ISSN No. 0976-5697

Volume 6, No. 2, March-April 2015

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Review on Security Issues in Cloud Computing

Harmanjeet Kaur
M. Tech Computer Science
Punjab Technical University, India

Ms. Neha Bhardwaj
AP, M.Tech Computer Science,
Department of CSE,India

Abstract: Cloud computing has different meaning to different people, the privacy and security issues also differ between a consumer using a public cloud application, a medium-sized Company using a customized Design of business on a cloud platform, and Some Companies are using Platform on Public level which are Public to Public Network The security requirements in cloud computing environment is to find the Security threats in the Structure of clouds To find the security solutions, and finding basis so that Pre Security Step Should be taken in concerned with security future model. In this paper is to build a trusted computing environment for cloud computing system by Combining the trusted computing platform into cloud computing system Which is free from attacks and threats and system is designed with a model system in which cloud computing system is combined with trusted computing platform and trusted platform models.

Keywords: cloud computing, data breaches, Api Attack Deniel Attack, Account high Jacking, Deniel of Services

I. INTRODUCTION

Cloud Computing has formed the concept and infrastructural basis for tomorrow's computing. The global computing infrastructure is rapidly moving towards cloud based architecture. While it is important to take advantage of cloud based computing by means of deploying it in diversified sectors, the security aspect in a cloud based computing environment remains at the core of Internet [1]. Cloud computing emerges as a new computing paradigm that aims to provide reliable, customized and quality of service guaranteed computation environments for cloud users. Applications and databases are moved to the large centralized data centers, called cloud [5]. Cloud Computing is set of resources and services offered through the internet. Cloud services are delivered from data centers located throughout the world. Cloud Computing facilities its consumers by providing virtual resources via internet. General example of cloud services is Google apps, provided by Google and Microsoft share point [2]. The Cloud Computing concept offers dynamically scalable resources provisioned as a service over the Internet. Economic benefits are the main driver for the cloud, since it promises the reduction of capital expenditure (CapEx) and operational expenditure (OpEx) [4]. Several studies have been carried out relating to security in cloud computing but this work presents a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing deployment types and the service delivery types.

A. Cloud Deployments Models:

In the Cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that increase or decrease depending on the demand. The cloud computing model has three main deployment models which are: [3]

a. Private Cloud:

Private cloud is a new term that some providers have recently used to illustrate services that follow cloud computing on private networks. It is set up within an organization's internal enterprise data center. In the private cloud, scalable resources and virtual application's internal enterprise data center. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are united together and available for cloud users to share the use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to intranet functionality. 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].

b. Community Cloud:

The cloud infrastructure is shared by several organizations and supports a specific community that has communal concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party, and may exist on premise or off premise [7].

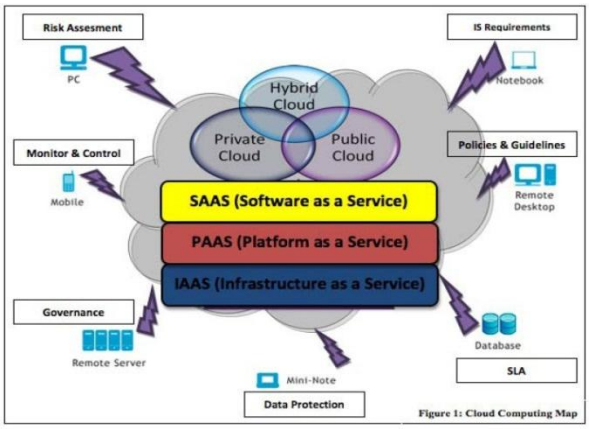

Figure 1: Cloud deployment model [3]

b. Public Cloud:

Public cloud describe cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the internet, via web applications/web services, from an off-site third party provider who shares resources and bills

on a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks [3].

c. Hybrid Cloud:

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed,[3]
provisioned as a single unit, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems. Hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services [3]. It can also describe configurations combining virtual and physical, collocated
assets -for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter.

B. Service Models:

a. Software as a Service (SaaS):

This kind of cloud computing transfer programs to millions of users through browser. In the user's view, this can save some cost on servers and software [6]. Software's are provided as a service to the consumers according to their requirement, enables consumers to use the services that are hosted on the cloud server [2].

b. Platform as a Service (PaaS):

Platform as a service, another SAAS, this kind of cloud computing providing development environment as a service [6]. Clients are provided platforms access, which enables them to put their own customized software's and other applications on the clouds [2].

c. Infrastructure as a Service (IaaS):

Rent processing, storage, network capacity, and other basic computing resources are granted, enables consumers to manage the operating systems, applications, storage, and network connectivity [2].

