LAUTECH Journal of Engineering and Technology 8(2)2014: 84 - 93

EMPIRICAL EVALUATION OF ROLE-BASED ACCESS CONTROL AND BELL- LA PADULA CONFIDENTIALITY SECURITY MODELS

[1]Nureni A. Azeez, [2]O.B Okunoye O.B [3]F.A Oladeji, [4]O.O Vaughan

[1,2,3,4]Department of Computer Sciences,
University of Lagos, Nigeria

[1]nurayhn@yahoo.ca, [2]bokunoye@unilag.edu.ng, [3] foladeji@unilag.edu.ng, [4]nifemivaughan@gmail.com

ABSTRACT

Medical records are well known to contain vital, sensitive and treasurable information about patients and it is therefore important to guard them against any form of unpermitted or unauthorized access. The motive behind this paper is to benchmark Role Based Access Control (RBAC) and Bell-la Padula security models in a medical domain. Attempt was made to implement these models by evaluating their efficiencies, protection capacity, precision and speed. Role Base Access Control is a security model which allows a user at a higher level to access roles and permissions of a user at a lower level of his organization hierarchy. Bell-la Padula on the other hand uses the "no read-up, no write-down" method of implementation; that is, it does not allow a user at a higher level to write to a user at a lower level. Also, a user at a lower level cannot read up the hierarchy. Comparison of these two access control security models were evaluated in the medical domain based on the above listed metrics. The prototype of this work was implemented using Microsoft C# on the .Net framework with Microsoft's SQL as the backend. The result shows the prototype of the RBAC models is better in terms of efficiency, protection capacity, precision and speed.

INTRODUCTION

There is fear in the heart of patients of many hospitals; particularly in Nigeria about the security of their information when compelled to be given to a doctor or any medical personnel for references. It is believed that anybody can come across the information, view and modify it illegally.

Before the advent of ICT, patient records were stored manually with the use of papers, cards and files (Alessandro, Roberto, Alberto, & Nino , 2009). As a result of this, files were misplaced, old papers became dirty and torn, some of the write-ups even became missing, therefore proper supervision and up to date track of records of particular patients are impossible.

With the invention of programming languages for application development, several systems have been developed to make work and tracking of patient records more convenient (Ferreira, Cruz-Correia, Antunes, Farinnha, Oliveira-Palhares, & Chawick, 2006). This leads us to the development of the Electronic Medical Records (EMR) (see Figure 1). Record keeping through papers and files are therefore reduced to its minimal level since they are done electronically (Foster, Kesselman, Tsudik, & Tuecke, 1998). Electronic Medical Records (EMR) can be defined as the computerization of information of patients in a medical organisation. It is on this clinical information that health care personnel base their decisions regarding health care of individual patients (Houmb, Georg, France, & Matheson, 2004).

There is also the need to control the access of users to patient records on the EMR database since different departments of the hospital needs different information about patients. The pathologist only needs the blood group, type and sample of a patient while the optician might only needs details about his eye colour and type (Imine, Cherif, & Rusinowitch, 2009). Efforts were made to implement two different access control models; RBAC and Bell-la Padula. The objective is to assess the best for achieving a dependable and efficient access control in EMR.

The sensitive nature of medical information undoubtedly calls for restriction of unauthorised users. Cases reported in the past on the effects of vulnerable medical information have put people at alert on the need to avoid future occurrences.

To handle possible future undesirable effects and to ensure that medical information is well protected, this study benchmarks the application of two different security models to see which one is better at safeguarding information of patients in hospitals.

Research questions
To provide satisfactory answer to the challenges being addressed in this paper, the following questions were posed:

- How can we ensure that sensitive information in the hospital is not vulnerable?
- How do we ensure appropriate, adequate and efficient security policy in medical domain?
- How do we benchmark the performance of the chosen security models: BLP and RBAC when implemented for health-based information?

