SECURITY ATTACK ISSUES AND MITIGATION TECHNIQUES IN CLOUD COMPUTING ENVIRONMENTS

Subramaniam.T.K[1*], Deepa.B[2]

[*1]M.E.Scholar, Department of Computer Science & Engineering Nandha Engineering College, Erode, Tamil Nadu, India
[2]Assistant Professor, Department of Computer Science & Engineering, Nandha Engineering College, Erode, Tamil Nadu, India

ABSTRACT

In computer networks attacks plays a vital role. It also degrades a cloud services nowadays. The attacks reduce the quality of services in the computer networks as well as cloud platforms. The attack that makes services engaged to the intended users. For effective use of cloud computing we need to reduce the attacks vulnerabilities and improve the security. This study discuss about the different types of attacks that affects the cloud environments and also possible mitigation techniques to reduce the attacks. Issue mitigation

KEYWORDS

Attacks, cloud services

1. INTRODUCTION

In the network computer system's large number of computer system is associated with different machine that are geographically distributed network. Network attacks, threats security are major difficulty in computer system networks. The network security or web services are method of earning unofficial admittance to network. And also the attacks take part in a chief role in security. The attacks are classified into two related type's that is passive attacks and active attacks. The network impostor capture data travelling through the network is said to be a passive attack. Idle scan, wire patter, and port scanner are some of examples of passive attacks. Intruder instructs command to disrupt networks usual operation. This is called active attacks. Man-in-middle attack, Denial-of-service attack, spoofing are some of the examples of active attacks. This attack can be accepted in various ways and various policies. The essential facet would be to block victim's network system and thus make it unreachable by other client computer system [1] [2]. There are numerous ways of creating service that are unavailable to target users. Rather than just flooding with copious IP packets. The dupe could also be hit at various loopholes [12]. By creating it unstable which may depends on the nature of the attack.

DOI:10.5121/iju.2016.7101

2. RELATED WORK

Cloud computing other wise said to be an on-demand computing. Cloud computing is one of the types of Internet-based computing in which sharing of cloud resources, data and information. Normally data and programs are run on individual desktop computers. Instead these are run on cloud environments. Cloud computing provides platform, communications services and end user application services. The Cloud computing plays a vital role in IT industry [2] [3]. The network of networks gives a remote access to set of resources that would be a decentralized. Cloud computing is flexible, multi-tendency and scalable. In this study the section 3 provides a deployment model of cloud computing, section 4 provides security attack in cloud computing and solutions.

2. CLOUD SERVICE MODEL

Cloud computing connect delivering computing resources such as remote servers machines, data storages space, and cloud users applications are services to end users by cloud computing service supplier. End users access on-demand cloud services via web browsers. Cloud computing service providers propose specific cloud services and make sure the significance of the services. Essentially, cloud computing consist of three layers: the system layer, the middle layer or platform layer, and the top layer or application layer.

Infrastructure as a service

The bottom layer is the system layer, which comprise of additional resources such as communications of servers, network devices, and memory storage. It is said to be Infrastructures-a-service (IaaS). The computational resources are prepared and accessible for users as on-demand services [14]. With the exploit of virtualization technology, IaaS also offer virtual machines that allow clients to build composite network infrastructures. This model not only diminish the cost in importing physical apparatus for commerce, it also reduces the weight load of computer network administration since IT professionals are not essential to frequently monitor the health of physical network resources. The examples of a cloud computing service supplier of IaaS are Amazon’s EC2. It offers a virtual computing environment with web service interfaces. By using the boundary, users can deploy Solaris or Windows based virtual machines, Linux, and execute their own tradition applications.

