Acta Scientific COMPUTER SCIENCES

Volume 5 Issue 1 January 2023

Review Article

Analysis and Survey of Eavesdropping on Cloud Platform and Software as a Service with Security

Sudipta Dey[1]* and Tathagata Roy Chowdhury[2]

[1]Student, Final Year, Department of Computer Science and Engineering, Brainware University, India

[2]Assistant Professor, Department of Computer Science and Engineering, St Marys Technical Campus, Kolkata, India

***Corresponding Author:** Sudipta Dey, Student, Final Year, Department of Computer Science and Engineering, Brainware University, India.

Received: November 24, 2022

Published: December 26, 2022

Abstract

In this paper, the cloud security with different authentication techniques had been discussed including the models of cloud infrastructure and the securities on those models. This paper focuses on the different attacks which are probably possible at the cloud end and the user end. Here, the attacks like Eavesdropping, Spoofing, DoS or DDoS along with some recent incidences throughout the world had been analyzed in addition to the analytical way to solve those attacks and the probable ways to prevent them.

Keywords: Cloud; Security; Authentication; Platform; SaaS; PaaS; IaaS; Spoofing; Eavesdropping; Dos

Introduction

Basics of cloud

Actually, cloud does not refer to any physical entities; cloud is a term which is used for describing a network of servers with unique functions. That means, cloud refers to a wide network of servers which are under a single system and can be controlled residing at any part of the world. These servers can be useful by storing data with management capability, running applications or delivering services like streaming videos, software, web mail etcetera. The files and data can be accessed online instead of personal computers which will be available around the globe.

Public cloud points towards sharing resources and offering services using internet towards the public. However, private cloud is opposite to the public cloud which does not refer to share resources and offer services to the public network but the private cloud operation is possible in the internal network mainly on-premise architecture. But hybrid cloud offer services between public and private clouds according to the purpose.

Platform as a service (PaaS)

Platform as a Service (PaaS) allows focusing on the deployment and management of applications pulling out the necessities of organizations in order to manage the infrastructure like hardware, operating system which lies under the hood. Moreover, it makes us more efficient by sharing the headache of resource procurement, software maintenance, patching, planning of capacity and so on. In a nutshell, PaaS provides the infrastructure along with the platform to develop an application through cloud.

AWS Lambda is an example of PaaS providing robust services enabling developers to use every AWS platform services.

Benefits

- The availability of the environment of developing an application saving users' time and money.
- Platform maintenance and backup services are done by cloud technology and users do not need to worry
- The users can access the infrastructure from the cloud as it is stored in the cloud directly.
- Flexibility in application development according to the users' need.

Disadvantages

- Dependency grows on functional capabilities, speed and reliability of provider
- The rising of the problems of compatibility can occur when the existing infrastructure is included into a new environment
- Security questions may arise due to its availability in the public environment

Software as a service (SaaS)

Actually, it is a software distribution model where the software hosted over the internet for making the application discoverable to the clients. In order to take the taste of this model, one shall need to have the access to the application in an addition to its security, availability, performance which is managed by provider.

Benefits

- One can have the ability to use the application with the help of network without the installation of any software
- Data can be accessed through the internet using any devices
- Same data warehouse cab be accessed.

Disadvantages

- It is hard for integrating with existing applications and services
- Security risks are there as it is publicly available
- Having no operational control

Security in cloud

Authentication

Authentication is nothing but a process through which the user can be identified by asking some credentials like username, password. There are some common methods to put authentication on console port, AUX port or vty lines. It can be controlled by network administrators how a user should be authenticated if someone wants to have the access. A default or customized method list for authentication can be used in case of specifying the method decided for authentication.

Authorization

Authorization provides abilities to ensure policies after the user has gained the access on network resources through authentication. That means, authorization used for the determination of the user's access of resources after successful authorization along with the operations to be performed by the user.

Accounting

At first, accounting refers to the monitoring and capturing the user events after accessing. Also, it monitors the user's longevity of access over the network resources. Actually, it is possible to create an accounting method list what should be accounted in an addition of whom the records should be sent.

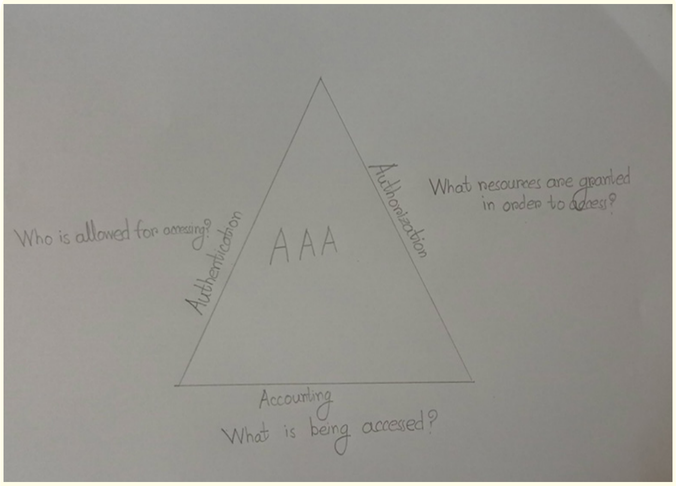
AAA
Authentication
Who is allowed for acessing?
Authorization
What resources are granted in order to access?
Accounting
What is being accessed?

