RESEARCHERID
THOMSON REUTERS

[Adamu* 4(4): April, 2017] ISSN 2349-4506
Impact Factor: 2.785

Global Journal of Engineering Science and Research Management

ACCESS CONTROL IN DISTRIBUTED HEALTHCARE INFORMATION: THE KEY FEATURES

Abdulkadir .A. Adamu*, Dong Wang, Abdul-Fatou Adam
* College of Information Science and Engineering, Hunan University Changsha, China

DOI: 10.5281/zenodo.569969

KEYWORDS: Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC).

ABSTRACT
Information and communication technologies (ICTs) today provide ubiquitous possibilities to share electronic patient's data across several healthcare organizations and hospital departments. Data security is therefore a strong requirement to ensure compliance with confidentiality and privacy rule of medical records. However, access control mechanism in Nigeria's health information systems do not sufficiently guarantee managed access, data and resource protection. To conquer the problems existing in the current access control mechanism available to University of Abuja Teaching Hospital (UATH), Nigeria, a new access control mechanism called multi-device TBPM-RBAC (MD-TBPM-RBAC) is proposed in this paper. According to the demand for unified users' management in the network management system (NMS), MD-TBPM-RBAC uses Role-Based Access Control (RBAC) for the center, and expands the TBPM-RBAC. In MD-RBPM-RBAC, the users, resources and permissions are stored in the remote server, when a user lands, the device will communicate with the server to authenticate and authorize. As the MD-TBPM-RBAC implements the users' unified authentication and authorization, the user's management is centralized, it protects the resources effectively, and prevents the important resources from illegal access. In essence, the access control mechanisms and authorization structures of information systems must be able to realize the Need-To-Access principle. This paper introduces the design principles and critically evaluates the concept.

INTRODUCTION
The Nigerian medical services have endured a few down-falls. Despite Nigerian's key position in Africa, the nation is incredibly underserved in the health care cycle. Health care offices are insufficient in Nigeria, particularly in rural areas. While different changes have been put forward by the Nigerian government to address the boundless issues in the health care sector, they are yet to be executed at the state and local government area levels. According to a 2009 communiqué of the Nigerian national health care conference, healthcare framework stays feeble as proven by absence of coordination, discontinuity of administrations, lack of assets, including medication and supplies, etc.[1]. This has led to suggestions to improve the health care situation in Nigeria using access control models.

Due to the increasing adaptation of information and communication technology in healthcare, one of the important areas of improvement in healthcare organizations is the use of Electronic Patient Records (EPR) that is distributed over many locations in order to provide access to medical information about a patient to healthcare professionals. This enables medical personnel to gain access to personal health information, test results, clinical or pharmaceutical data, from everywhere in and around the healthcare institution. Mobility and improved availability allows health personnel to dynamically access patient information enhancing efficiency in healthcare management [2]. Sharing sensitive patient data in a large distributed and heterogeneous environment, inherently introduces security and privacy risks [2]. These risks are further increased by the enhanced openness that can be achieved by the use of Web-based applications and pervasive devices in e-Health [4]. Despite the sensitivity of the data and the growing threat, relatively little attention has been paid to the complexities of real-world access constraints in middleware development. Much attention has been given to encryption techniques but, while encryption is certainly important, it protects only the communication and authentication in the system. It provides only the basis for a secure access control mechanism [6]. Therefore design of an access control mechanism to protect the confidential health information system data from unauthorized visiting and modification is inevitable [2, 10].

Access control mechanism is a series of measures of protecting the resources to detect and prevent unauthorized access of systems - Role-Based Access Control (RBAC) models are receiving increasing attention as a recent generalized approach to access control [10, 12]. In RBAC models, user's rights to access computer resources (objects) are determined by the user's assignment to a role and by the roles' permissions to perform operations on objects [2]. Through this mechanism, it can be decide who can access what resources of the information system and how to use these resources, thus the confidentiality, integrity and availability of the computer information system can be further ensured [10].

RBAC is a proven advantageous concept offering simplified authorization administration because a security administrator needs only to revoke and assign the new appropriate role membership if a user changes its job function. Secondly RBAC shows to be policy neutral and offers flexibility with respect to different security policy objectives and it is widely accepted in the industry and deployed in several products like ORACLE DBMS. RBAC privacy extensions could be easily deployed in systems already adopting RBAC, thus allowing one to seamlessly introduce access control policies specialized for privacy enforcement [2, 4].
Therefore, this paper proposes a solution to the problem of managing unified users and protection of confidential data from unauthorized visiting and modification. The next section reviews the access control mechanism used. A TBPM-RBAC model is proposed, while the analysis of the MD-TBPM-RBAC using NMS is analyzed.

