A Review on Security issues in Multi Cloud Computing and prevention by security measures

[1]Binu C T, [2]Dr.S.Mohan Kumar

[1]PhD Scholar, Computer Science & Engineering, CMR University, Bengaluru
[2]Supervisor, Director, QA Research &Innovation, CMR University, Bengaluru

Email: [1]binu.ct@cmr.edu.in, [2]drsmohankumar@gmail.com

DOI: 10.29322/IJSRP.13.06.2023.p13835
http://dx.doi.org/10.29322/IJSRP.13.06.2023.p13835

Paper Received Date: 14th May 2023
Paper Acceptance Date: 16th June 2023
Paper Publication Date: 21st June 2023

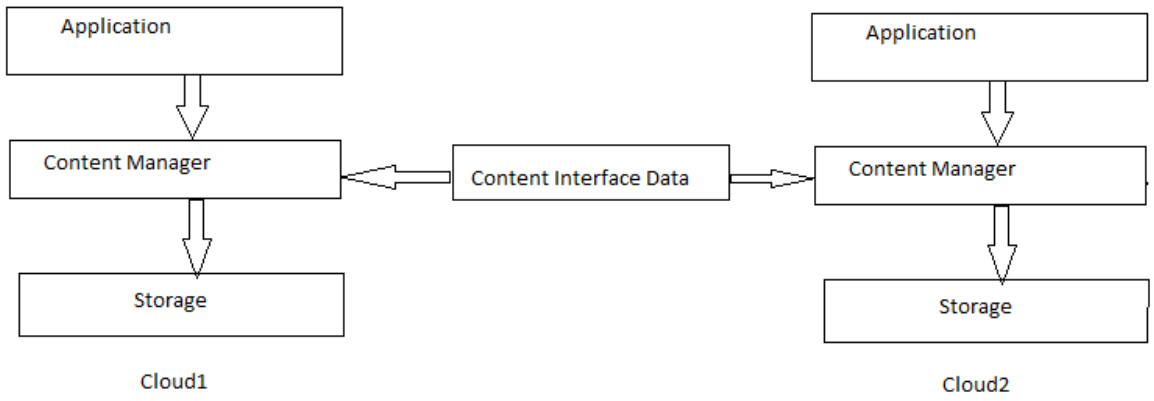
Abstract: The Cloud computing is a platform where we can connect and work from anywhere due to the availability and scalability of resources. Security to cloud environment and the application is a challenging topic which we need to pursue. The security issues in cloud a review where we discuss about all the security breaches in cloud. The security issues include external hackers gain access to databases in such environments using hacking techniques like session hijacking and network channel eavesdropping. Virus like Trojan can be uploaded to cloud systems and can cause damage to the system. Compromised credentials and broken authentication, Data breaches, Hacked interfaces and APIs, Exploited system vulnerabilities, Account hijacking, Permanent data loss, Cloud service abuses, DoS attacks, Service hijacking, VM Hopping, Platform-as-a-service (PaaS) security issues, Third-party relationships, Underlying infrastructure security Cloning and Resource Pooling, Unencrypted Data, Network Issues XML Signature Element Wrapping, Browser Security, Flooding Attacks, SQL Injection Attack. This paper reviews all these issues and security measures to prevent them in cloud computing.

Keywords: Multi Cloud computing model, Security issues in cloud computing, Cloud computing services, Security measures in Multi cloud

I. INTRODUCTION

Cloud computing services is enabled in information communication technology delivered to a customer as services like Infrastructure As A Service, Software As A Service and Platform As A Service through the Internet on a leased basis and have the scalability property helps to requirements for its needs. The Cloud Service Provider owns the resources and allocated to the customer based on their requirements. Cloud computing model has many advantages including scalability, flexibility, elasticity, efficiency and outsource the service. The multi Cloud offers an innovative business concept for organizations to combine all the needs into a single platform. This model enables convenient, shared pool of IT computing resources like networks, servers, storage, applications, and services. There is a specific data to communicate one cloud with the other in multi cloud computing. Security issues are the major factors which regularize the growth of cloud computing service model due to handling of confidential data by the third party is risky such that the consumers need to be more careful in understanding the risks of data breaches in this cloud environment.

II. MULTI CLOUD MODEL



In multi cloud model the application and data are placed in the storage and is managed by Content Manager. Content Manager of one cloud connects with the other through Content interface Data.

