Journal of the Nigerian Association of Mathematical Physics
Volume26, (*March, 2014*), pp 319 – 324

A Comparative Study of Access Control Schemes In Database Security

Nicholas Oluwole Ogini and Noah Oghenefego Ogwara

Department of Mathematics and Computer Science,
Delta State University, Abraka, Delta State, Nigeria.

Abstract

A very important issue in today's computer and information systems is database security. In recent times considerable resources has been put into researching and addressing security needs of organizations because of the repeated reports of the impact of theft of organizational resources, unauthorised disclosure of corporate resources, and other corrupt practices which has disrupted organisational operations thereby causing serious financial, legal, personal privacy, and public confidence problems. Several different approaches have been developed in an attempt to provide security to the database resources; amongst these are Auditing, Authentication, Encryption, and Access control. In this work, Access Control as a means of providing database security is considered, and three popular access control schemes namely Mandatory Access Control, Discretionary Access Control, And Role-Based Access Control were comparatively studied.

1.0 Introduction

The rapid growth of networking and spread of database technologies globally, has had major impacts on the availability of information and its processing.

This arguably, has made information one of the most critical resources in organisations today, such that, irrespective of the location of individuals in our world today, data and information can be easily accessible from the numerous information systems available. According to Bertino et al. [1], the web is becoming the main information dissemination means in public and private organizations.

Wide spread use of the internet, lower technology costs, and a great need for data access and sharing in a competitive market has driven the development of new technologies and standards. Looking for a competitive edge, increased productivity, and security, both system vendors and implementers have been looking for the means to properly administer these rapidly expanding and costly infrastructures. More so now than ever, the downtime of users and the delay in account creation can mean losses in the thousands. With this growth, holes in security have generated media frenzy and have forced accrediting and governmental agencies to act by imposing requirements regarding security and privacy of information. From credit card transactions to patient health information, privacy is quickly becoming the centrepiece of a new wave intechnological advance, not just in hardware but also in conceptual approaches to Security. But it is the security concern within that often times goes unacknowledged. Account security in many organizations is loose at best, perpetuated by a high volume of requests and a security administration model grossly overpowered by the infrastructure it is forced to support. According to Alturi and Gal[2], gathering and disseminating information introduce new security challenge. It becomes very vital therefore, that organizations consider with all seriousness the manner in which its members access the resources of the organization, standardize the organizational policies to control access given to those who can use the information in their databases, and to what extent they can do so.

Most organizations depend on distributed information systems for discharging routine business needs today, and the database is a very vital store on which resources are made available to be accessed by members of that organization. Their susceptibility to security compromises increases, methods like electronic signatures and encryptions are presently accessible for safeguarding data at the time of its transmission. This work stresses the importance that a practically broad strategy for data protection should cover methods for putting in place access control policies which are dependent on subject

Corresponding author: Nicholas Oluwole Ogini E-mail: oginino@yahoo.com, Tel.: +2348033724497

qualifications. And it is most important that every member gets access only to that information that is relevant to his individual duties as defined by the organization.

Several database management systems are in use today; examples include the Oracle database management system, Microsoft Access, MYSQL database management system, Microsoft SQL database management system, etc. Within most of the above listed database management systems, are their inbuilt mechanisms for controlling access to database objects through access control.

Access control can be defined as the means by which the ability to perform an operation with a computer resource is explicitly enabled or restricted in some way.

The computer based access control can prescribe not only who or what process may have access to a specific system resource but also the type, level, and degree of access that is permitted.

2.0 Materials and Methods

A survey of several access control methodologies was carried out, and three of them were identified to be most commonly implemented. They are the Mandatory Access Control, Discretionary Access Control, and the Role-Based Access Control. Each of these methodologies have some common definable metricsupon which they can be easily defined. These indices include the following:

i. granting of access
ii. management of access
iii. ease of modification
iv. flexibilty
v. security
vi. human factor
vii. transitivity

3.0 Discretionary Access Control (DAC)

The discretionary access control (DAC) permits the granting and revoking of access control privileges to be left to the discretion of the individual users. Its mechanism allows users to grant or revoke access to any of the objects under their control. Under this scheme, the users are said to be the owners of these objects under their control. It is the owner of the file who controls other users' accesses to the file. Only those users specified by the owner may have some combination of read, write, execute, and other permissions to the file. DAC policy tends to be very flexible and is widely used in the commercial and government sectors. However, DAC is known to be inherently weak for two reasons. First, granting read access is transitive; Secondly, DAC policy is vulnerable to Trojan horse attacks. Thus, formally, the drawbacks of DAC are as follows:

- Information can be copied from one object to another; therefore, there is no real assurance on the flow of information in a system.
- No restrictions apply to the usage of information when the user has received it.
- The privileges for accessing objects are decided by the owner of the object, rather than through a system-wide policy that reflects the organization's security requirements.

