A Survey on Cloud Computing Security Threats, Attacks and Countermeasures: A Review

Arun Kumar M[1] . K Ashok Kumar[2]

[1,2] Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology (Deemed to be University), Chennai, Tamil Nadu, India

Received: 16 August 2022 / Revised: 28 August 2022 / Accepted: 13 September 2022

Abstract — The security challenges are more in the area of Cloud computing platform. The On-demand service of Cloud Computing secures a vital role in the industrial development and other IT sectors. This paper will try to provide the information based on the current threats and attacks on Cloud Computing and the solution to those attacks. Cloud Computing provides various set of service models like Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS) respectively. The cloud security measures are still a challenging task for organizations and other IT Sectors to handle the external attacks. Concluding that this survey will leads to give an overview of threats, attacks and vulnerabilities in the era of Cloud platform as well as some of the countermeasures to protect the cloud.

Keywords — Authentication attacks, Malware Injection, Side- Channel, Denial of Service (DoS), Flooding

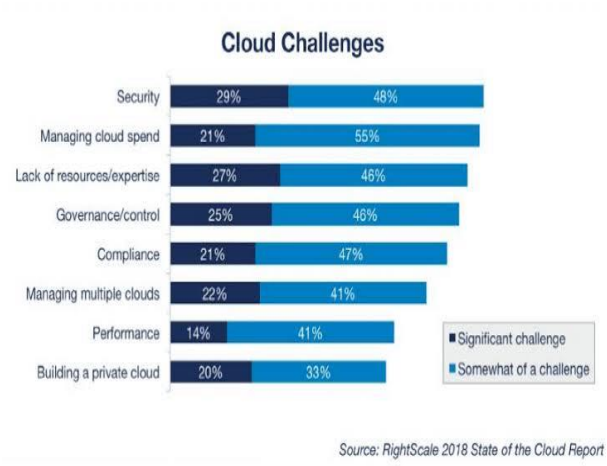
I. INTRODUCTION

Today's Internet computing platform, Cloud computing is the most secure on demand platform. It shows computing and distributing things in the remote data centers and is completely handled by an external third-party vendor. In the cloud, the remote data centers are provided services on-demand basis, which purely depends on which services they are adopting. PaaS (Platform as a Service), IaaS (Infrastructure as a Service) and SaaS (Software as a Service) are the mostly used service models provided by the cloud. The fundamental delivery models of cloud form the core of the cloud and these specific behavior exhibit certain characteristic like on-demand service to the users. The service delivery model certainly depends on some deployment models namely private, community, public and hybrid. The third party vendors may not fully trustworthy and the data security, transferring of data, application security of the deployment data are only limited.

Cloud security is a major concern of this on demand service model. By considering the Cloud computing security, the data allocation and the storage of data in remote location is a momentous factor now [2].In the era of Cloud computing, the Location Transparency is one of the major flexibility and at the same time which is a security threat. The data protection act for some standard region might be heavily affected and violated even though they are unknown about the storage location [2].

The personal data security of cloud users' might be a crucial concern in a cloud computing scenario (Joint, Baker & Eccles, 2009; Ismail, 2011; King & Raja, 2012). Yet another problem which uplift security concerns to use cloud service is the trust (Ryan & Falvy, 2012), which is the reason behind the credibility and

authenticity of the cloud service providers [2].The common reliance between the cloud service provider and end user is the most important thing in setting up the cloud environment. In security concern a lot of external attacks also possible to deny the access of data communication between service providers and users.



Our major offerings of this paper can be summarized as follows:

- We produce here a detailed classification of existing attacks in Cloud Computing and the solutions to those attacks.
- We propose a comparison of different attacks, reason for vulnerability, security violation areas and its consequences.
- Other security risk and threats in Cloud environment is proposed and discussed.
- Finally, we identify the different sort of attacks coming under cloud and how to prevent the attacks using an effective way.

