Security Issues In Cloud Computing

Sunaina Choudhary
Dept of CSE
CET-MUST, Lakshmangarh

Abstract- *This paper is an effort to bring forth the security issues in cloud computing in spite of the fact that cloud computing is an emerging technology in the world of science and in our life. Cloud computing refers to the internet based platform for computing and information technology paradigm where computing is moved from our personal computer to a common platform where several computers shares the common server known as „cloud" of computers. Its importance is increasing day by day and this technology is blooming in the scientific and industrial communities. But due to several security issues which are faced by the users it create doubts in the mind of owner to go further with it and to share their data with the third party. Thus this paper lists the architecture and characteristic of cloud computing followed by all the common security issues, all types of attacks, with the future perspective that one can secure themselves from all of these issues as security is the prime concern for all.*

Keywords- Cloud Computing, Security, Platform

I. INTRODUCTION

Cloud computing is an valuable evolution in Information Technology sector meant to provide computing services like platforms, infrastructure and applications which can be used via internet. From a study by Gartner considered cloud computing as first among the 10 most important emerging technologies in the successive years by the organizations. Cloud computing is a model that allow ubiquitous, suitable, on-demand network accessible to a shared computing resources (e.g., networks, servers, storage, applications, and services) implementing engineering principals to obtain best quality of service for the user. Service of cloud computing offers various features like flexibility, high scalability, reliability and dynamic approach. Cloud computing is a way to reduce the cost of hardware and software services as everything is provided via internet. The merits of cloud computing technology are broad. The very most important one is that the users don‟t need to buy the resource from a third party or the service provider instead they use the resources and pays for it as a service thus cloud helps the users to save time and also money. But because the information is kept at the third party location or it can be termed as cloud or service provider, this leads to a lot of insecurities in the minds of end user about their data to be hacked. Hence, it leads to a lot of security concerns and security issues too. This model is also applicable and used by small and medium enterprise. Therefore one can use it anywhere, anytime and on their personal network. Google apps are one of the good examples of cloud computing because all users store their own data on a common platform.

The letter of word cloud itself depicts its meaning:

C stands for common that is a single platform for all its users.
L stands for location independent that means it can be accessed from anywhere.
O stands for online.
U stands for utility which implies pay for use.
D stands for demand.

Cloud further contains different models which are divided into two type delivery and deployment models which depict the architecture of the cloud. It is also discussed in this paper. One of the advantages of cloud is that the user does not require any knowledge about the infrastructure. The main disadvantage of cloud is that it has many issues related to security point of view especially on data theft, data loss and privacy of data. This paper firstly lists the architecture of the cloud and then the parameters which affect the security of the cloud. It also traverse the cloud security issues and problems faced by service provider and by cloud service consumer such as data problems, infected application, privacy concerns and security issues while using it.

II. CLOUD COMPUTING ARCHITECTURE

Cloud Computing architecture involve multiple cloud components which deals with each other for various data, thus allowing the end user to access to the data on a better rate. When we look cloud it contains both the front end and the back end. Front end is for the end user side those who will access the data, whereas the backend is the data storage device, provided by the server on a common platform. Cloud computing is categorized into two different categories of models one is the delivery model and another one is the deploy model. There are several service provider of cloud computing like Amazon, Microsoft, Yahoo etc. Deployment Models:

Private cloud- The private cloud infrastructure is designed only for the single organization which is comprised of multiple users. It may be owned or used by a single organization. It ismore secure because it is accessible by the customer of a single organization and not by everyone thus the data loss and other security issues are reduced to some extent. Example forthis kind of cloud is Eucalyptus Systems.

Public cloud- The public cloud infrastructure is designed for everyone accessible fromanywhere and used by general public. People may own it or it can be operated by a single organization or a combination of them. It is less expensive and also less secure as it can be accessible by anyone by the end user side and from everywhere. Example of public cloud is Microsoft Azure and Google apps.

Hybrid cloud- It is also known as the community cloud. This is the model which is shared between two or more organization. It is the combination of both private and the public model. It is managed, owned and operated by an organization or more than one having shared concern or by a third party. It is hard to process and maintain. Example of this kind of cloud is Amazon Web Services.

