Work

Many authors have investigated on cloud security concern. In 2010, Amarnath et al. [4], stated that the VMs using shared physical infrastructure is grown at faster rate in cloud platform. However, with this advance it has introduce a vulnerability such as VMEscape and VM-Hoppingg. In this paper, the authors has shown importance of virtual networks in cloud computing. The study is limited to the threats resulting from virtualization techniques only.

In 2011 Shengmei Luo et al [31] provided a details of the security issues, challenges related to cloud virtualization and requirements. He also suggested some security frame works to avoid threats related to virtualization. However, he not discussed in details the implications of virtualization technology on cloud service models.

Hsin-Yi Tsai et al [11], considers security issues in service models based on benchmarks (Integrity, Availability and Confidentiality) , but it was restricted to only cloud virtualization.

In 2012, S.U.Muthunagai et al. [30], author surveyed and proposed an architecture for cloud protection, it was intended to provide a gap of security between host VM and Guest VM. However, its aim was restricted to vulnerabilities in cloud infrastructure.

In 2010, Kresimir Popovic et al [19] surveyed security in Cloud Computing, he explaned security issues and challenges. However, His research was not able to explain the effects of different threats on cloud service models.

Akhil Behl [2] investigated the security issues related to the cloud. He discusses the security approaches to safeguard the cloud infrastructure, applications and their drawbacks. His work did not discuss in deep on threats to virtualization and cloud service models.

Wayne et al. [34], detailed the importance of Cloud Computing along with the basic security concern. His research stated the basic problem in terms of cloud security and privacy. He limited his work to focuses only on public clouds. Moreover, He not stated any tool or framework to overcome the identified issues.

Although there is a huge amount of ongoing research for creating security tools; there is a need to consider the specific challenges faced by Cloud Computing. As virtualization plays important role in Cloud Computing, it is required to consider the additional amount of threats added by virtualization. Providing such a kind of complete survey becomes the motivation for us to present our survey.

3. Classification of Security Threats

Cloud security threats are classified into different categories as shown in belowdiagram.

The efficiency of cloud services can be considered as providing equal opportunities for advantages as well as threats. The structure of a cloud application shows that it has much more points of failure than traditional IT options like Abuse and Nefarious use, interfaces and unknown risks.

The diagramshown in Figure 2 classification of security threats at different levels. It further shows that Virtualization may cause additional four important security threats namely,Dependency on Hypervisor, Service Disruption, Isolation Failure and Shared Technology. The classification also lists the new-age threats like VM- Escape and VM - Hopping, where VM-Hopping is a threat by which an attacker can to spy another user's VM(s) using his own VM(s) and in VM Escape an attacker gets access to host machine and gain access to all the VMs. The survey also showsother possible vulnerabilities which would exist in networks by hypervisor with consequences Downtime in cloud service and Lost or Data Theft which are due to poor cloud infrastructure. In this section we discussing

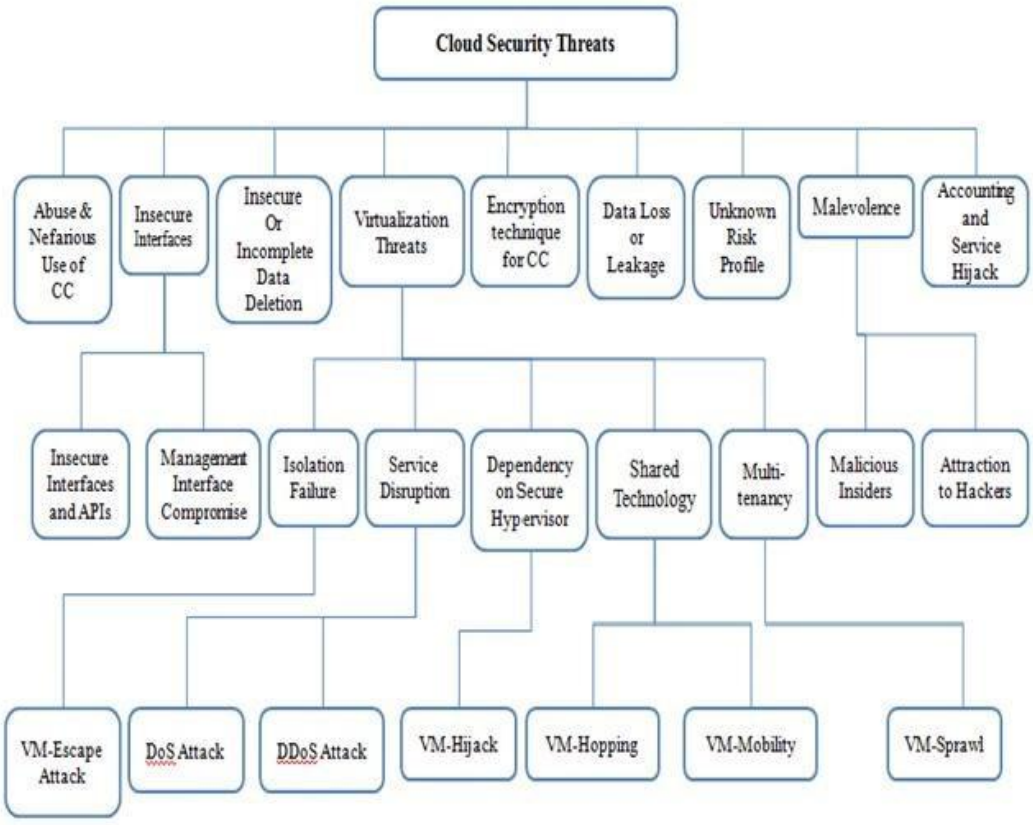

Figure 2: Various categories of cloud security threats

these issues and investigate other risks related to virtualization.

