Cloud Computing

A review paper on security issues in SAAS

Komal Yadav
Mtech CS&E
Amity University, Noida

Neha Agarwal
Asst . Professor
Amity University, Noida

Abstract—**Cloud computing provides a way to enhance the capacity or services and add capabilities to the services dynamically without buying new infrastructure, licensing new software and training newly build organizations. It enhances the capabilities existing in Information Technology's (IT). In recent years, cloud computing has grown as a very big business promising concept for all fast growing segments of Information Technology's (IT) industry. But issues are beginning to grown on cloud as large amount of information of individuals and companies are stored on cloud, which raises a question about its safe environment-how safe an environment it is. So the major issue on cloud is security which decreases the growth of cloud and increases complications with data privacy and data protection. This paper is a review paper on more specific to the different security issues that has spread from various service delivery model i.e. SAAS(software as a service) on cloud.**

Index Terms— Security, Security issues, Cloud Service Provider.

I. INTRODUCTION

A) Cloud computing:

Cloud computing is a collection of networked and integrated hardware, software and infrastructure called Platform. It provides different types of services like SAAS, PAAS and IAAS. This platform provides on demand services to the users which are always on anywhere, anytime and anyplace. Cloud computing technology virtualizes and offers many services to the users across the network.

Cloud is a large collection of easily usable and accessible resources and services. These are virtualized resources those can be accessed and used by the users for different purposes. Cloud provides optimum resource utilization as these resources are reconfigured dynamically to the users to adjust variable load. It is a pay per use service in which the service providers provides services to the users by means of Service level agreements (SLA). SLA is an agreement between the user and service provider offers guarantees typically exploiting a pool of resources. Large companies provide cloud services with stable and strong cloud architecture which is very much beneficial for the individuals and organizations for various services as mass computing and storage centers.

Now a day, small and large business companies are realizing that they can gain fast access to the business applications or they can boost their infrastructure resources at minimum or negligible cost by using the cloud services. Cloud providers enjoy opportunities in the marketplace. The cloud providers must ensure that they will provide the full security aspects to the clients because if things go wrong then providers will be responsible for that. Cloud provides many beneficial services to the clients such as fast deployment, pay-for- use, lower costs, scalability, rapid provisioning, rapid elasticity, ubiquitous network access, greater resiliency, hypervisor protection against network attacks, low-cost disaster recovery and data storage solutions, on-demand security controls, real time detection of system tampering and rapid re-constitution of services . Cloud computing transfers the databases and the application software to the big data centers, where the management of the services and data are not trustworthy. This attribute creates many new security issues [14]. These security issues include but not only limited to virtualization vulnerabilities, accessibility vulnerabilities, , web application vulnerabilities like SQL (Structured Query Language) injection and cross-site scripting, physical access issues, privacy and control issues arising from third parties having physical control of data, issues related to identity and credential management, issues related to data verification, tampering, integrity, confidentiality, data loss and theft, issues related to authentication of the device or devices and IP spoofing.

B). Service Models:

1)Software as a Service (SaaS):

Software as a service are those services that are provided to the consumers to use the providers applications running on cloud. These services can be accessed by clients anywhere, anytime, anyplace with the help of various devices like thin client interface as web browser or by program interface. The main thing is that the consumer needs not to manage and control the cloud infrastructure which includes operating systems, storage, servers, network or even individual application, with the exception of limited user specific application configuration settings.

2) Platform as a Service (PaaS):

PAAS is one of the categories of cloud computing service models that provides a platform as a service. It is a way to rent operating system, hardware, storage, network over the internet. This service model allows the consumers to rent virtualized resources and their services for running applications or developing and testing newly created applications.

3) Infrastructure as a Service (IaaS):

It is a model in which an organization provides the equipments used for operation which includes storage, hardware, networking and servers. Infrastructure is provided by the service providers, who is the owner of these services and is responsible for running and maintaining it. The consumer pays as per- use basis, It is also called as Hardware as a service (HAAS). Customer has control over operating system, storage, applications and limited control of networking components (host firewalls) but customer does not manage or control the cloud infrastructure.