Figure 1: Security details in cloud.

Different attacks on cloud

Spoofing

We are being observed by the artificial satellites launched on the space after receiving our information like real-time location and this type of information is used in many fields; communication system one of the most famous field. The receiver might receive misleading information if there are some problems are found in the navigation system of satellite which shall might be dangerous to us and spoofing attack is one of them where the receiver end will might get misleading information assuming the sender a trusted face. Because of having data transparency carried in satellites used for civilians, misuse of information may lead to damage of the society. The attackers deliberately hamper the information because of wrong intention after being the middleman between the sender and receiver end.

Eavesdropping attack

Now-a-days, the packets of data communications are recorded legally which is also known as network eavesdropping. This is done mainly security reasons of a country through which criminals can be punished and reduce the crime rate. Actually, this is a type of attack which is the act of recording or tracking someone without informing. There are certain ways in order to eavesdrop or sniffing someone and hacking devices is one of the most famous techniques of eavesdropping; also known as snooping where devices connected with audio and video devices are being hacked and safely handover to the legal authorities. But if this attack is done illegally, it shall might lead to the multiplication of crime rate by which the sovereignty of a country may be hampered.

DoS attack

Today, cloud is a rising technology and entrepreneurs are shifting their web- based works on cloud. But it is heading towards the security related issues as the cloud vendors can access those resources; DoS attack is one of them in this case which refers to the attempt of snatching the access of network. In this case, the business organizations must focus on the security cases of cloud because of giving access to the cloud vendors.

Advantages and disadvantages of spoofing attack

As spoofing attack refers as the act of being someone else in order to gain confidential information; a spoofing attacker might cause damage to the society even the sovereignty of a country might be in danger. For an example, a person will might be looted by being biased to wrong place through the spoofing attack. In fact, a GPS based weapons of any military can be used to that country because of stealing secret information by doing spoofing attack. Also, looting a bank or aeroplane hijacking can happen by successfully implementing spoofing attack plan.

Despite of all drawbacks of spoofing attack, spoofing attackers can be used for the wellbeing. Any hijacking can be stopped using spoofing attack by being aliasing to be someone else. Additionally, the sovereignty of a country will be in safe hand by biasing the enemies of a nation.

Advantages and disadvantages of eavesdropping attack

A person who is suspected of doing illegal works like selling drugs illegally, human trafficking and so on can be proved whether that person is a criminal or not by eavesdropping the telephonic conversation or stealing the texting information through mobile. In fact, by legalizing the eavesdropping, the groups of law enforcement team can decrease the crime rate of a country.

On the contrary, an eavesdropping attacker can hamper the confidentiality of the military troops of a country and that attacker might handover that secret information to the enemy troops. In a nut shell, violation of privacy right will be caused.

Spoofing and eavesdropping comparison

Both spoofing and eavesdropping attack can be harmful for the society if the intentions of those attackers are not good though the welfare of the society is possible using those attacks.

For eavesdropping attack, one must need to hack the devices so that the attacker can successfully eavesdrop which is also a crime if it is not done legally. For an example, if an attacker tries to steal the business documents like balance sheet, that attacker will might need to hack the website ir the account on social media platforms so that a criminal activity can be successfully done. In case of spoofing attack, heinous activities like hacking are not necessary. All it is needed to be the middleman between the sender end and receiver end of a communication tool to be aliasing someone else or acting as a trusted contact; at least multiple illegal activities is not necessary. In fact, one can be safer from spoofing attacks through machine learning; it can be easily distinguished if we go through stopping spoofing attack like email spoofing which email messages are vulnerable.

DoS and spoofing comparison

DoS and Spoofing attacks both are illegal to all if these are not done with the legal permission. In case of DoS attack, one must need to send huge amount of traffic in order to slow down or stop the sever. In fact, the attacker’s location cannot be traced easily because of arbitrary distribution of the systems where the attackers are sitting and this is an extension of DoS attack knowing as DDoS attack which motivates ransom; ultimately it causes economical loss to a person because of having difficult detection of attackers. Bur after looking spoofing attack at a glance, it can be lower if we use training sets to dtect in the communication medium which message contains spoofing or not.