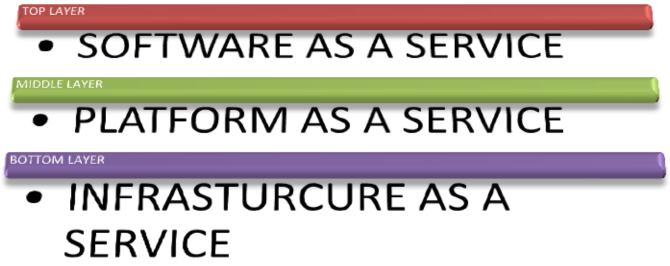

Fig 1: cloud service Deployment Model

Platform as a service

The middle layer is the platform layer and is said to be a Platform-as-a-Service (PaaS). It is planned to supply a development platform for users to design their explicit applications. Middle layer services offers by this cloud model contain tools and libraries for application enlargement, permit users to have organized over the application deployment and configuration settings. With Platform-as-a-Service model, programmers are not necessary to obtain software development tools, therefore dropping the cost of buying tools. Google Apps is an example of Platform- as-a-Service model it is a suite of Google tools that comprises Google Talk, Gmail, Google Groups, Google Docs, Google Calendar, and Google Sites. It permits users to modify these tools on their own domain names [12]. Windows Azure is another Platform-as-a-Service provider. It enables users to construct own applications using various languages and domains, tools or frameworks. Users can then incorporate the applications into their presented IT environments.

Software as a service

The top layer is the application layer, also called as Software-as-a-Service (SaaS). This layer permits users to lease applications runs clouds as a substitute of paying to purchase these applications. Because of its ability to decrease costs. Software-as-a-Service is popular in the middle of companies that install their businesses. Group on is an example that uses Software-as-a-Service[13]. With the use of the online bearer solutions provided by Zen desk, Groupon processes its thousands of daily customer tickets more efficiently.

Benefits of cloud computing

Lower IT costs Infrastructure

Moving to cloud computing may diminish the cost of running and preserve IT systems. Rather than acquire costly systems and equipment for your business, cloud computing can decrease the costs by using the resources of cloud computing service supplier. It may be able to diminish the working costs because: the cost of system upgrades, original hardware and software may be built-in in the agreement; cloud computing no longer need to pay wages for expert staff, the energy utilization costs may be condensed, there are fewer time delays.

Timeliness

The business can scale up or scale down the procedure and storage desires quickly to suit situation, permit flexibility as needs change. Rather than purchase and install expensive upgrade in individual computer, cloud computer service provider can handle this all works. Use the cloud frees up the moment so we can get on with managing business.

Durability in Business

Defending data and systems is an imperative part of business durability development. Whether experience a natural tragedy, power collapse or other predicament, encloses the data accumulate in the cloud environments ensure that it is backed up and confined in a secure and safe position. Being able to right to use data again rapidly permit conducting business as usual, minimizing any downtime and overcome of productivity.

Effective collaboration

Collaboration in a cloud computing environment gives the business capacity to commune and share more easily external of the traditional communication methods. If cloud computing operating on a project across different locations, might use cloud computing to provide employees, contractors and third parties admission to the equal files. The cloud users choose a cloud computing representation that formulates it easy for to share your report with adviser.

3. Cloud Computing Attacks

Cloud computing faces a some of following types of attacks. Proper mitigation techniques should be taken care to avoid or reduce these types of attacks.

