A Survey on Security Issues and Vulnerabilities on Cloud Computing

K.L.NEELA
Department of CSE, University college of Engineering, Thirukkuvalai, Tamil Nadu, India.
Email-klneelaaut@gmail.com

Dr.V.KAVITHA
Department of CSE, University College of Engineering, Nagercoil, Tamil Nadu, India
Email-**kavinayav@gmail.com**

Abstract Cloud computing has gained significant traction for recent years. It is a form of distributed computing whereby resources and application platform are shared over the internet through on demand and pay on utilization basis. Several companies have already built Internet consumer services such as search engine, use of some websites to communicate with other user in websites, E-mail services, and services to purchase items online that use cloud computing infrastructure.However this technology suffers from threats and vulnerabilities that prevent the users from trusting it. The occurrence of these threats may result into damaging of confidential data in cloud environment. This survey paper aims to analyze the various unresolved security threats in cloud computing which are affecting the various stake-holders linked to it. It also describes the pros and cons of the existing security strategy and also introduces the existing issues in cloud computing such as data integrity, data segregation, and security and so on.

Keywords:- Cloud computing, data integrity, segregation and security, PaaS, IaaS, SaaS, and Denial of service attack.

1. INTRODUCTION

Internet has been a driving force towards the various technologies that have been developed since its inception. Arguably, one of the most discussed among all of them is ***Cloud Computing*** [1].

Cloud computing is a general term for anything that involves delivering hosted services over the Internet. It is an emerging computing technology that uses the internet and central remote servers to maintain data. This system is very helpful for different users so that they can easily use the system without any external support to software and hardware. They can also access their personal files at any computer on internet. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. The overall framework of cloud computing is shown in figure 1.

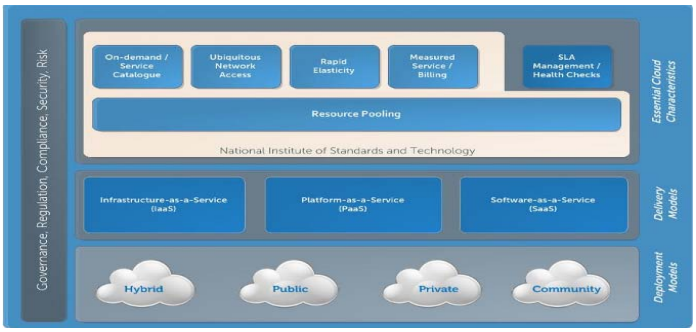

Figure 1 overall framework of cloud computing

Cloud computing is seen as a trend in the present day scenario with almost all the organizations are try to enter in to it. The advantages of using cloud computing are: i) Hardware and maintenance cost are reduced, ii) easy to access around the world, and iii) flexibility and the highly automated process wherein the customer need not worry about software up-gradation which tends to be a daily matter [2].According to the different types of services offered, cloud computing can be considered as of three layers. Infrastructure as a Service (*IaaS)* is the lowest layer that provides basic infrastructure support service. Platform as a Service (*PaaS)* layer is the middle layer that provide executive environment for developing software. Software as a Service *(SaaS)* is the topmost layer which features a complete application offered as service on demand [1]. Figure 2 explains the services models of cloud computing.

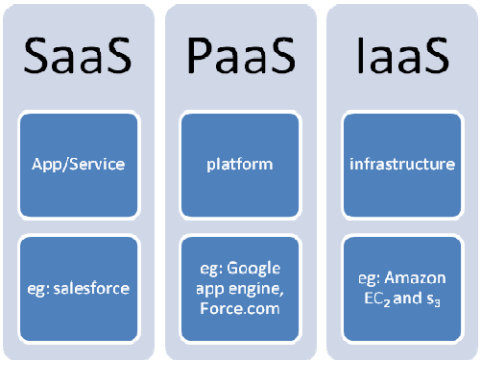

Figure 2: Cloud service models

Infrastructure as a Service (IaaS) this is the base layer of cloud service model. It can be used to deliver the computer hardware as a service. It enables the provider to offer unlimited virtual server to customer and make cost effective use of hosting hardware. Eg. Amazon, Rackspace etc.,

Platform as a Service (PaaS) this is the middle layer of cloud service model. It provides an executive environment for software development for developers over the internet. Developers write the code and the paas provider provides a way to upload the code into the internet. Eg. Google App Engine,

Software as a Service (SaaS) this is the highest layer of the cloud stack. It is designed to simply rent out the software to the user. Eg.Facebook,SalesForce etc

The using of cloud system usually depends on customer need [2].Based o that the system is divided into four ways:

a. ***Public Cloud:*** It is used if the services can be used by large group or commonality. Ex: an entire industrial sector used one provider.

b**.** ***Private Cloud****:* It is used only for one institution. It may be organized by institution itself.

c**.** ***Community cloud****:* Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider

d. **Hybrid Cloud**: It is the combination of public cloud and private cloud.

