Modified Role Based Access Control Model For Data Security

Bukohwo Michael Esiefarienrhe, Abubakar Hashimu Ekka

ABSTRACT: This Paper presents a modified Role Based Access Control model by extending traditional role based access control in SQL (Structure Query Language) data storage. The said model evaluates and executes security policies which contain versatile access conditions against the dynamic nature of data. The goal is to devise a mechanism for a forward looking, assertive yet flexible security features to regulate access to data in the data storage that is devoid of rigid structures and consistency. This is achieved by integrating roles and authenticated fine-grained access rules and implemented through effective audit trail. The model and the rules used are presented and shows that when implemented, it is capable of outperforming existing models that are role based.

Keywords: Role based access control, security, policy access control, Database management, modeling, enterprise environment

I INTRODUCTION

Access control is and instrumental to data security and can be done through authentication, authorization, and physical control. These three mechanisms are distinctly different but can effectively manage all requests for access to systems and it can protect the unauthorized access to the database resources. Role based access control (RBAC) has emerged as a proven technological approach for managing and enforcing security in large-scale enterprise systems. It can provide more flexibility to security management over the traditional approach of using user and group identifiers. Role-based access control system is divided into the user functions and positions consistent with their roles. In the role-based access control model, the permissions to perform certain operations in an organization are assigned to specific roles instead of assigning permission to each user directly. That is why role-based access control is appropriate for managing access to enterprise and government software systems. Role-based access extends various access control models to satisfy the requirements for access control. As one of the earliest methods for protecting data, Database Management Systems (DBMS) traditionally use some form of access control to enforce policies regarding the data they manage. Using data access policies allows defining the data that each user is authorized to access and the actions that he/she is authorized to execute. This is accomplished through user authentication, which is the process of verifying the user’s identity in the system and applying the set of policies defined for the user or the role to which he/she belongs.

Presently, Data Base Management System (DBMS) have audit control, complying with ACID (Atomicity, Consistency, Isolation, and Durability) requirements, and supply extensive authentication, authorization, and access control (AAA) features to ensure that the right users access and/or modify only the data that they are supposed to access and/or modify. Data Base Management System also has available data masking and encryption packages that can be used transparently with databases and user applications in a straightforward manner. These preventive techniques work effectively in guaranteeing that only authorized users may access and manage the data that they are supposed to access and manage. However, they are unable to distinguish if the user that has logged in is truly who he/she is supposed to be and/or if that user has or does not have malicious intentions; if a masqueraded user or malicious insider that has gained clearance by hacking or taking advantage of valid login credentials, those preventive mechanisms are unable to protect data Given the increase of sophisticated attacks (for example, Distributed Denial of Service attacks) and rising internal theft with data masking and/or encryption are no longer enough to protect data (McKendrick et al,2012). Furthermore, attackers that gain direct access to databases mostly represent authorized users logging with permission to access data, meaning that they are able to bypass traditional intrusion detection systems (IDS), typically work at the network and operating systems (OS) levels. This research is meant to solve the above issues raised and to further provide an authentication system that can prevent authorized users from malicious practices when logged into the system. Section II of the paper discusses related work to this research, while section III provides the methodology used in the research.

II. BACKGROUND

Data is a major asset for any enterprise, not only for the past, but also to support today’s business and to predict future trends. Stored data in a large repository which can be used for data mining, report generations and decision making. It can also be used to consolidate disparate database that enables executives and managers to work with vast stores of transactional or other data to respond fast to markets trends and generate summarized reports. These reports contain useful and important information which needs security measure from some unauthorized users. This supports the thinking of Kobielus in Kobielus, (2009) that data are today’s backbone for enterprise