C. Security issues in service models:

Cloud computing utilizes three delivery models by which different types of services are delivered to the end user. The three delivery models are the SaaS, PaaS and IaaS which provide infrastructure, application platform and software as service to the consumer. These service models also place a different level of security requirement in the cloud environment. IaaS is the foundation of all cloud services, with PaaS built upon it and SaaS in turn built upon it. Just as capabilities are inherited, so are the information security issues and risks. There are significant trade-offs to each models in the terms of integrated features, complexity vs. extensibility and security. If the cloud service provider takes care of only the security at the lower part of the security architecture, the consumers become more responsible for implementing and managing the security capabilities [8].

SaaS is a software deployment model where applications are remotely hosted by the application or service provider and made available to customers on demand, over the Internet. The SaaS model offers the customers with significant benefits, such as improved operational efficiency and reduced costs. SaaS is rapidly emerging as the dominant delivery model for meeting the needs of enterprise IT services. However, most enterprises are still uncomfortable with the SaaS model due to lack of visibility about the way their data is stored and secured [8].

IaaS completely changes the way developers deploy their applications. Instead of spending big with their own data centers or managed hosting companies or colocation services and then hiring operations staff to get it going, they can just go to amazon Web services or one of the other IaaS providers, get a virtual server running in minutes and pay only for the resources they use. In short, IaaS and other associated services have enabled startups and other businesses focus on their core competencies without worrying much about the provisioning and management of infrastructure [8].

PaaS is one layer above IaaS on the stack and abstracts away everything up to OS, middleware, etc. This offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on underneath the service. It offers developers a service that provides a complete software development lifecycle management, from planning to design to building applications to development to testing to maintenance. Everything else is abstracted away from the "view" of the developers. The dark side of PaaS is that, these advantages itself can be helpful for a hacker to leverage the PaaS cloud infrastructure for malware command and control and go behind IaaS applications.

D. Security issues in SaaS:

In SaaS, the Service provider Play important role for proper security measures. The duty of provider is to keep multiple users' from seeing each other's data. The emphasis is on substituting new software applications for old ones. So that , the focus is not upon portability of applications, but on preserving or enhancing the security functionality provided by the legacy application and achieving a successful data migration.[8]

The SaaS software vendor may host the application on its own private server farm or deploy it on a cloud computing infra- structure service provided by a third-party provider (e.g. Amazon, Google, etc.). The use of cloud computing coupled with the pay- as-you-go (grow) approach helps the application service provider reduce the investment in infrastructure services and enables it to concentrate on providing better services to customers. Over the past decade, computers have become widespread within enterprises, while IT services and computing has become a commodity. Enterprises today view data and business processes (transactions, records, pricing information, etc.) themselves as strategic and guard them with access control and compliance policies. However, in the SaaS model, enterprise data is stored at the SaaS provider's data center, along with the data of other enterprises. Moreover, if the SaaS provider is leveraging a public cloud computing service, the enterprise data might be stored along with the data of other unrelated SaaS applications [8]. The cloud provider might,

additionally, replicate the data at multiple locations across countries for the purposes of maintaining high availability. Most enterprises are familiar with the traditional on- premise model, where the data continues to reside within the enterprise boundary, subject to their policies. Consequently, there is a great deal of discomfort with the lack of control and knowledge of how their data is stored and secured in the SaaS model. There are strong concerns about data breaches, application vulnerabilities and availability that can lead to financial and legal liabilities.

E. The following key security elements should be carefully considered as an integral part of the SaaS application development and deployment process:

a. Data security
b. Network security
c. Data locality
d. Data integrity
e. Data segregation
f. Data access
g. Authentication and authorization

a. Data Security:

In a traditional on-premise application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However, in the SaaS model, the enterprise data is stored outside the enterprise boundary, at the SaaS vendor end. Consequently, the SaaS vendor must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained author- ization to control access to data.

b. Network Security:

In a SaaS deployment model, sensitive data is obtained from the enterprises, processed by the SaaS application and stored at the SaaS vendor end. All data flow over the network needs to be secured in order to prevent leakage of sensitive information. This involves the use of strong network traffic encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for security.

In case of Amazon Web Services (AWS), the network layer provides significant protection against traditional network security issues, such as MITM (Man-In-The-Middle) attacks, IP spoofing, port scanning, packet sniffing, etc. For maximum security, Amazon S3 is accessible via SSL encrypted endpoints [8].

c. Data locality:

In a SaaS model of a cloud environment, the consumers use the applications provided by the SaaS and process their business data. But in this scenario, the customer does not know where the data is getting stored. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architecture (Softlayer, 2009). For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of local laws, there's also the question of whose jurisdiction the data falls under, when an investigation occurs. A secure SaaS model must be capable of providing reliability to the customer on the location of the data of the consumer [8].

d. Data integrity:

Data integrity is one of the most critical elements in any system. Data integrity is easily achieved in a standalone system with a single database. Data integrity in such a system is maintained via database constraints and transactions. Transac- tions should follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity [8].

