Open access Journal International Journal of Emerging Trends in Science and Technology
IC Value: 76.89 (Index Copernicus) Impact Factor: 4.219 **DOI:** https://dx.doi.org/10.18535/ijetst/v4i6.05

Security Issues in Cloud Computing

Authors
P.Joseph Charles[1], Meenakshi.K[2]
[1]Asst. Prof in Info Tech, St.Joseph's College, India
[2]PG Student, Dept of Info Tech, St.Joseph's College, India

ABSTRACT
Safety and security are the two important things in everyone's life in today's scenario. More and more organizations are moving towards cloud network as they find it very difficult to maintain the records. But, reducing the duty comes with lot of other problems. The first and the foremost being the data security. Exposing important data to the third-party providers makes it difficult for the organization because nothing can be maintained as a secret. There may be many chances of hacking too. There are many ways where the privacy is disturbed when it comes to the data security in cloud. These are the problems that must be dealt with when it comes to data security in cloud.
Keywords: *cloud, data security, cloud network, third-party provider.*

INTRODUCTION

The cloud services have been growing in a faster rate because the data is also growing every second. Many organizations and companies were finding a way to find a solution for the problem. Hence, arrived the cloud which hiped in storing a large amount of data.

Not only data cloud environment can be used in any form it can be used as software and also infrastructure. But it is mostly used to save the data in larger scale. However, security is one of the most factors that is not found in cloud. Keeping the data in cloud means the privacy of the data is damaged.

Privacy and security in the cloud has become a big threat since the data are being maintained by some third party. By saving the data in the third party service provide server there are many chances that the data will be changed based on the will of the provider and also he can have an upper hand in any organization because of this data.Security has been at the core of safe computingpractices.When it is possible for any unwanted party to 'sneak' on any private computers by means of different ways of 'hacking'; the provision of widening the scope to access someone's personal data by means of cloud computing eventually raises further security concerns. Cloud computing cannot eliminate this widened scope due to its nature and approach.

This lead to the security breach in the cloud computing. There are some threats which may cause a serious threat to the cloud.

SECURITY ISSUES IN CLOUD

DATA BREACHES

Cloud environments faced the same threats as the normal database environment. Data breaches may cause to expose some financial activities of an organization out to open. When there is a data breach, the company may incur fines and law suit charges.

Though the cloud service provider has certain duties but the ultimate will come to the organization to the organization as they are responsible for the problem if anything occurs during data breach.

HIJACKING OF ACCOUNTS

Hijacking of accounts means using the login and password without the one's wish. Using the stolen

password the attackers can use the data to their malicious activities. By hijacking the account the attacker will be able to manipulate the data, insert the false data and also redirect the data to the illegitimate clients.

Cloud hijacking can effect the organization in a higher rate. Legal complications are also possible in case of big industries, if the data is being laundered then it is considered as a serious crime and not only that the name of the organization will also be damaged in these cases which will result in the heavy loss of the company.

INSIDER THREAT

Threat inside the organization does not likely to happen but there are many chances that it can happen. The employees can use their own login and they can access their companies cloud and access the unwanted information such as customer accounts and some other sensitive information. There are certain ways through which they can implement a secure strategy, such as business partnerships, prioritizing initiatives, controlling access, and implementing technology.

Cloud Services have vastly expanded the scope of insider threat. The sheer number of cloud applications and immature auditing and governance controls to relative to on-premise applications result in a broad range of vectors for data exfiltration.

MALWARE INJECTION

Malware injections are scripts or codes embedded in the system that can cause damages to the data in the system. This can be malicious and the attackers can eavesdrop and also change the records which may affect the company heavily. These malware can totally eradicate the data which will affect the organization in a larger scale.

ABUSE IN CLOUD SERVICES

Abuse in cloud has been a common occurrence since the cloud came into existence. Because the main problem in cloud that it does not contain any registration which makes it weak. Though enforcing strong registration policies in cloud is also found to be a difficult task.

To make the threat more abuse, as the cloud provides a free trial for the users to experience the cloud environment. But, the cyber criminals found it as a best time to abuse the data, which will be used by them for some illegal activities in future.

ACCOUNT HIJACKING

It is being taken place in a larger scale. Software and keeping everything in the cloud can affect the users in a larger scale. It is being taken place in a larger scale. Software and keeping everything in the cloud can affect the users in a larger scale. The key is to protect account credentials from being stolen.

PERMANENT DATA LOSS

The cloud security has been improved to a greater extent. The loss of data is also reduced. But, there are still hackers and attackers who can erase the entire data of the organization which will result in greater problem.

So, to protect the data should be in a distributed format. So, if one part of the data is getting affected. The other will be safe. Many organizations think that if they sent an encrypted data to the cloud then the data can be safe but once the key of the encrypted data is lost.

So, the organization must be aware of the problems and they should act accordingly.

DOS ATTACKS

DOS attacks have been around for many years but they gained a prominent place when cloud environment came in to picture. These attacks take a large amount of processing power and the consumer are the one whose has to pay the ultimate price. The main key is to plan the attack before it occurs. It will ensure the access to the resources when it is needed.