- *Bukohwo Michael Esiefarienrhe, Abubakar Hashimu Ekka*
- *Dept. of Math/Stat/Computer Science, University of Agriculture, Makurdi, Nigeria.*
- *College of Education Akwanga, Nasarawa State, Nigeria*
- *Emails: esiefabukohwo@gmail.com, hashimuabubakar75@yahoo.com*

business intelligence, playing a major role in the enterprise’s outcome. The role of data in business intelligence introduces the need for integrating effective security measures into databases, given that they are the central component of enterprise information systems. Regardless of their security purpose, the techniques that are selected for implementing data security need to consider that data environments have unique types of user activities, as well as database features and performance requirements, which do not exist in any other type of database system. In this paper, we consider a feature as a variable for accessing the characteristics of a given subject. For example, a database features can be the storage size of a database or its throughput, among other variables. In this paper, we focus on enhancing data security in databases, specifically in the context of stored data environments which concerns data masking, encryption and intrusion detection. Thuraisingham et al. (2007) proposed an Extended Role Based Access Control for securing enterprise stored data. The approach integrates a stored data include secure heterogeneous database integration, statistical databases, secure data modeling, secure metadata management, secure access methods and indexing, secure query processing, secure database administration, general database security, and secure high performance database. Since stored data keeps summary information, techniques used to manage statistical databases need to be examined for stored data. As new types of data models such as multidimensional data models and schemas such as star schemas have been proposed for data security. We need to integrate these models. Depending on who is using the data, different views of the data could be provided to the user. An appropriate access methods and index strategies have been developed for the stored data. The authors claimed that their technique gives better privacy and confidentiality for organizations’ data. Kundu et al. (2010) proposed a temporal analysis technique which detects any queries that request execution outside a predefined time schedule and may therefore deny them execution and prevent the intrusion action. The sequence analysis technique used may enable intrusion prevention by avoiding subsequent user actions when it detects a suspicious sequence of actions. However, it needs to wait for a significant amount of actions that make up that sequence, meaning that it will probably only detect the intrusion after some of those actions have finished their execution, which makes it only capable of partial intrusion prevention. Santos et al. (2011a) proposed the role based access control mechanism which is used for securing stored data. The author highlights the security issues in federated stored data. They proposed security measurements for assurance of patient privacy of medical data. Their model enables security of stored data in medical field(hospitals). A stored data contains consolidated, historical, and summarized data to support decision makers at different levels. Kangsoo et al. (2013) proposed a Role-based access control approach which reflects the functionality hierarchy in various organizations. However, their research suggests a relationship-based access control model that considers the relation with surrounding users in organization. Relation is significant context information but it is not considered in existing access control models. The proposed technique is different from that in traditional research in two ways. First, we regard the relationship among employees as contextual information. As a result, the administrator can manage fine-grained access control for cooperative work in an organization. Secondly, we design access control architecture with usability and security problems. Moreover, we propose a protocol for enforcing the suggested access control model in real world. We report performance analysis and security evaluation. Raimundas et al. (2015) proposed a Role-based Access Control (RBAC), which restricts system access to unauthorized users. Their proposed model-driven approach to manage Structure Query Language (SQL) database access under the Role-based Access Control (RBAC) paradigm. The starting point of the approach is a Role-based Access Control (RBAC) model captured in Secure Unified Modelling Language (UML). This model is automatically translated to Oracle Database views and instead of triggers code, which implements the security