International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Cloud Security Risks DDOS Attacks and Defense Mechanisms

G.K. Sandhia, S.V. Kasmir Raja,

Abstract: ***Protecting data privacy becomes an important issue with the greater rate of using cloud storage. The most effective solution is to encrypt data prior to uploading to the cloud. Due to benefits such as scalability and reliability, cloud - hosted services are increasingly being used in online businesses such as retail, health care, manufacturing, entertainment. Attackers are attempting to steal confidential information, interrupt services, and damage the cloud computing network of enterprises. How to search data encrypted with different keys efficiently, however, is still an open problem. This paper gives an overview of various security and privacy concerns related to the cloud computing environment and also provides the related solutions for each issue especially for DDOs attacks.***

Index Terms: Cloud Storage, DDOS Attacks, Mitigation techniques, Security.

I. INTRODUCTION

Cloud computing is the important paradigm in digital world that provides pay per usage computing and storage resources to the users over internet. Cloud has major advantages like huge storage, ease of access over multiple resources, etc. These benefits will result in security challenges to the data stored in the cloud such as Data breach, computation breach, replay attacks, DDoS attacks, etc. Entire cloud is controlled by cloud service provider and cloud users are trusting the security mechanisms provided by the cloud service providers. The security issues to be improved to enhance the existing security mechanisms available. There are three key areas to be focused more in cloud, they are data or information, identity and infrastructure. The objective of security is to protect data from unauthorized access, usage, breach, deletion, modification, tamper, etc. The basic security requirements to secure the data through confidentiality, integrity, authentication and availability of data. Major Roles involved in cloud architecture are:

1. Cloud User: individual or organization that accesses the services provided by cloud service providers.
2. Cloud Service Provider: individual or organization that offers the services to cloud users.
3. Cloud auditor: Party or an individual that assess the cloud services and responsible for cloud data security.

There are three service delivery models such as IaaS, SaaS and PaaS and three deployment models such as public, private and hybrid in the cloud environment. Cloud Security reports states that there is risk in cloud since cloud usage is more. Recent evidences confirms that there is a possibility of attacks such as data breaches, DDoS, Man-in the Middle attack, malware injection, replay attack, etc. in cloud environment. Cloud computing is the integration of software and hardware resources from a huge number of PC organize. It grants digital data to be shared at less expense and extremely quick to utilize. Cloud is assaulted by viruses, worms, attacks and cybercrimes. Adversaries will hack the sensitive or confidential data, interfere with administrations, and cause harm to the endeavor cloud computing system. Many of them were focusing on traditional way of identifying the attacks, threats and risks. This paper gives a countermeasures for cloud storage attack in cipher text policy attribute based encryption.

II. TYPES OF ATTACKS

A Data breaches

Data breaches can lead to the loss of personal and sensitive information during normal data processing and storage. If the database is not properly designed, a single flaw in one of the user's applications can allow an attacker to access the user data. Such advanced techniques have not yet been used, however, but still act as an obstacle to the cloud computing by the company. The best way to resolve data breaches is to encrypt the data and to protect encryption keys using key management policies and practices. Encryption protects the data, but the entire data is lost if the encryption key is lost. There are three ways to protect the keys for encrypted data: Keys can be stored in the cloud or host or system [2]. The cloud copies data regularly to prevent data loss due to an unexpected server crash. But the more copies, the higher the risk of breaches of data. User ID credentials should be secured and encrypted on the cloud side, and the user should try to protect his credentials from falling into the wrong hands.

B Data Loss

Data loss can occur as a result of data breach by malicious and intrusive actions of attackers intentionally. There are so many reasons for data loss: Before uploading the data to the cloud, the owner can encrypt the data, but lose the encryption key. Data loss can also occur on the side of the cloud service provider, a bug in the cloud service or a cloud service provider might deleted the data without any intention.

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author
G.K.Sandhia, Assistant Professor, Department of Computer Science & Engineering, SRM Institute of Science and Technology,
Dr.S.V. Kasmir Raja, Dean Research, SRM Institute of Science and Technology

The loss of data can be prevented by replicating data or saving data on various physical servers. However, more copies can increase the risk of data breaches, as stated earlier. In addition, data centers for the storage of data should be free of environmental risks such as fire, earthquakes, floods, etc [3].

