An Optimized Security and Threat prevention mechanism for multi cloud network Application

Binu C T

Binuct143@gmail.com

ABSTRACT: Security is the primary factor to select cloud as the platform. Security threat like man in the middle attack, SQL injection, IP Spoofing increases threats in the system. The existing systems focus on performance than the security of the system. The proposed system with multi cloud application increases the security of the application with Threat Prevent Routing mechanism. Security Check Cloud for security check and Secure App cloud for the secure application. There is Pass Code named Application id is generated in the SC Cloud based on the application run in the client environment to the SA cloud using incident App. The Pass code is the authentication to enter in to the SA cloud and run the Secure App.

KETWORDS: Security, Multi Cloud, Routing, Network Security

I. INRODUCTION

Information Security is the process of implementing measures and systems designed to securely protect all kind of information and prevent unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure and preserve security services include confidentiality, authentication, integrity, availability and perform the decide functionality. Cloud security includes examining how the data attain the security services which mentioned above in the context. The cloud platform provides Infrastructure as a service, Platform as a service and provide resources.

Different Types of clouds are:

PaaS: Platform as a Service is to provide the platform to run the application.

SaaS: Software as a Service is to provide software to run the application.

IaaS: Infrastructure as a service is to provide environment to the application other than PaaS and SaaS

II. REQUIREMENTS IN CLOUD SECURITY

Most of the applications which are moved to cloud as a platform for security. The requirements of cloud security includes avoid data breaches, Secure Cloud Account Management without negligence, API Security, Denial of service and sufficient Due Diligence.

A. Avoid of data breaches:

Usage of data for other applications to do fraud is what’s called data breaches. The security service availability to authorized user which avoid data breaches.

B. Secure Cloud Account Management:

The cloud access is given to users with role to access to avoid the negligence in Secure Cloud Account Management.

C. API Security:

API services to authorized user which prevent the insecurity in API. Verify the user with postman helps to authorize the user.

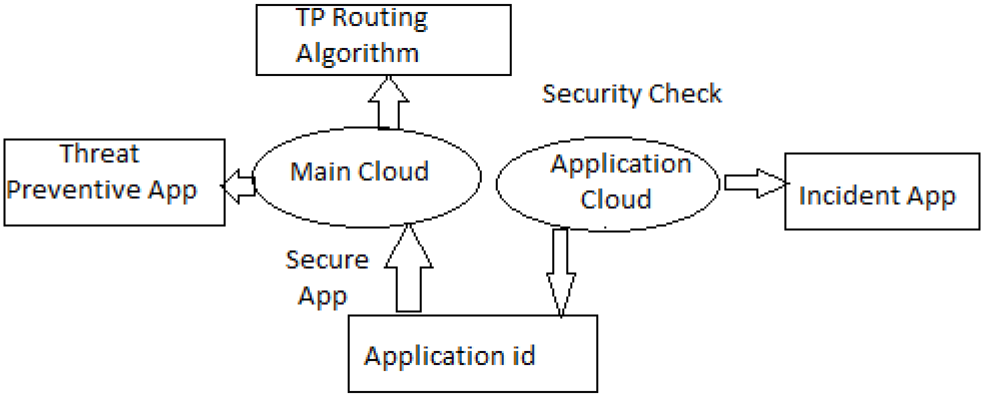
D. Denial of service:

Denial of services to hackers prevent the attack in the cloud and provide information and network security.

E. sufficient Due Diligence:

The requirement of application added to which the security of the cloud is biased.

III. ARCHITECTURE DIAGRAM

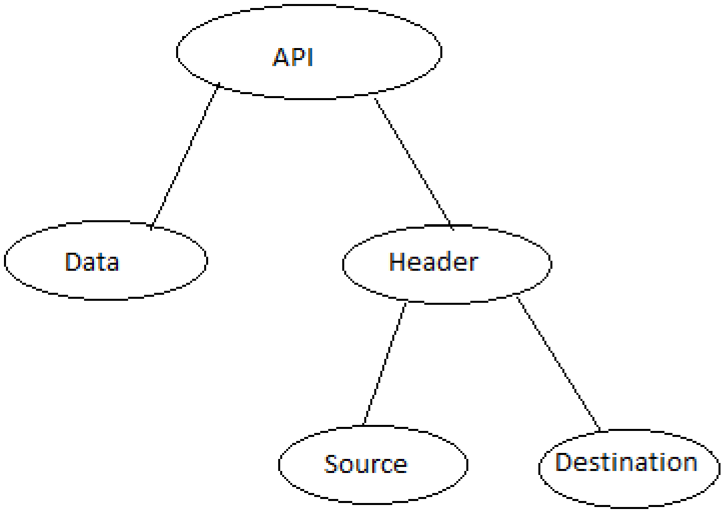


A. TP Routing Algorithm:

Threat Preventive Routing algorithm designed to provide high security services to all the application. In TP Routing have API which contain data and header. The data contain the encrypted data and header contain the destination and source address of the user and the application respectively. It each time check the header to reach the authorized user of the application.

Source->Nearest of Source->Nearest of Destination->Destination

Find the nearest of Source and Nearest of destination by using equation or ABL tree.



B. Security Check (SC) Cloud:

Security Check Cloud otherwise called Application cloud connect with incident App to provide security of the decide application. This cloud contain Blank Database which prevent SQL injection. Compute Engine service agent in the SC Cloud is to navigate from SC Cloud to SA Cloud.

C. Incident App:

Incident App runs all the applications which run the cloud to access the decide application. There is pass code for each user and it is generated based on the application status. If hackers access the system with some application which check in the incident app and respond with status fail and display the denial of service. All other users return an application id to access the decide application.

D. Application ID:

It's an encrypted ID passed from SC Cloud to SA Cloud to access the application.

E. Threat Preventive App:

Threat Preventive app uses the TP Routing mechanism to deliver the application. Threat Preventive App runs in the Secure App Cloud.

F. Secure App (SA) Cloud:

Secure App otherwise called main cloud in the threat preventive App runs. Content Delivery Network (CDN) provide the service by checking the application ID.