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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

A Study on Trusted Computing in Cloud Architecture

Neelam, Rachna

M.Tech Student, Department of CSE, New Green Field College of Engineering and Technology, Palwal (NGFCET), India

Assistant Professor, Department of CSE, New Green Field College of Engineering and Technology, Palwal (NGFCET), India

ABSTRACT: The cloud could be a next generation platform that gives dynamic resource pools, virtualization, and high availableness. Today, cloud computing have the power to utilize climbable, distributed computing environments inside the reach of the internet. This paper represent clear description of cloud computing. Customers also are terribly involved regarding the risks of Cloud. They continuously worry regarding "S" word: Security. Cloud computing security could be a sub domain of laptop, network and knowledge security during a broader side. Aim of this document is to explain completely different security threats and their countermeasures and investigate its role in cyber world whereas two trustworthy resources and dealing in same cloud to confirm secure communication below the reactive security.

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

I.INTRODUCTION

Cloud computing is a machinery that uses the internet as well as middle remote servers to preserve data and applications. Cloud computing allows customers and businesses to utilize applications without installation and contact their private files at any computer by internet access. This machinery allows for much more capable computing by centralizing storage, memory, processing and bandwidth. A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc.

2.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service is only tenant cloud cover where the Cloud computing vendor's devoted resources are only shared with contracted customers at a pay-per-use fee. This is really minimize the need for huge initial savings in computing hardware such as servers, networking strategy and processing authority. Infrastructure as a Service could be a single tenant cloud layer wherever the Cloud computing vendor's dedicated resource measures solely shared with contractile purchaser at a pay-per-use fee. This greatly minimizes the requirement for heavy or weighty initial investment in computing hardware like servers, networking devices and process power and resource bundling.

2.2 Software as a Service (SaaS)

Software as a service is wherever computer/laptop/smart devices applications are measured with accessed scenarios over the web instead of being put in on native computing machine or during a local information Centre. SaaS is changing into associate progressively rife delivery model as underlying technologies that support internet services and service-oriented design (SOA) mature and new organic process approaches, like Ajax, become standard. The supply of IaaS services could be a key enabler of the SaaS model [8]. info security officers can got to think about numerous ways of securing SaaS applications.Web-Services (WS) , Extensible-Markup-Language (XML) Secured- inscription, Secure

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Socket Layer (SSL) and on the market choices that effective measure utilized in imposing information protection transmitted over the web.

2.3 Platform as a Service (PaaS)

Platform as a service cloud cover work like paaS other than it provides an extra level of "rented" functionality. customers using PaaS services move still more costs from capital savings to operational expenses but must admit the extra constraints and possibly a number of degree of lock-in posed through the extra functionality layers [8]. Platform as a Service (PaaS) is an result of Software as a Service (SaaS), a software sharing model in which hosted software applications are complete available to customers in excess of 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 specific resource [12]. Once the high employment on the flooded services notifies by Cloud Computing package then it'll begin providing a lot of machine power to address the extra employment. Thus, the server hardware boundaries for optimum employment to method do now not hold. Therein sense, the Cloud system is making an attempt to figure against the assailant (by providing a lot of machine power),but in some extent this may facilitate by enabling him to try to most potential injury on a service's handiness, ranging from one flooding attack entry purpose. Thus, the assailant doesn't need to flood all an server that give a definite service in target, however simply will flood one, Cloud based mostly address so as to perform a full loss of handiness on the meant service.[10]

3.2 Man-in-the-middle attack

The **man-in-the-middle attack** (often abbreviated **MITM).** As the name specifies, 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 additionally outlined as active eavesdropping wherever wrongdoer makes freelance connections between users and relays messages between them. Man-in-the-Middle attacks square measure usually cited as "session hijacking attacks", within which the entrant aims to realize access to a legitimate user's session.