C Malicious Insider

A malicious insider is an existing or ex-employee or a trusted third party who has access to the network, system or data of an organization or has authorized it. Hackers can therefore misuse the fact that access to sensitive information negatively affects the confidentiality, integrity or availability of the organization [4]. System admin can turns as a malicious insider and bypass firewall, IDS and access potentially sensitive information in a cloud scenario that has been improperly designed.

D Web Browser and API Vulnerabilities

Application Programming Interface (API) is a set of software interfaces (SOAP, REST and HTML) used by client software (Web Browser) to provide various services in the cloud. . The API and the web browser suffer from various vulnerabilities that an attacker can take advantage of and affect the cloud system adversely [5]. Weak credentials, insufficient authorization checks and insufficient validation of input data are some of the problems. Examples of attacks that can be executed due to web and API vulnerabilities are SSL certificate spoofing attacks, browser cache attacks, SQL injection, clickjacking and phishing attacks.

E Side Channel Attacks

This attack is based on information gathered from the physical implementation of a cryptosystem, rather than by brute force or weak algorithm, such as timing information, energy consumption / power consumption, other information that can be used to damage the system or electromagnetic leakage [6].

F Service Hijacking

In the hijacking of services, the attacker deceives a legitimate user to an illegitimate website in order to gain unauthorized access to their accounts to monitor transactions / activities, return falsified information and manipulate data [7]. Phishing, software vulnerability exploitation, fraud and reused credentials may pose a hijacking risk. Security policies, strong authentication and activity monitoring are some of the defense techniques to mitigate this threat.

G Malware Injection Attack

This attack is performed by injecting a malicious code into the cloud as a useful service. The intention can be eavesdropping and include data changes, deadlock creation and functionality changes. The attacker creates and attaches a malicious service module or instance to the cloud. By pretending to be a new valid service, the malicious service misleads the cloud system. The attacker then redirects the benign user's request to the malicious module and gains access to the victim's service rights [8]. When the instance is running, the only thing checked is whether the service is a valid service or not, but no integrity checks are carried out. This attack is also known as meta-data spoofing attack.

H Botnet Attack (Stepping Stone Attack)

IaaS users are provided with abundant access to computing resources such as bandwidth, processing and storage to rent high - performance virtual machines (VMs). These abundant resources can be used as a feasible ground for attacks of high magnitude. A botnet is a network of compromised hosts or VM's called stepping stones. The attack is carried out by gaining unauthorized access to a high-performance cloud server with the help of forged/stolen credit card details [9]. The attacker then establishes a control over the stepping stones to steal sensitive information, perform DoS / DDoS attacks or perform port scans to find new victims. This is done by using a sequence of compromised VM's called stepping stones to attack the victim indirectly. The attacker also mitigates the probability of detection and traceback due to the use of stepping stones. There have been many ways to detect botnets / stepping stones and to defend botnet / stone attacks. However, encrypted traffic and authentication forging or introducing jitter can fake these defense techniques, while other techniques are inefficient due to the enormous traffic that needs to be observed and examined [10]. xFilter is used against stepping stone attacks. xFilter runs in the VMM for pinpoint active response and uses information about transmitter processes for packet filtering in compromised VMs.

I Audio Steganography Attack

This attack is considered to be one of cloud storage systems dangerous attacks. A user can hide his confidential data in regular audio files with the help of audio steganography. An attacker can secretly transmit information via media files that appear to be normal audio files using steganography. Intruders can exploit this feature by hiding malicious code in sound files and sending it to victim servers to avoid current security mechanisms such as steganalysis. When using steganography, three factors must be considered: file format, hiding area, and steganography scheme. The steganography tool will analyze the file format and search for suitable information hiding areas, then divide the information into blocks and replace the original information in the hiding areas. A solution called StegAD (Active Defense Steganography) is designed and implemented to address the threat of Audio Steganography attacks from data leakage. There are two algorithms in StegAD [11], the improved RS algorithm, and the SADI algorithm. In the first step, through the famous RS image grayscale steganalysis algorithm, the hiding place of audio files is scanned under the cloud storage system. If any suspicious files are purchased, the SADI (Steganography Audio Dynamic Interference) technique is used to interfere with these suspicious files in all possible places [12].