constraints. The approach has been fully instrumented as a prototype and its effectiveness has been validated by means of a case study. Shermin et al. (2013) proposed a context agents model that sends a context query to one of the context agents for each access request. The context agents authenticate and validate the data integrity aggregated from interfaces. The access control layer is responsible for managing context-based access to resources based on personalized permissions. The Context Agent Role Base Access Control (CA-RBAC) programming framework consists of operational layers - context management and access control. The context management layer is responsible for aggregating data to generate context information required by any system. The Context Agent Role Base Access Control (CA-RBAC) model transcends the basic model when a permission invoked by different role members needs to be invoked on different object instances based on each role member’s individual context. Kambiz et al. (2015) proposed a model that uses a dynamic interface that applies Role Based Access Control (RBAC) policies as the output of policy analysis and limits the amount of information that users have access to according to the policies defined for roles. This interface also shows security administrators, the effect of their changes from the user’s point of view while minimizing the cost by generating the interface automatically. While changes to access control policies in databases are inevitable, having a dynamic system that generates interfaces according to the latest access control policies becomes increasingly valuable. Lack of such a system leads to unauthorized access to data and eventually violates the privacy of data owners. Ankit et al. (2015) uses the methodology of policy based file access using attribute based model of encryption with cipher text scheme to secure the storage and sharing of the stored data with the user. In their approach, they discuss the policy of revocation for file assured deletion so that no one can recover the deleted file from storage and also discuss the policy for access to data storing Centre so that the right user will access. An access control is one of the most important security mechanisms in data security. Attribute-based access control provides a flexible approach that allows data owners to integrate data access policies within the encrypted data. Therefore, their proposed methodology is policy based file access using attribute based encryption with cipher text policy scheme. Tarai et al. (2013) proposed a concept on Role Based Access Control(RBAC) policy that instead of access control through role assigned to the users, the users are assigned some level of access control. The proposed model assigns different category of roles under some levels of a system with the concept in view that a particular level can be granted authorization up to a certain maximum level described by Database Administrator. The proposed model uses two components namely Static Separation of Duty (SSD) relation and Dynamic Separation of Duty (DSD). Static Separation of Duty (SSD) relations, adds relations among roles with respect to user assignments. The constraints on the relations between elements take the form of Static Separation of Duty (SSD) relations and Dynamic Separation of Duty (DSD) relations. The Static Separation of Duty (SSD) relation specifies the constraints on the assignment of users to roles. Once a role is authorized to a user, then the user can not be the member of a second role. The Dynamic Separation of Duty (DSD) relations place constraints on the roles that can be activated in a user’s session. If one role that takes part in a Dynamic Separation of Duty (DSD) relation is activated, the user cannot activate the related (conflicting) role in the same session. Rosic et al. (2015) proposed the Role Base Access Control Area of Responsibility(RBACAOR) model, which was developed and tested on the Windows operating system platform using .NET Framework role-based security. The Role Base Access Control Area of Responsibility(RBACAOR) system comprised two processes, authentication and authorization, which are combined to ensure that resources are accessed only by authorized users. The Role Base Access Control Area of Responsibility(RBACAOR) model authentication framework utilizes .NET Integrated Windows authentication (IWA) as a first step toward gaining access to the system. The Role Base Access Control Area of Responsibility (RBACAOR) authorization framework consists of independent authorization processes which are combined to determine the final access control decision based on information encapsulated into the Role Base Access Control Area of Responsibility (RBACAOR) security principal.