Moreover, Users can typically connect to clouds via different types of web based services or web browsers. Cloud system provides lot of pros and cons to the consumers.This paper discusses the various unresolved security concerns and the security risk associated with enterprise cloud computing including its threats, risk and vulnerability. This paper is originated as follows: section 2 deals with literature survey for existing security techniques available in cloud computing and section3 deals with security issues that exists in cloud computing and section 4 deals vulnerabilities available in cloud computing and section 5 deals with current status of security in cloud computing and section 6 deals with conclusions derived from the survey.

2. RELATED WORK

Several papers have been studied in the area of cloud computing security. Jinpeng et al [3] proposes a model to manage the virtual machine image in a cloud environment in secure manner. The advantage of this system is that the access permission is private so that untrusted parties cannot access the system. The main drawback is that the image filters cannot be accurate so that system does not eliminate the risk entirely.

Miranda, Siani [4] proposes a client based privacy manager for reducing the risk of misused the user's private data and also assist the cloud computing provider to conform the privacy law. The service provider has to provide honest cooperation with the privacy manager. Otherwise this method is not effective one.

Cong et al [10] proposes the system uses homomorphic token with distributed verification of erasure-coded data. It effectively detects an unauthorized access in cloud environment. Weichao Wang et al[11] provides efficient access to the outsourced data in the cloud environment. But this approach is not generic in nature.

Flavio, Roberto [5] proposes Transport Cloud Protection System (TCPS), is a middleware whose core is located between the kernel and virtualization layer. This system is effective in detecting most kind of attacks. But this is not generalized one and it cannot be implemented in all scenarios.

Kevin Hemalen et al [6] presents a layered framework for secure cloud. This system builds a trusted application from untrusted components. Abdul Ghafoor[12] proposes a method which is securely distributes the software modules, to authorize user. But still there is a problem of distribution of software protection key in grouped environment.

Alvin, Chaudhary [7] proposes a Security Acess Control Services (SACS) model to improve the security in cloud data. But still unknown killer application cannot be avoided. Ayesha ,Nazir [8] approach a framework for execution of data and information securely in cloud environment. Even though secure framework is used to protect the data, still cloud service providers face problems in encryption mechanism.

Shantanu et al [9] proposes a trust based agent framework which provides security both at service provider level as well as at the user level in cloud environment. But it is able to handle only a limited number of security threats in a fairly small environment.

Song et al [20] proposes data protection as services, which offer data security and privacy on cloud platform. These services can be provided using full disk encryption technique but it slow down data access time. Saravanan et al[21] propose the method to provide the security by implementing the RSA algorithm to the data stored in third party area. But still there is a lack of security exists in cloud computing.

3. SECURITY ISSUES IN CLOUD COMPUTING

Even though there is many advantage concerned in cloud computing, the organization are slow in accepting it due to security issues associated with it. Security is one of the primary issues in cloud environment. Here there are various security concerns given below which are applicable in cloud computing environment [13]:

- Virtualization
- Network Security
- Policy and Compliance
- Data location
- Data integrity

3.1 Virtualization:

Virtualization is one of the main components of a cloud. Virtual machines are dynamic in nature so that it is difficult to maintain security consistency. Vulnerabilities or configuration errors may be generated easily.The main issue in virtual machine is to keep maintaining the security state for a given time [13].

3.2 Network Security:

Networks have more security problem to deal with such as DNS attacks, Sniffer attacks, issue of reused IP address, etc

DNS attack

It is the corruption of Domain Name System (DNS) server. A DNS server performs the translation of a domain name to an IP address. In this case, the user request one IP address but it is redirected to some other unauthorized cloud. Counter measure for this attack is that Domain Name System Security Extensions (DNSSEC). But this security measures prove to be inadequate one. [13].