J Denial of Service (DoS) Attack

This attack aims to reduce the performance of a cloud system and temporarily or indefinitely suspend its services by flooding it with nonsense messages / requests. A Distributed DoS (DDoS) is where more than one compromised node or bot is the source of the attack, often thousands of unique IP addresses. It is undoubtedly one of cloud computing's most dangerous and pervasive attacks. The attacker uses a master program known as the handler to propagate commands to the bots under his control, then start the target attack until the target's service goes down. DDoS affects all cloud layers and can occur internally or externally. Starting from outside the cloud environment, an external cloud-based DDoS attack targets cloud-based services. It affects the availability of data. An internal cloud-based DDoS attack takes place within the cloud and internally attacks victim's machine [13].

When the load increases under attack, the cloud starts delivering additional computational power in the form of more virtual machines and service instances to handle the extra load. Actually, the cloud system works against the attacker by offering more computational power, but in fact helps the attacker do more possible damage to service availability. There are 3 broad categories of DDoS attacks: volume - based DDoS attacks in which the target is flooded with high packet volume or connections overwhelming networking equipment, servers or resource bandwidth. DDoS - based application attacks targeting various applications like HTTP, VoIP or DNS. Low - rate DoS attacks that take advantage of weakness and design flaws in application implementation.

K Flooding attacks

In such attacks, the attacker uses bots to flood the target with massive traffic volumes such as ICMP (ping), SYN or UDP packets to saturate the target network drastically and slow down the network infrastructure. The ICMP flood attacks work simply by sending the victim enormous volumes of ICMP echo requests. The victim's bandwidth will be maximized to respond to such a huge volume of requests, resulting in inaccessibility to benign users [13]. SYN flood attack exploits the TCP three - way handshake by sending a SYN message to the server in which the client requests a connection. The server responds to the client with the SYN - ACK acknowledgement message. Then the client responds with an ACK message and the connection is set up. The attacker does not respond with the expected ACK to the server in a SYN flood attack but spoofs IP source address or it does not respond to the SYN - ACK. UDP flood attack will be initiated by sending a huge volume of UDP packets to random ports on the target system. The system observes that at that port no application listens and responds with an unattainable ICMP destination packet. Consequently, the victim is forced to respond with numerous ICMP packets if the number of UDP packets are sent. Usually these attacks are accomplished by spoofing the source IP address of the attacker.

L Amplification attacks

This type of attack uses the broadcast address feature to send an enormous amount of packets to a broadcast IP address that causes the nodes in the broadcast IP to send a response to victim servers resulting in malicious traffic [13]. DNS amplification attack, Smurf attack, and Fraggle attack are examples of this attack. The attacker sends spoofed address queries to an open resolver in a DNS amplification DDoS attack, which sends the larger number of response to the spoofed address target.

M Smurf attack

In this type, an attacker transmits a huge number of ICMP packets to a network using an IP broadcast address with the victim's spoofed source IP. This causes the response of all devices in the broadcast network by sending an ICMP echo response to the IP address of victims.

N Fraggle attack

Another name for fraggle is Smurf attack, UDP echo packets are sent to ports that support the generation of characters with the spoofed IP address of the victim generating an infinite loop. The target port that supports the generation of character that a broadcast address reaches. All range systems echo back to the victim's character generator port.

O Encrypted SSL DDoS attacks

During the encryption and decryption process, these types of attacks allow attackers to consume more CPU resources, thus amplifying the impact on the target.

P IP Spoofing attack

In this type of attack, data communication between the end user and the cloud server are intercepted and their headers modified. Attackers can use a authentic IP address or an inaccessible IP address to forge IP source fields in the IP packet. Because the server responds to the legitimate user machine and affects it, or the server is unable to complete the transaction for the IP address that affects the server resources.

