Security Issues Survey in Cloud Computing

Sarbojit Banerjee[1], Prasenjit Kumar Das[2]

[1]Editorial member , Kuwait Journal of Science, Kuwait
[2]Assistant Professor, Computer Science Department, NIT Silchar, India

***Abstract*—Cloud computing is a kind of architecture which provides services through the internet due to the high demand by the users and they have to pay in order to access shared resources like servers, storage, applications etc, without acquiring them physically. Therefore this technology saves time and cost for those organizations which uses it. In cloud computing the user data is maintained and stored at data centers of providers like Salesforce, Amazon, Google etc. There are many security issues and threats in cloud computing including insecure interface, data leakage, resource sharing etc. This research paper includes cloud computing technology details and the security issues that are present currently in this industry. This paper also shows the research challenges that are present in cloud computing technology.**

***Keywords* : Cloud Computing, Cloud Architecture, Data Protection, Security Issues.**

I. Introduction

Cloud computing is a computing terminology which is recently evolved and a metaphor based on consumption of computing resources and utility. It includes deploying of groups of remote servers that allows data storage which is centralized and access to computer resources or sevices via internet. The service providers of cloud provide platforms for users to use web services. This technology is an architecture that allows on-demand and convenient network access to a shared resources like applications, servers, storage, networks. There are three types of services provided by cloud i.e. Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). One of the important reason for organizations to choose cloud computing because they only require to consume resources on payment basis. This helps the organizations to meet the needs of changing markets easily and to get a leading edge for their customers. It appeared that cloud computing is a necessity in business, by the idea of using the infrastructure without managing it. Many companies like Amazon, Microsoft, Yahoo, Salesforce and Google provide cloud computing services. This helped startup companies and developers to give importance to the business value rather than the starting budget to enter the markets. With the help of this technology, consumers can access applications which is heavy via lightweight devices such as laptops, mobiles and tabs etc. The customers need not require knowledge to control the infrastructure of clouds as it is abstracted. The cloud services provides quality of service, high computing power, higher throughput and high scalability.

II. Cloud Computing Models

The cloud computing is generally divided in three categories and they are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Software as a Service (SaaS) : SaaS is at times called as "on-demand software" and is priced to the customers on a pay-per-use basis. The SaaS providers price the applications using fee by subscription.

In this model, the cloud providers will operate and install application software in the cloud and the users access the software from clients of the cloud. Users need not require to manage the platform and infrastructure of the cloud where the application executes. This helps in the elimination of the need to install and run the software application on the user's own computers, thus simplifying support and maintenance. In order to accommodate a large number of cloud consumers, the applications of cloud can be multitenant, which is, any machine can serve multiple cloud user organization.

The drawback of SaaS is that the data of the consumers are kept on the provider's server. So, there can be access to the data in an unauthorized way. Due to this reason, customers are adopting other third-party management systems in order to help secure their data. Examples of SaaS are Salesforce.com, Google Apps.

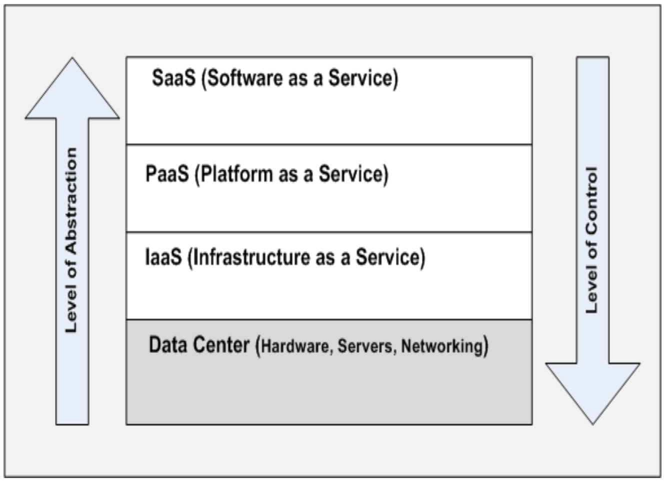
SaaS (Software as a Service)
PaaS (Platform as a Service)
IaaS (Infrastructure as a Service)
Data Center (Hardware, Servers, Networking)
Level of Abstraction
Level of Control

Fig 1 : Cloud Computing Architecture

Platform as a Service (PaaS) : PaaS is like providing a computing platform as a service without the need to download software's or install it for developers, consumers and IT managers. The developers can do coding and execute their software on a cloud platform without the cost of managing and buying the underlying software and hardware layers. By the help of PaaS, underlying storage and computer resources can scale automatically to match the demand, so that the consumer need not have to manually allocate resources. Examples of PaaS are, Google App Engine, Microsoft Azure.