II. SECURITY ATTACKS ON CLOUD

Existing Attacks and its Solutions

Most of the organization uses Cloud platform to share their secrecy data with other external users. Many of the Cloud resources are not at all secure because of the external attacks that happen. Millions of hackers around the world are trying to steal the data from the cloud computing environment through external attacks. Following are the different types of existing attacks that happen in the Cloud and how the hackers are deny the services from the legitimate users.[3].

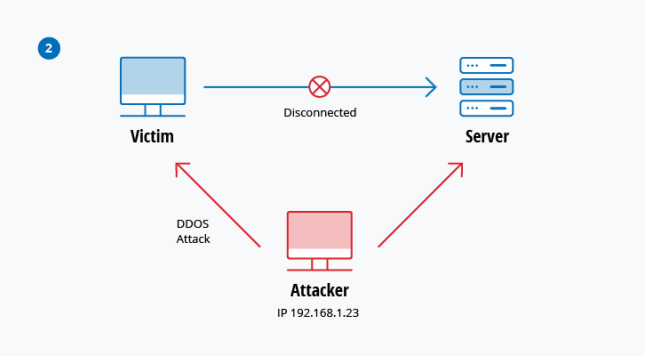
Denial of Service attack

In DoS attack, the external attacker tries to prevent the recognized user to access their resources in the Cloud environment. These types of attack, the huge volume of messages are sent by the attacker to close down the entire network of the legitimate user. The attacker sends invalid addresses with valid messages and the server will not be able to find out the exact user.

DoS attacks are affected by the victim machine in the following way:

(i) The external attacker can find some loopholes in victim software environment to access the service. [5]

(ii)Some of the DoS attacks completely destroy the bandwidth or resources of the user machine. [5]



Source: Netwrix Blog

Major types of DoS attacks are:
i). Attack from several sources like brute force or Classic DDoS. [7]
ii). Specific System exploit attack. [7] (Attack target on a pointed system like feed streaming, image rendering and content delivery etc)

DoS Attack avoidance
1. Prominent IDS: The Intrusion Detection System used should be accurate and up to date in nature. Based on the credential and behavioral factors, the machine needs to be able to locate the backend traffic and given an early warning to the

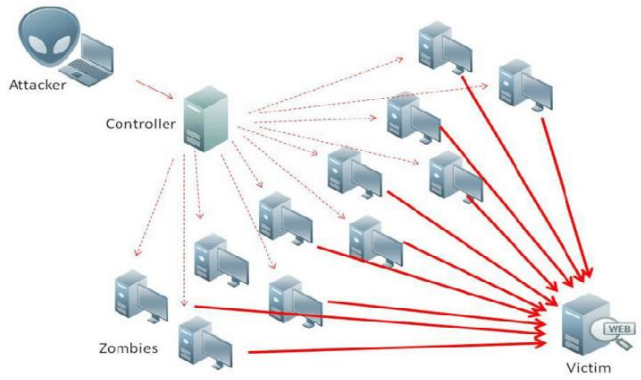
system. It is act as the Cloud Security Break- in alarm. [7]

2. Feature for Firewall Traffic type inspection: It will check the root and target for incoming traffic and also access the nature of traffic using tools like IDS. This feature is able to arbitrate good and bad traffic flow during the inspection.[7]

3. Limiting the Source Rate: One of the major issue faced with DoS attack is, it should consume the entire bandwidth. The source of the attack should be identified and block / limit the corresponding IP address.

Malware Injection Attack

In a malware injection attack, some of the code or service that already executed in the cloud that should be converted into mischievous code or service by the attacker. This type of external attack is also known as metadata spoofing attack. Here the attacker steals the data from the internet and pressurize the end users to load the baleful information instinctively without the knowledge of the user. This is one of the important attacks that inject the implementation of malicious service to the cloud [3].



