Review of Security Methods in Cloud Computing

AZAZ KHAN & NASIB SINGH GILL
Department of Computer Science & Applications, Maharshi Dayanand University,
Rohtak, Haryana, India.

Received: May 16, 2018 Accepted: June 30, 2018

ABSTRACT *In modern computing, Cloud computing is an important part of any small or large organization. Today cloud computing can be considered as a service, similar to the way that electricity is considered a service in urban areas. A cloud user can utilize different computing resources (e.g. network, storage, software application), whenever required, without being concerned with the complex underlying technology and infrastructure architecture. The most important feature is that the computing resources are available whenever they are needed. Additionally, users pay only for the resource they actually use. As a result, cloud users can easily scale their information technology infrastructure, based on their business policy and requirements. However, there is often a lack of security when realizing such cloud-based solutions. In the longer term, the problems caused by this lack of security might inhibit companies from taking advantage of cloud-based solutions. This paper provides literature review on various methods for implementing security in cloud environment.*

Keywords: *Cloud Computing, Cloud computing Services, Malware Attack*

I. INTRODUCTION

Cloud computing, often referred as just the *Cloud*, is a new buzzword in the IT world. However, the concept of cloud computing is not very new, as the concept dates back to the1950s. At that time academia, as well as industry, used terminals to connect to (often remote) mainframe computers. These terminals initially had no computing capabilities. The idea was to share resources (e.g. CPU time) of these costly mainframe computers among multiple users, and thus to make the use of a mainframe computer more cost effective.

Cloud computing [1] can be considered as a service provided by a service provider. The user of this service does not need to know or worry about how the service (e.g. network, storage, application) is provided or maintained. Instead, the user is only concerned that the service is available whenever the user needs this service. The cloud computing approach relieves companies from needing to have their own datacenters. It avoids purchase, management, and updating costs for hardware, cooling systems, storage, and power supplies. As a result, the use of the cloud computing enables companies to quickly startup a new business and to scale their business efficiently.

Figure 1 shows that cloud services (e.g. network, storage, application) reside inside a cloud network. Cloud users can access the various different cloud services from heterogeneous client platforms (e.g. smart phones, laptops, other computers in the same or another cloud, etc.), without knowing the exact location of the services. Additionally, the cloud service user need not know the processes to develop, manage, or maintain the services.

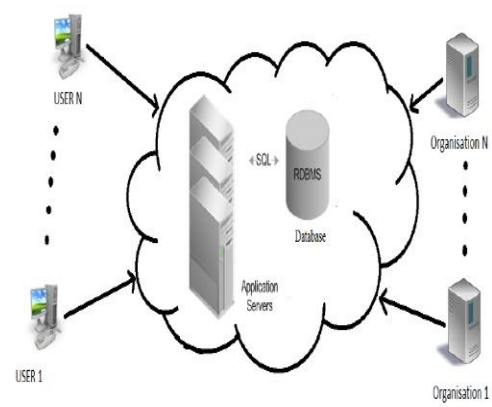

Figure 1: Cloud Computing [11]

One of the inherit problem with cloud environment is lack of security therefore companies or organizations cannot fully utilize the functionalities of cloud computing. This paper provides literature review on various methods for implementing security in cloud environment.

II. CLOUD COMPUTING SERVICES

The three building blocks of cloud computing, as defined by NIST [2], are:

1. Software as a Service (Saas)
2. Platform as a Service (Paas)
3. Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS)

IaaS provides users with a wider variety of features than SaaS or PaaS. In IaaS a cloud service provider provides the user with storage, network connectivity, and other necessary computing resources. The user then uses these resources to

set up a complete environment with their own choice of operating systems and applications according to their own needs. In IaaS the user has control over the operating system, storage, and deployed applications. However, the users do not manage or control the underlying cloud infrastructure.

Platform as a Service (PaaS)

In the Platform as a Service (PaaS) model, the CSP offers a development platform on top of the services delivered with IaaS. The CSP offers a development platform, on which applications can be built. In other words, software developers can develop their application through virtual development platform, accessible via a Web browser, without the need to install the software building tools on their own computer. This helps the developers to later distribute or deploy their apps to the cloud easily. In order to avoid confusion of this service with SaaS, it is good to imagine it as a cloud OS. The providers of the service enable its users to install their applications on a platform, which can provide any operating system or even emulate various types of hardware.

