ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

A Study on Reactive Security in Cloud Computing

Manisha Yadav, SumanAggarwal

M.Tech Student, Dept. of CSE, AITM, Palwal, MD University, Haryana, India

Assistant Professor, Dept. of CSE, AITM, Palwal, MD University, Haryana, India

ABSTRACT : The cloud is a next generation platform that provides dynamic resource pools, virtualization, and high availability. Today, cloud computing have the ability to utilize scalable, distributed computing environments within the confines of the Internet. This paper represent clear description of with different characteristics of cloud computing. Customers are also very concerned about the risks of Cloud. They always worry about "S" word: Security. Cloud computing security is a sub domain of computer, network and information security in a broader aspect. The purpose of this document is to describe different security threats and their countermeasures and investigate its role in cyber world whereas two trusted resources and working in same cloud to ensure secure communication under the reactive security.

KEYWORDS: Security,Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as aService (IaaS), Security, Trusted Cloud Computing, Cryptography, Digital Signatures, Third Party Auditor.

I.INTRODUCTION

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc.

II.ARCHITECTURE

Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services.[9] The architecture of Cloud computing can be categorized according to the three types of delivery models, namely Infrastructure as a service (IaaS), Software as a service (SaaS) and Platform as a service (PaaS).

2.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service is a single tenant cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee. This greatly minimizes the need for huge initial investment in computing hardware such as servers, networking devices and processing power.

2.2 Software as a Service (SaaS)

Software as a service is where computer applications are accessed over the Internet rather than being installed on a local computing device or in a local data centre. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support Web services and service-oriented architecture (SOA) mature and new developmental approaches, such as Ajax, become popular. The availability of IaaS services is a key enabler of the SaaS model [8]. Information security officers will need to consider various methods of securing SaaS applications. Web

Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) and available options which are used in enforcing data protection transmitted over the Internet.

2.3 Platform as a Service (PaaS)

Platform as a service cloud layer works like IaaS but it provides an additional level of "rented" functionality. Clients using PaaS services transfer even more costs from capital investment to operational expenses but must acknowledge the additional constraints and possibly some degree of lock-in posed by the additional functionality layers [8]. Platform as a Service (PaaS) is an outgrowth of Software as a Service (SaaS), a software distribution model in which hosted software applications are made available to customers over the Internet**.**

III. LITERATURE REVIEW

Consider all of the risks, threats, and vulnerabilities from a technical perspective, he could probably add approximately 500 different items. The respondent also stated that some threats are common to all public and online services, such as distributed denial of service (DDoS) attacks and thus, they are not specific only to the cloud. Hence, some of the identified threats are not specific to cloud computing. In addition, he believes that a more generic term needs to be used for DDoS in a cloud environment, which is 'service discontinuity' because this term will have much more vulnerabilities than DoS. According to him, "For example, there are more than ten types of DDoS attacks and you do not want to go deep into that and your job is to make sure the continuity of the connection", which is defining threat from a business perspective. Illustrating the case of a SQL injection attack, he said that he "may not have a SQL server on the cloud or the database at all, on that particular service that I am having on the cloud." Moreover, DDoS attacks are common to all public and online services, and thus, they are not specific to the cloud only. Therefore, the types of threats in cloud computing need to be redefined because the above 41 threats are not the concern of the company, but to the cloud service provider.

3.1 Denial of service attack

The aim of a denial of service attack is to deny legitimate users access to a particular resource[12]. When the high workload on the flooded services notifies by Cloud Computing operating system then it will start providing more computational power to cope with the additional workload. Thus, the server hardware boundaries for maximum workload to process do no longer hold. In that sense, the Cloud system is trying to work against the attacker (by providing more computational power),but in some extent this will help r by enabling him to do most possible damage on a service's availability, starting from a single flooding attack entry point. Thus, the attacker does not have to flood all n servers that provide a certain service in target, but merely can flood a single, Cloud based address in order to perform a full loss of availability on the intended service.[10]

3.2 Man-in-the-middle attack

The **man-in-the-middle attack** (often abbreviated **MITM).** As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. It is also defined asactive eavesdropping where attacker makes independent connections between users and relays messages between them. Man-in-the-Middle attacks are often referred to as "session hijacking attacks", in which the intruder aims to gain access to a legitimate user's session.