Cloud Malware Injection Attack [10]

When a new client gets started with a cloud account, the cloud vendor automatically creates an image of the client's virtual system in the cloud repository. [10]

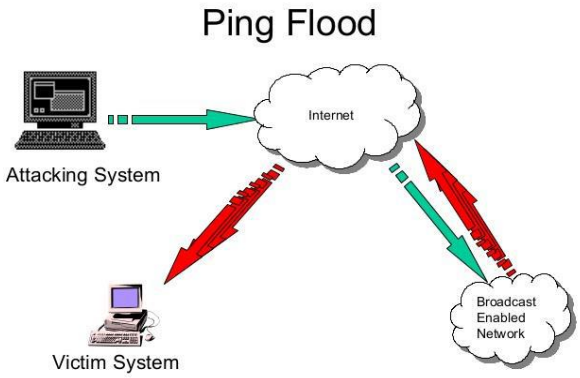
Solution of Malware Injection Attack

i). Creating an account and storing the same image in a cloud image storage environment prevents the exploitation of this process. The same image can be inspected and authenticated using the File Allocation Table.

ii). Another countermeasure is to store the account's OS type as the customer tries to open it. This method works by creating a crosschecking procedure that checks the account holders' O.S type against the OS type of the customer.

Flooding Attack

Flooding is a type of denial of service attack that occurs when a large number of traffic is initiated on a network or service. It causes the server or host to overload the memory of the system.



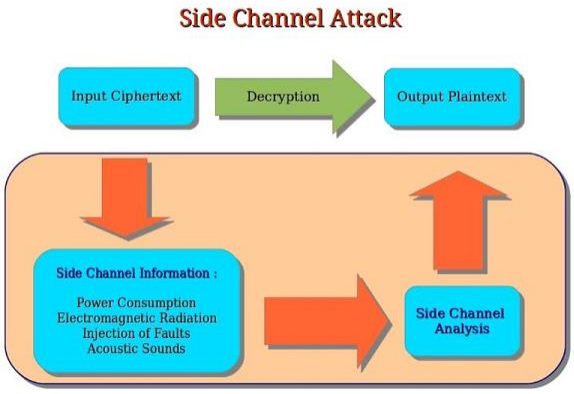
Flooding Attack [3]

Solution of Flooding Attack

The message passing technique prevents the flooding attack by preventing all the servers to communicate with each other.

Side Channel Attack

In order to place a malicious virtual machine that close to a target cloud server will create a side channel attack [11]. It is a security exploit that happens when performing the cryptographic operation and reverse engineer the machine cryptographic details while collecting information about an entire host machine.



Side Channel Attack [12]

Unlike other security attacks, side channel attacks are affecting both software as well as hardware platform. Instead of focusing vulnerability in software causes error in coding or mismatching codes, it will affect the hardware requirements like device operating system. This sort of attack can be affected any operating system like windows, Linux etc. [13]

Types of Side Channel Attack

i) Acoustic Cryptanalysis Attack

This component can monitor the emission of electronic circuits when the user is using the computer. It can also collect information about the power consumption and the electromagnetic fields emitted by the device.

ii) Cache Attack

In a physical system environment, cache attacks will exploits when and how the cache is processed.

iii) Fault Analysis Attack

These sorts of attacks that collects information from a system when fault occurs during computation of system.

iv) Timing Attack

This sort of attack that tracks the movement of data in CPU and memory.

Solution to Side Channel Attack

The virtual firewall appliance is combined with randomly encryption decryption to achieve the security against side channel attack. This combination will provide security from both the front and back end of the cloud computing architecture. [3]

Authentication Attack

The authentication attack is a soft and targeted issue in the virtual service platform. There are so many ways to authenticate a particular user in the cloud computing platform with or without knowing the user knowledge. By securing the authentication process, the main focus of the attacker is to target the mechanism and its methods. The IaaS architecture will be the most suitable platform other than SaaS and PaaS for secure data communication. [3]

Solution to Authentication Attack

Major authentication techniques are depending on the username and password mechanism to secure the web account or user account except some financial sites and banking websites uses some alternative way like 2 step authentication, shared secret password, virtual keyboard etc.

The below mention table shows the comparison of different attacks, reason for vulnerability, security violation areas and consequences.