Q H-DoS attack and X-DoS attack

The attacker uses the HTTP Get / Post request messages in an H - DoS or HTML - based DoS to flood the victim. During SSL sessions, the HTTP GET request attempts to get some information (images etc.) from the server [14]. Using the CPU and memory, the server is overloaded with GET requests and as such will not be able to respond to any additional requests. The HTTP POST request is more complex because it includes input data from forms that require more cloud server computation. A DoS attack based on X - DoS or XML occurs when a network is flooded with XML messages rather than packets to prevent genuine users from accessing network communications. It also affects the availability of web services if the attacker floods the web server with XML requests. There are three ways to start an X - DoS attack: oversized payload, external entity references and expansion of the entity. HX - DoS attack is a combination of intentionally flooding HTTP and XML messages and destroy the cloud service provider's communication channel [15].

R E-DoS attack

An Economic Sustainability Denial or an E - DoS attack is a new form of DoS attack that targets the cloud environment specifically. As cloud services are delivered in the form of a Service Level Agreement (SLA) defining the type of service the user requires. Some SLA will restrict resource utilization while others will provide infinite resources. In the former SLA type, the resources (CPU, memory) will be depleted when the cloud is under attack and legitimate users will be denied service. In the latter, more and more resources will be allocated by the cloud to handle the additional load to maintain SLA. Many solutions have been proposed to detect, analyze and prevent cloud DoS / DDoS attacks using e.g. Covariance Matrix approach, NSA Algorithm, Multivariate Correlation Analysis, Hop Count filtering, Confidence - based filtering, Random Port hopping, Ingress and Egress filtering, Path Identification mechanism, etc [16].

S Phishing Attack

In this type of attack, by using social engineering techniques, the attacker attempts to request personal / sensitive information (passwords, credit card details, etc.) from the victim. Usually the attack is performed by creating an exact replica of a website and sending the link to the victim from the wrong website. If the victim enters his / her credentials, the same will be passed on to the attacker and the attacker will be able to access sensitive data [17]. The attack can be divided into two categories: First, to host phishing websites, the attacker can use the cloud services.

Second, to gain unauthorized access to the cloud service, the phishing attack can be used. A recent type of phishing attack called Homograph attack uses Punycode to help register foreign character domain names [18]. As a result, the browser displays normal characters rather than Unicode characters, making it impossible to detect the attack. One way to prevent phishing attacks is PhishTank, which works by maintaining a blacklist of all known phishing web pages, nowadays in all popular web browsers these lists are implemented.

T Man in the Cloud Attack

This type of attack is predominantly carried out on file sync services, the attacker steals the synchronization token used to access cloud services without entering the password. After the victim successfully authenticates to the cloud service, the synchronization token is saved in the victim's machine and the same token can be used to access the service across multiple devices. However, if the victim changes the password, the token will not change. All the attacker has to do is intercept and copy the token and install it on his / her machine to gain access to a victim cloud service successfully. The attack can be undetectable and untraceable as the attacker copies the user token back into his account at any time. Encrypting files in the cloud and storing the encrypted keys outside the cloud can prevent the attack. Another solution may be to use two - factor authentication if it is offered by the cloud service or to allow log - in alerts from a new device to be informed about log – in [19].

III. Defense in the DDoS Attack

DDoS attacks are used on the network infrastructure of today. Till now, there are many methods used for defending DDoS attacks; but still effectiveness need to be improved. Mitigation of DDoS attacks is a huge mission, but such types of attacks to be detected and prevented. This would require more effort to enhance security over the network of organizations. The mitigation of the DDoS attacks can be classified into three categories, i.e., before the attack, during the attack, and after the attack [20].

IV. Attack Prevention Mechanisms

A. Ingress Filter

This process stops incoming packets with a source address that is not legitimate. To this end, routers are used. This technique prevents the IP address spoofing of the DDoS attack [21].

B. Egress Filter

It uses an outbound filter. This technique enables packets with a network - specified valid IP address to leave the network [22].