Delivery Models:

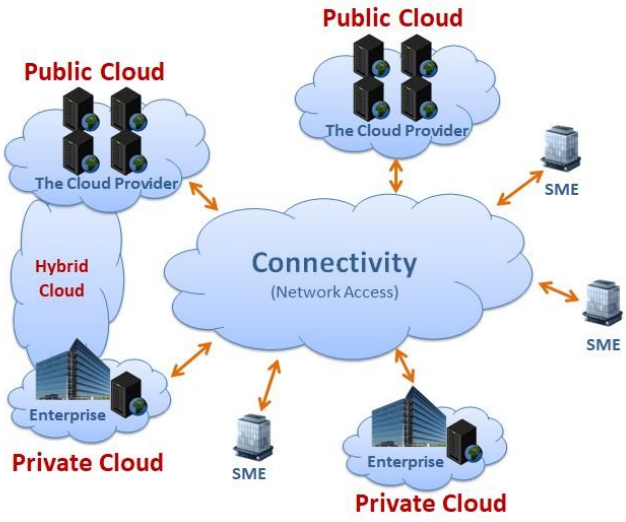

Figure 1. Deployment Models

It is divided into three categories Software as a Service (SaaS), Infrastructure as a Service(IaaS), Platform as a Service(PaaS).

Software as a Service (SaaS) – It is also called a delivery model where the software and the data can be described as a process by Application Service Provider(ASP) by the third party and that is cloud service provider, like your Gmail account that you can use on someone else's system. This makes the customer to get rid from installing and operating the application on own computer and also eliminate the work of software maintenance .The ability is to provide the use the provider‟s applications running on a cloud infrastructure to the user. The user does not manage the cloud infrastructure including networks, storage, or any security issues with the possible exception of limited user-specific application configuration settings. All the responsibility is under the SaaS vendor about network, storage and managing the IT infrastructure .Examples of SaaS includes: Salesforce.com, Google Apps.

Infrastructure as a Service(IaaS) - Infrastructure as a service (IaaS) provides services to the companies by sharing of hardware resources with computing resources using Virtualization technology which includes servers, storage, networking on a pay use basis. It provide the consumer processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which includes operating systems and applications. Therefore it offers on demand services using API for interaction with host, routers etc. The user need not to manage the hardware, operating system and deployed application but has control over some network components. Examples of IaaS are Amazon S3, GoGrid.

Platform as a Service(PaaS)- It is a computing platform offers service without softwaredownload and installation. The customer is to deploy on the cloud or application created using programming language, services, tools supported by service provider. In this we can use web based tools in order to develop application in order to run them on system software provided by a company. There is no need to manage operating system, database etc. The user works on pre-built application components. Examples of this class of services include Google App Engine, Windows Azure Platform and rack space.

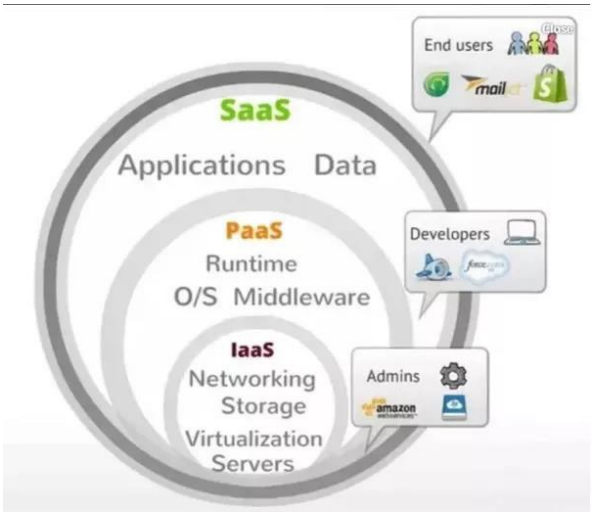

Figure 2. Delivery Models

III. CLOUD SECURITY ISSUES

As we know that cloud computing is an emerging technology and security is considered as a primary and prime factor in any technology therefore it should be up to the mark. But in this case cloud computing lacks and thus it has many issues.