REVIEW OF ACCESS CONTROL MECHANISM

Access control models are sometimes categorized as either discretionary or non-discretionary. The three most widely recognized models are Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC). MAC and RBAC are both non-discretionary.

Discretionary Access Control (DAC)
Discretionary access control (DAC) is an access policy determined by the owner of an object. The owner decides who is allowed to access the object and what privileges they have. Two important concepts in DAC are:

i. File and data ownership: Every object in the system has an owner. In most DAC systems, each object's initial owner is the subject that caused it to be created. The access policy for an object is determined by its owner.
ii. Access rights and permissions: These are the controls that an owner can assign to other subjects for specific resources.

Access controls may be discretionary in ACL-based or capability-based access control systems. (In capability-based systems, there is usually no explicit concept of 'owner', but the creator of an object has a similar degree of control over its access policy [13].

Mandatory Access Control (MAC)
Mandatory Access Control (MAC) is an access policy determined by the system, not the owner. MAC is used in multilevel systems that process highly sensitive data, such as classified government and military information. A multilevel system is a single computer system that handles multiple classification levels between subjects and objects.

Sensitivity labels: In a MAC-based system, all subjects and objects must have labels assigned to them. A subject's sensitivity label specifies its level of trust. An object's sensitivity label specifies the level of trust required for access. In order to access a given object, the subject must have a sensitivity level equal to or higher than the requested object.

Data import and export: Controlling the import of information from other systems and export to other systems (including printers) is a critical function of MAC-based systems, which must ensure that sensitivity labels are properly maintained and implemented so that sensitive information is appropriately protected at all times [1].

Role-Based Access Control (RBAC)
With the continuous complexity of application system, the traditional access control models are not conducive to realize the system unity and the overall access control increasingly. Role-based access control (RBAC) is an

access policy determined by the system, not the owner. Compared with DAC and MAC, the concept of role which is a method of indicating the many-to-many relationship between user and permission is introduced into RBAC. In this mechanism, the role is used to show user's responsibilities and authorities, all the authorizations are given to roles, not users or groups, which makes the changes between roles and permissions more stable than that between roles and users. Therefore, the complexity of authorization management can be decreased, the administration burden can be reduced, and the security administration can be greatly simplified. In RBAC, all the relationships between users and roles, roles and permissions, roles and resources are many-to-many. That is to say, a user can have many roles, a role can be granted to multiple users, a role also can possess a number of permissions, and permission can be possessed by multiple roles [15].

TBPM-RBAC

Task-Based Permissions Management in RBAC (TBPM-RBAC) was proposed in 2005 by [10]. TBPM-RBAC was developed to solve the following problems existing existing in RBAC.

1. Difficulty in solving in configuring permissions due to the differences between roles and permissions in abstraction layer.
2. Secondly difficulties associated with dependencies.

Embedding TBAC model into RBAC, TBPM-RBAC retains all the elements of RBAC. So it can be used to describe RBAC, and has a better description capability than RBAC. In TBPM-RBAC, the permissions are granted to tasks at first, the tasks are granted to roles next, and the permissions are not granted to roles directly at all.

TBPM-RBAC model can support the principle of least privilege well. During the permissions configuration, the users are granted the needed roles only, the roles are granted the needed tasks only, and the tasks are granted the needed permissions only. So the users can use the corresponding permissions during executing tasks only, and cannot use them at any other time, which can prevent authority from abusing and misusing effectively. TBPM-RBAC can also support responsibility isolation well, that is to say, we can set up exclusive roles, exclusive missions and exclusive permissions during configuration permissions. At the same time, exclusive roles must be assumed by different users, exclusive tasks must be executed by different roles, and exclusive permissions must be granted to different tasks. Certainly, the relationship among the tasks granted exclusive permissions is mutually exclusive; the relationship among the roles executing exclusive tasks is mutually exclusive, too. Dividing sensitive jobs of system into several mutually exclusive parts can prevent the vandalism caused by user's excessive powers effectively [14].

PROPOSED ACCESS CONTROL MECHANISM

An integrated system as described in this paper, integrates safety management into traditional NMS, including the following functions: automatic topology discovery, traffic and link utilization statistics, remote monitoring, fault management, performance maintenance, security management and so on. In this NMS, it is necessary to manage the entire network's devices unified, that means the users of these devices need to be authenticated and authorized unified. But the centralized management of users for multiple devices was not involved in the past access control strategies, so a new access control called Multi-device task-based permissions management in RBAC(MD-TBPM-RBAC) is proposed in this paper. At the core of RBAC, MD-TBPM-RBAC does the further expansion of TBPM-RBAC. According to the device identification, the permissions are granted to tasks first, and then the tasks are granted to roles, finally the authorities are assigned. The MD-TBPM-RBAC model and related definitions are introduced as follows.

MD-TBPM-RBAC Model

The model of the proposed access control mechanism is shown below in Figure 1.