C). Deployment Models:

1) Private cloud: It is an infrastructure operated for a single or private organization, which can be managed internally or by a third party. It is a platform which is implemented under the control of the IT department within the corporate firewall. Private cloud require allocation of space, hardware and environmental control which have to be refreshed periodically, it results in additional capital expenditure.

2) Community cloud: In community cloud, infrastructure is shared by more than one organization and supports a specific community that has shared concerns like mission, security requirements, policy, and compliance considerations. It can be managed and controlled by the organizations or a third party.

3) Public cloud: In Public cloud, infrastructure is available for the general public or for a large organization and is owned by an organization which sales cloud services.

4) Hybrid cloud: In Hybrid cloud, infrastructure is a combination of two or more clouds such as private, community, or public, that are unique entities but are bound together with the help of standardized technology that enables data and application portability (e.g., “cloud-bursting” for load-balancing).

D).Characteristics of cloud computing:

1) Broad network access: Services of cloud are available over the network and can be accessed by anyone with the help of standard mechanisms that help to use by heterogeneous thin or thick client platforms like tablets, workstations, mobile phones and laptops.

2) Measured service: The usage of services on cloud can be measured, controlled and reported by both the providers and consumers of the utilized service. Cloud computing services have capabilities which enable to control and optimize resource use. It is based on pay per use basis, the more you use the service, the higher the bill to pay.

3) On-demand self-service: It refers to the services provided by the vendors of cloud that enables end users to provision network, storage, computing and software in a flexible and simple way. These cloud services are accessed through online control panel.

4) Rapid elasticity: It is capability in cloud computing which provides scalable provisioning. It is an ability which provides scalable services. It allows users to request extra space in the cloud or other different types of services. It is very essential part of the cloud computing in which resources appears very large in number or infinite and available automatically.

5) Resource pooling: Resource Pooling is a collection of resources available for completion of tasks of different projects. A resource pool can be assigned to a task and can be shared by different projects. In this customer does not has knowledge over the exact location of the provided resources, it has a sense of location independence. Some examples of resources are as memory, network bandwidth, storage and compute.

II. LITERATURE SURVEY

A). Service Providers of Cloud Computing

1) Amazon’s Elastic Compute Cloud (EC2) allows users to run their own software on an extremely powerful server. Such use can drastically cut computation times for unique, complex databases and other types of software calculations. [5]

2) Google provides large number of software on demand using their enormous server power. There is no requirement to install software on the user’s computer, everything actually runs on Google’s machines and is accessed by the user’s web browser. It has nothing to install for the user and hence the application runs on Google’s servers. A simple phone web browser can write data, documents and presentations utilizing the computing and processing power contained in the cloud.

3) Salesforce.com provides clients the capability to independently utilize powerful servers with inbuilt databases, mapping utilities, and other interfaces of different applications. SaaS model is supported with the use of a web browser, an alternative to the SaaS approach is offered, which allow clients to use their own frontend software suite, which is more correctly defined as client-server.6

B) Security issues in service models

Cloud computing uses three types of delivery models by which different types of services are delivered to the end user. The three delivery models of cloud are SaaS, PaaS and IaaS which provides different types of services like application platform, infrastructure resources, and software as services to the consumer. These three types of service models require different level of security services in the cloud environment. IaaS contains all cloud services as it is called as the foundation of all cloud services, with PaaS built upon it and SaaS in turn built upon it. Information security issues and risks are inherited as the capabilities are inherited from one service model to another. There are different trade-offs in each service model in the terms of complexity vs. extensibility, integrated features and security.

According to a recent survey by Cloud Security Alliance (CSA) & IEEE it is indicated that across sectors enterprises are interested to have cloud computing but security is needed for both to expand cloud adoption on a wide scale and to respond to regulatory handlers. Cloud computing is shaping the future of IT's but it has dramatic impact on cloud computing growth because of the impact of absence of a compliance environment. By using services like infrastructure as a service, organizations critically like to test the security and confidentiality issues for their critical insensitive applications in business. In cloud it is difficult to guarantee the security of corporate data, as they provide different types of services like SaaS, PaaS, and IaaS. Each of these services has their own security issues.[6]

SaaS is a service model to deploy software where applications are remotely hosted by the service provider or applicaton and made available to customers on demand, over the Internet. SaaS model provides several benefits to the customers with, such as it increases operational efficiency and reduced costs. SaaS is rapidly rising as the dominant delivery model to fulfill the needs of enterprise IT services.

