International Journal of Computer Application (2250-1797)

Volume 7– No.1, January– February 2017

SECURITY ANALYSIS IN CLOUD COMPUTING

S.AROCKIA PANIMALAR

SRI KRISHNA ARTS AND SCIENCE COLLEGE

DEPARTMENT OF COMPUTER APPLICATION AND SOFTWARE SYSTEM

ASSISTANT PROFESSOR

J.YUGASHINI

IV M.Sc SS

ABSTRACT

Cloud computing is the web-based computing for sharing the data between the client and the server. Cloud computing is the structure for establishing the computer service through internet. It enables the user to share the distributed resources and services which belongs to different organization. Thus the open environment is used by the distributed resources, so that it is important to ensure the security and trust while sharing the data in the cloud. Security is the major played by the cloud while transferring the data. In this paper, security issues, challenges, risk and threat have been discussed. The measures taken to reduce the risk is also been discussed in this paper.

INTRODUCTION

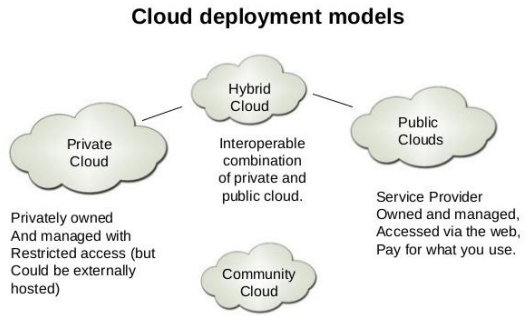
Cloud computing is an upcoming style of computing where applications, resources and data are provided to user as service over the web. The services provided may be available globally, for all time, low in cost, on demand, extremely scalable, pay-as-you-grow. Cloud computing is a technology that allows users to access software applications, stores information, develop and test new software, creative virtual servers, draw on disparate IT resources. Cloud platforms are offered by the cloud services providers (CSP's). The purpose of the cloud platform is for their customer to use and to create their own

websites. Cloud computing has three types of services (i.e) Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS).

Clouds are location-independent, providing abstracted versions of datacenter components that are not tied to a specific datacenter: virtual storage, virtual servers, virtual networking etc. a datacenter is a facility used to house computer systems and associated components, such as telecommunications and storage systems.

CLOUD INFRASTRUCTURE

Cloud computing infrastructure is built on the variety of level of virtualization technologies. It also consist the service delivering through the data centers. There are three basic types of services: private, hybrid and public.



PUBLIC CLOUD:

According to the customer premises, public clouds are hosted. Because this is the helpful way to reduce the customer risk and even provide flexible cost. Third party runs the public cloud. When performance, security, data locality are implemented in the public cloud, then the existence of the other application should be transparent to the end user and the cloud architects. The advantage of using the public cloud is ability to scale up and down on demand, and shifting infrastructure risks from the enterprise to the cloud provider,

The virtual private data center can be created by use of single client with the help of craving the part of the portion of public cloud. The infrastructure of the virtual private data center gives the greater visibility for the customer. Creating all the components with the same facility in the virtual private data center may help to reduce the issues from the data locality. This is because the when the resources are connected with the same facility then it will be free and the bandwidth is abundant.

PRIVATE CLOUD:

Private cloud is built for the purpose of the one client. It provides the security, data over control and quality of service. It is

been implemented in an organization. The infrastructure is owned by the company and the controls over applications are deployed on it. An enterprise datacenter is deployed by the private cloud. And they can also be deployed at a collocation facility. The advantage of private cloud choosing by the company is there is high level of control over the use of resources.

HYBRID CLOUD:

Hybrid is the combination of the public and the private cloud. It is externally provisioned scale. It mainly helps to provide the on-demand. To handle planned workload spikes, hybrid cloud is been used. Complexity of determination about how to distribute the application between both the public and the private cloud is introduced by the hybrid cloud. Hybrid cloud can be successful when there is small amount of data. For a small amount of process, large amount of data should be moved to the public cloud.

THREATS IN THE SECURITY

Cloud platform faces so many threats in their network due to the storage of the larger amount of data which has become the provider's attractive target. The following threats are be found in the security of the cloud computing in the upcoming days:

I. Data breaches:

Data breach involves sensitive, protected or confidential data which can be viewed, stolen or unauthorized user can be used. It mainly involves personally identifiable information (PII), personal health information (PHI), trade secrets or intellectual.

II. Compromised credentials and broken authentication:

The result of this threat is the authentication is no strictly provided. And some other issues are week password, poor key or certificate management. The main fault is when the job functions gets completed or the user leaves the company they forget to remove the access of the user in the organization. Anthem breach was the main cause for the credentials. Because there was failure in implementing multifactor authentication where the attacker attacks the credentials the game was over.