Parameters affecting cloud security

There are many security issues in cloud computing as it include technologies with has networks, databases, operating systems, virtualization load balancing, resource allocation, memory management, transaction processing and concurrency control. Security issues for these technologies are related to cloud computing. Data security can be done by encryption of data as well as ensuring that all the policies are enforced for data sharing for security. In addition to it, resource allocation and memory management algorithms should be secured. At last the data mining techniques may be applied for malware detection in cloud.

Figure 3 Parameters affecting cloud security

Security issues faced in cloud computing

There are many issues which are faced by the user in cloud computing including their data loss, data theft and many more. The issues are basically classified into four types which are raised while discussing about security of a cloud.

1. Data Issues – When there is a data on a cloud, everyone can access the data from the cloud anytime since data is available on the common platform in a cloud. Secondly, data stealing or theft is a one of serious issue in a cloud computing in which data gets stolen by any hacker. The cloud service provider does not provide their own server therefore they acquire server from other service providers. Data loss and theft is a most common problem in cloud computing. If the cloud computing service provider shuts his services due some financial problem then the data will be lost for the end user. Sometime it may happen that data may be lost, damage or corrupted due to natural disaster or some other calamities. Due to this condition, data may be not be in the reach of users. Lastly, data location is one of the issues which require focus and to be solved in a cloud computing. Data storage is very useful and crucial. It should be seen by the user or customer. Vendor should not tell anyone where the data is stored.

2. Privacy issues- The third party involved in cloud computing should keep in mind that the customers important information such as password, username should remain fully secured from other service providers, customer and end user. As we know most of the cloud servers are public, the cloud service provider should take care of the user about who is accessing the data and passwords and also maintain it on the server or with themselves so that it will help the provider in security issues related to customer‟s personal data.

3. Infected Application- The cloud computing service providers should have the access to the servers, so that server can be accessed and maintain by them. Due to the data and application is only accessible by the service provider then there will be less chances and a barrier is created for the user to input or install any infected file or virus into the cloud.

4. Security issues- There are two sides one is the backend user side and another one is the frontend user. The Cloud computing service developers that work on the backend should be fully secured from the outside threats caused by the outer environment that may appear in the cloud. They should provide good security layer and measures to save data of customers before using the services of cloud computing. A cloud is only considered as a good and beneficial for the user when there is a good security mechanism provided by the service provider to its consumers.

There are some common most common security threats shown in the figure 4 which give rise to security issues in cloud.

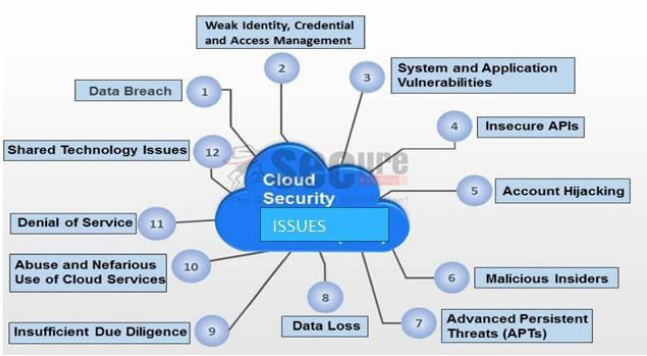

Figure 4 Cloud security issues

Data Breach: In this type of attack the information is stolen or taken without the prior knowledge to the system owner. Stolen data may contain important information, database, passwords, credit card details, customers data. The damage may include financial losses, betrayal of trust attributed to hacking and malware attacks.

Weak Identity: Hackers access cloud as users and through that they read, modify and delete data other than this they also control and manage the cloud. As a result weak identity security helps them to stole the data and they can damage the authorization and end users.

System and application vulnerabilities: Cloud computing systems contains vulnerabilities that are basically bugs in program that attackers can use to access a system in order to steal data or create disruption in service operations. It basically present in networks and third party platforms. With the multi-tenancy in cloud various organization work on the same place with shared resources resulting in the attack.