With this kind of access control scheme the organizational policies cannot be completely implemented and this often leads to uncoordinated access to the organizational resources from a policy point of view, thereby threatening the security of database objects.

4.0 Mandatory Accesss Control (MAC)

Mandatory access control (MAC) policy means that access control policy decisions are made by a central authority, not by the individual owner of an object, and the owner cannot change access rights. An example of MAC occurs in military security, where an individual data owner does not decide who has a Top Secret clearance, nor can the owner change the classification of an object from Top Secret to Secret

The need for a MAC mechanism arises when the security policy of a system dictates that:

1. Protection decisions must not be decided by the object owner.
2. The system must enforce the protection decisions (i.e., the system enforces the security policy over the wishes or intentions of the object owner).

Usually a labelling mechanism and a set of interfaces are used to determine access based on the MAC policy; for example, a user who is running a process at the Secret classification should not be allowed to read a file with a label of Top Secret. This is known as the "simple security rule," or "no read up." Conversely, a user who is running a process with a label of Secret should not be allowed to write to a file with a label of Confidential. This rule is called the "*-property" (pronounced "star

property") or "no write down." The *-property is required to maintain system security in an automated environment. A variation on this rule called the "strict *-property" requires that information can be written at, but not above, the subject's clearance level. Multilevel security models such as the Bell-La Padula Confidentiality and Biba Integrity models are used to formally specify this kind of MAC policy.

For organizations that are interested in MAC, security objectives often forms the foundation for higher level organizational policies which are derived from existing laws, ethics, regulations, or generally accepted practices.

5.0 The Role Based Access Control

The Role Based Access Control (RBAC) scheme is an access control model that is found in most of the Database Management Systems in the market today e.g. Microsoft SQL and Oracle 10g. According to Alturiand Gal [2], due to the relevance of the RBAC, it has been widely investigated. It is based on the premise that authorizing a particular user to access organizational information and modify it is based on the roles and responsibilities the user has within the organization. According to Bertino et al [3], the RBAC is receiving increased attention as a generalized approach to access control.

A role can be thought of as a set of transactions that a user or set of users can perform within the context of an organization.

Transactions are allocated to roles by a system administrator. Such transactions for instance include the ability for a doctor to enter a diagnosis, prescribe medication, and add an entry to a record of treatments performed on a patient. The role of a pharmacist may include the transactions to dispense but not prescribe prescription drugs.

Membership in a role is also granted and revoked by a system administrator.

Roles are group oriented. For each role, a set of transactions allocated the role is maintained. A transaction can be thought of as a transformation plus a set of associated data items. In addition, each role has an associated set of individual members. As a result, RBACs provide a means of naming and describing many-to-many relationships between individuals and rights.

Three basic rules are required:

1. Role assignment: A subject can execute a transaction only if the subject hasselected a role or been assigned a role:The identification and authentication process (e.g. login) is not considered a transaction. All other user activities on the system are conducted through transactions.Thus all active users are required to have some active role.
2. Role authorization: A subject's active role must be authorized for the subject:

With (1) above, this rule ensures that users can take on only roles for which they are authorized.

3. Transaction authorization: A subject can execute a transaction only if the transaction is authorized for the subject's active role:

In this scheme, decisions on access control are based on the role that individual users have as part of an organization. From this survey it is observed that most corporate organizations today, tend toward this type of access control and its modified heirarchical form. However, the areas of operations should be properly investigated to meet the organizations' functional requirements. Botha, R. [4]

Here roles are created, permissions are granted to the roles, and users are made to belong to these roles based on their level of need in the organization. Figure 1 shows a single role with three users. All users by this structure can perform exactly the same operations.

The process of defining the roles is based on a thorough analysis of how the organization operates. It should include inputs parameters from a wide spectrum of users in the organization. Access rights are grouped by role names and the use of resources is restricted to individuals authorized to assume the associated role. This access control scheme is an effective means for developing and enforcing enterprise specific security policies and streamlining security management process. Role - Based Access Control (RBAC) system enables users carry out a broad range of authorized operations and provides flexibility and breadth of application.

Brinkley and Schell [5] opine that when implementing this model three fundamental notions must be considered.

1. A security policy
2. The functionality of internal mechanisms to enforce that security policy in 1
3. Assurance that the mechanisms do enforce the security policy.

In the heirarchical structure, the roles are organised in such a way that any user on a higher role can perform the operations of users below them in the structure asshown in fig 2.