Software as a Service (SaaS)

SaaS is a very popular service in which cloud service providers deliver software applications over the Web. A SaaS provider deploys their software, which is hosted on their own server infrastructure or use another vendor's hardware, on user's demand. This operation is usually done using a licensing model where applications may be licensed directly to an organization, group of users or, a user or, or through a third party that manages multiple licenses between user organizations, such as an ASP. The user then can be able to access the applications through any well-defined and Internet device, which is most probably a Web browser.

These building blocks are also referred as cloud service models [1]. Figure 2 shows each of these alternative cloud service models.

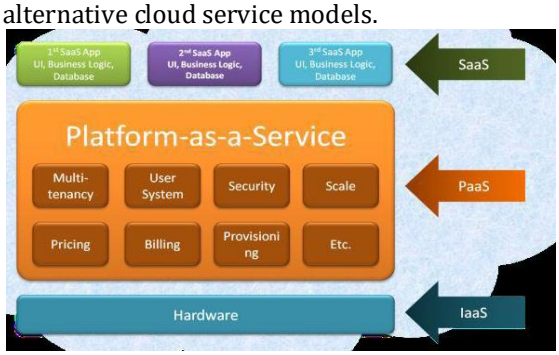

Figure 2: Cloud Service Models [14]

III. LITERATURE REVIEW

Various types of cloud security techniques are available. In this section, we provide the literature review of work done in this field.

In 2010 S Subashini and V Kavitha [4] proposes a security framework by different methods provided dynamically, that one of the components of this framework refers to provide data security by storage and access to data based on meta-data, which is similar to storing related data in different areas based on meta data, and if the destruction of user data takes place, it can be retrieved. Each part of the framework in "security as a service" is provided for practical applications by providers of security as a layer or multiple layers of required applications.

In 2011 V. Krishna Reddy and Dr. L.S.S. Reddy [5] proposed the security problems at different levels of the architecture of cloud computing services have been studied. Security of customer-related data is a substantial need for services which is provided by each model of cloud computing. They have studied matters of on-going security software as a service (SaaS), platform as a service (PaaS) and Infrastructure as a Service (IaaS).This paper focuses on the use of cloud services and security for working cross-domain Internet connected.

In 2011 Syam Kumar P and Subramanian R [6] propose an effective and safe protocol by use ECC and Sobol sequence. This protocol provides integrity and confidentiality of data. Moreover, their system also supports dynamic data operations, which performed by the user on data stored in cloud while maintaining same security assurance.

In 2012 Punyada M. Deshmukh et. al. [7] wrote a paper. In this paper they have proposed a system which ensures the data storage security using a distributed scheme. A set of Master servers are used which are responsible for processing the users requests. File chunking operation is performed in order to store replicas of file at Slave server providing backup for file recovery. Unlike the previously proposed systems, efficient and dynamic data operations are performed by users. This efficiency is achieved by imparting the data blocks for different users. The functionality is extended to the Android users and the chatting application is included to add ease and comfort to the working environment of users.

In 2013 Sajjad Hashemi [8] wrote a paper. In this paper he attempted to review and highlight security challenges, particularly the security of data storage in a cloud environment. Also, provides some offers to enhance the security of

data storage in the cloud computing systems that by using these opinions can be overcome somewhat on the problems.

In 2014 Sudhansu Ranjan Lenka et. al. [9] wrote a paper. In this model they have implemented a combination of RSA encryption and digital signature technique which can easily with all types of cloud computing features like: PaaS, SaaS and IaaS. This combination mechanism provides three way security i.e. data security, authentication and verification. In this paper, they have proposed RSA encryption algorithm for confidentiality of data and for authentication MD 5 algorithm have been implemented.

In 2014 Swarnalata Bollavarapu and Bharat Gupta [10] propose data storage security system in cloud computing. This system use algorithms like RSA, ECC and RC4 for encryption and decryption techniques.

In 2015 Karun Handa et. al. [11] described that Cloud Computing is a technology that readily makes available resources that otherwise may require huge amount of investment. Besides, it increases the availability of resources since anyone can access the data using web. But this advantage comes at a cost. Firstly, the data is uploaded unsecurely which has a high risk of being hacked by some malicious people. Secondly, the data saved at remote servers is under the surveillance of unknown people who can do anything with our data. So, these data security risks are causing a hindrance in the development of the field of cloud computing. Thus, this paper has designed a scheme that can help, solve this issue.