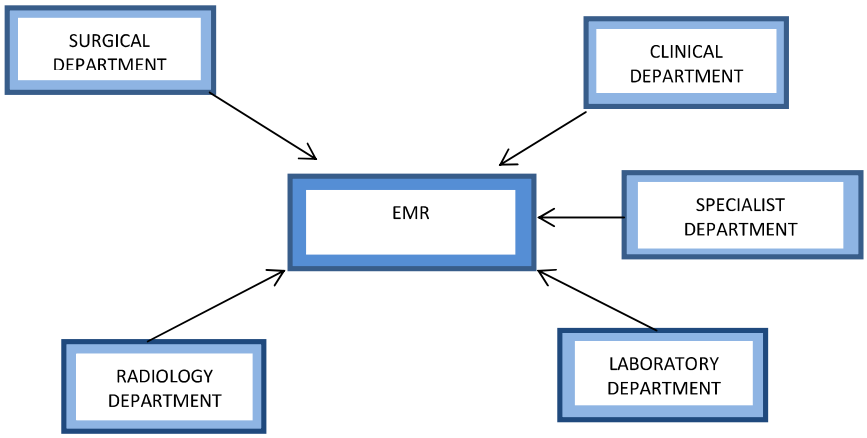

Figure 1: The illustration of the Electronic Medical Records (EMR) database.

Figure 1 shows a typical database for Electronic Medical Record in a typical hospital. The EMR contains five different departments, namely: surgical department, clinical department, radiological department, laboratory department and specialist department.

Table 1: assigning roles to several permissions

1. ROLES	PERMISSIONS
3. Doctor	*{read TEXT, write TEXT, read ROS}*
4. Nurse	*{ read ROS, write ROS, read TEXT}*
5. Surgeons	*{read TEXT, write TEXT, read ROS, read RIS, read PACS}*
6. Matrons	*{read PAS, write ROS, read ROS}*
7. Psychotherapist	*{ read RIS, read TEXT, write TEXT, read PACS}*
8. Pathologist	*{read TEXT, write TEXT, read ROS, read PAS}*
9. Dentist	*{read TEXT ,write TEXT, read ROS ,read PAS, read PACS}*
10. Dietician	*{read TEXT, write TEXT, read ROS ,read PAS, write PAS}*
11. Psychiatrist	*{read TEXT ,write TEXT, read PAS ,write PAS}*
12. Paediatricians	*{read ROS ,read RIS, read PACS}*
13. Gynaecologist	*{ read TEXT, read ROS, read PAS, write TEXT}*
14. Neurologist	*{read ROS, read RIS, read PACS, write TEXT, read TEXT}*
15. Cardiologist	*{read ROS, read/write TEXT, read PACS, read RIS}*
16. Pharmacist	*{ read TEXT, write TEXT}*
17. Radiologist	*{Read RIS/PACS, Write RIS/PACS}*
18. Laboratory assistant	*{Write ROS}*
19. Receptionist	*{read PAS, write PAS}*
20. Radiographer	*{Write RIS/PACS, Read PAS, Write PAS}*
21. Secretary	*{Read PAS, write PAS}*
22. Ophthalmologist	*{read TEXT, write TEXT, read RIS/PACS)*

To have specified permissions for different roles with reference to this paper, Table 1 shows permissions given to different hospital roles. The implication of this is that, if specific permission is not given to a role, there will not be access privilege and constraint in any form to such a role.

Description of short terms used in this project
TEXT- text part of patient's records
ROS- Result of Samples
RIS- Roentgen (x-ray image) Information System
PACS- Picture Achieve and Communication System
PAS-Patient Administration System
Application of Bell-la Padula Confidentiality access control model on Electronic Medical Records.
Implementing the Bell-la Padula confidentiality model on the radiology department gives the following illustration.

There is a presence of a large database called the Electronic Medical Record which allows different users to get information from it depending on their given permissions. In a Clinical ward for example, the users that gain access to the EMR are the nurse, doctor, matron, and secretary/receptionist.
The Radiology department consists of the radiographer, radiologist and the doctor. The Surgical ward consists of a surgeon, a doctor, nurse, matron and pathologist. Applying the Bell-la Padula confidentiality model on ward of a hospital gives the following illustration; The **Specialist ward** consists of the Psychotherapist, Pathologist, Dentist, Dietician, Psychiatrist, Paediatric, Gynaecologist, Neurologist, Cardiologist and the laboratory assistant.