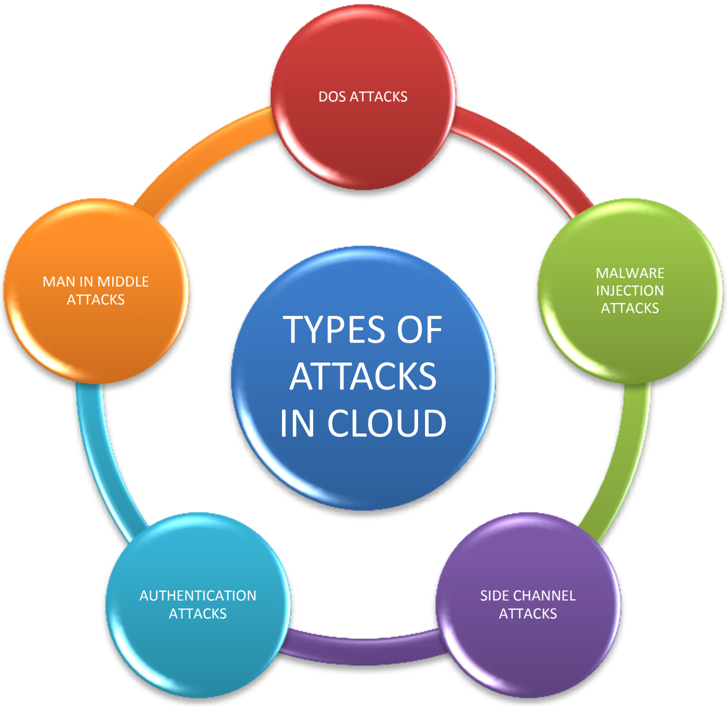

Fig 2: Types of attacks in cloud

3.1. Denial of service attacks

Cloud computing plays a vital role in IT industry. Many users are involved in cloud environments. Cloud environments provide a cost effective services to the users. Denial of service can easily occur in the environments. Cloud increases the computational power by with help of virtual machines. The Denial of service overloads the servers. The attackers can perform the attacks by sending huge number of request to the target servers. Hence the server cannot process the further requests. Denial of service can be performed in several ways such as UDP Flood Attack, ICMP flood attack. This type of denial of service attack happens in User Data Gram protocol. It establishes a session less connection by user datagram protocol. It enters into any one of the port in host computer with one or more numerous UDP packets. This session-less service roots the port that will require confirming the port wether the packets will be reached or not. Internet Control Message Protocol Attacks. Normally ping request packets are send to destination host to check whether the host is connected are not. This is identified by ping replies. Attackers send more number of packets without waiting for replies [5,6]. This consumes more bandwidth and cause ICMP flood attacks.

3.1.1. Solution to Denial of Service attacks

This type of attacks can eliminated by using following approaches such as filter based approach, signature based approach, firewalls.

Filter based approach: Flow level filter is used to detect the low rate DoS attack. Low rate DoS attack which gradually increase the traffic rate and attack the network host. Flow level filter which blocks the DoS attacks [34, 35].

In computer network, the traffic of the network is monitored along with signature pattern. The attacks pattern is compared with help of signature database. The database encloses one or more number pre-defined signatures. If the traffics match with database signature traffic it will take necessary steps to block the attacks.

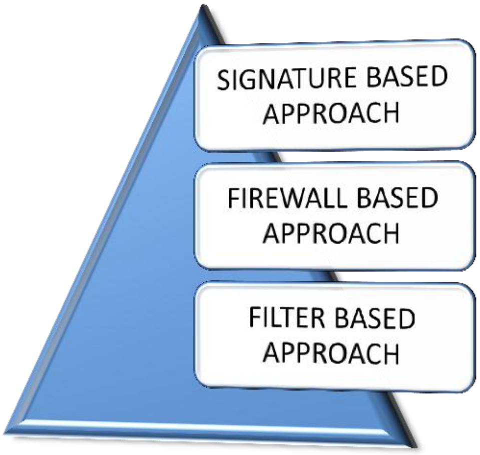

Fig 3: Approaches to DoS attacks

Firewalls are one of the methods of Intrusion Prevention System. The main idea of using firewall within the environment to impose endeavour strategy and preserve association state information for genuine users both internally and also externally and not to prevent high volume DoS / DDoS style attacks.

3.2. Malware Injection Attacks

In the cloud computing environment the client’s request is processed based on authentication and authorization, at that time there is a enormous chances of raw data’s control over between the web server and web browser. An attacker can take advantage during this switch over time of metadata. During this time the attacker attempts to introduce a harmful code or any other service to cloud computing environments. This infuses service or code that looks like a service that are already available in the cloud environments. Once the malicious code is injected in cloud, it will run continuously as a single instance. And it affects the cloud environments [15,22]. This will create a loop hole for attackers in cloud environments. It is one of the major security challenges in cloud.