III. SECURITY ISSUES IN MULTI CLOUD

Broken authentication:

Organizations may encounter issues with authentication management as they try to grant permissions inappropriate to the user rights. They sometimes forget to remove user access from the authentication management when the user leaves the organization. Many developers made the mistake of embedding credentials as well as cryptographic keys with source code and cause hacking while executing the application. Multi factor Authentication is the primary solution to this attack avoid sharing credentials in source code.

Data breaches:

The service providers may become a target because of all the data are stored on cloud servers.The hackers can attack using false credentials created by just creating a change password option and cause data breaches. Data breaches DNS Authentication helps to avoid data breaches completely.

API Hacking

APIs and other interfaces may expose to security issues such as confidentiality and availability. Threat Preventive Routing mechanism can be used to prevent Hacked Interfaces and APIs. The header of the Postman contain source and destination address and that will helps to prevent these issues.

System vulnerabilities attack:

Any bugs in programs have become the source of exploiting system vulnerabilities in cloud computing. It may cause through share memory, databases and other resources in close proximity to one another. Unit Testing helps to avoid exploited system vulnerabilities.

Phishing:

The attackers manipulate transactions, and modify data through phishing. Attackers may use the same cloud application to launch other attacks. Multi factor authentication to protect the credentials. The integrity services such as MD5 can be enabled to prevent the attack.

Data loss:

Data loss can be occurred in the data centres because of disasters and it can be avoided by electronic waste management system.

Diligence knowledge:

The risks is associated with the customer because of lack of knowledge and it may enter into a number of commercial, financial, technical, legal, and compliance risks The policy enforcement is the security measure to avoid inadequate diligence.

Cloud service abuses:

Some attackers use Cloud services to break an encryption key in order to launch an attack. The service providers need to recognize this kind of abuse to identify DDoS attacks customers need to monitor their cloud environments. Customers should make sure that providers offer them a mechanism for reporting abuse. The monitoring data with policy verification avoids cloud service abuses.

Denial of Service attacks:

High-volume of DoS attacks are very common. There are two types of DoS include asymmetric and application level. Unique URL for each user which avoid denial of service attack.

Malicious attacks:

The attack may occur from outside as well as inside. Security token is the solution to avoid malicious attacks from inside and outside.

Backup and Storage:

There may be unauthorised attackers uses data centers.The data center should have high security to avoid that. High security encryption techniques to avoid backup and storage issues in cloud.

Platform security issues:

The cloud may allocate system software as a service and the network should be good enough for a better performance. The intruders may enter the same network and attack the platform as a service and it is avoided by running as a batch file.

Third party relationship:

The programming language is the third party along with system software as a service and security issues may occur though that. It can be avoid by using known functionalities which support the platform.

Software Development Life Cycle:

The security issues while developing the application for the cloud is very important and is handled by using security software such as firewall and anti-virus software in the organisation.

Infrastructure Security:

Infrastructure as a service has the functionalities to allocate the machine for the cloud and attckers find its address and may cause harm. The infrastructure which located in different locations and connected through a virtual private network (VPN) can avoid this issue.

Cloning:

Replicating the data by same users is called cloning and it cause data leakage and is avoided by using high authenticity to replicate the data .It is necessary to kept single data to avoid this issue.

Unencrypted Data:

Unauthorized users can easily access the unencrypted data. It can be avoided by using encryption standard .Encrypted data is accessed only by the authorized user. Encryption may be symmetric and asymmetric. Strong keys can protect the data for high level application

Identity management:

Identity management allow us to authenticating the users through their credentials. Two factor authentication in the content manager helps avoid the issue related to identity management

XML Signature attack:

The XML Signature attack changes the content with sign and does not tamper the signature. Digital Signature with cryptographic encryption and decryption technique with a key to avoid this issue.

Browser Security:

Some hackers from the intermediary host in the same network may obtain the credentials by using sniffing packages installed on the intermediary host. This issue can be avoided by always clear the cache and cookies in the network.

.

Flooding Attack:

The attackers request for a resource for a large number of times and the cloud may expand or scale up based on the request. We can provide session limit to access the resources to avoid the issue and use synchronization mechanism to avoid that.

SQL Injection:

The attacker may use some SQL query to access the database and stole the credentials and this can be avoided by multi cloud. One cloud with blank database and try to execute the user's application and only the valid user is allowed to access the actual application through Content Interface Data(CID).

IV. REFERENCES

[1].Cloud Computing Security issues challenges and opportunities Vaikunth Pai T.1 & P. S. Aithal1,
International Journal of Management, Technology and Social Sciences (IJMTS), 2016