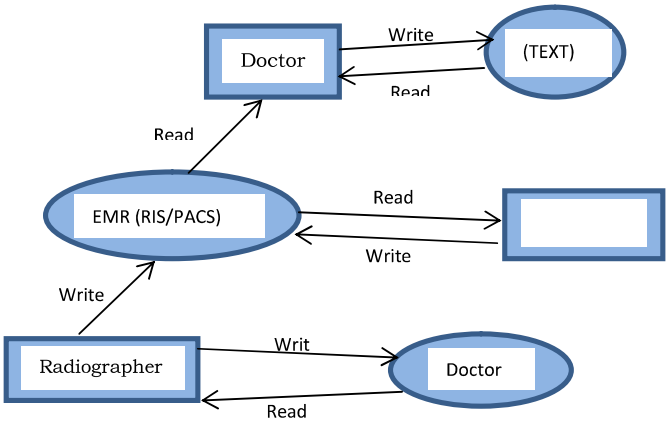

Figure 2: Information flow of bell-la Padula model in a Radiology department.

A specialist is referred to as someone who majors in the treatment of a particular medical condition or the treatment of a particular sex or age group of patients. The area of specialization of the specified specialist is already discussed above.
When specific blood tests/x-rays has been done, the pathologist deciphers the medical condition of the patient and refers him to the specialist in charge of his medical condition. The following is the application of bell-la Padula access control model on the specialist ward of a hospital.
It is clearly evident that the application of Bell-la Padula as demonstrated in both Figures 2 and 3, allows the usage of "no read-up, no write-down" method of implementation; that is, it does not allow a user at a higher level to write to a user at a lower level. Also, a user at a lower level cannot read up the hierarchy. This is completely different from implementation of RBAC.

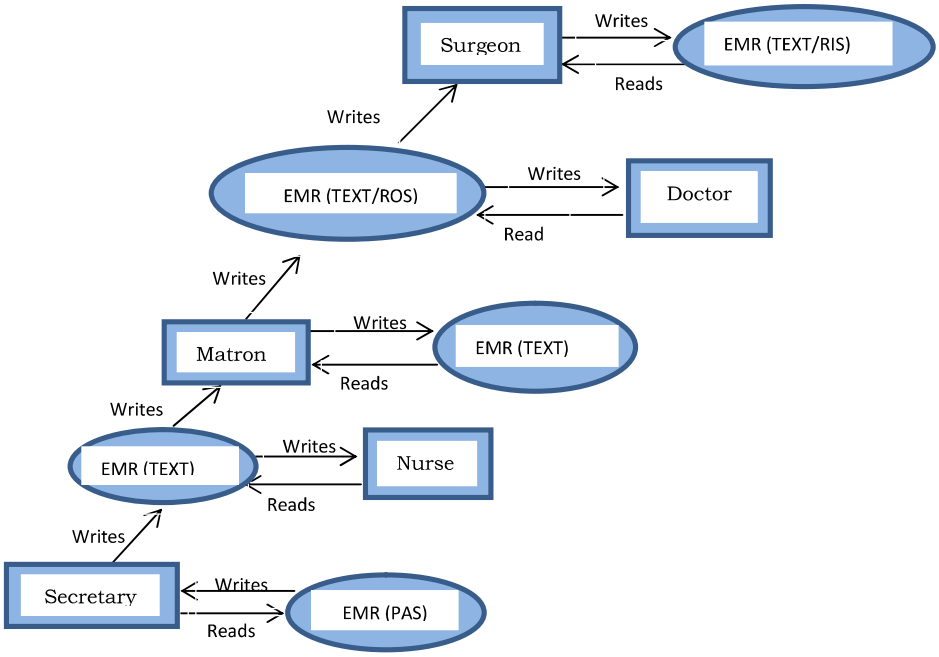

Figure 3: Representation of Bell-la Padula model in a surgical ward.