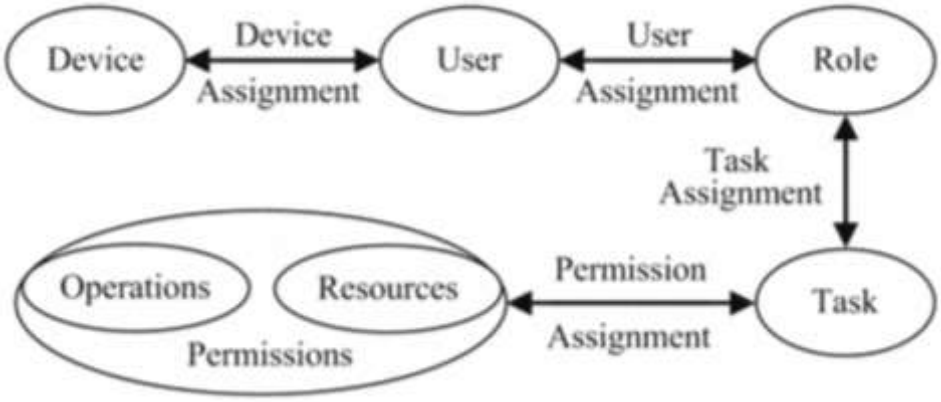

Figure 1: MID-TBPM-RBAC Model [10]

The Related Definition of MD-TBPM-RBAC

The MD-TBPM-RBAC model is defined as follows;

MD-TBPM-RBAC = (Device, User, Role, Task, Permission).

1) Device (D): all the kinds of equipment managed by the User Management Center (UMC) in the network, including PC, Router, Switcher, Terminal, Server and so on.

2) User (U): the subject who can visit the system on his/her own. It may be a person, a computer, a process, or software with the function of self-government.

3) Role (RO): the semantic expression of job functions in the organization [10]. It represents that the user who has been granted certain roles has certain qualifications, powers and responsibilities.

4) Task (T): a logical unit during the operation. One task can contain many sub-tasks, can be completed by one user and also can be done by a lot of users in collaboration.

5) Permission (P): the permit of subject to object. For files and directories, it can be set to read-only, writing, modifying the access rights, and whether to audit. For process resources, it can be set whether to end some processes or not; for network resources, it can be set whether the businesses or the processes can use its data to communicate or not; for the service, it can be set whether to start or stop.

6) Operation (OP): the action of visiting resources in the system. It can be reading, writing or executing in the file systems and it may be inserting, deleting, adding, or updating in the database management systems.

7) Resource (RE): a passive entity. It can be dictionary, file, process, service, network resource and so on, but the access to these resources must be controlled.

8) Device Assignment (DA): express the situation of assigning unique device identification in the system, and express which device the user belongs to. *DA ~ D xU,* if *(u, d)* E *DA,* then the user *U* is the user of device *d.*

9) User Assignment (UA): express the situation of granting roles to users in the system UA~UxRO, if *(u,ro)EUA,* then the user *U* has been granted to the role *ro.*

10) Task Assignment! (TA): express the situation of assuming tasks in the system. *TA ~ RO* x *T,* if *(ro, t) ETA,* then the role *ro* has assumed the task *t.*

11) Permission Assignment! (PA): express the permissions of tasks during the execution in the system. *PA ~ T* x *P,* if *(t, p) EPA,* then the task *t* has the permission *p* during the execution.

c. *Permission List in the Database*

The information used to decide the permissions of users of each device in the network, is stored in the form of permission list in the User's Authority Database. The permission list is shown in table I.

For instance, *(D1, V1, R01, T1, RE1, Read)* in the list means the *V1* of *D1* whose role is *R01* can read *RE1* during the execution *of T1.*

Table 1:Permission List

Device	User	Role	Task	Resource	Permission
D1	U1	RO1	T1	RE1	Reed
D1	U2	RO2	T2	RE2	Write
D2	U1	RO2	T3	RE3	Execute
D3	U3	RO2	T1	RE2	Read, Write

ANALYSIS OF MD-RBPM-RBAC USING THE NMS

An agent used to get the resource information of devices has been installed in every device in the network. When the device is started by users, the resource information would be collected to send to the User Management Center (UMC). So the user information and resource information will be stored in the remote UMC, and the access control information will be saved in the form of access control list. When the user input his/her username and password, it will communicate with UMC to authenticate its legitimacy. During the authentication, except that a UMC is to be needed as the authentication system, an authentication server which Radius Server (RS) has been used to be in this NMS is also necessary. When the user has input his/her username and password to ask for authentication, the execution will be completed by UMC and RS through communication with each other, finally the authentication result will be returned to devices by UMC. After the authentication is successful, the MD-TBPM-RBAC access control mechanism is used to access the User's Authority Database in accordance with the username and device identification, and then the permission resources of this user will be returned to the management platform, so the user can only visit the permission resources.