3.2.1. Solution to Malware injection Attacks

Normally when a cloud customer opens an account in the cloud environments, the service providers creates an image of the customer's Virtual Machine in the image database repository system of the cloud. The applications that the customer will execute are measured with high efficiency and integrity. Cloud proposes to think the integrity in the hardware level, because it is very complex for an attacker to intrude in the Infrastructure as a Service level. They utilize the File Allocation Table (FAT) system construction, because it is one of the clear-cut technique .It hold up by virtually all existing operating systems. From the File Allocation Table they can identify about the code or application that a cloud customer is going to execute. They can confirm with the preceding instances that had been previously accomplished from the customer's device to establish the validity and integrity of the upcoming instance. For this purpose, need to install a Hypervisor in the provider's end [23]. This Hypervisor will be measured the most secured and sophisticated part of the cloud system those security cannot be violated by any resources. The Hypervisor is accountable for preparing all the instances, but prior to scheduling it will make sure the integrity of the instance from the File Allocation Table of the cloud customer's Virtual Machines.

One more solution is to store the Operating System type of the cloud customer in the first phase when a cloud customer opens an account in cloud environments. As the cloud is totally Operating System platform independent, prior to launching an instance in the cloud, cross checking can be done with the Operating System type from which the instance was requested from with the account holder's Operating System type.

3.3. Side channel attacks

This side channel attacks happens in Infrastructure as a Service Platforms. Infrastructure as a Service (IaaS) model in cloud computing make available infrastructures like a collection of several computers, virtual machines(VMs) and storage resources to store confidential information, data documents etc., An attacker endeavor to concession the cloud system by placing a malevolent virtual machine in target cloud server system and then entrance a side channel attack [24]. Side channel attacks follow two steps that is placement and Extraction. Placement is placing virtual machines and arranging the machines in cloud environments. Second thing is extraction .After placing the virtual achiness stars extracting confidential information from other servers in cloud computing environments.

3.3.1. Solutions to side channel attack

Virtual Firewall

Firewall is a collection of related programs that shield the resources of users from other networks and impostor. In this approach executing a virtual firewall in the cloud server's .It is possible to detect the new malicious virtual machines in cloud computing environments [24]. With the help of virtual firewall server these types of attacks can prevented in cloud computing environments.

The attacker tries to place virtual machines in cloud environments. This virtual firewall system blocks these types of new malicious virtual machine placements.

Encryption and Decryption

Side channel attacks can be prevented in cloud computing environments by means of virtual firewalls. This can prevent side channel attacks in environments. In order to provide a more security to cloud computing data’s and confidential information they use an Encryption and Decryption. The client side Data’s are randomly encrypted that uses the concept of confusion and diffusion [24]. The different security keys and different encryption algorithm are used to encrypt the client side data’s. Even though side channel attacks can occurs it is difficult to decrypt the client’s data’s. It provides a more security to cloud computing environments.

3.4. Authentication attack

This type of attacks can be easily occurs in the cloud environments. The attackers easily target the servers by these types of authentication attacks [18]. The attackers target the mechanism that is followed user. The mechanism used for authentication is captured and attackers and tries to access the confidential information. They use different encryption and decryption mechanism to transfer the data as more confidential. The service provider stores the key value of users and must be authorized before going to access a service.

3.4.1. Solution to Authentication Attack

This problem arises when using a simple authentication mechanism such as simple username and password. More than one authentication mechanism must be established in the environments. The secondary authentication mechanism must be used and also use advanced authentication mechanism must be used to avoid these types of attacks. Advanced authentication attacks such as one time password, virtual key boards, site key etc.

3.5. Man-in-middle attack

This type of attacks can be occurs while communication established in two node or computer system. The attackers in the communication system modify the message content or message sequences [20]. A man-in-the-middle attack permits a malevolent actor to interrupt, send and receive data between two users.