Table 2: Different wards and their members of staff

WARDS/DEPARTMENT	MEMBERS/STAFFS
Clinical	Receptionist, Secretary, Nurse, Matron, Doctor, Pharmacist.
Surgical	Secretary, Nurse, Matron, Doctor, Anaesthetics, Surgeon
Radiology	Laboratory attendant, Radiographer, Radiologist, Doctor
Laboratory	Laboratory attendant, Pathologist, Doctor
Specialist	Doctor, Physiotherapist, Ophthalmologist, Dietician, Gynaecologist, Paediatrics, Neurologist, Cardiologist, Dentist.

Illustration of Role Based Access Control Model on Electronic Medical Records.

There are four types of the Role Based Access Control model (Dynamic, Static, Core and hierarchical). However, for the scope of this study, the hierarchical RBAC shall be considered. In hierarchical RBAC, users at a higher level of the organization organogram inherit roles and permission of the users at the lower levels in addition to theirs which they have access to. In the case of a medical organisation, there are different departments such as the radiology, clinical and specialist departments.

Each head of the department inherits all the roles and permissions of the younger staffs under his supervision in addition to his. The head of the medical organisation such as the medical practitioner inherits all the roles and permissions of all heads in the various departments.

The **Clinical Ward** consists of the Receptionist, Secretary, Nurse, Matron, Doctor and the Pharmacist. Implementing the RBAC model gives the following illustration:

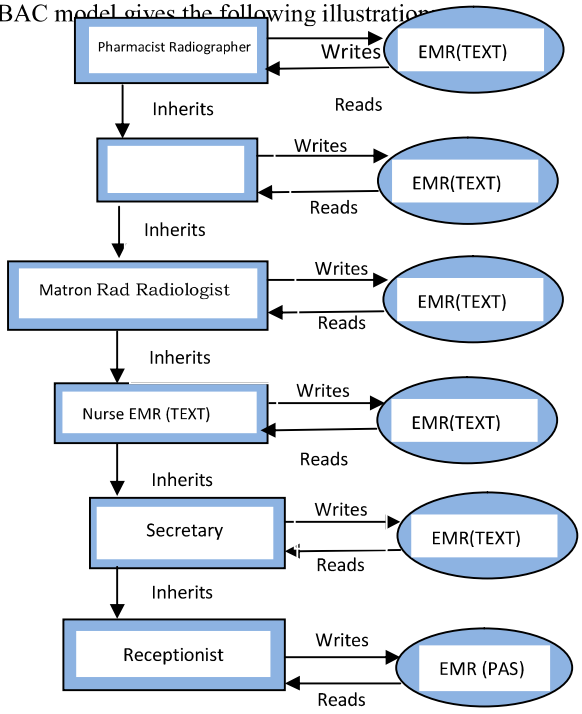

Figure 4: The representation of the RBAC model in a Clinical Ward.

The **Radiology department** consists of the Laboratory attendant, Radiographer, Radiologist, and the Doctor. Implementing the RBAC model on this department gives the following illustration:

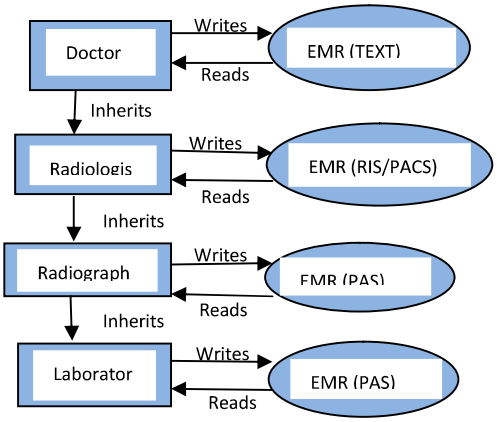

Figure 5: The representation of the RBAC model in a Radiology Department.