In this NMS, in order to achieve unified management of users, four steps are designed.
Step 1: When the user lands on the equipment, he/she need to register through the interface of registration if he/she has no username and password. If he/she was a registered user, he/she can enter the login interface and input his/her username and password to authenticate through the interface of authentication. The authentication needs to be complemented at the remote UMC. Finally all the user information will be stored through the Unified User Information (UDI) module.
Step 2: After the authentication is successful, the program which is used to get the resources information, including File Information (FI), Device Information (DI) and Process Information (PI), and device number will be run. Then the information will be saved through the module of Unified Resource Dictionary (URD), and sent to the UMC.
Step 3: After the UMC has received the information, whether the record of the device exists, the authority of database should be selected at first. The information of the device would be saved if there are no records, or the update should be checked. If there is some new information of the device, the update must be done, or nothing needs to be done.
Step 4: The UMC traverses all the permissions of these users in the device, and returns them to the User Unified Management Platform (UUMP) through the interface of access control. So when the user has landed on the device, he/she can only visit the authority resources.

CONCLUSIONS

In accordance with the demand for unified user management in the NMS, an access control mechanism which is suitable to the NMS is proposed in this paper, which is improved based on the TBPM-RBAC. In the MD-TBPM-RBAC, a centralized user management is implemented through a unified authentication and authorization. The mechanism allows the users to visit the authorized resources only, so the resource information and the critical process being stopped illegally can be protected, and the important resources being visited illegally can be prevented.

REFERENCES

[1] Hansen, F., & Oleshchuk, V. (2003, June). Application of role-based access control in wireless healthcare information systems. In *Scandinavian Conference in Health Informatics* (pp. 30-33).
[2] Ferreira, A., Chadwick, D., & Antunes, L. (2007). Modelling access control for healthcare information systems. In *Doctoral Consortium at the 9th International Conference on Enterprise Information Systems, ICEIS*.

[3] Martino, L. D., Ni, Q., Lin, D., & Bertino, E. (2008, January). Multi-domain and privacy-aware role based access control in ehealth. In *Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference on* (pp. 131-134). IEEE.
[4] Røstad, L., & Alsos, O. A. (2009, March). Patient-administered access control: a usability study. In *Availability, Reliability and Security, 2009. ARES'09. International Conference on* (pp. 877-881). IEEE.
[5] Evered, M., & Bögeholz, S. (2004, January). A case study in access control requirements for a health information system. In *Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation-Volume 32* (pp. 53-61). Australian Computer Society, Inc..
[6] Xiao, L., Hu, B., Croitoru, M., Lewis, P., & Dasmahapatra, S. (2010). A knowledgeable security model for distributed health information systems. *computers & security*, *29*(3), 331-349.
[7] Al Kukhun, D., Codreanu, D., Manzat, A. M., & Sedes, F. (2012). Applying Pervasive and Flexible Access Control to Distributed Multimedia Retrieval. In *IMMoA* (pp. 41-48).
[8] Liu, X., Chen, L., & Duan, C. (2009, December). Access control in network management system. In *Power Electronics and Intelligent Transportation System (PEITS), 2009 2nd International Conference on* (Vol. 1, pp. 227-230). IEEE.
[9] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer*, *29*(2), 38-47.
[10] Bertino, E., Bonatti, P. A., & Ferrari, E. (2001). TRBAC: A temporal role-based access control model. *ACM Transactions on Information and System Security (TISSEC)*, *4*(3), 191-233.
[11] Yu, W. A. N. G. (2005). QING Si-Han Engineering Research Center for Information Security Technology, Institute of Software, Chinese Academy of Sciences, Beijing 100080; A New Access Control Model——TBPM-RBAC [J]. *Computer Science*, *2*.
[12] Bindiganavale, V., & Ouyang, J. (2006, September). Role based access control in enterprise application-security administration and user management. In *Information Reuse and Integration, 2006 IEEE International Conference on* (pp. 111-116). IEEE.
[13] Harn, L., & Lin, H. Y. (1992). Integration of user authentication and access control. *IEE Proceedings E (Computers and Digital Techniques)*, *139*(2), 139-143.
[14] Zhao, H., Fang, Z., Xu, P., Zhao, L., Liu, J., & Wang, T. (2008, April). An improved role-based workflow access control model. In *Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on* (pp. 551-556). IEEE.
[15] Yu, W. A. N. G. (2005). QING Si-Han Engineering Research Center for Information Security Technology, Institute of Software, Chinese Academy of Sciences, Beijing 100080; A New Access Control Model——TBPM-RBAC [J]. *Computer Science*, *2*.