International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 11, pp: 452-455 www.ijaem.net ISSN: 2395-5252

Enhanced Role-Based Access Control Delegation System for Tertiary Institutions

[1]Nkechi Faustina Esomonu, [2]Ikenna Caesar Nwandu
[1]Department of Information Technology, Federal University of Technology, Owerri, Nigeria.
[2]Department of Software Engineering, Federal University of Technology, Owerri, Nigeria.

Date of Submission: 15-12-2020 Date of Acceptance: 30-12-2020

ABSTRACT: The difficulties inherent in manual control approaches usually pose obstacle to the smooth running of tertiary institutions. This led researchers to developing access control systems that assign roles to authorized users. Role-Based Access Control systems are proved to be driving tool that motivates the subordinate to do better and perform well. This paper presented a role-based access control delegation (RBACD) system which provides an approach that allows one to assess the trustworthiness of potential delegates in the context of the task that is to be delegated. The proposed system is targeted at tertiary institution administration and how administrative functions can be carried out with less stress. The paper explains how the proposed system delegates roles to tertiary institutions' staff by granting them permissions to perform specific roles.

KEYWORDS:Role-based, Access control, Delegation, Permission, Authorization

I. INTRODUCTION

The protection of information in multi-user computer systems has become increasingly important as a result of the rapid development and widespread deployment of computer systems in our daily life. The most common protection measures used in computer system are:

i. prevention,
ii. detection, and
iii. recovery (Gollmann, 2005).

Prevention is applied to prevent information from being damaged. In other words, its purpose is to prevent all unauthorized access to information. Detection allows us to detect when information has been damaged, how it has been damaged, and who has caused the damage. Recovery allows us to restore the information that has been damaged or to assess and repair any damage to the information. In this thesis, we are only concerned with prevention. These security goals are concerned with prevention of unauthorized disclosure of information, unauthorized modification of information, and unauthorized withholding of information, respectively.

In order to keep resources and the information integrity from the unexpected use by unauthorized users, Role-Based Access Control (RBAC) systems introduced the idea of role hierarchy. Role hierarchy aims at reducing administrative burden and to ensure that permissions are inherited upwards and the set of roles available to a user is aggregated downwards. In this case, roles are identified with various job functions in an organization and users are assigned to roles based on their job responsibilities and qualifications. Further, Role-Based Access Control is being increasingly recognized as an efficient access control mechanism that facilitates security administration (Sandhu et al., 1996).

The original Role-Based Access Control model was formally introduced in 1992 by Ferraiolo and Kuhn at the 15th National Computer Security Conference. The model worked in such a way that roles must be authorized, and transactions must be authorized for a role as well. This maiden version has metamorphosed into INCITS 2004 Information Technology – Role Based Access Control (RBAC) published in 2004 by the InterNational Committee for Information Technology Standards. RBAC provides many advantages for organizations with requirements for more granular, role-based controls over who can access what data based on roles within their organizations. They can be used to protect data from the wrong employees, as well as to aid in compliance.

II. ROLE ASSIGNMENT IN ROLE-BASED ACCESS CONTROL SYSTEMS

The distinguishing factor that places Role-Based Access Control above other access controls (discretionary access control (DAC) and mandatory access control (MAC)) is the concept of role. Bammigatti et al. (2005) defined role as a job function within the organization that describes the authority and responsibility conferred on a user assigned to the role. A role is essentially a collection of permissions, and all users receive permissions only through the roles to which they are assigned, or through roles they inherit through the role hierarchy.

The role hierarchy generally supports two different types of inheritance namely upward inheritance and downward inheritance (although a cross-sectional inheritance is also possible). There are role hierarchies in which a senior role inherits the permissions of a junior role i.e. a junior performs one or more tasks of a senior. The phenomenon of role hierarchy greatly simplifies the management of permissions in an administrative setting. Role therefore acts as a "bridge" between users and permissions. Permission can be viewed from two dimensions:

i. Administrative delegation
ii. User delegation

An administrative delegation allows an administrative user to assign access rights to a user and does not, necessarily, require that the administrative user possesses the ability to use the access right. An administrative delegation operation is often long lived and more durable (permanent) and intended for a specific purpose (Schaad, 2003).

A user delegation allows a user to assign a subset of his available rights to another user. However, a user delegation operation requires that the user performing the delegation must possess the ability to use the access right. Furthermore, a user delegation operation is short-lived (temporary) when compared with an administrative delegation (Schaad, 2003).

The indirection introduced by roles is very similar to one that can be expressed by groups. However, while groups have only users as members, roles can form collections of users, permissions, and other roles (Sandhu 1995). This mechanism, as illustrated in figure 1, shows that unlike the case for groups, users can act in specific roles upon request, i.e. a user activates a role only when she needs the privileges associated with the role.

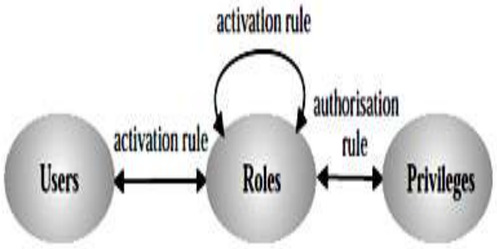

Figure 1: General Form of Role Concept. (Source: Sandhu et al., 1996)

III. RELATED WORK

Varadharajan et al. (1991) considered the problem of delegation of rights, otherwise known as proxy, in distributed systems. Their model works in a manner that some objects may be authorized to act on behalf of other objects. They considered the essence of the delegation problem to be the verification that an object that claims to be acting on another's behalf is indeed authorized to act on its behalf (object to object delegation). In practice this means that there is need to ensure that the information is securely transferred between the objects.