Implementing the RBAC model on the **Laboratory department** gives the following illustration:

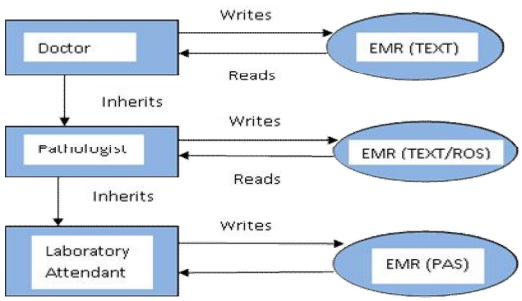

Figure 6: The representation of the RBAC model in the Laboratory Department.

Implementing the RBAC model on the **Surgical Ward** gives the following illustration:

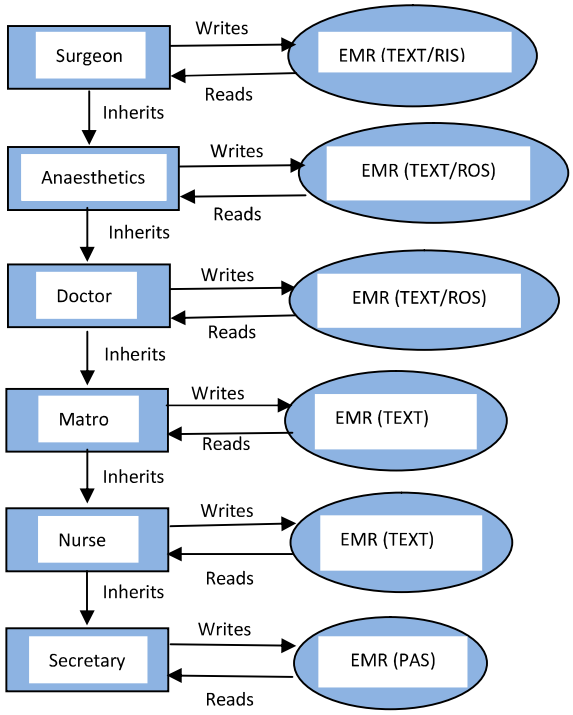

Figure 7: The representation of RBAC model in a Surgical Ward.

For Figures 4, 5, 6, and 7, there is hierarchical access of roles from upper level of each of the wards to the bottom of the hierarchy. In other words, users in the topmost hierarchy can conveniently access all roles at the lower levels. Conversely, the lower level roles cannot be permitted for any access at his top level.

Definitions of Entities Used in RBAC
U, R, P, GR {Users, Roles, Permissions, Group roles}

U = {User_1, User_2, User_3 … User_n}
R = {Role_1, Role_2, Role_3 … Role_n}
P = {read/write TEXT, read/write ROS, read/write RIS, read/write PACS, read/write PAS}
GR CG×R {A group to role assignment}

Data Flow Diagram of the implementation
To better understand the inner workings of the system, we expand on the context diagram to expose the important data stores and processes. The Level 1 Data Flow Diagram is shown below.

