Abstract

The first and primary law of network access control is to limit the access of network resources among the various types of users. NAC basically decides whom to let go onto the network. It decides the validity of user based on their identity and role. But its work does not stop on user authorization. What happens when user gets access to the network resources? This will be described in this paper. In this paper we present a way to secure the network resources using identity-based, role-based and behaviour-based network access control techniques. Resources will be divided into 5 categories and according to the role of user; access to these resources will be defined. These permissions can be changed on the bases of behaviour of the user. This will make NAC dynamic. And for dynamic user management, clusters of user will be formed based on their behaviour. To secure the network location-based security will be used.

References

and Information Technology.


**Index Terms**

Computer Science  
Network Security

**Keywords**

Network Access Control  
User And Resource Management  
And Location-based Security