National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Brief Study on Cloud Security

Harlin Sheeba. M
Department of Computer Science, Darshan college R.V College Post, Mysore Road, Kengeri, Bangalore, Bangalore University, Karnataka, India

ABSTRACT

Cloud security is a protection of data, application, and network into the cloud environment (whether it's a public, private or hybrid cloud). In the cloud environment resources are shared among servers, users and individuals since the data centre of cloud provider is spread all over. We can access the data from any corner of the world. Even though cloud computing is becoming popular, security concerns start to arise. While using the cloud infrastructure the client gives up the control to the cloud provider on many issues which may affect security. The most critical one is when the owner starts to lose the control of information which is spread into the cloud.
This article briefly explains about how to get the advantages and benefits of cloud computing technology while getting rid of disadvantages like data, network and application attacks. It describes the security issues associated with cloud and cloud security providers like AWS (amazon web service) platform.
Keywords : Issues related with cloud Security, Cloud security attacks, Encryption and Security, Cloud Security control, AWS platform.

I. INTRODUCTION

Cloud security means keeping your data stored online safe. According to the recent study the average cost of a data breach worldwide now equals $ 3.86 million. However, the number vary greatly from country to country.

When it comes to security, timing is everything. The earlier you detect and fix the problem, the safe you are.The cloud technology is facing many technological challenges in different aspect of data and information handling and storage.

As you can see, knowing about the possible dangers are being ready to react to them fast can be a real lifesaver so, in this paper you will study about the security issues in the cloud you should be ready to face.

Cloud security issues

Virtualization:

It refers to the creation of a virtual resources such as server, file, storage, network. virtualization changes the definition of what the real resources is, so security is no longer trying to protect the privacy. The lack of

visibility and control over virtual networks is the main issue in the cloud security.

1. Access control and identity management:

Access control in the cloud security is a system with which the owner can regulate and monitor permission to access the data by formulating various policies. The owner should control unauthorized user access.

Identity management has to check whether it is a valid user, what does the user wantto do and what access does the user need to do his job.

2. Weaker authentication:

A lack of proper authentication is responsible for data breach multi-factor authentication system, like one-time password and phone-based authentication, protect cloud services by making it harder for attackers to steal the password. This isa preventative discussion that every business that has a online presence should have to ensure the safety of its customers.

1) Cloud security attacks:

- Data Attack
- Application Attack
- Network Attack

Data attack

1.a. Data breach:

A data breach is possibly the most important cloud security concern. When unauthorized user or program gains access over confidential data and can view, copy or transmit it leads to attack.

1.b. Data loss:

Data loss often happens due to physical destruction or it can also be a result of a target attack. It may also lead to permanent loss of data without backup.

1.c. Data removal:

Both the data of an individual or a company will be removed from the cloud. Unauthorized disclosure of data is dangerous if the cloud contains sensitive data.

1.d. Data Theft:

Data theft is the illegal transfer or storage of any information that is confidential, personal or password. The data can be theft by portable hard drive, memory cards, remote sharing and by USB drive.

1.e. Data integrity:

When a data is on a cloud anyone from any location can access those data. Then cloud does not differentiate between a sensitive and a common data thus enabling anyone to access those sensitive data's. Thus, there is lack of integrity.

1.f. **Data location:**

When the user uses the cloud, user probably won't know exactly where the data is hosted and where it will be stored.

2. Application attack:

2.a. Cloud Malware Injection:

This attack focuses on injecting a service implementation or evil virtual machines to the cloud environment. The main goal of this type of attack is to take control over the victim's data in the cloud, so the attacker uploads a crafted and tricks the image to be a part of the victim's cloud environment. After the user request will start forwarding to it causing the vulnerable code.

2.b. Cookie Poisoning:

Cookies stored on your computer's hard drive maintain a bit of information on that allows website you visit to authenticate your identity. Cookie poisoning is the modification of a cookie personal information in a web user's computer byan attacker. To gain unauthorized information about user for purposes such as identity theft. The attacker may

use the information to open a new account or to gain access to the user's existing accounts.

2.c. backdoor:

Another threat on a virtual environment empowered by cloud computing is the use of backdoor virtual machines that leak sensitive information and can destroy data privacy.

2.d. Hidden File Manipulation:

A developer working on the application could possibly assume the information will stay unharmed in the hidden field. However, a hacker can subsequently alter that using a common HTML editor.

3. Network level attack

3.a. Network Sniffing:

Sniffing involves inspecting, capturing, decoding and interpreting the information inside a network. The sole purpose behind this is to steal information which is very usual in the form of user id, password, network detail. This attack can be silent or invisible on the network.

3.b. IP Spoofing:

Sending and receiving the internet protocols(IP) packets is a primary way in which networked computers and other dives communicate.it consist a header and important routing information including the source address. If the packet has been spoofed, the source address will be forged.

3.c. Man in the middle:

It occurs when the third-party places itself in the middle of a connection and intercept or modify communication between the two

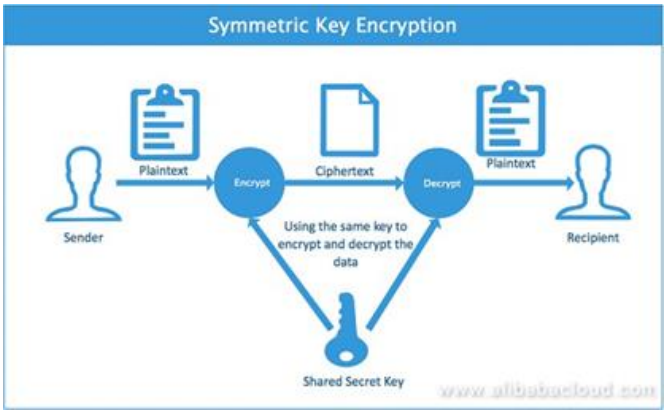
Encryption and security

When the data and information is shared through a network that data can be hacked so, encryption is used to make the data safe and secure.