The DOS attack is mainly divided in to two types mainly Bandwidth depletion and Resource Depletion.

Bandwidth Depletion occurs mainly due to the bandwidth problem with is not legitimate. The bandwidth is also divided into flood and amplification attacks.

FLOOD ATTACKS

This attack is launched by an attacker sending huge volume of traffic to the victim with the help of zombies that clogs up the victim's network bandwidth with IP traffic.

For preventing a flooding attack, our proposed approach is to organize all the servers in the cloud system as a group of fleet of servers. Each fleet of servers will be designated for specific type of job, e.g. one fleet will be engaged for file system type requests, another for memory management and another for core computation related jobs, etc. In this approach, all the servers in the fleet will have internal communication among themselves through message passing. So when a server is overloaded, a new server will be deployed in the fleet and the name server, which has the complete records of the current states of the servers, will update the destination for the requests with the newly included server.

AMPLIFICATION ATTACKS

The attacker sends a large number of packets to a broadcast IP address. In turn causes the systems in the broadcast address range to send a reply to the victim system thereby resulting in a malicious traffic.

SHARED TECHNOLOGY, SHARED DANGERS

Shared technology poses a great threat to the cloud computing. Cloud service providers share everything. They share data layers, platforms, infrastructures and applications.

If one application or infrastructure gets collapsed everything collapses with it. Shared devices likes google drive, Drop box, Windows Azure makes the user or the organization to chare the data in it. Once sharing a single data the privacy is damaged then and there. But when it comes to the sharing of file via a three party nothing is kept secret. The organization and the user is giving all the rights to access their system.

To reduce the problems with shared technologies as data gets affected and to reduce now many organizations have come up with the idea of BYOD. Bring Your Own Device(BYOD) is a win-win situation by asking the employees to bring their own terminal. It saves the organizations their fund to buy new terminals, Stolen or misused it will directly affect the employees and not the organization. So, the employees will be more careful while handling these type of data may save the data in the cloud.

THE APT PARASITE

APT are nothing but Advanced Parasite Terminals. APT's infiltrate systems to establish a foot hold, then stealthily exfiltrate data and intellectual property over an extended period of time.

There are many entry points through which the data can enter the system which include spear phishing, direct attacks, USB drivers preloaded with malware, and compromised third- party networks.

Common points of entry include spear phishing, direct attacks, USB drives preloaded with malware, and compromised third-party networks. In particular, the CSA recommends training users to recognize phishing techniques.

MALICIOUS INSIDERS

An insider threat has many faces it could de anyone. They may be a present employee, a former employee, a system administrator, a contractor or even a business partner. In the cloud, they are hell bent in destroying the whole mass of data and they can even manipulate the data. The organizations which are solely depend on the Cloud service providers security are at a greater risk. Because, they can also able to manipulate the data.

If an employee copy's the significant data in his own device without knowledge then, it may also leads to some security problems in cloud.

COMPROMISED CREDENTIALS AND BROKEN AUTHENTICATION

Data breaches and other attacks frequently result from lax authentication, weak passwords, and poor key or certificate management. Organizations often struggle with identity management as they try to allocate permissions appropriate to the user's job role. More important, they sometimes forget to remove user access when a job function changes or a user leaves the organization.

Multifactor authentication systems such as one-time passwords, phone-based authentication, and smartcards protect cloud services because they make it harder for attackers to log in with stolen passwords. The Anthem breach, which exposed more than 80 million customer records, was the result of stolen user credentials. Anthem had failed to deploy multifactor authentication, so once the attackers obtained the credentials, it was game over.

CONCLUSION

In this paper, the security issues of the cloud is being discussed. The attacks which are present in the cloud security. Even though, many organizations use cloud because of the amenities they are providing in it. Some current solutions were listed in order to mitigate these threats. However, new security techniques are needed as well as redesigned traditional solutions that can work with cloud architectures. Traditional security mechanisms may not work well in cloud environments because it is a complex architecture that is composed of a combination of different technologies.

REFERENCES

1. Ricardo Puttini,"Cloud Computing: Concepts, Technology and Architecture", Prentice hall Publication, 2014.
2. 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*. Heidelberg: Springer Berlin; 2009:347–358.
3. I. Ennajjar, Y. Tabii and A. Benkaddour, "Security in cloud computing approaches and solutions", 2014 Third IEEE International Colloquium in Information Science and Technology (CIST), 2014.
4. H. Eken, "Security threats and solutions in cloud computing", World Congress on Internet Security (WorldCIS-2013), 2013.
5. L. Badger, T Grance, R. P. Comer and J. Voas, DRAFT cloud computing synopsis and recommendations, Recommendations of National Institute of Standards and Technology (NIST), May-2012.
6. F. Gens, New IDC IT cloud services survey: Top benefits and challenges, IDC exchange, February 2010.
7. Karthik Kumar, Yung-HsiangLU,"Cloud Computing For Mobile Users:Can Offloading Computation Save Energy" IEEE J, Computer Volume:PP , Issue: 99, 18 March 20 10.