III. SECURITY ISSUES IN SAAS:

In SaaS, the major security issue is that client has to depend on the provider for all security measures. So it is provider's duty keep multiple users' from watching and accessing each other's data. So the users are not ensured about the security measures on cloud, it becomes difficult for the users to ensure that right security measures are provided to the data and also they are not assured whether the application will be available when needed.

Computers have been spread widely within business, while IT services and computing has become asset. Nowadays, enterprises view data and business processes (pricing information, transactions, records, etc.) themselves as vital and watch them with access control and assent policies. In the SaaS model, enterprise data is stored at the service provider's data center, which has the data of other enterprises. Moreover, if the SaaS provider favours a public cloud computing service, the enterprise data might be stored along with the data of other unrelated SaaS applications.

The SaaS vendors should host the application on its own private server farm or deploy it on a cloud computing infrastructure service provided by a third-party provider (e.g. Amazon, Google, etc.). Cloud computing provides the services with the pay- as-you-go approach which helps the application service provider to decreases the investment in building or buying infrastructure services and it also enables it to focus on providing better services to cloud users.

Few security elements which should keep in mind as an essential part of the development and deployment of SAAS application service process:

1) Data access

Data access issue is related to the issues in accessing the data stored on cloud. It is related to the various security policies provided to the users during accessing the data on cloud. Each cloud provider has its own security policies, for example if a small business organization can use a cloud provided by some other cloud provider for carrying out its business processes then this organization will have its own security policies because of which no employee can access data of other employee but has access to a particular set of data. The security policies may allow some attention in which some of the employees are not given access to certain amount of data. These security policies should be held by the cloud to avoid leakage of data by unauthorized users [20]. The SaaS service model should be flexible to incorporate the rules and policies and put forward by the organization.

2) Network security

In network security all confidential data flow over the network that is needs to be secured to prevent unauthorized access to sensitive information. In SaaS deployment model, confidential data is obtained from the various business, SaaS application processed this data and stores at the vendor's end. It involves the use of various strong network traffic encryption techniques for security such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS).

3) Data integrity

Data integrity is the most important element in any system. Data integrity can be achieved easily in a single or standalone system with a single database. In these systems data integrity is maintained by database transactions and database constraints. All the transactions should follow ACID (atomicity, consistency, isolation and durability) properties to confirm data integrity. Most of the databases follows ACID transactions and can prevents data integrity.[15]

4) Data security

In a traditional application deployment model, the sensitive data of each enterprise always reside within the enterprise boundary and is concern to its logical, physical and access control policies and personnel security. Whereas, in the SaaS model, the business data is stored outside the enterprise boundary i.e. at the SaaS vendor's end. So, the SaaS vendor must follow additional security survey to ensure data security and prevent breaches due to security vulnerabilities in the application or with unauthorized access of employees. This process of preventing data involves the use of strong encryption techniques for data and strong authorization to control access to data.

5) Authentication and authorization

Not all but most of the companies are storing their employee information in Lightweight Directory Access Protocol (LDAP) servers. In SMB companies, Active Directory (AD) used as the most popular tool for managing users [18], when a segment that has the highest SaaS adoption rate. Most of the times user documents are stored in the SaaS providers' databases and not as part of the corporate IT infrastructure. As with SaaS, the software is hosted outside of the corporate firewall.

6) Data locality

In SaaS model of a cloud environment, the customers use the applications given by the SaaS and process their business data. But in this case, the customer does not know the location i.e. where the data is getting stored. Sometimes, this can be an issue. Because of assent and data privacy laws and regulations in various countries, locality of data has much importance in many enterprise architecture. For example, in many countries like South America countries, different types of data cannot go out of the country because of potentially sensitive information.[7]

7) Data segregation

Multitenancy is one of the major characteristics of cloud computing. Because of multi-tenancy multiple users can store their data by using the applications provided by SaaS. In these cases, data of different users will placed at the same location. Intrusion of data of a user by another user becomes possible in this environment. This intrusion can be done either by injecting client code into the SaaS system or by hacking through the loop holes in the application or. A client can write their masked code and can inject into the application. If this code is executed without verification, then there is a high potential of intrusion into other's data.[16]

IV. CONCLUSION

Security is a critical aspect for providing a reliable environment and then enables the use of applications in the cloud and for moving data and business processes to virtualized infrastructures. Many of the security issues were identified were observed in other computing environments: Authentication, network security and legal requirements etc.