III. A MODIFIED ROLE BASE ACCESS CONTROL MODEL

The existing model uses Role Base Access Control (RBAC) which has more limitations with respect to resource management. It has many issues regarding decision process, multiple roles, multiple session and many other temporal dependencies leading to unfulfilled and unsatisfactory roles that are easily compromised.

An Existing model: Role Base Access Control 96 Model

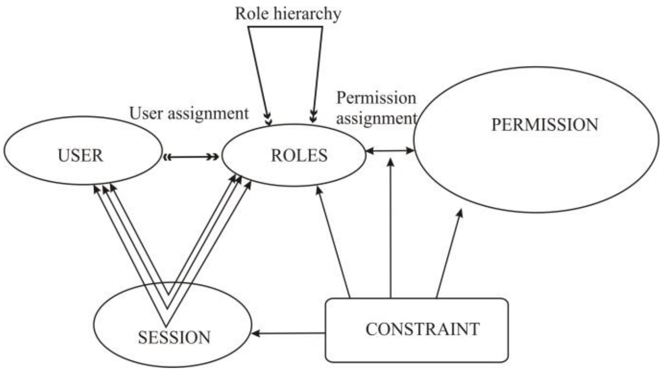

Figure 1: *Role Base Access Control 96 MODEL (Shermin et al, 2013)*

An Access control is a fundamental security technique in which multiple users share access to common resources. It is the process of stating and enforcing security policies that determine whether a subject (example, process, computer, user, etc.) is allowed to perform an operation (example, read, write, update, delete, etc.) on an object (example, a tuple in a database, a table, a file, a service, etc.). This mechanism maintains the subject's permissions (rights to carry out an operation on an object) in a system in order to achieve the desired level of security. There are several access control models, among which is the Role Based Accesses Control (RBAC) models; which provides systematic access control security for Enterprise solutions. One of the main advantage of Role Base Access Control (RBAC) over other access control models is the ease of its security administration (Shermin et al, 2013). Role Base Access Control (RBAC) enables an Organization to model its security mechanism to closely match the individual business process. Role Base Access Control (RBAC) models are policy neutral; they can support different authorization policies, including mandatory and discretionary policies, through the appropriate role configuration. In Role Base Access Control, permissions are granted with roles and users are assigned to appropriate roles. This greatly simplifies management of permissions. Roles are created for the various job functions in an organization and users are assigned roles based on their responsibilities and qualifications. Users can have reassigned from one role to another. Roles can be granted new permissions as new applications and systems are incorporated, and permissions can be revoked from roles from roles as needed. The role's concept was introduced between the users and authority, and the roles and users will be linked, through the role authorization to control the access of system resources. Role Base Access Control 96 model is a typical representation of the Role Base Access Control model. This model used three sets of entities called users (U), roles(R), and permissions (P) and also shows a collection of sessions(S). A user in this model is a human being. The concept of a user can be generalized to include intelligent agents such as robots or even network of computers. A role is a job function or job title within the organization with some associated semantics regarding the authority and responsibility conferred on a member of the role.

Proposed Model: A modified Role Base Access Control model for Data Security.

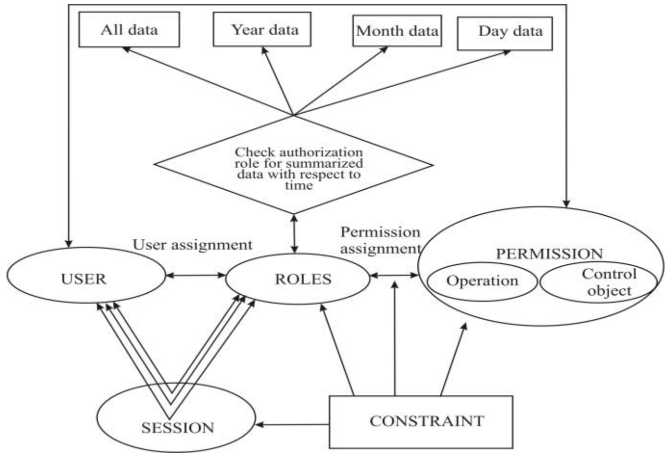

Figure 2: *A modified Role base Access Control model for Data security*

From figure 2, each session is a mapping of one user to possibly many roles, that is, a user establishes a session during which the user activates some subset of roles. The double headed arrow from session to Role in figure 2 indicates that multiple roles are simultaneously activated. The permissions available to the user are the union of permissions from all roles activated in that session. Each session is associated with a single user, as indicated by the single headed arrow from the session to User (U). This association remains constant for the life of a session. Role hierarchies are natural means for structuring roles to reflect an organization's line of authority and responsibility. Constraints are powerful mechanism for laying out higher level organizational policy. With respect to Role Base Access Control 96 model constraints can apply to the User Access (UA) and Permission Access (PA) relations and the user and roles functions for various sessions. Constraints are predicates which, applied to these relations and functions, return a value of "valid" or "not valid".

IV. THE MATHEMATICAL FOUNDATION OF PROPOSED SYSTEM.

The proposed modified Role Base Access Control has the following mathematical foundation drawn from the table 1.