There are two types of encryption:

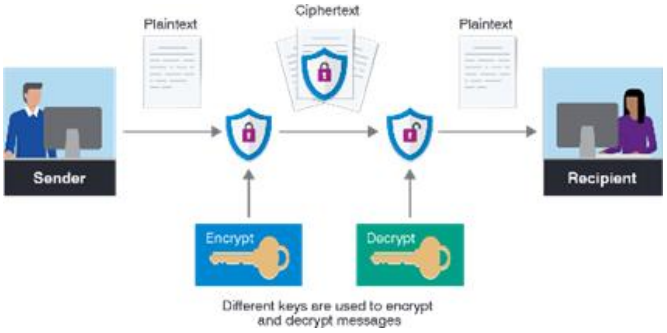
- Symmetric encryption
- Asymmetric encryption

1. Symmetric



When the same key is used for both encryption and decryption it is known as symmetric and it is also known as secret key cryptography

2. Asymmetric:



It uses public key for encryption and private key for decryption, it is also called as public key cryptography.

Encryption is regarded as one of the most effective approaches to data security.

Scrambling the content of any system, database, or a file in such a way that it's impossible to decipher without a decryption key. By applying encryption and practicing secure encryption key management, companies can ensure that only authorized users have access to sensitive data.

Even if lost, stolen, or accessed without authorization encrypted data is unreadable and essentially meaningless without its key.

Security

1. Data security:
It focuses on protecting the software and hardware associated with the cloud. It should secure from physical attack and external treats avoiding unauthorized access.

2. Application Security:
The measures taken to improve the security of an application often by finding, fixing, and preventing security vulnerabilities.

3. Network security:
Protecting the network over which cloud is running from various attacks like IP spoofing. Attack on data affects a single user whereas a successful attack on the network has the potential to affect multiple users, therefore network security is of foremost important.

Cloud security controls

1. Detective Control:
It helps to address the issues to detect and react instantly and appropriately to any attack.

2. Deterrent Control:
It means to reduce the purposeful attack on the cloud system, it reduces the threat level by giving a warning sign.

3. Preventive Control:
It is the strength of the system against any attack from vulnerabilities. It reduces the extent of potential damages and reduces the chances of attack.

4. Corrective Control:
It reduces the consequence of an attack by controlling/limiting the damage.

2) AWS platform

Amazon web Service(AWS) is the world's most broadly adopted cloud platforms. Millions of customers trust AWS to their power infrastructure.

Cloud security at AWs is the highest priority. As an AWS custom will benefit from a data centre and networkarchitecture built to meet the requirements of the most security of sensitive information.

3) Benefits:

1. **Keeps your data safe**: The Aws infrastructure puts storing safeguards in the place to help and protect privacy. All the data are stored in highly secure AS data centres.
2. **Saves money:** Cut cost by using Aws data centres, maintain the highest standards of security without having to manage yourown facility.
3. **Scale quality**: Security scales with your Aws cloud usage. No matter the size of your business the Aws

infrastructure is designed to keep your data safe.

4. **Cloud directory**: It enables you to build flexible, cloud directories for organizing hierarchies of data.
5. **Organizations**: It helps you to create group of AWS accounts that can use to more easily manage security and automation setting.
6. **Guard duty**: Provides intelligent threat detection to protect your AWS accounts

Amazon web service is a secure cloud service platform, offering compute power, database storage, content delivery and other functionality to help every organization.

In simple AWS allows you to do the following:

1. Running web and application server in the cloud to host dynamic website.

2. Securely store all your files on the cloud so you can access them from anywhere.

3. Using managed database like MySQL, oracle or SQL server to store information.

2. Adjust cloud access policies as a new service come up.

3. Remove malware from a cloud server.

4. Deliver static and dynamic files quickly around the world using a content delivery network(CDN).

Measures for cloud security

- Understand cloud usage and risk:
- Protect your cloud:

1. Data protection

2. Encrypt sensitive data

3. Set limitation on shared data.

4. Stop data from moving to unmanaged devices you don't know about.

5. Apply advance cloud provider.

• Respond to cloud security issues:

6. Require additional verification.

II. CONCLUSION

This paper gives a complete understanding about how the cloud security is attacked and it is clear that cloud security issues are increasing. To achieve complete security a organization or an individual should check their cloud infrastructure every time (not only if something happens) and to make sure to keep it up to date. Also, choose reliable cloud security provider with advanced version.

III. REFERENCES

[1]. www.skyhighnetworks.com
[2]. www.veracode.com
[3]. www.cloudcomputing-news.net
[4]. www.w3schools.in
[5]. www.techopedia.com
[6]. www.sciencedirect.com
[7]. http://www2.gemalto.com/cloud- security/
[8]. http://zerotoprotraining.com

Cite this article as :

Harlin Sheeba. M, "Brief Study on Cloud Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 27-31, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT19475