Volume 6, Issue 1, January 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Security Attacks on Cloud Computing With Possible Solution

**Priyanka Chouhan, Rajendra Singh**
Jaipur Engineering College, Kukas, Jaipur, Rajasthan,
India

***Abstract— Cloud computing is an emerging technological paradigm that provides a flexible, scalable and reliable infrastructure and services for organizations. Cloud data are stored and accessed in a remote server with the help of services provided by cloud service providers. Some example of cloud service providers are Amazon, Google's Application, IBM, etc., which provide facility for users to developing applications in cloud system environment and allow to access them from any remote location. Services of cloud computing is based on sharing thus it is open for attacker to attack on its security. The main thing that grabs the organizations to adapt the cloud computing technology is cost reduction through optimized and efficient computing, but there are various vulnerabilities and threads in cloud computing that affect its security. Providing security in such a system is a major concern as it uses public network to transmit data to a remote server. Therefore the biggest problem of cloud computing system is its security. In this paper we discussed different type of security issue related to cloud computing and some possible solution for them.***

***Keywords—Cloud Computing, Security Attacks, DoS Attack, Malware Injection Attack, Side Channel Attack, Authentication Attack, Man-in-The-Middle Attack***

## I. INTRODUCTION

Today network security is very challenging task, as it is an integral part of network service. But due to rely on computer network for secret and important file, security has become very important part of it. Network security becomes much more difficult to control when the environment becomes as dynamic and demanding as cloud computing. Main aim of cloud computing is to reduce the cost of using resources such as storage, processing power, services etc. These help users to focus on their business without worry of resources. The evolution of cloud computing is from many different technologies such as virtualization, grid computing, autonomic-computing, and some other technologies. New challenges arise whenever a new technology comes. In general, cloud computer security identifies following main objectives:

1) Availability: The goal of availability for Cloud Computing systems is to ensure that data and services are always available for its users at any time, at any place.
2) Confidentiality: The goal of confidentiality is to keep users data secret in the Cloud systems by making it available only to eligible entities and no unauthorized access to data can be obtained.
3) Integrity: The goal of Data integrity in the Cloud system is to assure that data has not been altered in any way while it is stored or while its transport over the network.
4) Authentication: The goal of authentication is to assure the identity of the entity involved in the communication.
5) Accountability: The goal of accountability is to assure that no entity can deny its participation in a data transfer between them.

These security objectives require the employment of certain security mechanisms and services to be implemented. A security mechanism can be defined as a process, or a device, which aimed to detect, or prevent, or recover from a security attack. Security mechanisms like steganography, encryption, hashing etc. are commonly used in providing security to a system. A Security Service can be identified as a processing or communication service aimed to enhances the security of data and the information transfers of an entity. These services help in countering security attacks. Security services usually employ one or more security mechanism to achieve its goals.

## II. SECURITY ATTACKS ON CLOUD

As the world is moving towards cloud computing, it become more sophisticated and attackers look to follow it. Some of the potential attacks on cloud computing are:-

### *A. Denial of Service (DoS) attacks*

In DoS attack, an attacker overloads the target cloud system with service requests so that it stop responding to any new requests and hence made resources unavailable to its users. Some Cloud Security Alliance has identified that the cloud is more vulnerable to DoS attacks, because it is used by so many users which makes it much more damaging. DOS attacks are of many types,

 

1) An attacker can overload the target with large amount of junk data that consume the network bandwidth and resources, for example UDP floods, ICMP floods etc.
2) An attacker can make use of blank space (lacuna) that associated with various networking protocol to overload target resource, for example SYN floods, fragment packet attack, ping of death etc
3) An attacker can make HTTP request in large amount so that it can not be handle by the server for example HTTP DDOS attack, XML DDOS attack etc.

*Possible solutions against DoS attacks*

For restricting DoS attack we can classify traffic on the basis of authorization, so we can block traffic that are identify as unauthorized and allow traffic that are identify as authorized. For this firewalls can be used to allow or deny traffic on the basis of access protocols, ports or IP addresses. Today most of the switches have capability of rate-limiting on the basis of Access Control List that can provide automatic rate limiting, shape traffic, bogus IP filtering, binding and can deeply inspect packets. Similar to switches routers have also some capability like ACL and rate-limiting which can be set manually to create rules and regulations.

Application front end hardware can be used on networks in colligation with routers and switches which can analyze data packets as they enter into the network system to check their authority and priority so that flow of traffic can be controlled..

After DoS attack one can send all the traffic on attacked packet to a null interface or to a non existing interface, this helps to reduce the effect of DoS attack.