3.3 Network Sniffing

A Network-snifferis a utility or device-application that can read, monitor, and scan network packets [11]. Knowledge packets with mal-intention measure transmitted from one network device to a different that causes the

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

chance that outsider may see our knowledge or crucial information can be classified for any purposes. Sniffing is employed to examine what style of traffic is being passed on a network and to seem for things like passwords, master-card numbers, then 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 goal host on each port in a order. It is a method used to recognize open ports and services accessible on a network host but it also used by hackers to target victim. If recurring port scan are complete, a denial of service can be created. Hackers typically use port scanning because they can easily identify services which can be broken. They conduct tests for open ports on private Computers that are linked 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 through internet therefore security risks linked 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 SQL-injections, malicious user can modify the secured and protected data, breach or intrude the sensitive or classified information or damage/crash/catastrophic the entire system

3.6 XML Signature Element Wrapping

In cloud computing, customers are connected through a web browser or web service which increases the possibility of web services attacks in cloud computing. XML signature element wrapping is common attack for Web service. XML sign are designed to make easy integrity protection and source verification for a variety of documents types. It is use to protect a constituent identity, characteristic and value from unlawful festivity but unable to protect the position in the documents. (Jamil&Zaki, 2011b)[16]**An attacker** is capable to manipulate a SOAP message by copying the target component and inserting whatever value the attacker would like and stirring the innovative constituent 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. Amalgamation of WS-security with XML signature to a particular component.

3.7 Browser Security

In a cloud computing system, the computational processes are done in the cloud server but 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 important feature of the cloud system is to give dynamically scalable resources. Once there are more requests from client, cloud system frequently increases its size. Flooding attack is basically distributing a large amount

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

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 distinguished to serve normal customer requests. These attacks charges additional cost to the consumer for the usage of resources

3.9 Cloud Malware Injection Attack

Cloud malware injection attack is to build attempt to insert a malicious service, application or even virtual machine into the cloud system depending on the cloud service models (SaaS, PaaS and IaaS) In order to perform this attack , the first step of intruder is to produce his private vindictive application[3]. Once the vindictive software is entered into the cloud structure the attacker had to trick the cloud system to treat the malicious software as a suitable instance. If successful user request for the vindictive service then malicious is implemented. Attacker can also upload the virus list in to the cloud system. Once the cloud system treats it as a valid service, the virus list is automatically executed and the cloud system infects the virus which can cause damage to the cloud system[10].

3.10 Incomplete Data Deletion

In cloud computing, replica's knowledge of information is placed in over totally different server owing to this data doesn't take away fully. This can be referred to as incomplete information Deletion [16]. once letter of invitation to delete a cloud resource is formed, most operational systems this may not take away accurately correct information deletion isn't potential as a result of copies of data are hold on another sever however aren't on the market.

Table 1: Different security threats and their countermeasures

Denial of Service:	Reduction of the human rights of the customer that connected to a server..
Man in the Middle Attack	Proper installation of SSL
Network Sniffing:	utilize of encryption methods for securing the information.
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.

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

International Journal of Innovative Research in Computer and Communication Engineering

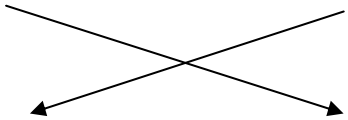
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

IV.RESULTS

Proposed Trusted Hash based Algorithm for Trusting Computing Measures in Cloud Architecture

	Trusting		**Trusted**
Trusting and Trusted Resources publically share a generator and XOR value.	$g \wedge n$, $p \wedge n$	Common info	$g = x$, $p = x$
Each then secretly picks a number n of their own.	$n = 8$	secret number	$n = 6$
Each evaluate g^n mod p	$3^8 \bmod 17 = 16$		$3^6 \bmod 17 = 15$
They then exchange these resulting values.	$A = 16$  $B = 15$		$B = 15$ $A = 16$
Each then raises the value they received to the power of their secret nXor$p$.	$B^n \wedge p$ = XOR $15^8 \bmod 17 = 1$	mix in secret number	$A^n \wedge p$ =XOR $16^6 \bmod 17 = 1$
The result is the shared secret key.	XOR Value	shared secret key	XOR Value

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

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

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