# An Enhanced Approach of Access Control Method in a Distributed Environment

Abdullah Shakoor, Ali Raza
*Department of Computer Science*
*University of Agriculture*
*Faisalabad, Pakistan*

***Abstract***

*The purpose of this research is to enhance access control method in a distributed environment. An analysis was discussed among different access control methods. Data on a distributed link is at high risk now days. It should be secured from both internal and external attacks. An unauthorized access towards a data may harm the privacy and policies of an organization. So, it is necessary to secure the database from unauthorized access in a distributed environment. Different Access control techniques were used to secure the database from an intruder. With the growth of internet distributed databases are being used a growing number of rate. It is very important to control the access mechanism in a distributed data-base. Distributed database is distributed physically in a variety of web sites and is integrated logically together. To access the data different privileges are granted to make sure that your data is secure from an unauthorized access as well as from bad use. An approach that works efficiently was preferred by comparing all approaches. In this regard major focus was on privilege of data authorization*

**Keywords** - *Access Control; Authorization; Distributed Environment*

## I. INTRODUCTION

Information Access Control has been measured a chief issue in the data innovation group. The primary center of analyst is to give a system to secure information, and give the entrance of information in view of character and traits of a known clients or a procedure by utilizing a reference screen and concentrated approval rules. With the improvement of PC and Internet, security issue turns out to be increasingly genuine. In the early section of 2009, there are many people as many times' Trojan assaults in China. Access control is a technique to confine the entrance to secured assets. It is a key innovation to give framework security. Optional access control and compulsory access control are two principle access control means which are utilized as a part of framework security [1].

The approval strategies are characterized to constrain the entrance of information in view of client qualities or part. A few diverse methodologies have been proposed in view of the necessities of various areas. At present, information sum and accessibility is expanding quickly; a significant part of the information is put away on remote record frameworks. Emerged Views is another expansion in Relational Database Management Systems. This empowers a great deal more productive access of information. It might be a neighborhood duplicate of information found remotely or a subset of the lines or segments of a table or join come about, or might be an outline considering accumulations of a table's information [2].

## II. RESEARCH OBJECTIVES

The main objective of this research is to enhance the security regarding access control in a distributed network. Authorization is the main focus of research. To limit the user by his user rights is very useful to maintain the privacy and secrecy in an organization.

## III. PROBLEM STATEMENT

Provision of better approach by comparing different approaches in access control methods. Advancement in authorization system in a distributed network is to be analyzed.

## IV. USING THE TEMPLATE

Access control is an essential idea in software engineering. It gives security to various clients while getting to assets in frameworks. In the beginning of science, projects and assets were just accessible to individual clients, henceforth there was little need to limit clients' entrance to assets they were essentially the proprietor of those assets. However, as the frameworks developed, projects and assets that were obvious to different clients showed up. These new applications support correspondence and coordination among clients in frameworks, yet this presents the new issue of controlling clients' activities, in view of their [3].

Henceforth get to control ideas were created as answers for the issue. In many access control plans clients need to first give their personalities to a focal power, and after that the power (which may likewise call the portion) would choose to permit or deny the entrance demand. In any case, as frameworks become significantly bigger and more mind boggling, the

populaces of clients likewise increment incredibly, and the structure of frameworks changes. Straightforward access control plans can't stay aware of the improvement of these frame works, accordingly new thoughts are proposed by analysts for giving more refined functionalities to ensure the security of frameworks. This work is a piece of this pattern. The theory presents a better control approach pointing towards the control of practices in disseminated situations. These practices incorporate predefined groupings of activities and redundancies of executions for some sort of activities.

## V. MATERIAL AND METHODS

A technique combined by two techniques is presented and a survey is conduct to evaluate the result of this method. Here the Research purpose is to analyze the two different access control methods and then provide an enhanced and better solution for it. Fist method is Role Based Access Control Method is discussed with its algorithm. Second method is Context Based Access Control with its proper implementation. After this comparative analysis an enhanced approach of Access Control is introduced with the collaboration of both terms. A survey is conduct to know how these two methods and proposed method are known for professional point of view.

Role Based Implementation is the Process to Implement User's Allocation on the base of Role. In recent years, role-based access control (RBAC) has emerged as a model for enforcing dynamic access control policies across a wide range of enterprise resources. There are three main benefits of using RBAC. First, RBAC models have been shown to be "policy neutral", that is by using role hierarchies and constraints a wide range of security policies can be expressed. Second, security administration is simplified by using roles to organize access privileges. For example, if a user moves to a new function in an organization, the user's role can simply be reassigned. In contrast, without RBAC, permissions on individual files would have to be updated. Third, by using constraints on the activation of user assigned roles, the principle of least privilege can be enforced. In fact, today, RBAC models have matured to the point where they are prescribed as a generalized approach to access control Permissions [4].

The context-based access control model, proposed in meets these requirements. These models use roles and attributes as a base for the access granting decision. The roles are static and set up by a system administrator. The context-based access control model is closer to the ABAC model, but also uses roles, which are assigned dynamically, based on the user trust level and help to manage access to the resources. The trust level calculation is based on the participant's context, which includes attributes, identifying the user (user ID and public key); user location; current date; device, which requests the information, etc. A special smart space service implemented within the access control broker has been proposed for this model. This service grants access to the resources for the smart space services guided by the security policies. According to this model the public information can be published to smart space and processed by all participants, but the private information is provided only for appropriate participants through virtual private spaces when the corresponding access permissions are granted [5].