Table 1: *Authorization levels of summarization with respect to time*

Levels of summarization	Category of Users
Day	Ordinary user
Month	Classified user
Year	Confidential user
All Time	Executive user

The levels of summarization and the time span in the proposed modified Role Base Access Control model are as follows:

Authorization level of ordinary user is given as

$$= \sum_{n=1}^{1} Dn \qquad (1)$$

From equation 1, an Ordinary User of this software can only access data/ information for only a day from the database. Any attempt to go beyond that will be denied.

Authorization level of Classified User is given as:

$$= \sum_{n=1}^{30} Dn \qquad (2)$$

From equation 2, Classified User can only access data/information for only a month duration that is (from n= 1 …30 days' duration) from the database. Any attempt to go beyond that will be disallowed.

Authorization level of a Confidential User is given as:

$$= \sum_{n=1}^{360} Dn \qquad (3)$$

From equation 3, Confidential User can only access data/information for only a year duration that is (from n= 1…360 days' duration) from the database. Any attempt to go beyond that will be disallowed.

Authorization level of an Executive User is

given $= \sum_{n=1}^{w} Dn$ (4)

From equation 4, Executive User can access the all data/information from the database.

VI. REFERENCES

[1]. McKendrick, J. (2012), IOUG Enterprise Data Security Survey 2012: Closing the Security Gap, The Independent Oracle Users Group (IOUG) Security Report November, 2012.

[2]. Kobielus, J. (2009), "The Forrester Wave: Enterprise Data storage Platforms, Forrester Research Report, and 1. http://searchdatamanagement.techtarget.com/news/1356934

[3]. Thuraisingham, B., M. Kantarcioglu (2007)."Extended RBAC-based Design and implementation for a secure data storage "An International Journal of Business Intelligence and Data Mining vol2, Issue 4: pp 367- 382.

[4]. Kundu, A., Sural, S. and A. K. Majumdar (2010)" Database Intrusion Detection Using Sequence Alignment" An international journal of information Security, volume9, Issues3 (Jun 2010): pg179-191.

[5]. Santos, R. J., J. Bernardino, et al (2011). "A survey on data security of stored data: Issues, challenges and opportunities "An IEEE International Conference on Computer as a Tool (EUROCON), Lisbon.

[6]. Kangsoo J and Seog P (2013) Context-Aware Role Based Access Control Using User relationship "An International Journal of Computer Theory and Engineering", Vol. 5, No. 3, June 2013.

[7]. Raimundas M and Henri L (2015) A Model-driven

Role-based Access Control SQL Databases: Complex Systems Informatics and Modeling Quarterly CSIMQ, Issue 3, July, 2015, Pages 35-62, A Journal of Institute of Computer Science, University of Tartu, J. Liivi 2, 50409 Tartu, Estonia. https://csimq-journals.rtu.lv/article/view/1074

[8]. Shermin, M (2013) "An Access Control Model for NoSQL Databases" An Electronic Thesis and Dissertation Repository. Paper 1797. http://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=3294.

[9]. Kambiz, G and Mehdi, G" (2015) Dynamic Modeling for Representing Access Control Policies Effect "An International Journal of advanced studies in Computer Science and Engineering IJASCSE, Volume 4, Issue 7, 2015.

[10]. Ankit.V, Ratish.A and Sachin. G" (2015) A Methodology for Development and Verification of Access Control System in Cloud Computing" An International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 3, March 2015.

[11]. Tarai.T and Pradipta. K.M. (2013)" Enhancing database access control policies" An American International Journal of Research in Science, Technology Engineering & Mathematics, 3(1), June-August, 2013, pg 109- 113 AIJRSTEM.

[12]. Rosic. D, Imre. L, Srdjan. V (2015) "A Role-based Access Control Model Supporting Regional Division in Smart Grid System" Acta Polytechnica Hungarica Vol. 12, No. 7, 2015.