3.5.1. Solution to man-in-middle attack

This type of attacks is avoided by proper authentication mechanism. The advanced authentication mechanism can be used. The encryption is used for sender’s side and decryption is used for receiver side. This mechanism is to be used. The attacker cannot modify the encrypted data. The different encryption and decryption algorithm such as AES, DES, and Triple DES etc is to be used.

3.6. Wrapping attacks

Wrapping attacks use XML signature wrapping to increase a weakness when web servers validate the signed requests [15]. The attack is done at the time of the translation of SOAP messages between a valid user and the web server. By replica the user's account and password in the login period, the hacker inserts a bogus element into the communication structure, shift the original message body under the wrapper that replaces the content of the message content with harmful code, and then sends the message packets to the server. Hence the original body is still valid; the server will be scam into approve the message that has actually been distorted. As a result, the attacker is able to gain unauthorized admittance to secured resources and succession the proposed operations.

3.6.1. Solution to wrapping attacks

The attacker can infringe in the Transport Layer Services. They enhance the security by using a SOAP message while communicating with web server and web browser. In this add an additional bit called redundant STAMP bit. This bit will be toggled when the message is interfered with by a third party during the communication between web server and web browser. When the message ruches the other ends it verifies any toggle in the STAMP bit. At the end the source receives a signature value from the other end.

3.7. Data Stealing Problem:

Data stealing problem is the most conventional approach to break a user account in cloud computing environments [14]. The account password is stolen by attackers. Then the attacker cracks the confidential information the cloud computing environments. In sometimes they crash the system information's.

The service providers and cloud users are affected by those kinds of problems.

3.7.1 Data Stealing Solution

At the time of logout the service provider send an email messages to the customer about session used duration with a special number. This number is used for further login. In this approach customer can known about the usage time and charges and also unique random number is generated for next login. By using this become more confidential.

4. CONCLUSION

Attacks affect the cloud computing environments. It leads to data loss and also financially loss to the cloud owners and cloud service providers and cloud users. This study focuses on cloud computing attacks and possible solution to those attacks. Attacks are to be prevented before going to occur. By applying these solutions we can prevent the attacks in cloud computing environments.

REFERENCES

[1] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N " Cloud Computing: A Statistics Aspect of Users. In: First International Conference on Cloud Computing (CloudCom)," Beijing, China. Springer Berlin, Heidelberg, pp 347–358, 2009.

[2] Zhang S, Zhang S, Chen X, Huo X "Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China" IEEE Computer Society, Washington, DC, USA, pp 93–97, 2010.

[3] R. Sherman, Distributed systems security, Computers & Security 11 (1) (1992).

[4] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing," in Cloud Computing, 2009. CLOUD'09. IEEE International Conference on, pp. 109–116, IEEE, 2009

[5] A. M. Lonea, D. E. Popescu, and H. Tianfield, "Detecting ddos attacks in cloud computing environment.," International Journal of Computers, Communications & Control, vol. 8, no. 1, 2013.

[6] M. H. Sqalli, F. Al-Haidari, and K. Salah, "Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing," in Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on, pp. 49–56, IEEE, 2011.

[7] T. Grance and P. Mell, "The nist definition of cloud computing," National Institute of Standards and Technology (NIST), 2011.

[8] cloud Security Alliance. Top threats to cloud computing, Cloud Security Alliance, 2010.

[9] D. Lekkas, S. Gritzalis, S. Katsikas, Quality assured trusted third parties for deploying secure Internet-based healthcare applications, International Journal of Medical Informatics (2002).

[10] Cloud Security Alliance "Security guidance for critical areas of focus in Cloud Computing V3.0.. Available: https://cloudsecurityalliance.org/ guidance/csaguide.v3.0.pdf, 2011.

[11] Marinos A, Briscoe G "Community Cloud Computing. In: 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Springer-Verlag Berlin, Heidelberg"2009.