Gladny (1997) considered the security requirements for a digital library that emulates massive collections of paper and other physical media for clerical, engineering, and cultural applications. He described an access control method that mimics organizational practice by combining a subject tree with ad hoc role granting. The method was made to control privileges for many operations independently, that treats privileged roles such as auditor and security officer like every other individual authorization and that makes access control information part of ordinary objects. This access control method scales efficiently from a very small number to a large number of users. The method is accomplished by emulating vertical delegation in organizational hierarchies, extended to permit privilege delegation from any one node to any other node, up, down, or across the organization tree. This provides a way to represent special administrative roles like security officers. A driving objective is that every privilege should be traceable as a sequence from a custodial user to its holder.

Cubaleska (2009) designed a model that implemented Discretionary Access Control (DAC) which centers on the concept of users having control over system resources. The access principles of his model was based on the identity of the subject and identity of the object which leaves access control to the discretion of the owner (i.e. the person that is permitted to use the function). The subject/object owner determines who and how access can be given.

Despite the innovative contributions of the existing systems, none of them have been able to remove the manual approach completely. Hence, this paper proposed a Role-Based Access Control Delegation (RBACD) model which will automate most of the institutional activities in a secured manner. The proposed model is an ongoing project which hopes to change the work-lives of users, staff and students alike, by reducing the cumbersome processes involved in administrative duties to mere click and acknowledge functions. This software would be used in tertiary institutions, and would be used in all the departments of the institution to serve as a university information system having each user accessing the system based on their privilege.

IV. FRAMEWORK OF THE ROLE-BASED ACCESS CONTROL DELEGATION SYSTEM

Staff and students in tertiary institutions are usually bugged with one or two roles to play on the institution's portal, either to make requests of some sorts or to initiate solution to certain problems. However, most times, it is seen that they are confused with the system due to inability to decipher the input and output requirements of the system, posed by system complexity. In the light of these, the proposed model presented in this paper is one which design an access control model that would be standardized, scalable, logical in design, non-system dependent, and would have positive economic ramifications upon implementation. The model uses delegation principles to grant permissions to different categories of users on the functions they are authorized to perform. The model transfers certain higher roles to some junior staff to ease off the work loads of senior staff with more responsibilities. The framework of the proposed system is shown in figure 2.

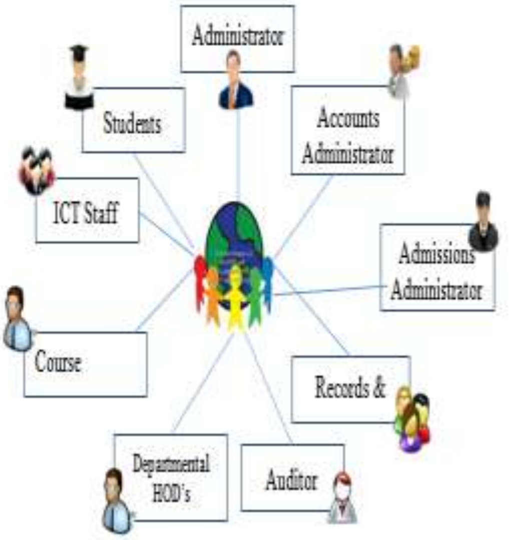

Figure 2: Architecture of the Proposed Model.

V. METHODOLOGY

The proposed model is a product of Structured Systems Analysis and Design Method. The model utilizes modular programming to achieve a system that ensures an efficient coordination of administrative activities within tertiary institutions. The model is furnished with functionality which ensures that:

i. The system that would automate most of the procedures and activities of the members of tertiary institutions.
ii. Both administrative control and authorization control are provided.
iii. Efficient and quality improvements in tertiary institutions administrative system are achieved.
iv. Error of conflict by students is restricted.
v. Security is improved via fraud detection.

VI. CONCLUSION

This paper presents a model framework that enhances the administrative duties in tertiary institutions via automation. This paper therefore succeeded in presenting a Role-Based Access Control Delegation (RBACD) model that simplifies the complexity of administrative processes obtainable in tertiary institutions. The model was designed to grant permissions to authentic users using delegation techniques, with the aim of relieving some heavy-burdened staff of excess roles and assigning them to the less-burdened ones. Our future work is to apply the model framework to a named institution to ascertain its workability, reliability and efficiency. We will go further to compare existing systems with our proposed model with the intent of unleashing the pros and cons that exist between them.

REFERENCES

[1]. Sandhu, R; Coyne, E; Feinstein, H. L; and Youman, C.E., 1996, “Role-based access control models,” IEEE Computer, pp 2.

[2]. Ferriaolo, D; Cugini, J; and Kuhn, R., 1995,“Role-based access control (RBAC),” New Orleans, LA, pp 241-248.

[3]. Bammigatti, P. H; and Rao, P., 2005,“A User-Role Based Data Security Approach, in Database Security.”

[4]. Schaad, A., 2003,“A Framework for Organisational Control Principles,” PhD thesis, The University of York, York, England.

[5]. Varadharajan, V; Allen, P; and Black, S., 1991,“An Analysis of the Proxy Problem in Distributed systems,” pp 24-25.

[6]. Gladny, H., 1997,“Access control for large collections,” ACM Transactions on Information Systems, 15(2), pp 154-194.

[7]. Cubaleska, S., 2008,“On mutually exclusive roles and separation-of-duty” (PDF), 11th ACM conference on Computer and Communications Security, pp. 42–51.