Sniffer attack

Sniffer attack is a more critical issue of network security in which unencrypted data are hacked through the internet during the communication between two parties. Figure3 represents the attacker . Counter measure for this attack is that the parties should use efficient encryption method for securing the data.

Figure: 3 showing the attacker

I*ssue of Reused IP Addresses*

Each node of a network is provided with an IP address and the number of IP addresses that can be assigned is limited. When a User leaves the network hen the IP-address assigned to him will be given to a new user. But it causes lot of security issues to the new user if any time lag occurs between the variation of IP address in DNS and deleting of address in DNS Caches. [13]

3.3 Policy and Compliance

Cloud providers have to ensure that the customer's data won't be breach any regulations even when they left the organization.

3.4 Data location

Clients might never know where the data is located [14].

3.5 Data Integrity

Data Integrity is essential in cloud storage which is critical for any data center. Keeping data in the clouds means users may lose control of their data and rely on cloud operators to enforce access control.

4. VULNERABILITIES OF CLOUD COMPUTING

"Vulnerability" refers to the unauthorized access to the resources within the cloud environment. It may be a service running on a server, unmatched applications or operating system software, or an unsecured physical entrance. There are several significant vulnerabilities that should be considered when an organization is ready to move their critical applications and data to a cloud computing environment, these vulnerabilities are described as follows [15]:

4.1 Session Hijacking

Session hijacking occurs when the attacker steals the user's session id to gain unauthorized access for the information or services residing on a computer system. The diagrammatic representation of session hijacking is shown in figure 4. This can be prevented by using Secure Socket Layer (SSL) connection because SSL creates an encrypted connection between client and server, in order to avoid this attack. But SSL does not fully secure against this attack.

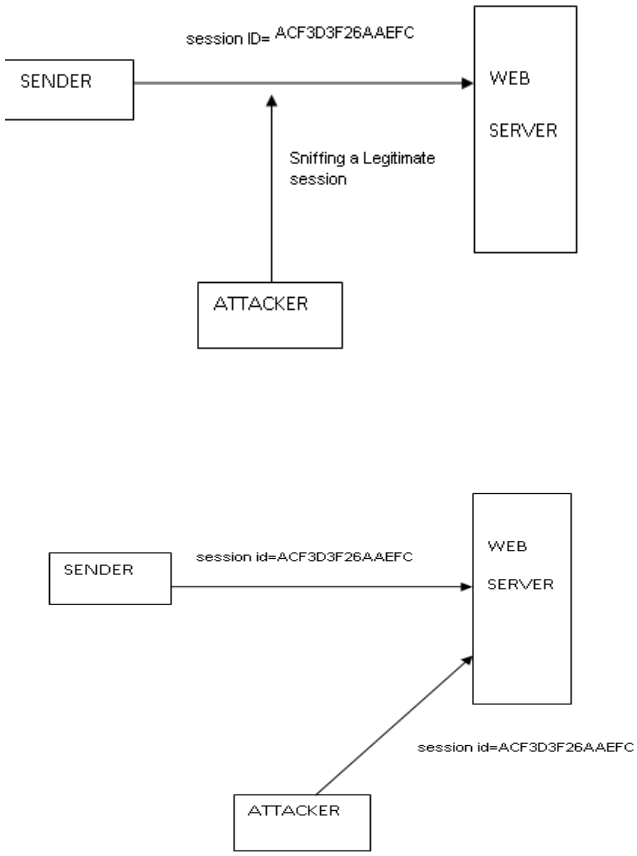

Figure 4: Diagrammatic representation of Session hijacking attack

4.2 Virtual Machine Escape

*V*irtual Machine (VM) escape is an exploit in which the attacker runs code on a VM to gain access on the host operating systems. It is considered to be the most serious threat to virtual machine security.

4.3 Insecure Cryptographic storage

Insecure cryptographic storage means sensitive data such as username, password etc aren't stored securely i.e malicious users can access the insecurely stored data with a little effort. This vulnerability can be prevented by using strong encryption algorithm.

4.4 Vendor Lock-in

Vendor lock-in is seen as one of the potential drawbacks of cloud computing. Lock-in, makes a client dependent on a provider for products and services so they will be unable to deal with another provider without substantial switching costs [17]. Clients must be sure of their potential provider prior to provider selection process. Lack of standards may also lock-in the clients with only one provider. Due to heterogeneous standards and policies settled by each provider, clients are not able to easily migrate from one provider to another even though they want to do so.