3.3 Network Sniffing

A *sniffer* is an application or device that can read, monitor, and capture network data exchanges and read network packets[11]. Data packets are transmitted from one network device to another which causes the risk that outsider could see our data. Sniffing is used to see what type of traffic is being passed on a network and to look for things like passwords, credit card numbers, and so forth.

3.4 Port Scanning

Port scanning can be defined as "hostile Internet searches for open 'doors,' or ports, through which intruders gain access to computers"[1]. The basic step is simply sends out a request to connect the target host on each port sequentially. It is the technique used to identify open ports and services available on a network host but it also used by hackers to target victims. If repetitive port scans are made, a denial of service can be created. Hackers typically utilize port scanning because they can easily identify services which can be broken. They conduct tests for open ports on Personal Computers that are connected to the web.

3.5 SQL Injection Attack

There is a big influence of web application on our life. Several business houses and governments and society in general depend on this. All these web applications are accessed via internet therefore security risks associated with it. Usually RDBMS (Relational Database Management Systems) is used for database by web applications [11]. They provide interface to the user to input the information in the form of SQL statements which are executed on the RDBMS. By using SQLinjection, malicious user canalter the protected data, leak the sensitive information or crash the entire system.

3.6 XML Signature Element Wrapping

In cloud computing, clients are connected via a web browser or web service which increases the probability of web services attacks in cloud computing. XML signature element wrapping is common attack for Web service. XML sign are designed to facilitate integrity protection and origin authentication for a variety of documents types. It is use to defend a component name, attribute and value from illegal party but unable to protect the position in the documents. (Jamil&Zaki, 2011b)[16]. An attacker is able to manipulate a SOAP message by copying the target element and inserting whatever value the attacker would like and moving the original element to somewhere else on the SOAP message. Suppose we use a signature to secure the transmit data then outsider can't be able to change that data. But this attack allows a malicious user to change the signed information what is being sent.combination of WS-security with XML signature to a particular component.

3.7 Browser Security

In a cloud computing system, the computational processes are completed in the cloud server whereas the client side just send a request and wait for the result. Web browser is a common method to connect to the cloud systems. Before a client can request for services on the cloud system, the client is required to authenticate himself whether he has an authority to use the cloud system or not. . As a client sent the request to the server by web browser the web browser have to make use of SSL to encrypt the credentials to authenticate the user [16]. But SSL support point to point communication means the attacker may get the credentials of the user and use in these credentials in the cloud system as a valid user by installing sniffing packages on intermediary host.

3.8 Flooding Attacks

The most significant feature of the cloud system is to provide dynamically scalable resources. Once there are more requests from clients, cloud system repeatedly increase its size. Flooding attack is basically distributing a large amount of non-sense requests to a certain service[16]. Once the attacker throws a batch of unused requests by providing more recourses cloud system will attempt to work against the requests, ultimately system all recourses are consumed by the system and it is notable to serve normal user requests. These attacks charges extra cost to the consumer for the usage of resources.

3.9 Cloud Malware Injection Attack

Cloud malware injection attack is to make attempt to inject a malicious service, application or even virtualmachine into the cloud system depending on the cloud service models (SaaS, PaaS and IssA) In order toperform this attack , the first step of intruder is to generate his personal vindictive application[3]. Once the vindictive software is entered into the cloudstructure the attacker had to trick the cloud system to treat the malicious software as a valid instance. If successful user ask for the vindictive service then malicious is implemented. Attacker can also upload virus program in to the cloud system. Once the cloud system treats it as a valid service, the virus program is automatically executed andthe cloud system infects the virus which can cause damage to the cloud system[10].