Attack	Type of attack	Reason for Vulnerability	Security violation	Consequences
Denial of Service (DoS) attack	External/ Internal attack	Storage vulnerability Datacentre vulnerabilities	Virtualization level security Issues.	Software interruption and Modification. Unable to respond to legitimate service.
Malware Injection Attack	External attack	Loss of power and environmental control	Physical level security issues.	Hardware modification and theft
Flooding Attack	External/ Internal attack	RREQ or data flooding vulnerability.	Traffic flow level security issues as well as communication buffer overflow issues.	Network traffic congestion , no further connection made resulting DoS attack.
Side Channel Attack	Passive/ Active attacks	Operating System vulnerability	Using malicious VM to attack the cloud	It will affect both the hardware and software platform
Authentication Attack	Internal/ External attack	User data vulnerability, Access vulnerability	Data Breaches, Hijacking of accounts.	Unauthorized access, legitimate user issues.

Table 1: Compare and analyse the different types of attacks

Cloud services typically require some mechanisms to manage their identity and authentication, as well as their authorization and auditing. These elements are the core elements of IAAA, and they can be considered as stand-alone services. Most of the IAAA-related issues are cloud-specific and can be exploited by attackers with the proper credentials and account credentials.

In most cases, cloud computing providers don't have a mechanism that enables them to reset user credentials in the event of lost or forgotten credentials. The security features and procedures of Web-based apps and repair cloud services are often vulnerable to unauthorized access and actions. A faulty authorization check can allow an attacker to collect sensitive information from a user without requiring the user to provide specific credentials.

One of the main reasons why cloud services are prone to security issues is due to their management interfaces that are too coarse. This means that their users can no longer rely on predefined security measures.

Currently, there are no standards or mechanisms that allow cloud customers to manage and secure their logging and monitoring facilities. This issue can create a severe problem for customers as they cannot easily log and monitor all their events. This vulnerability is the first security issue that affects cloud services that puts user data in danger.

III. OTHER SECURITY RISK AND THREATS

Cloud Cyber Security Threats

In the future of Cloud environment, the following threats are seriously considering by the companies.

API Security flaws

APIs are the crucial element of SaaS Solutions. So they are specially useful as well as vulnerable. Business are going to become more vigilant while selecting the third party solutions and connecting them into their undeviating infrastructure. [8]

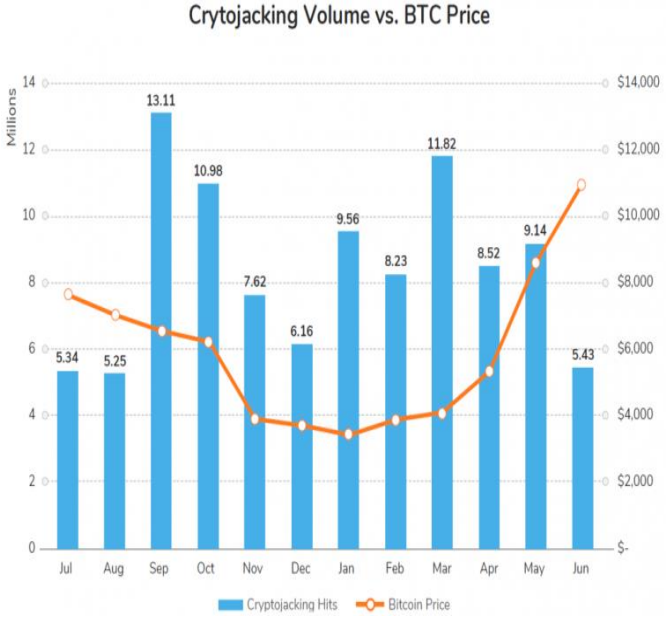
Out- of- the- Box Security

The issue has affected even with the biggest Cloud providers like Box. Even though Box offers a variety of security solutions, they are not enough to keep your data secure. [8]

Cryptojacking attack

Cryptojacking is a type of attack that started in late 2017 and is mainly focused on attacking enterprise cloud environments. The most notable attack that used this technique was the WannaCry worm. [8]