In 2016 AL-Museelem Waleed, Li Chunlin [12] assesses how security and privacy issues transpire in the context of cloud computing and examines ways in which they might be addressed. This paper aims to solve privacy and security issues in cloud computing using UEC (Ubuntu Enterprise Cloud). The methodology used involves encrypting and decrypting data to ensure privacy and security in the cloud**.**

In 2016 Nidal Hassan Hussein et. al. [13] wrote a paper. In this paper a comprehensive survey of existing literature for cloud computing security challenges and solutions is presented. At the end of this paper the authors propose a model for cloud computing security.

In 2017 Ashok Deokar [14] described that Cloud computing is an Internet-based computing, where shared resources, software and information, are provided to computers and devices on-demand. It provides people the way to share distributed resources and services that belong to different organization. Since cloud computing uses distributed resources in open environment, thus it is important to provide the security and trust to share the data for developing cloud computing applications. In this paper we have shown Successful implementation of cloud computing in an Organization, enterprise requires proper planning and understanding of emerging risks, fear and possible countermeasures. This paper show how we secure the cloud security, privacy and reliability when a third party is processing sensitive data.

Sokratis K. Katsikas et. al. [15] described that the initial reaction of the security community to the security issues of cloud computing was that these could be resolved using existing techniques inherited from conventional IT systems or even distributed systems that are the ancestors of cloud computing environments. Unfortunately, this approach does not work, because of the scale and the architecture of the cloud computing model. Hence, a need to re-consider security, privacy and trust concerns in the context of the cloud computing paradigm arises.

IV. CLOUD COMPUTER SECURITY

Cloud computing is a growing area of concern in the IT security community because cloud architectures are literally popping up all over. Public clouds are available from Google, Amazon, Microsoft, Oracle, Eucalyptus, and many other vendors. The basic concerned with cloud computing is about security. While there is no “ultimate security” solution, security experts will try to minimize the potential for security threats as much as possible. Although they have tried to minimize security risk as much as possible, cloud computing still possesses many security risks. Some of these security risks are well known and some of them are new.

Confidentiality, integrity, and availability (CIA) are the three key aspects of security. Ensuring confidentiality means that no one can read our data unless we want them to read it, integrity ensures that no one can modify our data without the modifications being detected, and availability means that we can access our data at any time. Cloud computing also needs to deal with security risk/threats just as any other service. These attacks can subvert one or more of the three key aspects of security [1].

A. Confidentiality related attacks

The first category of attacks that we will consider is attacks on confidentiality. Loss of confidentiality for a web-based service can destroy the trust which customers place in the company and could lead to financial losses for both the company and the customers. For these and other reasons, it is

essential that the system preserve confidentiality. In the case of a cloud-based service, the attacks we consider are malware injection and data stealing.

A1. Malware Injection Attack

The use of a malware injection attack method is spreading very rapidly and many websites have been affected. The objective of the attack can be to spread malware to anyone who utilizes the web server or to place malware into the web server in a direct attack on the service.

Examples of malware injection attacks

Normally a malware injection attack is done via a compromised FTP server. A virus attempts to sniff FTP passwords and sends these passwords (and the user name) back to the attacker. The attacker then uses this FTP user name and password to access the website in order to add malicious coding to the site's web page. These web pages are used to infect visitors who browse to this website.

In a cloud-based system, a web client's request is executed based on authentication and authorization. During this authorization and authentication process a large amount of metadata is exchanged between the web server and web browser. An attacker can take advantage of this metadata. In another form of malware injection attack, an adversary attempts to inject malicious service or code. In this case, the injected malicious service or code appears as a valid instance of services running in the cloud. If the attacker is successful, then the cloud service will be vulnerable to eavesdropping and deadlocks, the later forces a legitimate user to wait until the completion of a job, which was not generated by the user. This type of attack is also known as a meta-data spoofing attack.