Insecure API: API can be considered as a threat to cloud security issues as the customers interact with cloud using API. They not only provide access but also affect encryption of data as all the management and monitoring of data is done through it. Therefore they should be designed in a way to protect all the attacks.

Account hijacking: Attackers have the ability to access the data or login information of an organization through which they can eavesdrop on the transactions, redirect clients and manipulate information. The most known threat in hijacking is Man In Cloud Attack which begins with the theft of user tokens which the cloud platform uses to verify devices of their employees without login into account during update and sync.

Malicious Insider: An attack which happens when a person or itself the service provider ofthe cloud misuses the data or access some confidential details of an organization. Systems that are completely depend on the service provider of cloud without any security to their account suffers this threat in common.

Advanced persistent thread: It is a form of network attack where the attacker access the network and stays in it for a long period of time through which they steal data.

Data loss: Data can be locked by the ransom ware or encrypted when the data is backed up or synced. It can be lost by some natural calamities, malicious attack or service provider can itself wipe the whole data. Amazon is the best example that suffered from this issue in 2011.

Insufficient due diligence: When an organization does not develop a good road map, not having proper goal set, resource and service provider then this may lead to a security risk for it.

Abuse and nefarious use of cloud: Cloud has provided a common platform for both large andsmall scale enterprise but hand in hand it is very easy for the hackers to spread malware and threats into it. This can be done through fraud sign up, fake id on email etc. It affects both the user and the service providers. Examples are phishing, email spam etc.

Denial of service: This attack prevent the user or service provider to access their own data orapplications. The attackers may install some software or enforce cloud to use more memory, network bandwidth which leads to system slowdown.

Shared technology issues: As we know that cloud uses the public and hybrid models in which the resources are shared between two or more organization thus the data gets stolen.

Solution to cloud security issues

There are several researcher and group that are working on cloud security issues. Some of the parameters and solutions are gathered by Cloud Security Alliance (CSA) which came into existence in 2009. It has overviewed all the threats and working on it in order to overcome those. There is a need for advanced technologies and concepts that will work on cloud to secure it. A layered framework is proposed which consists of four layers as shown in figure 5.

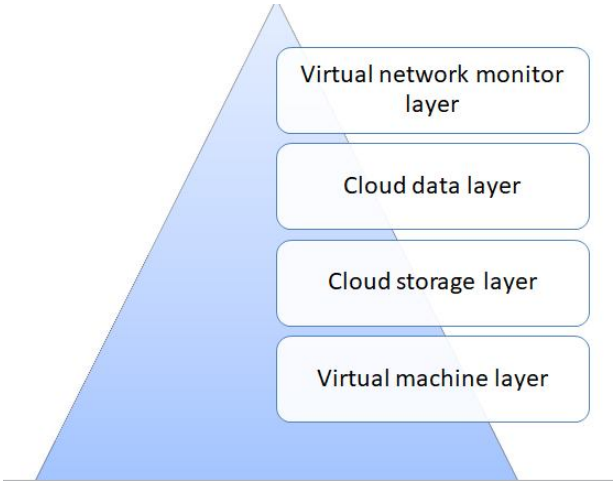

Figure 5 Layered framework for cloud security

First layer is the virtual machine layer for the user. The next one is the cloud storage layer which is responsible for the infrastructure which integrates resources from multiple cloud service provider. The cloud data layer is responsible for the data security on the cloud. The last layer is the mixture of both hardware and software in the machine which handles the problem such as key logger.

There are several groups which are working on the cloud security issues that collect and work on the information about cloud related standards and maintain the list of vulnerabilities Cloud Security Alliance (CSA) and Open Web Application Security Project (OWASP) are two of them.

Some of the tips are listed below which a user should keep in mind before working with cloud.