C. Route based distributed packet filtering

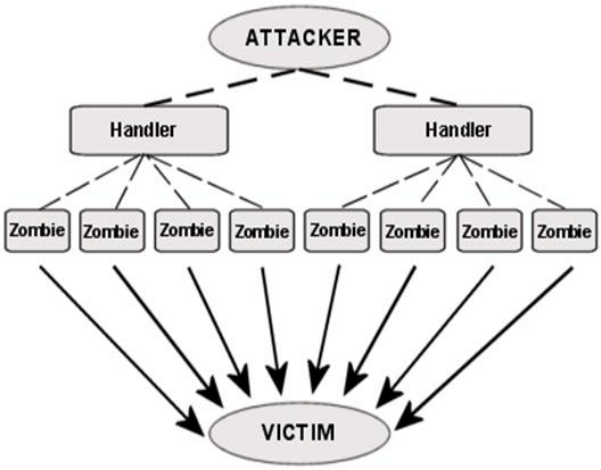
It captures / filters the IP address spoofed packets using the route information and prevents the attack. It's also used back in the IP trace. But it requires global information on the topology of the network [23].

D. Secure Overlay Services (SOS)

SOS is a distributed architecture that protects the victim system. If it comes from the legitimate servers, it assumes to be valid. Overlay filters the other packets. With replicated access points, a client must authenticate itself. SOAP to access the overlay network [24].

V. System Model

The system model of DDoS attack is shown in the below Fig. 1. The attacker floods the message in the network or cloud using the compromised machine in the cloud which are known as handlers. The legitimate users are not allowed to access the resources or data in the cloud. The legitimate users are handled by the handler. Later those authorized users are called as zombies since by sending multiple requests. This is clearly shown in the architecture. The victim machine will not provide the services to the legitimate users in turn this will affect the efficiency, availability of resources. To avoid these types of flooding or attacks the legitimate users traffic will be analyzed and monitored using the proposed technique.



VI. Proposed DDoS Attack Detection Method

The DDoS defense mechanism is used to observe, manage and mitigate the effects of various malicious DDoS attacks. Access control list is used to identify system log, modular policy framework and attacks can be prevented by limiting the resources. As soon as DDoS attack is detected, block the attack and betray the attacker to find out the identity of the attacker. This can be done in two days, first by hand or automatically using ACL. The cloud - based DoS attacks survey says that as cloud use increases the rate of DDoS attacks will also increase rapidly. Cloud system works against the attacker, but to some extent it supports the attacker making it possible to do as much damage as possible to the availability of the service, starting from a single point of entry.

VII. Experimental Results for Testing Attacks in Cloud

Experimental results shows the effectiveness and accuracy of the proposed defense model for DDoS in this section. The DARPA intrusion detection dataset is used for testing the efficiency of the proposed DDoS attack model and various DDoS attacks are simulated in the OpenNebula cloud.

The false positive and true positive rates are calculated based on the number of packets attacked with respect to non-attacked packets in the cloud which is shown in the Table 1.Mutiple false and true negative value rates are shown with respect to different random values.

Value (rating parameter)	Attacked packets	Non-attacked packets	False positives	True positives
0.09	421722	1511054	24192	399385
0.01	421722	1511054	29678	399749
0.10	421722	1511054	344961	400847
0.10	421722	1511054	455880	401210
0.40	421722	1511054	717503	417340
0.70	421722	1511054	1300762	421720
0.00	421722	1511054	0	0
1.00	421722	1511054	1511047	421722

Table 1: True Positive and False Positive rates

VIII. CONCLUSION

As DDoS pose a major threat in cloud environment. This paper provides the brief survey of DDoS attacks, then taxonomy of attacks and different counter-measures to mitigate DDoS attacks. By implementing a firewall, we defended the DDoS attacks. If attack traffic has increased rapidly, the firewall may go down.