***B. Cloud Malware Injection Attack***

In Cloud Malware Injection Attack an attacker tries to inject malicious service or virtual machine into the cloud. In this type of attack attacker creates its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and try to add it to the Cloud system. Then, the attacker has to behave so as to make it a valid service to the Cloud system that it is some new service implementation instance among the valid instances. If the attacker succeeds in this, the Cloud automatically redirects the requests of valid user to the malicious service implementation, and the attacker code starts to execute. The main scenario behind the Cloud Malware Injection attack is that an attacker transfers a malicious service instance into cloud so that it can achieve access to the service requests of the victim's service. To achieve this, the attacker has to derive control over the victim's data in the cloud. According to classification, this attack is the major representative of exploiting the service-to-cloud attack surface. The purpose of cloud malware injection attack can be anything in which an attacker is interested; it may include data modifications, full functionality changes/reverse or blockings.

*Possible solutions against malware injection attacks*

In cloud computing system application run by the customer are considered with high efficiency and integrity. So to prevent cloud from malware injection attack we can combine the integrity with hardware or can use hardware for integrity purpose because for an attacker it is difficult to intrude in the IaaS level. For this we can utilize a file allocation table (FAT) system, by using it we can determine the validity and integrity of new instance by comparing the current and previous instance. For this purpose, we need to deploy a hypervisor on the provider's side. In cloud system hypervisor is considered to be the most secure and sophisticated part of it whose security cannot be broken by any means. The Hypervisor is responsible for scheduling all the instance and services so we can make hypervisor to check file allocation table to validate and integrate an instance of customer.

Other approach is that we can maintain the information of the platform type version that a customer user to access the cloud in first phase when a customer open an account and can use those information to check the validity of new instance of the customer.

***C. Side Channel Attacks***

An attacker attempts to compromise the cloud system by placing a malicious virtual machine in close proximity to a target cloud server system and then launching a side channel attack. Side-channel attacks have emerged as a kind of effective security threat targeting system implementation of cryptographic algorithms. Evaluating cryptographic systems resilience to side-channel attacks is therefore important for secure system design. Side channel attacks use two steps to attack- VM CO-Residence and Placement i.e. an attacker can often place his or her instance on the same physical machine as a target instance and VM Extraction i.e., the ability of a malicious instance to utilize side channels to learn information about co-resident instances. It can be very easy to gain secret information from a device so security against side channel attack in cloud computing should be provided

*Possible solutions against Side Channel attacks*

To prevent cloud from side channel attack we can use combination of virtual firewall appliance. According to the case study of Amazon EC2 service it is possible for an attacker to instantiate new virtual machine to identified targeted virtual machine in cloud and extracts some confidential information. But a virtual firewall prevents this attempt of placement of malicious virtual machine during a side channel attack.

Another approach is to use randomly encryption decryption (using concept of confusion diffusion) because it prevent second step extraction of side channel attack. Here by confusion we mean that making relation between plain and cipher

 

text more and more complex; by diffusion we mean to dissipate the statistical structure of plaintext over the bulk of cipher text. Security against both front end and back end side of cloud computing architecture is provided by this combination and also provide RAS (Reliability, Availability, and Security). When we use randomly encryption decryption we mean that customer data or information encrypted through different encryption algorithm so attacker faces more difficulties to detect or extract cryptography key.

### *D. Authentication Attacks*

Authentication is a weak point in cloud computing services which is frequently targeted by an attacker. Today most of the services still use simple username and password type of knowledge-based authentication, but some exception are financial institutions which are using various forms of secondary authentication (such as shared secret questions, site keys, virtual keyboards, etc.) that make it more difficult for popular phishing attacks.

Some authentication attacks are:

1) Brute Force Attacks: In this type of attack, all possible combinations of password apply to break the password. The brute force attack is generally applied to crack the encrypted passwords where the passwords are saved in the form of encrypted text.
2) Dictionary Attack: This type of Attack is relatively faster than brute force attack. Unlike checking all possibilities using brute force attack, the dictionary attack tries to match the password with most occurring words or words of daily life usage.
3) Shoulder Surfing: Shoulder Surfing is an alternative name of "spying" in which the attacker spies the user's movements to get his/her password. In this type of attack the attacker observes the user; how he enters the password i.e. what keys of keyboard the user has pressed
4) Replay Attacks: The replay attacks are also known as the reflection attacks. It is a way to attack challenge response user authentication mechanism.
5) Phishing Attacks: It is a web based attack in which the attacker redirects the user to the fake website to get passwords/ Pin Codes of the user.
6) Key Loggers: The key loggers are the software programs which monitors the user activities by recording each and every key pressed by the user.