III. Hacked interfaces and APIs:

The cloud services are interacted and managed with the help of interfaces and API's. The cloud services mostly depend on the security of API's. The risk increases when the third parties rely on the API and the interfaces built on.

IV. Exploited system vulnerabilities:

Exploitable and system vulnerability are not new which brings bugs in the program. But now-a-days there is a much bigger problem which is multitenancy in cloud computing. The new attacks surface was created in the organization which is shared memory, database in close proximity.

V. Account hijacking

The main threat found is the attackers silently listening on activities modify data and manipulate transaction. Hijacking people may use the cloud application to launch the other attacks.

VI. Malicious insiders:

The insider's threat may be of a current or former employee, a contractor, a business partner or a system administrator. In the cloud scenario, to achieve all cost in the organization can destroy the whole infrastructure. The malicious have a data theft which leads to revenge. In the security of the cloud service the main risk is encryption.

VII. Permanent data loss:

To harm the business, malicious user will know how to delete the data's permanently in the cloud service. Data backup should be maintained day-to-day.

VIII. Inadequate diligence:

When the organization is implementing the cloud environment, the organization should be well known about the cloud. Organization should be aware of the "Myriad of financial, technical, legal, commercial and compliance risks". The company or organization may merge or mitigate the cloud from one company to another due to the diligence.

IX. Cloud service abuses:

Criminal activities are supported by the cloud services. User should be aware of the types of

abuse. There are two types of abuse wanted to be known they are scrutinizing traffic and to monitor the health of the cloud environment customers.

X. DoS attacks:

Experiencing a denial-of-service attack is like being caught in rush hour traffic gridlock. There is one way to get to the destination and there is nothing to do about it except sit and wait".

XI. Shared technology, shared dangers:

Shared technology in vulnerability is the main threat in cloud computing. Infrastructure, platforms and applications are shared through the cloud services. If any vulnerability occurs in one of the service then it affects all the services. The entire cloud providers are comprised due to the misconfiguration or a single vulnerability.

TO OVERCOME THE THREATS:

The cloud security alliance (CSA) has said little process to overcome the threats in cloud computing security. The following are recommend by the CSA to overcome the threats:

- The multifactor authentication and encryption must be used by the organization to protect from the data breach.
- To overcome the broken authentication things like one-time passwords, phone-based authentication, and smartcards which comes under the multifactor authentication system used to protect the cloud service which is made risky for the attackers to log in with the stolen password.
- A well secured public key infrastructure must be provided to overcome the credentials.
- "First line of defense and detection" must be followed for the control of API and interface. The process should followed is rigorous penetration testing and the security-focused code review should be undergone to overcome.
- Basically IT expenditures are less when compared to the system

vulnerability cost of mitigation. So that mitigation can be done with the basic IT process for the attacks on the system vulnerability.

- The strategy called defense-in-depth protection is been used to protect from damage. The sharing of account credentials between the user and the server should be prohibited. Also multifactor authentication schemes should be implemented.
- To reduce the access given to the user and to control the encryption process. To perform a routine job as "malicious" insider activity should try misconstruing a bungling.
- Phishing techniques should be learnt by the training user.
- To overcome the permanent data loss new EU data rule is been introduced. The user should be well versed in the rules.
- Customer should ensure that the providers provide the mechanism of report abuse. There can be service availability issues and data loss when there is abuse of cloud service.
- The plan is to mitigate the attack before it occurs, so that the administrator will have those resources when they want.
- The suggestion given to overcome is defense-in-depth strategy, including multifactor authentication on all hosts, host-based and network-based intrusion detection systems, applying the concept of least privilege, network segmentation, and patching shared resources.

TOP MOST RISK OF SECURITY

The top most risk which are faced by the organizations day-to-day in the security of the cloud computing are listed below:

- Loss or theft of intellectual property.
- Compliance violations and regulatory actions.
- Loss of control over end user actions.
- Malware infections that unleash a targeted attack.
- Contractual breaches with customers or business partners.
- Diminished customer trust.
- Data breach requiring disclosure and notification to victims.

- Increased customer churn.
- Revenue losses.

CONCLUSION

Any companies before adapting the cloud platform, they should be aware the cloud environment up to date. The level of the security should be given ah clear idea for the user by the cloud service. In this paper, the threats in the security of the cloud are been discussed. And the solution to overcome the threat is mentioned. The main risk caused by the security in the organization is also given. New security techniques must be brought with the high level security.