Infrasructure as a Service (IaaS) : Here the hardware resources are shared for executing services using the virtualization technology. Its sole purpose is to make resources like servers, storage, and network accessible by software applications and operating systems. So, it provides infrastructure services on demand and communicates with routers, hosts and switches using API's, in a transparent manner. The consumers does not manage the underlying hardware, but he/she controls the storage, operating systems, and applications which are deployed. It is up to the service provider who actually takes care for keeping, executing and maintaining it. Examples of IaaS are Amazon S3, Amazon EC2.

There are seven cloud models and they are Private Cloud, Public Cloud, Hybrid Cloud, Community Cloud, Distributed Cloud, Intercloud, Multicloud and they are given below.

Private Cloud : It is a cloud infrastructure which is operated for a single organization. It is hosted either internally or externally and managed internally or by a third-party. If a private cloud is undertaken then it requires a significant level of engagement to virtualize the business environment. It also requires the organizations of cloud to reevaluate decisions about existing resources. It can improve the business, but the project can raise security concerns that should be addressed in order to prevent security attacks.

Public Cloud : Here the services are public in nature and are rendered over a open network. This cloud service may be either free or provided on a pay-per-usage. There is very little little difference between private and public cloud architecture, but, the security may be different for services provided by the service provider for public consumers and when the communication is done on a non-trustworthy network.

Hybrid Cloud : A hybrid cloud service is a kind of cloud computing service that is the combination of private, community and public cloud services, from different service providers. This cloud service may cross boundaries so it can't be put only in one category.

Community Cloud : Here the infrastructure is shared by many organizations for a shared cause and can be managed by a third party service provider or by them. It is based on an agreement between organizations such as educational or banking organizations. A cloud environment may exist remotely or locally.

Distributed Cloud : Cloud services can be provided by a distributed machines which are running at different locations but are connected to a single network.

Inter-Cloud : It is globally interconnected "cloud of clouds" and also an extension of internet which is based on "network of networks".

Multi-Cloud : Multi-cloud is the use of more than one cloud computing services in a single architecture which is heterogeneous, in order to reduce the reliability on single vendors.

III. Security Issues in Cloud Computing

There are many security issues in cloud computing as many technologies are encompassed by it. Data security includes encryption of the data and also ensuring that the policies are appropriate are enforced on data sharing. The security issues concerned in cloud computing are given below :

(i) Server and Application Access
(ii) Virtual Machine Security
(iii) Data Transmission
(iv) Network Security
(v) Data Security
(vi) Data Location
(vii) Data Availability

Server and Application Access : The administrative access in cloud computing is conducted via the Internet, it is more prone to exposure and risk. It is very important to restrict these accesses to data and try to check this accesses in order to maintain visibility of changes in system control. The issue of data access is related to security policies which are provided to the consumers when data is accessed. There are organizations which are going to have its own policies on security based on which every employee would have access to a set of data. Due to these policies some of the employees will not given access to a certain amount of data. Therefore, these security policies should be adhered by the cloud in order to avoid malicious intrusion by unauthorized users.

Virtual Machine Security : It is the main components of the cloud. Virtual machines are dynamic. It ensures that instances executing on the similar machines are isolated from each other and that is a main task of virtualization. They can also be seamlessly moved between physical servers and can be cloned. Due to this dynamic nature VM sprawl made it not easy to achieve consistent security. There are vulnerabilities and error. Virtual Machine Monitor, is a software which tries to abstracts the physical hardware when it is utilized by virtual machines. It provides a processor which is virtual and also system devices like memory, I/O devices, storage etc. Many bugs have been found in virtual machine monitor. Again it was also found in VMware's shared folders mechanism as well.

Data Transmission : In data transmission the encryption technique is used. Here the Secure Socket Layer protocols are used. The data only goes where the user wants it to send using authentication and the data not changed during transmission. The cloud requires the data to be encrypted because it is no encrypted during processing. In order to process, the data should be encrypted. To provide the integrity of data transmission within cloud there should be using access controls like authentication, authorization and auditing for using resources. The cryptographic attack includes an attacker who places themselves in the path of communication between the customers and so they can interrupt and change communications.

Network Security : Issues associated with network security includes of Sniffer attacks, DNS attacks, reused IP address, etc and are given below :

In the sniffer attack there are applications which captures packets that is flowing in a network and if the data is not encrypted, then it can be read and the information can be traced or captured.

In domain name server or DNS, includes translation of domain name into IP addresses. But there are cases that the users they have been routed to other malicious cloud instead of the one which he/she asked for and so using IP address is not the secured way.

