A NOVEL USER PERSPECTIVE BASED SERVICE ACCESSING SCHEME FOR CAPABLE INTRUSION DETECTION SYSTEM IN CLOUD ENVIRONMENT

ABSTRACT:

The cloud is an environment which combines various resources and provides different services to access the resources. In general, the high cost resources are deployed to the cloud environment, and cloud service provider gives set of services to access the resources. The service provider does not know anything about the end user and in such loosely coupled environment, providing access restriction is difficult, and it is more disposed to various attacks. The external users who registered in the cloud environment can access the services available in the cloud.

Initially, proposed a service orient approximation method which restricts the user access in many ways and uses multi attribute encryption standards for data to form an intrusion detection system in secure cloud environment from various threats. The user request is approximated based on the service required, and the approximation of the application is performed in many ways using some factors like the frequency of access, user profile, user role in the organization and much more.

In second method generates the user-specific private key at the time of registration and distributes elliptic curve values at the time. The user will be verified the identity at the service request time and will be queried for a particular point in the curve. By receiving the curve point the user’s identity is authenticated and verified simply, the difficulty of predicting the curve point values of elliptic curve helps in securely checking the user identity.
In any cloud user who registers would access the cloud service in different tunings. It is not necessary that the cloud user should access the service in particular time. Whenever the user uses the cloud service, the cloud user must follow the rules of the service provider. Verifying the identity and secret key of the user are under the explicit scheme. But the moral and sincerity of any user can be analyzed by implicitly monitoring the user details. By overseeing the activity of the user in accessing the service without knowing the user would help the cloud environment.

Intrusion detection service access can determine, there are some methods available, and each uses various features. These methods maintain the list of user log who is identified as malicious at the earlier time. Based on the log available, the process determines the malicious request and denies the request. The problem with this approach is unidentified malicious cannot be stopped. Also, individual nodes use multiple identities for them, which compromise the detection scheme. Also, the method computes the entropy value for the packets received, based on the entropy measure the intrusion detection has performed.

Finally, the main role of this proposed research work is to resolve the general significance of intrusion detection. It is accomplished by need to achieve some important objectives dependent on the proposed intentions in cloud network.