If the roles are denoted by $R = \{r_1, r_2, r_3, r_4\}$

Then it implies that if $r_1 \geq r_2$, Where r_1 and$r_2 \in R$,

Then r_1 inheritsthe permissions of r_2

From the hierarchical structure in figure 2, we see that there are 4 roles implying 4 different categories and 12 users in the hierarchy. To each role is a unique set of permission granted. Such permissions include ability to write to database, read

from database, delete from database , update a database record, etc.

6.0 Results And Discussion:

This paper has shown the importance of providing security for database resources especially at this time of high incidences of information theft. It described three popular access control schemes used in most database management systems today and based on this study, a position is reached that, of the three most popular access control schemes considered, the role- based access control scheme has its strength, in that it is more likely to meet the requirements of most corporate organizations, especially when there is proper documentation of organisation layout and adherence to organizational policies. But when extreme security or a high degree of protection is required not minding the inflexible mode of managing the access then the mandatory access control is suggested. The discretionary access control cannot be relied on for providing an organization wide security, though it is very flexible to implement.

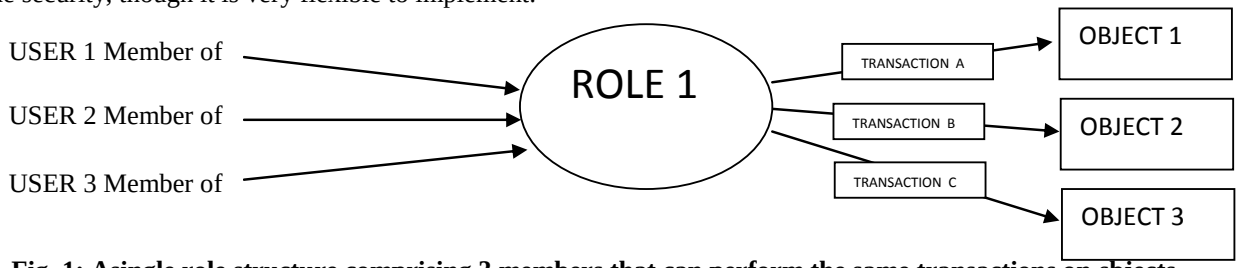

Fig. 1: Asingle role structure comprising 3 members that can perform the same transactions on sbjects