3.10 Incomplete Data Deletion

In cloud computing, replica's of data is placed in over different server because of this data does not remove completely. This is known as Incomplete Data Deletion [16]. When a request to delete a cloud resource is made, most operating systems this will not remove accurately Accurate data deletion is not possible because copies of dataare stored on another sever but are not available.

Table 1: Different security threats and their countermeasures

Denial of Service:	***Reduction of the privileges of the user that connected to a server.***
Man in the Middle Attack	Proper installation of SSL
Network Sniffing:	Use of encryption methods for securing the data.
Port Scanning:	Use of firewall to secure the data from port attacks.
SQL Injection Attack:	Web applications should not use one connection for all transactions to the database
Flooding Attacks	Intrusion detection system will filter the malicious requests and installing firewall.
XML Signature Element Wrapping:	Careful security policy specification and correct implementation by signed message providers and consumers.
Browser Security:	Use of WS-security concept on web browsers by vendors.

IV.RESULTS

Proposed Liner Hash based Algorithm for Passive Security Measures

	Sender		**Receiver**
Sender and Receiver publically share a generator and prime modulus.	$g = 3$, $p = 17$	Common info	$g = 3$, $p =17$
Each then secretly picks a number n of their own.	$n = 8$	secret number	$n = 6$
Each calculates g^n mod p	3^8 mod 17 = 16 $A = 16$		3^6 mod 17 = 15 $B = 15$
They then exchange these resulting values.	$B = 15$		$A = 16$
Each then raises the value they received to the power of their secret n mod p.	B^n mod p = 15^8 mod 17 = 1	mix in secret number	A^n mod p = 16^6 mod 17 = 1
The result is the shared secret key.	1	shared secret key	1

V. CONCLUSION

In the above scheme the users inside the cloud which hold the trust relationship as trusted or trustee resource will share the information under the secured umbrella of cloud security but also ensure that, the communication inside the cloud between two or more resources are secured using above mentioned algorithm thus, provide both proactive and reactive securities to the resources for better counterparts on security and such mal-intentions.

REFERENCES

[1] Abbadi, I.M. and Martin, A. (2011), Trust in the Cloud. Information Security Technical Report, 16,108-114. doi:10.1016/j.istr.2011.08.006

[2] Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated with Cloud Computing.International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS),257-259.

[3] Arshad, J, Townsend, P. and Xu, J. (2013).A novel intrusion severity analysis approach for Clouds.Future Generation Computer Systems, 29, 416–428. doi:10.1016/j.future.2011.08.009

[4] Atayero, A.A. and Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials ofHomomorphic Encryption. Journal of Emerging Trends in Computing and Information Sciences,2(10), 546-552.

[5] Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise CloudComputing. International Journal of Network Security & Its Applications, 3(1), 30-45.doi:10.5121/ijnsa.2011.3103

[6] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009). Cloud computing andemerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. FutureGeneration Computer Systems, 25, 599–616. International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014

[7] Casola, V., Cuomo, A., Rak, M. and Villano, U. (2013). The CloudGrid approach: Security analysisand performance evaluation. Future Generation Computer Systems, 29, 387–401.doi:10.1016/j.future.2011.08.008

[8] Celesti, A., Fazio, M., Villari, M. and Puliafito, A. (2012). Virtual machine provisioning throughsatellite communications in federated Cloud environments. Future Generation Computer Systems, 28,85–93. doi:10.1016/j.future.2011.05.021

[9] Che, J. Duan, Y, Zhang, T. and Fan, J. ().Study on the security models and strategies of cloudcomputing. Procedia Engineering, 23, 586 – 593. doi:10.1016/j.proeng.2011.11.2551

[10] Chen, D. and Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing.International Conference on Computer Science and Electronics Engineering, 647-651. doi:10.1109/ICCSEE.2012.193