4.5 SQL injection

This technique used to exploit web sites by altering backend SQL statements through manipulating application input [16]. SQL Injection happens when a developer accepts user input that is directly placed into a SQL Statement and doesn't properly filter out dangerous characters. The attacker steals the data from database and modifies it.

4.6 Denial of Service Attacks

Denial of service means making the resources unavailable for the users. Usually this type of attack temporarily or infinitely stops a service of the host. This will be shown in figure5.In the cloud system the hacker attack on the server by simply sending thousands of requests to the server that server is unable to respond to the regular clients in this way server will not work properly.

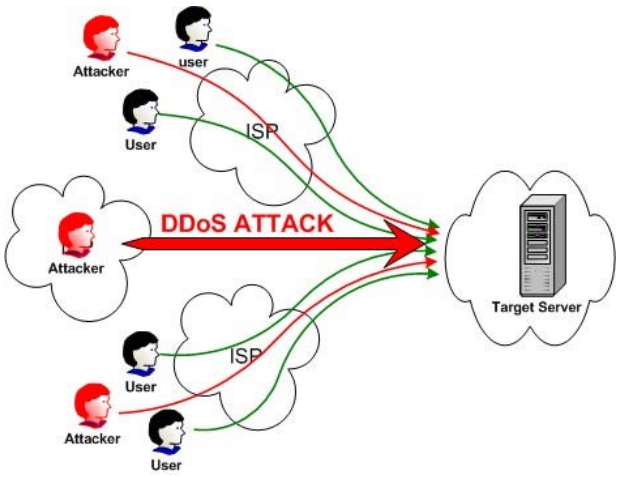

Figure 5.DoS attack

5. CURRENT STATUS OF CLOUD SECURITY

In order to secure cloud against various security threats, different cloud service providers adopt different techniques. The best solution to improve the security is that to develop the secured framework which has tough security architecture. So that we will protect user's data, message and information against various attack. The secured framework must use strong authentication and strong access control mechanisms .So that it will provide more security to data of customers from that are currently present within the cloud computing services. The secured framework must use strong encryption algorithm in order to protect the sensitive data before entering in to the cloud. There are several encryption techniques are available in cryptography. Among all Gentry [18] describes homomorphic encryption algorithm which is used to protect the data in cloud environment. One of the most used encryption techniques is Homomorphic encryption technique, which allows specific types of computations to be carried out on cipher text and obtain an encrypted result which decrypted matches the result of operations performed on plain text. MahaTEBAA[19] describes homomorphic encryption which is a new concept of security which enables providing results of calculations on encrypted data without knowing the raw data on which the calculation carried out, based on the data confidentiality. The secured framework can implement homomorphic encryption technique in order to provide data confidentiality on cloud environment.

6. CONCULSION

Cloud computing offers great potential to improve productivity and reduces costs. It also poses many new security risks. This paper describes the survey of the various unresolved security threats in cloud computing which are affecting the various stake-holders linked to it**.** More than ten papers were also surveyed regarding the cloud computing, merits of cloud computing, risks in cloud computing and various approaches to solve those risks each with their pros and cons. We believe that due to the complexity of cloud system , it is very difficult to achieve security.New security techniques need to be developed and older security techniques needed to be radically twisted to be able to work with the clouds architecture.

REFERENCES

[1] Rohit Bhaduria,Sugata Sugal, "Survey on Security Issues in Cloud Computing andAssociated Mitigation Techniques" ,*International Journal of computer applications*, Vol: 47,No:18,June 2012, pp:47-66.

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

[3] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons,Vasanth Bala,peng Ning."Managing Security of virtual machine images in a cloud environment ".CCSW'09:Proceedings of the 2009 ACM workshop *on Cloud computing security*, November 2009, pp 91-96.

[4] Miranda Mowbray, Siani Pearson "A Client –based privacy Manager for Cloud Computing"**.** *OMSWARE '09: Proceedings of the Fourth International ICST Conference on communication system software and middle ware*, June 2009.

[5] Flavio Lombardi, Roberto Di Pietro. "Transparent Security for Cloud". *SAC '10: Proceedings of the 2010 ACM Symposium on Applied Computing*, March 2010, pp 414-415.