Analysis of spoofing attack on recent case

A well-known company noticed a cyber attack in order to steal the details of some employees who work at Twilio by fooling them which then helped the cyber attacker to access the data of customers. Twilio noticed this sophisticated attack on 4th August in 2022. By using those credentials, the attackers then gained the ability of accessing the internal system of Twilio. Some current and former employees reported to receive text from the IT department of that company which motivated them to go for the investigation. They continued to alert the customers about the attack specially those who were being attacked. The text was like renewing passwords using the URL sent by the attackers which seemed like the message was sent from Twilio as the attackers used words on the URL like "Twilio", "SSO", "Okta" to fool the victims to click on the link created by those attackers. These text messages had come carrier networks of United States where they worked with the carriers to stop the attackers by shutting down the accounts of the attackers. Through this attack, Twilio came to know that they had good knowledge on attacking for matching the names of employees from the source.

Twilio came to know about the same attack from other companies. After working with the US carrier network to shut down the accounts of the attackers, the attackers then tried to rotate the carriers

Action of Twilio on that attack

The security team of Twilio revoked access to those employees account who were the victims. Even a forensic team was busy with them on their investigation. They made their security training more effective to be in safe position for this type of attack including awareness programs on social engineering attacks. They also issued security advisories to take measurement in case securing the site of Twilio. They were also observing the customer's data as the attackers had accessed the internal systems of Twilio. They also notified the customers mentioning that they shall ask or update security credentials on their portal.

Analysis of eavesdropping attack on recent case

A news on 1st August of this year has been updated that the police force of Israel had used Pegasus which is a powerful tool Developed by NSO group of Israel in order to keep eyes on prominent figures. The Israeli police also accused to target dozens of people who were not suspected to crime and this had been said by Calcalist. Calcalist also included some public figures or senior leaders of finance ministry, justice and communication ministries, mayors on their report. Avener Netanyahu who is a son of one of the former premier also expressed his news of being shocked by posting on Facebook after he came to know about this incident. But the justice ministry denied these claims as there was no proof of illegal activities by the police like hacking the phones according to the report of the Calcalist who brought the claim. NSO consistently denied this type of scandal made using the Pegasus including that they do not operate the system once they have been sold to someone. The point to be noted that Pegasus is a surveillance tools to harvest data through the camera of phone.

Deputy Attorney General Amit Marari who led the investigative team expressed to have no indication to eavesdrop personal phones without judicial order. But it was said to use that tool without any warrants. After that, the US had blacklisted the group.

Analysis of DDoS attack on recent case

Since the starting of Russia's attack on Ukraine, DDoS attacks have become a rising threat across the world which has been observed by world experts like Infosec and CISA (Cybersecurity and Infrastructure and Security Agency) specially some attacks from the attackers from Russia.

The first attacks has been observed few days before the attack was executed in February targeting the government and commercial websites from the Russian attacker. A global internet monitor named NetBlocks identified more than one region that have been targeted highly. It not only tracked DDoS attacks which had down the servers by 15 to 20% but also noted those zones where the connectivity has been dropped to zero. Even some larger disruptions had been observed on the cities like Kyiv, Luhansk, Mariupol. Threat actors also targeted national telecom provider Ukrtelecom; around 13% drop in late March had been seen by Ukrtelecom.

Rate of attacks

Separately, Cloudflare and Kaspersky analyzed the growth of DDoS attack during the beginning of moths of 2022. They came to the point that application-layer attack has been raised around 164% year over year and 135% quarter over quarter and the network-layer attack has been grown up to 71% approximately year over year but had gone down to near 58% quarter over quarter.

According to the overall report of Kaspersky, around 450% increment of DDoS attack had been observed from the 1st quarter of 2021 to the 1st quarter of 2022. The report also noted that the duration grew nearly 8000% higher than 2021.

Targeted nations

With Ukraine, multiple allied nations like United Kingdom, Italy, Romania, United States, a Russian group named Killnet launched DDoS attacks on those countries. They even declared war on ten countries around May, 2022.

Some tools for cloud security

Recent trends like work from home and cloud-native applications have put the cloud security tools on the spotlight. Maximum cloud security tools offer Web Application Firewall (WAF), misconfiguration monitoring, access control and different functionalities focusing the basics mainly.

Zscaler

This is a household name and regarded as one of the best cloud security providers in the market. It offers in four pieces. Those are:

- Zscaler Internet Access (ZIA)
- Zscaler Private Access (ZPA)
- Zscaler Digital Experience (ZDX)
- Zscaler Cloud Protection (ZCP).

These services can be subscribed in a bundle or separately.

Orca security

Instant setup without agent on cloud-based system is the key speciality of Orca Security. Agent-based security systems are less suitable for cloud applications specially serverless cloud based applications. The context-based security alerts of Orca Security attract the customers more.

VIPRE

VIPRE is also one of the most trusted security solutions in the cloud industry. Along with sophisticated architecture, VIPRE also provide security trainings which is one of the most effective tools for human being.