*Possible solutions against Authentication attacks*

Delayed response: Given a login-name/password pair the server provides a slightly delayed yes/no answer (say not faster than one answer per second). This should prevent an attacker from checking sufficiently many passwords in a reasonable time.

Account locking: Accounts are locked after a few unsuccessful login attempts (for example, an account is locked for an hour after five unsuccessful attempts.) Like the previous measure, this measure is designed to prevent attackers from checking sufficiently many passwords in a reasonable time.

Biometrics: Biometric is an image-based authentication system in which finger prints, face, iris, retinal, speech, signature verification are used to verify against the original specimen. The image is preprocessed first and then the classification of images is done. The advantage of this method is that it is real and unique signature and cannot be stolen. The disadvantage is that it is costly and difficult to implement. It is not a completely matured method and it can be easily compromised and is time consuming also.

### *E. Man-In-The-Middle Cryptographic Attacks*

A man in the middle attack is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other. In the process, the two original parties appear to communicate normally. The message sender does not recognize that the receiver is an unknown attacker trying to access or modify the message before retransmitting to the receiver. Thus, the attacker controls the entire communication. Some type of MIM attacks are:

1) Address Resolution Protocol Communication (ARP): In the normal ARP communication, the host PC will send a packet which has the source and destination IP address inside the packet and will broadcast it to all the devices connected to the network. The device which has the target IP address will only send the ARP reply with its MAC address in it and then communication takes place. The ARP protocol is not a secured protocol and the ARP cache doesn't have a foolproof mechanism which results in a big problem.
2) ARP Cache Poisoning: In ARP cache poisoning, the attacker would be sniffing onto the network by controlling the network switch to monitor the network traffic and spoof the ARP packets between the host and the destination PC and perform the MIM attack.
3) DNS Spoofing: The target, in this case, will be provided with fake information which would lead to loss of credentials. As explained earlier this is a kind of online MIM attack where the attacker has created a fake website of your bank, so when you visit your bank website you will be redirected to the website created by the attacker and then the attacker will gain all your credentials.
4) Session Hijacking: In this once the session is established between the host PC and the web server the attacker can obtain certain parts of the session establishment which is done by capturing the cookies that were used for the session establishment.

 

*Possible solutions against Authentication attacks:*

1) By using one time password because one time password is immune to MIM attacks.
2) By forensic analysis of MIM attacks
   - IP address of the server
   - Is the certificate self signed?
   - Do other clients, elsewhere on the Internet, also get the same certificate?
   - Is the certificate signed by a trusted CA?

3) By using mutual authentication, with many client and server implementations, the initial trust is only confirmed by one way verification between the client and the server. With mutual authentication, the server verifies the client and the client verifies the server to ensure legitimate communications are being exchanged. Verification can be conducted by using public and private keys.

## III. CONCLUSION

With the rapid increase in the adoption of cloud computing by many organizations, security issues arise. As cloud computing is on the rise, and especially due to its enormous attraction to organized criminals, we can expect to see a lot of security incidents and new kinds of vulnerabilities around it within the decades to come. Cloud security issues are active area of research and experimentation. Lots of research is going on to address the issues like cloud security, data protection, virtualization and isolation of resources. In this paper we discuss Denial of Service (DoS) attacks, Cloud Malware Injection Attack, Side Channel Attacks, Authentication Attacks and Man-In-The-Middle Cryptographic Attacks of cloud computing and also provide some possible solutions. The concepts we have discussed here will help to build a strong architecture for security in the field of cloud computation.