- Authentication of user should be done through encrypted passwords and identity should be strong that is one should not share their personal data or password with anyone.
- Data should be in encrypted form if it is personal or sensitive to the user.
- As cloud computing provide resources and information over internet. Therefore in order to secure it from attackers there should be an agreement between user and service provider. Another way is to provide authentication, accounting control so that user have to go through multiple levels to ensure authorize use of information and resources.
- Data access should be monitored that means when, by whom, from where and what data is accessed should be put into records to check the validity of the user.
- Malware injection attack solution should be done. It can be done with the help of FAT(File Allocation Table) and IDT(Interrupt Descriptor Table) . In this a number of client virtual machine is created and stored in a common place.
- The service provider should be sure about the device used by the customer or users that include computers, mobile phones, virtual terminals should be fully secured.
- The service provider should also verify the deletion and removal of data from the shared resources of devices.

IV. CONCLUSION

This paper is primarily based on focussing the security issues faced by the information owner and also demonstrates the cloud properties and characteristics. Security in cloud has been the most important parameter in determining the satisfaction of the customer therefore it tries to give a secure channel for maintaining trust between cloud provider and the customer. Cloud computing has immense and wide scope in future as it is considered as the most developing technology in the present era. Triple data encryption scheme and all the steps discussed in this paper can be considered for maintaining security of the data. Building trust between the user and service provider is the way to overcome these security issues in cloud and authentication at each step is required. There is no uncertainty that cloud computing has a bright future in IT sector.

REFERENCES

[1] ISO. ISO 7498-2:1989. Information processing systems-Open Systems Interconnection. ISO 7498-2 [2] Brodkin J, 2008, „Gartner: Seven cloud-computing security risks", Infoworld.

[2] http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing- security-risks-853?page=0,1

[3] "Advancing cloud computing: What to do now?, Priorities for Industry and Governments", World Economic Forum in partnership with Accenture – 2011.

[4] Security of Cloud Computing Providers Study Sponsored by CA Technologies Independently conducted by Ponemon Institute LLC Publication Date: April 2011

[5] National Institute of Standards and Technology, "The NIST Definition of Cloud Computing," document posted October 2009, http://csrc.nist.gov/groups/SNS/cloud-computing/.

[6] Cloud Security Alliance(CSA), "Top Threats to Cloud Computing V1.0", March 2010, http://www.cloudsecurityalliance.org/topthreats.

[7] Victor Chang, Muthu Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework", IEEE Transaction on Service Computing, vol. 9, issue. 1, pp. 138-151, ISSN: 1939- 1374, January 2016

[8] Cohen, Reuven, Rebello and Jagdish, "The State of Cloud Storage: A Benchmark Comparison of Speed, Availability and Scalability", White paper, Nausni, 2015

[9] Linlin Wu, Saurabh Kumar Garg, Steve Versteeg, and Rajkumar Buyya, "SLA-Based Resource Provisioning for Hosted Software-as-a-Service Applications in Cloud Computing Environments", IEEE Transactions on Services Computing, vol. 7, no. 3, pp. 465-485, July-September 2014

[10] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE transactions on Services Computing, 06 May 2011

[11] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, Daviv Patterson, Ariel Rabkin, Ion Stoica and Matei Zaharia. A View of Cloud Computing. Communications of the ACM, April 2010.

[12] C. Wang, K. Ren, W. Lou, and J. Li, "Towards publicly auditable secure cloud data storage services," IEEE Network Magazine, vol. 24, no. 4, pp. 19–24, 2010.

[13] Dooley B, 2010, „Architectural Requirements Of The Hybrid Cloud", Information Management Online, http:1/www. information-management. com/news/hybrid-cloudarchitectural- requirem ents-10017152- l.htmL

[14] Gruschka N, Iancmo LL, Jensen M and Schwenk J, 'On Technical Security Issues in Cloud Computing', '09 IEEE International Conference on Cloud Computing, pp 110-112, 2009.

[15] D. Wentzlaff, C. Gruenwald III, N. Beckmann, K. Modzelewski, A Belay, L. Touseff, J Miller, and A AgarwaL Fos: A Unified Operating System for Clouds and Manycore. Computer Science and Artificial Intelligence Laboratory TR, Nov. 20, 2009.