e. Data segregation:

The major characteristics of cloud computing is Multi-tenancy. The multiple users can store their data using the applications provided by SaaS with the help of Multi-tenancy. In this type of situation, data of various users will reside at the same place. Interference of data of one user by another becomes possible in this environment. This Interference can be done either by hacking through the loop holes in the application or by injecting client code into the SaaS system. A client can write a masked code and inject into the application. The application which executes this code without confirmation, then there is a high potential of interference into other's data. A SaaS model should therefore ensure a clear limit for each user's data. The limit must be ensured not only at the physical level but also at the application level. The service should be intelligent enough to segregate the data from different users.[10]

f. Data access:

The Issues Regarding data access is mainly related to security policies provided to the users while accessing the data. In a typical situation, for carrying out its business processes a small business organization can use a cloud provided by some other provider. This organization will have its unique security policies based on which a particular access will be provided on set of data to every employee. The security policies may entitle some considerations wherein some of the employees are not given access to certain amount of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users. The SaaS model must be flexible enough to incorporate the specific policies put forward by the organization. The model must also be able to provide organizational boundary within the cloud because multiple organization will be deploying their business processes within a single cloud environment [10].

g. Authentication and authorization:

Most companies, if not all, are storing their employee information in some type of Lightweight Directory Access Protocol (LDAP) servers. In the case of SMB companies, a segment that has the highest SaaS adoption rate, Active Directory (AD) seems to be the most popular tool for managing users (Microsoft White Paper, 2010). With SaaS, the software is hosted outside of the corporate firewall. Many a times user credentials are stored in the SaaS providers' databases and not as part of the corporate IT infrastructure. This means SaaS customers must remember to remove/disable accounts as employees leave the company and create/enable accounts as come onboard. In essence, having multiple SaaS products will increase IT management overhead. For example, SaaS providers can provide delegate the authentication process to the customer's internal

LDAP/AD server, so that companies can retain control over the management of users [8].

F. Prevention:

a) High redundancy and high availability network design:

In order to prevent a network from falling trap into a DoS attack it is crucial to design the network as such that there is not a single point of failure. However, such high availability will incur additional cost, especially in maintaining dual connection to the Internet. It is also desired that ISPs provide load balancing on the upstream router to load share the redundant link [9].

a. Perimeter Defense:

The router and firewalls should pass through only legitimate packets to reach its internal network. An example is, limiting the internal web server from initiating port 80 connection destined to external hosts. Such filtering can prevent propagation of Code Red Worm attacks which causes a stream of scanning to various IP Addresses on port 80.[9]

Preventing IP Address Spoofing using egress and ingress filtering are examples of filtering at the gateway or router level to prevent packet spoofing from internal hosts, and to internal hosts respectively. However, it will not prevent attacks from legitimate IP Addresses within the network. Every interface on a router should prohibit packets that logically could not come from that network interface.[9]

b. Defense In-depth:

Implementation of Intruder Detection System (IDS) will allow detection of "slave","master" or "agent" machines communications. Action can be taken to remove those infected host from the network [9]. However, IDS may be able to detect known attacks but not new variations of these attacks.[9]

c. Host Hardening:

Hardening the respective device on the network will prevent the host from DoS attack. Host hardening involves upgrading the operating system, applying relevant patches for the operating system and required applications, closing irrelevant services, customizing and tightening configurations, and applying Access Control Lists on the required services. Changing default passwords and applying good password policies. Known buffer overflow attacks can be prevented by keeping the host up to date with patches or version upgrades.[9]

d. Malware Detection and Prevention:

The hosts and the network must have antivirus installed and scanning any introduction of new data, while file integrity checkers is used to detect any unauthorized attempt to change the original data [9]. This will prevent infection of malicious codes and attempts to rootkit the host. Compromised host could make the host a potent host to become handlers for malicious users who wish to conduct DoS attack[9].

e. Periodic Scanning:

Periodic network vulnerability scanning will detect vulnerable host and detect new infection. It is necessary to conduct periodic vulnerability since in any network, there are always new production host going on-line, or new devices being connected to the network.[9]

f. Policy Enforcement:

Last but not least is having a strong policy enforcement on acceptable use and management of computing resources. It is also a daunting task to ensure that all in house and outsource code development apply good programming practices to avoid loopholes such as buffer overflow and DoS. Rigorous testing of preproduction system is inevitable to avoid unwanted loopholes.