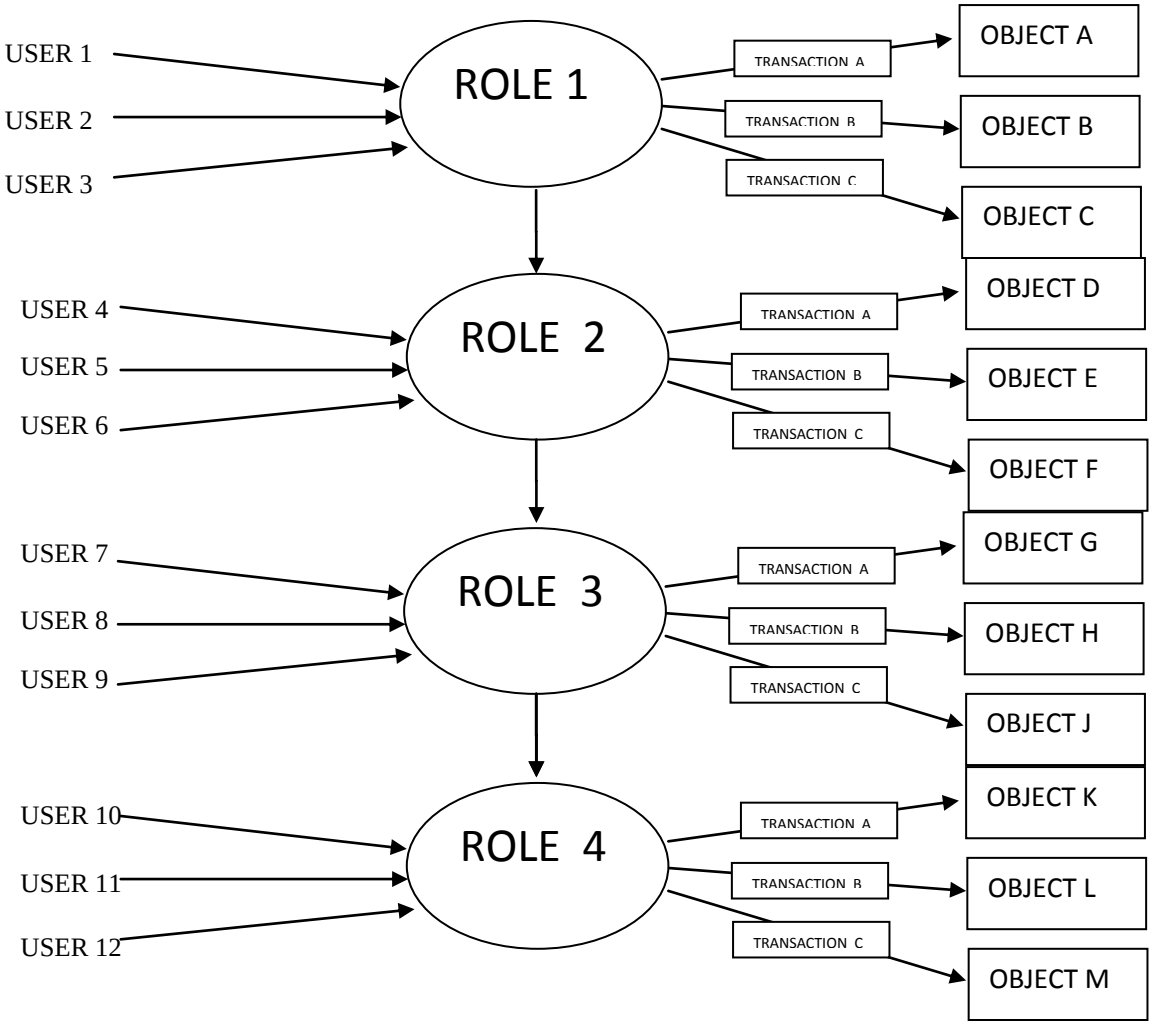

Fig.2: A HEIRACHICAL STRUCTURE ROLE BASED ACCESS CONTROL SYSTEM

TABLE 1: COMPARING THE ACCESS CONTROL MODELS THAT WERE DISCUSSED

	DISCRETIONARY ACCESS CONTROL (DAC)	**MANDATORY ACCESSS CONTROL (MAC)**	**THE ROLE - BASED ACCES S CONTROL (RBAC)**
GRANTING OF ACCESS	Administrator or group of administrators distribute access to the data, application and network devices and are responsible for changes in the management of access	Access to the resources is Hard coded in the application and the rule applies to all objects, resources application and end user	Has a structure which demands that there be roles, permissions, operations and objects well defined for each user to belong to based on organisational policy
EASE OF MANAGEMENT	Very complex or nearly impossible to manage in large organizations	It is best suited for speciality application for a group of users with similar needs. Hence, for constant corporate managers consolidated and cooperative relation it is unsuitable	Multiple users can be associated with one role and permission are assigned to each role it is easy to dissociate a user from each unwanted role either for change of job function or termination it is well suited for corporate organizations.
ACCESS MODIFICATION	Less account access change turnaround times	Well contained (inbuilt) little or no change in account access of need be it is minimal	Based on organizational policies. This could be a major requirement as users may move from one job function to the other
STANDARD ACCESS LEVELS	Users with same job functions could be different access values, hence, uniformity diminishes in terms of users with same job function	Every user has his rating clearly defined as it is unique to his/her clearance level	Users can be grouped to perform exactly the same functions under a given role. Demanding that care must be taken to define the organizational policies to ensure that they actually belong there
TRANSITIVITY	When a user moves from one job area to another it is possible to carry along the access he/she has to new job areas without proper monitoring.	The classification of objects and subjects makes this impossible	Roles make it impossible to carry access not defined within it to be available
SECURITY	Security in a major concern it is vulnerable	Security is guaranteed	Security is based on the management of proper documentation of organisation layout and adherence to organizational policies.
HUMAN FACTOR	Misinformation and social engineering could be inimical	Since it is coded in the software there is less possibility of interference in giving access	Based on organizational policies and adherence to it. There is little room for error.
FLEXIBLITY	It is very flexible because the resource owner can revoke it almost immediately.	It is difficult for the modification and development of roles within the application programmes must reviewed the coding of the application to make changes.	Easy to change a user from one role to another

References

[1] Bertino, E. Castano, S. Ferrari, E. and Mesiti, M. (2001): "Specifying and enforcing access control policies for XML Document sources", World Wide Web 3, Baltzer science publisher BV, 2000

[2] Atluri V. and Gal A. (2000): "An authorization model for temporal andderived data: securing information portals", ACM transaction oninformation and systems security, vol. 5, no 1, pp.62- 94

[3] Bertino, E. Bonatti, P. and Ferrari, E. (2001): "TRBAC: A temporal role based access control model", ACM transactions on information and system security, August 2001

[4] Botha, R. and Eloff, J. (2002): "A frame work for access control in work flow system", information management and computer security, vol 9 No. 3 , 2002, pp. 126-133, MCB University press. ISSN:0968-5227

[5] Brinkley, D. and Schell, R. (1995) "concept and terminology for computer security", information security: An integrated collection of essays, pp. 40-97, IEEE Computer society press, 1995, ISBN: 0-8186-3662-9