[12] Khalid A ," Cloud Computing: applying issues in Small Business. In: International Conference on Signal Acquisition and Processing (ICSAP'10),pp 27,2010.

[13] Gartner. Assessing the security risks of cloud computing, Gartner, 2008.

[14] Mather T, Kumaraswamy S, Latif S ," Cloud Security and Privacy". O'Reilly Media, Inc., Sebastopol, CA,2009.

[15] Li W, Ping L " Trust model to enhance Security and interoperability of Cloud environment. In: Proceedings of the 1st International conference on Cloud Computing",. Springer Berlin Heidelberg, Beijing, China, pp 69–79,2009.

[16] Rittinghouse JW, Ransome JF,"Security in the Cloud. In: Cloud Computing. Implementation, Management, and Security, CRC Press,2009

[17] Grobauer B, Walloschek T, Stocker E ,"Understanding Cloud Computing vulnerabilities." IEEE Security Privacy 9(2):50–57,2011.

[18] Subashini S, Kavitha V ,"A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl 34(1):1,2011.

[19] Onwubiko C," Security issues to Cloud Computing. In: Antonopoulos N, Gillam L (ed) Cloud Computing: principles, systems & applications. Springer-Verlag,2010.

[20] National Institute of Standards and Technology. Guide for mapping types of information and information systems to security categories, NIST 800-60,2008.

[21] Morsy MA, Grundy J, Müller I ," An analysis of the Cloud Computing Security problem. In: Proceedings of APSEC 2010 Cloud Workshop. APSEC, Sydney, Australia",2010.

[22] 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.

[23] 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.

[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] Jansen WA ," Cloud Hooks: Security and Privacy Issues in Cloud Computing. In: Proceedings of the 44th Hawaii International Conference on System Sciences, Koloa", Kauai, HI. IEEE Computer Society, Washington, DC,USA, pp 1–10,2011.

[26] Zissis D, Lekkas D ,"Addressing Cloud Computing Security issues. Future Generations Computer System ",28(3):583–592,2012.

[27] Kazi Zunnurhain and Susan V. Vrbsky, "Security Attacks and Solutions in Clouds"2013.

[28] Apurva Shitoot, Sanjay Sahu, Rahul Chawda, "Security Aspects in Cloud Computing", IJETT, Volume 6 number 3 - Dec 2013.

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

[30] Atici, A.C., Yilmaz, C., Savas, E.: An approach for isolating the sources of information leakage exploited in cache-based side-channel attacks. In: Software Security and Reliability-Companion (SERE-C), 2013 IEEE 7th International Conference on, pp. 74{83. IEEE, 2013.

[31] Varadharajan, V., Tupakula, U.: Counteracting security attacks in virtual machines in the cloud using property based attestation. Journal of Network and Computer Applications , 2013.

[32] He, X., Chomsiri, T., Nanda, P., Tan, Z.: Improving cloud network security using the tree-rule _rewall. Future Generation Computer Systems 30, 116{126, 2014.

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

[34] Subramaniam.T.K, Deepa.B , "A Review towards DDoS Prevention and Detection Methodology" International Journal of Computational Science and Information Technology (IJCSITY) Vol.3,No.1/2/3,August 2015.

[35] Subramaniam.T.K, Deepa.B, “A Survey On DDOS Attack Detection And Prevention Methodology” International Journal of Intellectual Advancements and Research in Engineering Computations, JUNE 2015.

T.K.SUBRAMANIAM received the B.Tech degree in Information technology from Nandha Engineering College in the year 2014.He is currently doing his M.E Computer science and Engineering in Nandha engineering college, Erode, India. His area of interest is web services. He has published many journal papers.

B.DEEPA received the M.E degree in Computer Science and Engineering from Nandha Engineering College in the year 2011.She is currently working as Assistant Professor in Nandha Engineering College, Erode, India. She has published many international and national research papers. Her area is Network security and web services. She has depth knowledge of her research area.