In Role Module, every user has a role that is defined by an organization. According to this module the difference between all users can be categorized. There are different types of roles are existed in an organization such as Manager, Officers, Accounts and Clerks. Every Role has different access and authorization level in an organization. These roles are defined in Roles Module.

Role-Context Combination Module is combination of two different approaches. First module is role based access control module and second is Context based access control module. Role module defines the roles of the users in an organization and context based module defines the event based or context based access control in an organization. These two modules provide a better security in an organization.

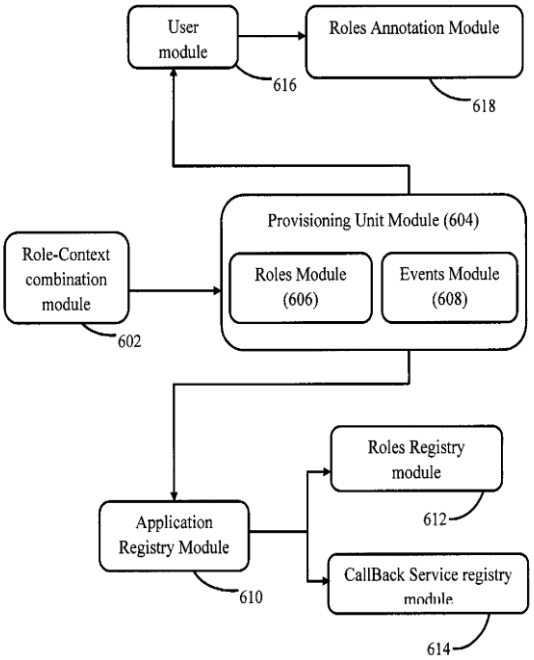


**Figure 1 Framework of Access Control Model**

Flow of Proposed Access Control Approach Is explained with diagram. This process starts with the login of a user and ends with the end of this session. Different mechanisms are defined in this flow. User has its username and password to login. When he enters his username and password then this request sends to roles module. This module defines the hierarchy and the authentication scheme for this user.

When the user is confirmed by the role module then next its request generates the context module. In this module the user has to be restricted according to his permitted area such as what he can do within his permission criteria [6].

## VI. RESULTS AND DISCUSSION

A survey is conducted to know the professional Point of View about Access Control Methods and the results are in favor of the proposed method because it is the combination of two major approaches RBAC and CBAC. Most of features gathered from Role based and some main features are collected from Context based. That is why this combined method is most frequented used in distributed system.

| | Frequency | Percent | Valid | Cumulative Percent |
|---|---|---|---|---|
| MAC | 5 | 20.0 | 20.0 | 20.0 |
| DAC | 4 | 10.0 | 10.0 | 40.0 |
| RBAC | 4 | 10.0 | 10.0 | 60.0 |
| CRBAC | 7 | 40.0 | 40.0 | 80.0 |
| Attribute Based | 2 | 8.0 | 8.0 | 88.0 |
| Trust Based | 3 | 12.0 | 12.0 | 100.0 |
| Total | 25 | 100.0 | 100.0 | |

**Table 1 the most useful Access Control Method today**

The table shows the frequency of the most used access control method today. Here we can see the frequency of CRBAC method.

## VII. CONCLUSION

Different approaches were analyzed to provide a better method to secure the data from internal and external threats. An approach was proposed to reduce the security risks in a distributed system. More future work will be initiated by considering the risk of authorization issues. More advancement can be achieved in this regard.

## VIII. SUMMARY

In this research first introduced all the terms used in this regard in section 1. Due to availability of data on internet, it is very easy for intruders to fetch the date of an organization without any permission. The data on internet is at high risk and is not secure. Therefore, for security purpose it is very important to secure the data both from internal and external thugs. The importance of access control has been explained in this chapter and the threats have been explained. Description about authorization and authentication has been told in this section. Different techniques and methods were explained in Chapter 1. There are many types of methods mentioned in this section. Their way of work and approach they used in this method have been discussed in this section. Different diagrams were there to represent the framework of these methods. Different cryptography methods are used but our main concern on access control method.

## REFERENCES

[1] Fan, Y., Z. Han, J. Liu and Y., Zhao. 2009. A mandatory access control model with enhanced flexibility. In 2009 International Conference on Multimedia Information Networking and Security. 1: 120-124.

[2] Gorla, D. and R. Pugliese. 2009. Dynamic management of capabilities in a network aware coordination language. The Journal of Logic and Algebraic Programming. 78(8): 665-689.

[3] Msahli, M., R. Abdeljaoued and A. Serhrouchni. 2013. Access control in probative value cloud. In Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for 607-611.

[4] Bacon, J., K. Moody and W. Yao. 2002. A model of OASIS role-based access control and its support for active security. ACM Transactions on Information and System Security (TISSEC), 5(4): 492-540.

[5] Bellavista, P., A. Corradi, R. Montanari and C. Stefanelli. 2003. Dynamic binding in mobile applications. IEEE Internet Computing. 7(2): 34-42.

[6] Cuppens, F. and A. Miège. 2003. Modelling contexts in the Or-BAC model. In Computer Security Applications Conference, 2003. Proceedings. 19th Annual.416-425.