[6] Kevin Hemalen, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham, The University of Texas at Dallas, USA, "Security Issues for cloud computing", April-June 2010,international Journal of Information Security and Privacy.

[7] F. A. Alvi, B.S Chaudhary," review on cloud computing security issues &challenges".

[8] Ayesha Malik, Muhammed Mohsin Nazir,"Security Framework for Cloud computing environment: Review', *Journal of emerging Trends in computing and information sciences*", Vol;3, No:3, March 2012, ISSN 2079-8407.

[9] Shantanu Pal, Sunirmal Khatua, Nabendu Chaki, Sugata Sanyal, "A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security", Annals of Faculty Engineering Hunedoara International Journal of Engineering (Archived copy), scheduled for publication in vol. 10, issue 1, January 2012. ISSN: 1584-2665.

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

[11] Weichao Wang, Zhiwei Li, Rodney Owens, Bharat Bhargava. "Secure and Efficient Access to Outsourced Data." *CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security*, November 2009, pp: 55-65.

[12] Abdul Ghafoor, Sead Muftic, "Crypto NET: Software Protection and Secure Execution Environment", *IJCSNS International Journal of Computer Science and Network Security*, VOL.10 No.2, February 2010

[13] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy "Cloud Computing: Security Issues and Research Challenges", *International Journal of Computer Science and Information Technology & Security (IJCSITS)*, Vol. 1, No. 2, December 2011

[14] Garter, "Seven Cloud computing security risks", 2008[Online] Available http://www.infoworld.com

[15] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," Security & Privacy, IEEE, vol. 9, no. 2, pp. 50-57, 2011

[16] Mervat Adib Bamiah, sarfraz Nawaz Brohi, " Seven Deadly Threats and Vulnerabilities in Cloud Computing" *International Journal Of Advanced Engineering Sciences And Technologies*, Vol No. 9, Issue No. 1, pp:087 – 090

[17] G., Petri, "Vendor Lock-in and Cloud computing", [Online], Available: http://cloud computing.sys-con.com/node/1465147, 2010, [Accessed: 23-Jul-2011].

[18] C. Gentry. A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009. Manuscript available at http://crypto.stanford.edu/craig

[19] Maha Tebaa, Saïd El Hajji, Abdellatif El Ghazi, "Homomorphic Encryption Applied to the Cloud Computing Security", Proceedings of the World Congress on Engineering 2012 Vol I WCE 2012, July 4 - 6, 2012, London, U.K.

[20] Song.D.,Shi.E,Fischer.I,Shankar.U," Cloud Data protection for the masses", IEEE computer Society,Vol: 45,issue:1,pg: 39-45,ISSN:0018-9162

[21] N. Saravanan, A. Mahendiran, N. Venkata Subramanian and N. Sairam," An Implementation of RSA Algorithm in Google Cloud using Cloud SQL" **,** *Research Journal of Applied Sciences, Engineering and Technology*, 4(19), October 01, 2012, ISSN: 2040-7467

AUTHOR'S PROFILE

Ms.Neela.K.L. received her B.E. degree in Computer Science and Engineering in 2006 from Oxford Engineering college,Trichy and Master's degree in Computer Science and Engineering in 2008 from J.J.college of Engineering and Technology, Trichy. She is working as Asst.Professor in University College of Engineering, Thirukkuvalai, TamilNadu, India. Her field of interest is Network security and cloud computing.

Dr.V.Kavitha obtained her B.E degree in Computer Science and Engineering in 1996 from Norrul Islam College of Engineering and ME degree in Computer Science and Engineering in 2000 from Mepco Schlenk Engineering College. She received PhD degree in Computer Science and Engineering from Anna University Chennai in the year 2009. Right from 1996, she is in the Department of Computer Science & Engineering under various designations. Presently she is working as Associate Prof in the Department of CSE at Anna University Tirunelveli. In addition she is the Director In-Charge of University College of Engineering. Nagercoil. Currently, under her guidance twelve research scholars are pursuing PhD as full time and part time. Her research interests are Wireless networks, Mobile Computing, Network Security, Wireless Sensor Networks, Image Processing; Cloud Computing .She has published 5 National journal and 30 International journals in areas such as Network security, Mobile Computing, wireless network security, and Cloud Computing.