A2. Data Stealing

Data stealing is one of the most common approaches to breach a user account. Often the user account and password are stolen. As a result, stealing and destroying of confidential data can hamper the storage integrity and security of the cloud. The providers face the first strike of such kind of problem. To protect against data stealing the customer will receive an e-mail about the resource usage and duration of the session at the end of each session. A special number (which acts as a numeric challenge) is sent in the same email. This number is used during the next login. By doing this, the customer will be aware of their usage & charges and due to the need to input anew numeric challenge every time they access the system it will be possible to detect if someone else has used the account in the meantime.

B. **Integrity related attacks**

We will only consider one type of integrity related attack: a XML signature wrapping attack (also known as a XML rewriting attack). Wrapping attacks aim to inject a fake element into a message structure so that the message seems to have a valid signature, as a result the malicious element will processed by the application logic. Using this method an attacker can make an arbitrary web service request while the request is authenticated as coming from a legitimate user.

Because he customer will be charged based on their usage of resources, one attack is to simply use lots of resources (for example to store and distribute malicious content or use lots of cycles running malicious code) as if you were the legitimate user and generate a high bill for the customer. Since the customer will not be aware of such an attack until the provider charges the customer, the customer can be left with a very large bill. This can lead to various problems since the provider believes that the customer used these resources, while the customer believes that the provider is charging them for resources that they did not use.

Several methods can be used to protect against an accountability problem. One approach is for the provider to: (1) check the identity of the user before launching any instance of a customer's VM, (2) securely record resource usage records, (3) perform auditing of all such records, and (4) collect sufficient evidence concerning the usage in order to resolve potential future accounting disputes.

V. CONCLUSION

Cloud refers to any form of Network which is present at remote and distance location. Almost all types of applications such as Email, Video Conferencing, game etc. execute in the cloud. Cloud Computing provides us facility to access any kind of information at any time. The cloud computing provides different services to their clients called front end and the cloud itself refer as back end that provides such services to the clients. One of the main challenges related to cloud computing called data security of multiple clients. This paper provided literature review of different security aspects of cloud data storage.

REFERENCES

1. Jaspreet Singh, Sugandha Sharma, "Review on Cloud Computing Security Issues and Encryption Techniques", International Journal of Engineering Development and Research, IJEDR, Volume 3, Issue 2, 2015.

2. P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," *NIST special publication*, vol. 800, no. 145, p. 7, 2011.
3. G. Anthes, "Security in the cloud," *Communications of the ACM*, vol. 53, no. 11, p. 16, Nov. 2010.
4. S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Network and Computer Applications, Elsevier, Vol. 34, pp. 1-11, 2010.
5. V. Krishna Reddy, Dr. L.S.S. Reddy, "Security Architecture of Cloud Computing", International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.
6. Syam Kumar P and Subramanian R, "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.
7. Punyada M. Deshmukh, Achyut S. Gughane, Priyanka L. Hasija, Supriya P. Katpale, "Maintaining File Storage Security in Cloud Computing", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 10, October 2012.
8. Sajjad Hashemi, "Data Storage Security Challenges in Cloud Computing", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol 2, No 4, August 2013.
9. Sudhansu Ranjan Lenka, Biswaranjan Nayak, "Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, June-2014.
10. Swarnalata Bollavarapu and Bharat Gupta, "Data Security in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014.
11. Karun Handa, Uma Singh, "Data Security in Cloud Computing using Encryption and Steganography", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 4, Issue. 5, May 2015, pg.786 – 791.
12. AL-Museelem Waleed, Li Chunlin, "User Privacy and Security in Cloud Computing", International Journal of Security and Its Applications Vol. 10, No. 2 (2016), pp.341-352.
13. Nidal Hassan Hussein, Ahmed Khalid, "A survey of Cloud Computing Security challenges and solutions", International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 1, January 2016.
14. Ashok Deokar, "Cloud Computing Security Issues, Challenges and Solution", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 2, February 2017.
15. Sokratis K. Katsikas & Costas Lambrinoudakis, "Security and Privacy in Cloud Computing", Special Session along with CLOUD COMPUTING 2017, February 19-23, 2017 - Athens, Greece The Eighth International Conference on Cloud Computing, GRIDs, and Virtualization.
16. [16] Pankaj Arora, Rubal Chaudhry Wadhawan, Er. Satinder Pal Ahuja, "Cloud Computing Security Issues in Infrastructure as a Service", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012.