## REFERENCES

[1] Buyya, R., Broberg, J., Goscinski, A.M.: Cloud computing: Principles and paradigms, vol. 87. John Wiley & Sons,2010.
[2] Shirey, R.: Rfc 2828: Internet security glossary. The Internet Society, 2000.
[3] Stallings, W.: Cryptography and Network Security, 4/E. Pearson Education India, 2006.
[4] Security in Cloud Computing Kazi Zunnurhain1, and Susan V. Vrbsky2 Department of Computer Science The University of Alabama . Q.Luo and Y. Fei, "Algorithmic collision analysis for evaluating cryptographic systems and sidechannel attacks," in Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on, pp. 75–80, IEEE, 2011
[5] Catteddu, D.: Cloud Computing: benefits, risks and recommendations for information security. Springer, 2010
[6] Bedi, H.S., Shiva, S.: Securing cloud infrastructure against co-resident dos attacks using game theoretic defense mechanisms. In: Proceedings of the International Conference on Advances in Computing, Communications and Informatics, pp. 463–469. ACM, 2012.
[7] Contractor, D., Patel, D.R.: Trust management framework for attenuation of application layer ddos attack in cloud computing. In: Trust Management VI, pp. 201–208. Springer, 2012.
[8] Karnwal, T., Thandapanii, S., Gnanasekaran, A.: A filter tree approach to protect cloud computing against xml ddos and http ddos attack. In: Intelligent Informatics, pp. 459–469. Springer, 2013.
[9] Manavi, S., Mohammadalian, S., Udzir, N.I., Abdullah, A.: Hierarchical secure virtualization model for cloud. In: Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on, pp. 219–224. IEEE, 2012.
[10] Perez-Botero, D., Szefer, J., Lee, R.B.: Characterizing hypervisor vulnerabilities in cloud computing servers. In: Proceedings of the 2013 international workshop on Security in cloud computing, pp. 3–10. ACM, 2013.
[11] Godfrey, M., Zulkernine, M.: A server-side solution to cache-based side-channel attacks in the cloud. In: Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on, pp. 163–170. IEEE, 2013.
[12] Zhang, Y., Juels, A., Reiter, M.K., Ristenpart, T.: Cross-vm side channels and their use to extract private keys. In: Proceedings of the 2012 ACM conference on Computer and communications security, pp. 305–316. ACM, 2012.
[13] Varadharajan, V., Tupakula, U.: Counteracting security attacks in virtual machines in the cloud using property based attestation. Journal of Network and Computer Applications , 2013.
[14] Patel, A., Taghavi, M., Bakhtiyari, K., Celestino J´uNior, J.: An intrusion detection and prevention system in cloud computing: A systematic review. Journal of Network and Computer Applications 36(1), 25–41 , 2013
[15] He, X., Chomsiri, T., Nanda, P., Tan, Z.: Improving cloud network security using the tree-rule firewall. Future Generation Computer Systems 30, 116–126, 2014
[16] Koushik, S., Patil, A.P.: Open security system for cloud architecture. In: ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol I, pp. 467–471. Springer, 2014.
[17] Winkler, V.J.: Securing the Cloud: Cloud computer Security techniques and tactics. Elsevier, 2011.
[18] Popovic K; Hocenski Z; (2010), "Cloud computing security issues and challenge", 5533317searchabstractMIPRO, 2010 Proceedings of the 33rd International Convention , pp 344,24-28 May 2010.
[19] D. Jamil and H. Zaki, "Security Issues in Cloud Computing and Countermeasures," International Journal of

 

Engineering Science and Technology, Vol. 3 No. 4, pp. 2672-2676, April 2011.

[20] K. Zunnurhain and S. Vrbsky, "Security Attacks and Solutions in Clouds," 2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, December 2010.

[21] Researchers Demo Cloud Security Issue With Amazon AWS Attack, October 2011. http://www.pcworld.idg.com.au/article/405419/researchers_demo_cloud_security_issue_amazon_aw s_attack/

[22] A. Tripathi and A. Mishra, "Cloud Computing Security Considerations Interface," 2011 IEEE International Conference on Signal Processing, Communications and Computing, Xi'an, China, September 2011

[23] H. C. Li, P. H. Liang, J. M. Yang, and S. J. Chen, "Analysis on Cloud-Based Security Vulnerability Assessment," IEEE International Conference on E-Business Engineering, pp.490-494, November 2010.

[24] B. Sevak, "Security against side channel attack in cloud computing," International Journal of Engineering and Advanced Technology (IJEAT), vol. 2, no. 2, p. 183, 2013.

[25] A. Singh and M. Shrivastava, "Overview of attacks on cloud computing," International Journal of Engineering and Innovative Technology (IJEIT), vol. 1, no. 4, 2012

[26] K. Zunnurhain and S. Vrbsky, "Security attacks and solutions in clouds," in Proceedings of the 1st international conference on cloud computing, pp. 145–156, Citeseer, 2010.

[27] Fujita, K. and Y. Hirakawa, 2008. A study of password authentication method against observing attacks. 6 International Symposium on Intelligent Systems and Informatics, SISY 2008.

[28] Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider, "A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication", World Applied Sciences Journal, vol. 19, pp. 439-444, Jan. 2012.

[29] Man-in-the-middle attack http://en.wikipedia.org/wiki/Manin-the-middle_attack

[30] K. Haataja and P. Toivanen. Practical Man-in-the-Middle Attacks Against Bluetooth Secure Simple Pairing. In 4th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM'08, pages 1–5, Oct. 2008

 