In a reused IP issue, when a user goes out of a network then his/her IP-address is assigned to a new user. So, sometimes this can be risky as there is a certain time lag between the change of an IP address in DNS and the clearing of that address in DNS caches. Hence this makes it vulnerable and so the data can be accessed by some other user since in DNS cache the address still exists.

Data Security :, Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) are the most common adoption in order to assure the information security and data integrity. The cloud providers like in Amazon, the Elastic Cloud or EC2 administrators does not have accesses to user instances and so cannot log into the guest operating system. So, they need cryptographically strong SSH keys in order to gain access to a host. Such accesses are routinely audited and logged. Again the data in Simple Storage Service or S3 from Amazon is by default also not encrypted, customers can encrypt data before it is uploaded to S3.

Data Location : The exact location of the datacenters are not known to the cloud and also they don't have any control over access to their data. Renowned cloud providers have datacenters all over the world. So, in many a cases, its an issue. Since there are data privacy and compliance laws in different countries, the actual locality of users data is very important. In order to maintain integrity in data in a cloud like distributed system, the transactions among different data sources needs to be controlled or handled correctly and safely. The central global transaction manager does this. Therefore, each application in the cloud should participate in global transaction via a resource manager.

Data Availability : The data owners suffer from system failures of the service provider when the data are kept at remote systems owned by others. If the service of the clouds goes out of operation, then the data will become unavailable as it depends on a single service provider. So, the cloud application needs to ensure that the provider provides service all the time. Therefore, it involves making architectural changes at the infrastructural and the application levels to add high availability and scalability. Hence, a multi-tier architecture should be adopted which is supported by application instances of a load-balanced farm, executing on many servers that should be resilient to software or hardware failures and denial of service attacks. There should be very good action plan for disaster recovery and business continuity during emergencies.

IV. Research Challenges in Cloud Computing

There are many research challenges in cloud computing technology and it tries to address this challenges in order to meet the requirements of next generation cloud architectures. The research is still at a very early stage. There are many issues in this technology which have not been fully addressed, while new challenges keep on emerging. Some of these challenges are :

(i) Data Encryption
(ii) Service Level Agreements (SLA’s)
(iii) Access Controls
(iv) Interoperability
(v) Reliability & Availability of Service
(vi) Multi-tenancy
(vii) Platform Management

V. Conclusion

Sharing of resources is one of the most security worries within cloud computing. The service providers should inform their users about the security provided on their cloud by them. In this paper, we first discussed about the architecture of cloud computing and various models, then the security issues and research challenges in it. Also there are other security challenges which includes security aspects of virtualization and network. This paper tried to describe all those issues. It is into our belief that it will be difficult to achieve end-to-end security because of the complexity of the cloud. Its high time that new security techniques should be developed. We sincerely hope that our work will provide a better understanding of challenges of cloud computing and help in future research in this technology.

REFERENCES

[1] Sarbojit Banerjee, Shivam Jain, “A survey on Software as a Service (SaaS) using quality model in cloud computing”, Volume 3 Issue 1, January 2014 Page No. 3598-3602.

[2] Prasenjit Kumar Das, Mr.Pradeep Kumar, Manubolu Sreenivasulu, "Image Cryptography: A Survey towards its growth", Advances in Electronic and Electric Engineering, Volume 4, Number 2,2014, pp 179-184.

[3] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., “Scientific Cloud Computing: Early Definition and Experience,” 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695- 3352-0.

[4] A. Kundu, C. D. Banerjee, P. Saha, “Introducing New Services in Cloud Computing Environment”, International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[5] B. R. Kandukuri, R. Paturi V, A. Rakshit, “Cloud Security Issues”, In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[6] R. L Grossman, “The Case for Cloud Computing,” IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.

[7] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou,“Ensuring Data Storage Security in Cloud Computing,” 17th International workshop on Quality of Service, USA, pp.1-9, July 13-15, 2009, ISBN: 978-1-4244-3875-4

[8] Hanqian Wu, Yi Ding, Winer, C., Li Yao, “Network Security for Virtual Machines in Cloud Computing,” 5th Int’l Conference on Computer Sciences and Convergence Information Technology, pp. 18-21, Seoul, Nov. 30- Dec. 2, 2010. ISBN: 978-1-4244-8567-3.

[9] S. Subashini, V. Kavitha, “A survey on security issues in service delivery models of cloud computing”; Journal of Network and Computer Applications, Vol. 34(1), pp 1–11, Academic Press Ltd., UK, 2011, ISSN: 1084-8045.

[10] V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S. Reddy, P.Sai Kiran “Research Issues in Cloud Computing “ Global Journal of Computer Science and Technology, Volume 11, Issue 11, July 2011