Despite applying all these measures there is still no guarantee that one will be immune to any DoS attacks but it will mitigate the effect of DoS attacks [9]. However, applying the above recommendations would also mitigate other forms of malicious activities such as session hi-jacking, buffer overflow attacks and reconnaissance. It will not only prevent your network from becoming targets of DoS attacks, but also prevent it from becoming the launching pad for such attacks.[9]

g. Legal infrastructure:

The legal framework in handling DoS and DDoS attacks differ based on the country's legal establishment. However, one common issue is that the legal definition of threats often misses out on DoS attack. The legal framework often defines "destruction of a communication device" as a crime, which defines it as a hardware. In a DoS and DDoS attack; the system may be recovered easily after a simple reboot, without damaging the hardware device [9]. The legal framework should define attacks as such attacks which causes failure of devices to function, or attacks which degrade the ability of the device to function, or attacks which attempt to overwhelm the bandwidth capacity of the network device to reflect DoS and DDoS attacks instead.

Another issue is spoofed IP addresses in DoS and using multiple points of attacks such as in DDoS, increases complexity of determining the original attacker's machine. It is often difficult to obtain the information from the infected host, unless with full cooperation from the affected organization and acted upon in a short period of time. Prolonged delay in investigation may cause the data to be lost. Even after the relevant information are being preserved, and analyzed, the integrity of the data will be questioned. These factors make it difficult to identify the person behind the computer.[9]

Legal proceedings require such information to be entangled and objectively determined and analyzed. Applying computer forensics procedures are crucial in the early process of evidence gathering.[9]

G. The Future of the Cloud Computing:

The following is a summary of ten cloud computing industry trends:

a. Cloud computing is widening, but focus on an open platform mainly.
b. Windows Azure is mostly a better platform of Exchange.
c. Google would increase the area of investment in the enterprise, more business users will use Google Apps.
d. The first batch of SaaS 1.0 companies will face the risk of bankruptcy.

e. The number of firms who abandon the use of its own server increased significantly.
f. Private cloud computing services have been popular.
g. Business Intelligence (BI) will be SaaS's next target.
h. SAP or Oracle will enter PaaS (Platform as a Service, PaaS, (Platform as a service) area[6].

II. CONCLUSION

Cloud computing is the promising paradigm for delivered IT services as computing utilities Cloud are designed to provide services to external user provider need to be compensated for sharing their resources and capabilities. This paper gives an overview of cloud computing service and deployment model to evaluate and improve the existing systems.

III. REFERENCES

[1]. Monjur Ahmed and Mohammad Ashraf Hossain, "Cloud Computing and Security Issues in the Cloud". International Journal of Network Security & It's Applications(IJNSA), Vol.6, No.1, January 2014.

[2]. Engr: Farhan Bashir Shaikh, Sajjad Haider, "Security Threats in Cloud Computing". 6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011, Abu Dhabi, United Arab Emirates.

[3]. Kuyoro S. O., Ibikunle F., Awodele O., "Cloud Computing Security Issues and Challenges". International Journal of Computer Network (IJCN), Volume(3): Issue(5): 2011.

[4]. Meiko Jensen, Jorg Schwenk, "On Technical Security Issues in Cloud Computing". 2009 IEEE International Conference on Cloud Computing.

[5]. Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jai, Yunlu Chen, Athanasios U. Vasilakos, "Security and Privacy for Storage and Computation in Cloud Computing". Information Sciences 258 (2014) 371-386.

[6]. Shuai Zhang, Shufen Zhang, Xuebin Chen, Xiuzhen Huo, "Cloud Computing Research and Development Trend". 2010 Second International Conference on Future Networks.

[7]. Dimitrios Zissis, Dimitrios Lekkas, "Addressing Cloud Computing Security Issues". Future Generation Computer Systems 28(2012)583-592, Department of Product and Systems Design Engineering, University of the Aegean, Syros 84100, Greece.

[8]. S.Subashini, V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing". Journal of Network and Computer Applications 34 (2011) 1-11.

[9]. Raja Azrina,Raja Othman "Understanding the various types of Denial of Service Attck."

[10]. Rashmi,,Dr G Sahoo,Dr S.Mehfuz "Securing Software as a Service Model of Cloud : Issues and Solutions". (IJCCSA), Volume 3, No. 4, August- 2013.

Short Bio Data for the Authors

Harmanjeet Kaur She obtained her B.Tech (computer science & engineering) from Sai Institute of Engineering and Technology, Manawala, Amritsar, Punjab, India, pursuing M.Tech (computer science & engineering) from Sai Institute of Engineering and Technology, Manawala, Amritsar, Punjab, India. Her area of interest is Cloud Computing and Security threat in cloud computing

Ms. Neha Bhardwaj is working as an assist. professor in Department of Computer Science & Engineering, Sai Institute of Engineering and Technology, Manawala, Amritsar, Punjab, India. She obtained her B.Tech (computer science engineering) from Amritsar college of Engineering and Technology, Manawala, Amritsar, Punjab, India, M.Tech (computer science & engineering) from Amritsar college of Engineering and Technology, Manawala, Amritsar, Punjab, India.