Analytical way to prevent those attacks

Eavesdropping Attack

Encrypting data

In order to access encrypted data, an encryption key is required. So, in that case, it shall be hard to decrypt personal information if the personal information is compromised. For an example, it is good to use HTTPS for websites.

Using updated software

The more software is updated; the software tends to be more secured because of lowering the vulnerabilities as loopholes on a system are good for attackers.

Spreading cyber security knowledge

Internet has become needs in the last few years. However, a huge number of people show less interest on taking steps in the case of preventing cyber attacks like eavesdropping attack because of having the lack of cyber knowledge. Avoiding shady links, strong passwords along with frequent changes on them- these are some practices to prevent eavesdropping.

Spoofing attack

Staying alert

Staying alert can prevent spoofing attacks. Having the knowledge on spoofing attacks in detail will be fruitful to lower the chances of being attacked as the reason of acknowledgement of alert.

Hiding IP address

Developing the habit of hiding IP addresses in the time of web surfing can help to prevent spoofing attacks like IP spoofing.

Securely opening unusual attachments

Before opening unknown attachments on email that is unknown, one must examine if that email from the known people or not.

Using virus defenders

A good virus defender helps to detect threats in devices and ultimately, it shall make spoof proof.

DDoS attack

Keeping eyes on warning signs

- Low connectivity
- Crashes

- Unusual traffics
- Slow response.

These are some common signs of DDoS attack. If these traits can be detected in time, correct measurements can be taken.

Network traffic monitoring

- Live monitoring helps to detect DDoS attacks before going out of hand
- The security team can easily identify unusual activities having deep look on daily network activities or operations.

Improving security levels of network security

- Correct use of firewalls and intrusion detection systems
- User trusted anti-virus and anti-malware software which removes viruses and malwares
- Correct uses of web security tools.

Conclusion

To sum up, some terminologies regarding the rising technology Cloud have been described through this paper with some possible attacks in addition. Moreover, there are some possible analytical ways by which it is possible to take prevention on those attacks which has been discussed through this paper [1-14].

Acknowledgment

For the guidance of completion of my paper, I should like to express sincere gratitude to Mr. Tathagata Roy Chowdhury who is an Assistant Professor of Computer Science and Engineering. Special thanks to my mother for her motivation and inspiration to head towards research work.

Bibliography

1. Marinescu Dan C. “Cloud computing: theory and practice”. Morgan Kaufmann, (2022).

2. Achar Sandesh. “Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape”. *International Journal of Computer and Systems Engineering* 16.9 (2022): 379-384.

3. Marinescu Dan C. “Cloud computing: theory and practice”. Morgan Kaufmann, (2022).

4. Kati Sherwin., *et al*. “Comprehensive Overview of DDOS Attack in Cloud Computing Environment using different Machine Learning Techniques”. Available at SSRN 4096388 (2022).

5. Kumari Sushila., *et al*. “Analysis of Cloud Computing Security Threats and Countermeasures”. 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). IEEE, (2022).

6. Alashhab Ziyad R., *et al*. “Distributed Denial of Service Attacks against Cloud Computing Environment: Survey, Issues, Challenges and Coherent Taxonomy”. *Applied Sciences* 12.23 (2022): 12441.

7. Wang Qingxuan and Ding Wang. “Understanding Failures in Security Proofs of Multi-factor Authentication for Mobile Devices”. *IEEE Transactions on Information Forensics and Security* (2022).

8. Sriram GS. “Resolving security and data concerns in cloud computing by utilizing a decentralized cloud computing option”. *International Research Journal of Modernization in Engineering Technology and Science* 4.1 (2022): 1269-1273.

9. Najm YA., *et al*. “Cloud computing security for e-learning during COVID-19 pandemic”. *Indonesian Journal of Electrical Engineering and Computer Science* 27.3 (2022): 1610-1618.

10. Kati Sherwin., *et al*. “Comprehensive Overview of DDOS Attack in Cloud Computing Environment using different Machine Learning Techniques”. (2022).

11. Mirkovic J and Reiher P. “A taxonomy of DDoS attack and DDoS defense mechanisms”. *ACM SIGCOMM Computer Communication Review* 34.2 (2004): 39-53.

12. Masdari Mohammad and Marzie Jalali. “A survey and taxonomy of DoS attacks in cloud computing”. *Security and Communication Networks* 9.16 (2016): 3724-3751.

13. Abusaimeh Hesham. “Security Attacks in Cloud Computing and Corresponding Defending Mechanisims”. *International Journal of Advanced Trends in Computer Science and Engineering* 9.3 (2020).

14. Somani Gaurav., *et al*. “DDoS attacks in cloud computing: Issues, taxonomy, and future directions”. *Computer Communications* 107 (2017): 30-48.