The mid- year Cyber threat report of the year 2019 shows that for the first six months of the year cryptojacking volume hit 52.7 million registered attacks. [9]



Source: mid-year update of the 2019 SonicWall Cyber Threat Report. [9]

AI Based attacks

AI has an upper hand in terms of security attacks due to its ability to detect and analyze the possible risks posed by Cloud computing. Due to its growing popularity, it is expected to carry out more attacks in the future. [8]

Ransomware

The ransomware attack are still affected with Cloud based platforms and it possibly a major threat in 2020. The big scale cloud providers like Google, Amazon and Cisco have huge amount of resources to defend these sorts of attacks in the cloud. These sorts of attacks may target both SaaS as well as IaaS platform. [8]

Unique Cloud Threats and Risks

- Reduced control and visibility from consumers
- Multiple talents fail separation
- Deletion of data is incomplete

Cloud and On-premise Risks and Threats

- Attackers may have stolen the Cloud credentials

- IT Staff complexity strain increases

- The supply chain of CSP is compromised

-Cyber security risk increase rapidly because the insufficient Due Diligence.

VI. CONCLUSION

This survey will discuss about an overview of the Cloud Computing Security Threats, attacks and countermeasures. Cloud security issues and its challenges are one of the major research areas now to focus on. A lot of research is going on to address the challenges like Cloud Security, Attacks on Cloud Environment, Cloud Computing Storage security etc. In this paper we discuss some of the major Cloud attacks like Cloud Malware Injection attack, DoS attack, Side Channel attack, Flooding, Authentication attack and its feasible countermeasures to avoid such type of attacks. The concepts we have discussed here will be able to get clear idea about the types of attacks and how we can prevent such attacks in an economic way.

REFERENCES

1. Survateja, P. S. (2018). Threats and vulnerabilities of cloud computing: a review. *International Journal of Computer Sciences and Engineering*, *6*(3), 297-302.
2. Ahmed, M., & Hossain, M. A. (2014). Cloud computing and security issues in the cloud. *International Journal of Network Security & Its Applications*, *6*(1), 25.
3. Kumar, P. (2016). Cloud computing: threats, attacks and solutions. *International Journal of Emerging Technologies in Engineering Research (IJETER)*, *4*(8), 24-28.
4. Ahmed, S. T., Kumar, V. V., Singh, K. K., Singh, A., Muthukumaran, V., & Gupta, D. (2022). 6G enabled federated learning for secure IoMT resource recommendation and propagation analysis. *Computers and Electrical Engineering*, *102*, 108210.
5. Parveen, A., Ahmed, S. T., Gulmeher, R., & Fatima, R. (2021, January). VANET's Security, Privacy and Authenticity: A Study. In *Proceedings of the First International Conference on Advanced Scientific Innovation in Science, Engineering and Technology, ICASISET 2020, 16-17 May 2020, Chennai, India*.
6. Sqalli, M. H., Al-Haidari, F., & Salah, K. (2011, December). Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing. In *2011 Fourth IEEE international conference on utility and cloud computing* (pp. 49-56). IEEE.
7. Deshmukh, R. V., & Devadkar, K. K. (2015). Understanding DDoS attack & its effect in cloud environment. *Procedia Computer Science*, *49*, 202-210.
8. Al-Shammari, N. K., Alzamil, A. A., Albadarn, M., Ahmed, S. A., Syed, M. B., Alshammari, A. S., & Gabr, A. M. (2021). Cardiac Stroke Prediction Framework using Hybrid Optimization Algorithm under DNN. *Engineering, Technology & Applied Science Research*, *11*(4), 7436-7441.
9. Ahmed, S. T., Ashwini, S., Divya, C., Shetty, M., Anderi, P., & Singh, A. K. (2018). A hybrid and optimized resource scheduling technique using map reduce for larger instruction sets. *International Journal of Engineering & Technology*, *7*(2.33), 843-846.
10. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/
11. https://theappsolutions.com/blog/development/cloud-security-risks/

MILESTONE RESEARCH PUBLICATIONS