An integrated security model targeting different levels of security of data for a typical cloud infrastructure is under research. Cloud Providers will find themselves in the role of needing to provide Service Level Agreements (SLA) for Digital Evidence collection for their clients.

Now in future I will focus on two directions to provide confidentiality, integrity, and security to the customer data. Firstly to extend techniques such as proposed in Anonymization by Intel to improve confidentiality and secondly integrity of the data.

V. ACKNOWLEDGMENT

This work was supported by Assistant professor Ms. Neha Agarwal. I would like to thank her for their guide and help.

VI. REFERENCES

[1] Special Publications 800-145 "National Institute of Standard and Technology (NIST)"

[2] Abhishek Goell, Shikha Goel ; Security Issues in Cloud Computing ; International Journal of Application or Innovation in Engineering & Management (IJAIEM) ; 2012 December ;Volume 1, Issue 4.

[3] Balachandran Reddy, Cloud computing security issues and challenges, 2009.

[4] Rohit Bhadauria, Rituparna Chaki, Sugata Sanyal, "A Survey on Security Issues in Cloud Computing", 2011.

[5] http://en.wikipedia.org/wiki/Cloud_computing.

[6] Dr. A. Askarunisa, N.Ganesh, A.Athiraja, Venkatesh ; Security Issues in Cloud Computing ; International Journal of Latest Trends in Engineering and Technology (IJLTET); 2013 September.

[7] IDC (2009) Cloud Computing 2010 – An IDC Update. Slideshare .net/JorFigOr/cloud-computing-2010-an-idc-update.

[8] Mell P, Grance T (2009) The NIST Definition of Cloud Computing. Technical Report 15, National Institute of Standards and Technology, www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

[9] Cong Wang and Kui Ren, Wenjing Lou, Jin Li,‖Toward Publicly Auditable Secure Cloud Data Storage Services‖ in IEEE Network July/August 2010.

[10] New IDC IT Cloud Services Survey: Top Benefits and Challenges. Retrieved April 8, 2011 from http://blogs.idc.com/ie/?p=730

[11]Salesforce (2011) Security Implementation Guide.login.salesforce.com/help/doc/en/salesforce security impl guide.pdf

[12]Amazon (2011) Elastic Compute Cloud(EC2). aws.amazon.com/ec2/.

[13] EMC, Information-Centric Security http://www.idc.pt/resources/PPTs/2007/IT&Internet_Security/12.EMC.pdf.

[14] C. Wang, Q. Wang, K. Ren, N. cao and W. Lou " Towards Secure and Dependable Storage Services in Cloud Computing", Accepted for publication in future issue of IEEE Trans. Service Computing. DOI:10.1109/TSC.2011.24.

[15] P. Syam Kumar, R. Subramanian, "Homomorpic Distributed Verification Ptorotocol for Ensuring Data Storage in Cloud Computing". International Journal of Information, VOL. 14, NO.10, OCT-2011, pp.3465-3476.

[16] Subashini S, Kavitha V., "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications (2011) vol. 34 Issue 1, January 2011 pp. 1-11.

[17] Q. Wang, C. Wang, K. Ren W. Lou, and J. Li, "Enablingpublic verifiability and data dynamics for storage security in cloud computing," IEEE Trans. Parallel and DistributedComputing.VOL.22, NO.5, May 2011, pp.847-859

[18] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina. Controlling data in the cloud: Outsourcing computation without outsourcing control. In ACM Workshop on Cloud Computing Security, 2009

[19] EMC, Information-Centric Security. Http://www.idc.pt/resources/PPTs/2007/IT&Internet_Security/12.EMC.pdf.

[20] Latest cloud storage hiccups prompts data securityquestions.http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130682&source=NLT_PM.