REFERENCES

1. Aaqib Iqbal Wani, Zubair Ahmad Lone, A Survey of Security Issues and Attacks in Cloud and their Possible Defenses, International Journal of Emerging Technologies in Engineering Research (IJETER) Volume 5, Issue 12, December 2017.
2. Duncan, A., S. Creese, and M. Goldsmith, An overview of insider attacks in cloud computing. Concurrency and Computation: Practice and Experience, 2015. 27(12): p. 2964-2981.
3. Yeboah-Boateng, E.O. and K.A. Essandoh, Factors influencing the adoption of cloud computing by small and medium enterprises in developing economies. International Journal of Emerging Science and Engineering, 2014. 2(4): p. 13-20.
4. Top 7 threats to cloud computing Help Net Security, https://www.helpnetsecurity.com /2010/03/01/top-7threats-to-cloud-computing/, 2010.
5. Tsai, W.-T., Z. Jin, and X. Bai. Internet ware computing: issues and perspective in Proceedings of the First Asia-Pacific Symposium on Internet ware, ACM, 2009.
6. Hlavacs, H., et al. Energy consumption side-channel attack at virtual machines in a cloud in Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on. 2011.
7. Habiba, U., et al., Cloud identity management security issues & solutions: a taxonomy Complex Adaptive Systems Modeling, 2014.
8. Zhang, Y., et al. Homealone: Co-residency detection in the cloud via side-channel analysis in Security and Privacy (SP), 2011 IEEE Symposium on. 2011.
9. Huang, S.-H.S. and W. Ding, a Hybrid Stepping-Stone Detection Algorithm to Counter Packet Jittering Evasion. Journal of Information Assurance & Security, 2014.
10. Kampasi, A., et al., Improving stepping stone detection algorithms using anomaly detection techniques. 2007: Computer Science Department, University of Texas at Austin.
11. Gopalan, K. Audio steganography using bit modification in Acoustics, Speech, and Signal Processing, 2003. Proceedings. (ICASSP'03). 2003 IEEE International Conference on. 2003.
12. Liu, B., et al. Thwarting audio steganography attacks in cloud storage systems in Cloud and Service Computing (CSC), 2011 International Conference on. 2011. IEEE.
13. Thangavel, M., S. Nithya, and R. Sindhuja, Denial of Service (DoS) Attacks Over Cloud Environment: A Literature Survey, in Advancing Cloud Database Systems and Capacity Planning With Dynamic Applications. 2017, IGI Global. p. 289-319.
14. Chonka, A., et al., Cloud security defense to protect cloud computing against HTTP-DoS and XML-DoS attacks. Journal of Network and Computer Applications, 2011. 34(4): p. 1097-1107.
15. Shruthi, B. and Y. Nijagunarya, X-DoS (XML Denial of Service) Attack Strategy on Cloud Computing. Imperial Journal of Interdisciplinary Research, 2016. 2(12).
16. Kumar, M.N., et al. Mitigating economic Denial of Sustainability (eDoS) in cloud computing using in-cloud scrubber service in Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on 2012. IEEE.
17. Tan, C.L. and K.L. Chiew. Phishing Webpage Detection Using Weighted URL Tokens for Identity Keywords Retrieval. in 9th International Conference on Robotic, Vision, Signal Processing and Power Applications. 2017. Springer.
18. Deng, Q., et al. A Phishing Webpage Detecting Algorithm Using Webpage Noise and N-Gram in International Conference on Cloud Computing and Security. 2016. Springer.
19. Man-in-the-Cloud Attacks Want Your Dropbox, Google Drive Files. pcmag, http://in.pcmag.com/google-drive/94851/news/man-in-the-cloud-attacks-want-your-dropbox-google-drive-file, 2015.
20. G. Dayanandam, T. V. Rao, D. Bujji Babu, S. Nalini Durga, DDoS Attacks—Analysis and Prevention, Innovations in Computer Science and Engineering, Springer 2018.
21. P. Ferguson, D. Senie, Network ingress filtering: defeating Denial of Service attacks which employ IP source address spoofing, in: RFC 2827, 2001.
22. Global Incident analysis Center Special Notice Egress filtering, Available from http://www.sans.org/y2k/egress.htm.
23. K. Park, H. Lee, On the effectiveness of route-based packet filtering for Distributed DoS attack prevention in power law Internets, in: Proceedings of the ACM SIGCOMM 01 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ACM Press, New York, 2001, pp. 1526.
24. A. Keromytis, V. Misra, D. Rubenstein, SoS: secure overlay services, in: Proceedings of the ACM SIGCOMM 02 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ACM Press, New York, 2002, pp. 6172.