Cloud Computing belongs to Internet-based technologies and it offers three types of services. They areInfrastructure as a service (IAAS), Platform as a service (PAAS)and Software as a service (SAAS) [22]. In next section we will see IAAS andPAAS.

3.1 Abuse and Nefarious Use of Cloud Computing

This type of security thread can occur during registration process of cloud. Providers offers online payment mode for cloud service. Attackers can be able to make susceptible activates during this processes of registration. They can using techniques such as Spamming and Phishing [26]. PAAS provides has been attached previous using this technique. Recent updates that now attackers have started attaching IAAS as well. The next section explains the use and security of these service interfaces.

3.2 Insecure Interfaces & Data Deletion Activity

Cloud providers provides API to customers to interact with clouds services. The security of cloud depends on this APIs [27]. If handled without proper authentication, it can lead to vulnerable environment. So to avoid this we should be designed properly. Since we use shared approach for storing data, it is impossible to delete data completed which can further make insure for content privacy

3.3 Virtualization Threats

Virtualization is animportant technology for the realization of Cloud Computing; but the services offered by Virtualization may introduce some risks to its applications [33] as detailed below:

- **IsolationFailure**: Isolation is one of the main benefits of Virtualization [31]. This benefit of isolation if not deployed correctly will provide threat to cloud environment [18]. Inappropriate access control policy will cause threat in between two VMs and its associated VMM. Since the host machine VM is the root of security of a VM system, the program which gains access to the host VM can also gains the root privileges.
- **ServiceDisruption**: The Denial of service (DOS) attack is an attempt made attacker to make resource unavailable to serve for customers. This threat occur when an attacker gains access to an organization's login credentials [32]. In this attack service get stopped and customer is unable to use the cloud computing feature. The attackers send a bogus request and flood it at such extent that no more resource is available for others [9]. An attacker typically uses multiple computers to launch an attack. We can detect DoS attacks using IDS (Intrusion Detection Systems) over the cloud [36]. Another excellent approach is to limit the resource allocation using proper configurations. Thus, DDoS attack is a major threat to Availability feature f cloud computing.
- **Dependency on Secure Hypervisor**: The security of a computer is dependent on the quality of the underlying software kernel that controls the execution of several processes. In case of multi-system 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**: when two VMs are deployed over the same host. An attacker on first Virtual machine can gain access over the second Virtual Machine by getting its 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 virtual machine. Hence he can attack the second VM by changing the flow of traffic or manipulate the traffic itself. Strong security architecture 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 in cloud computing.

- **Multi-tenancy**: In this different users share same application and hardware which can cause information leakage. In a virtual system, vulnerable 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 Cloud Computing

Encryption of data is one of the solutions to secure cloud information [20], but it limits the efficiency and speed of the cloud. This is because encrypted documents must first be decrypted before they can be manipulated or searched. Furthermore, cloud data must provide with encryption before storing. Performing encryption and decryption on large data sets can be 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

Data loss and Data leakage are the top threats for cloud computing. 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 Cloud Computing 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

Some key objectives of Cloud computing is the decrease hardware, maintenance and software ownership [12]. The operational and financial 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. Authorization plays a vital role in securing the cloud.

This key challenge can be addressed to a certain degree by enforcing strict supply chain management and conducting a comprehensive supplier assessment [38].

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

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. 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 security policy control may not be effective in the case of a Malicious Insider colluding with the attackers. The summary of impacts of these security threats on different cloud service models are presented in the following section.

4. Summary

From above discussion it is observed that IAAS is most vulnerable among three domains, in area of isolation failures, dependency on hypervisors, shared technology and multi-tenancy.

5. Conclusion and Future work

Security has an important role to play in cloud, we should consider all the different possibility of threating occurring in cloud computing. The approach and classification shown in the paper will help in minimizing the threat. No things is 100 % reliable in view of security. The next aim of author would be to detect and prevent the threats in cloud.

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. 129134.

[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.

[27] Ramgovind S, Eloff MM and Smith E, "The Management of Security in Cloud Computing", IEEE, 2010.

[28] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki and Sugata Sanyal, "A Survey on Security Issues in Cloud Computing", IEEE.

[29] S.U.Muthunagai, C.D. Karthic and S. Sujatha, "Efficient Access of Cloud Resources through Virtualization Techniques, IEEE, 2012, pp. 174178.

[30] 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.

[31] Udaya Tupakula and Vijay Varadharajan, "TVDSEC: Trusted Virtual Domain Security", IEEE, 2011, pp. 57-63.

[32] Wayne A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud computing", NIST, IEEE, 2011, pp. 1-8.

[33] Wentao Liu, "Research on Cloud Computing Security Problem and Strategy", IEEE, 2012, pp. 1216-1219.

[34] 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.

[35] Xiaojun Yu and Qiaoyan Wen, "A view about cloud data security from data life cycle", IEEE, 2010.

[36] Yoshiaki Hori, Takashi Nishide and Kouichi Sakurai, "Towards Countermeasure of Insider Threat in Network Security", IEEE, 2011, pp. 633636.

[37] Zhi Wang and Xu xian Jiang, "Hyper Safe: A Lightweight Approach to Provide Lifetime Hypervisor Control Flow", IEEE, 2010, pp. 380393.

[38] Nagaraju Kilari and Dr. R. Sridaran, "Survey on Security Threats for Cloud Computing" 2012.