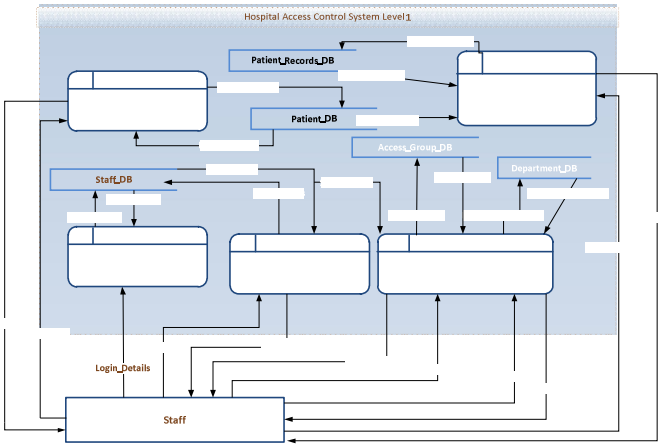

Figure 8: The Level 1 Data Flow Diagram of the System

Table 3: Comparison between RBAC and Bell-la Padula security models

TERM	RBAC	BELL-LA PADULA	BEST FIT
Efficiency	Very efficient as it works perfectly in any organisation.	More effective in military systems.	RBAC
Speed	The speed and time strength of feedback when request is made in the database is faster	Slower than RBAC.	RBAC
Security	Permissions are provided to roles in RBAC and not to individual users. Individual will NOT be able to alter and manipulate the information	Documents are attached an access level strength which might not be too strong	RBAC
Scalability	More roles and different users can be accommodated at any point in time	Limited roles are allowed. Strictly military roles.	RBAC

As depicted above, the data flow from external entity "Staff", introduced in the Context diagram is now broadly expanded to show the processes they interact with; as shown in Figure 8; five (5) different processes are used at this level and four (4) data stores are introduced.

User Interface Design

The home screen consists of the title of the project, the name of the student and the login screen. The user inputs his login details (username and password) on the login screen to gain access to the application. It also contains the settings icon which allows the user of the system to decide the access control model he wants to work with which is either RBAC or Bell La-Padula.

The main screen consists of four (4) menus namely; Staff management, Department Management, Bella access groups and the patient records. The user can then click on any menu he wants to gain access to. It is only the administrator that has access to the staff management menu. The detail of the user is shown at the bottom of the screen (see Figure 9).

Figure 9: The menu page of the application.

The staff management menu deals with all the details and information about the registered users on the database of the application. Here, the admin gives login details to each user, records information about them on the database, assigns Bella access level to them in the case of Bell La-Padula or assign roles to them in the case of RBAC. Only the administrator can access this interface.

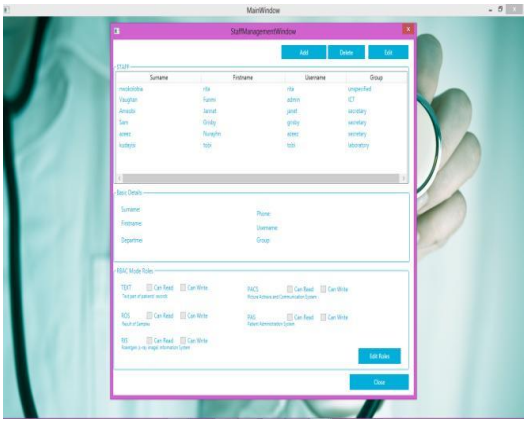

Figure 10: The admin page (Staff management window).

The department management allows the user of the system to view, add and edit departments in the database of the application. Details about the date and time when the departments are created are also included (see Figure 10).
Records can be added, viewed, deleted and the comprehensive report can also be generated.
It could be recalled that RBAC and Bell la-padula are considered. In RBAC, the user can only perform roles based on his permissions and he is denied access to operate on the records he does not have access to. In Bell-la Padula, he can only perform operations that are within his access level. A comprehensive report sheet can be generated consisting on all the records of the particular patient in view.
If a user does not have the permission to perform an operation and he wants to generate a comprehensive report, the report within his roles is generated while the ones out of his reach are seen as classified. Records such as ROS, RIS, and PACS require images to be uploaded (See Figure 11).

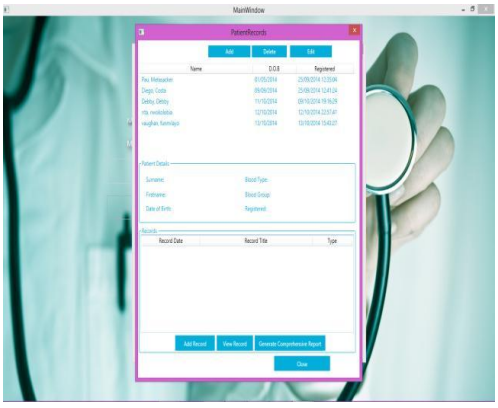

Figure 11: The interface of all records of registered patients.

Table 4: Effect of the response time on the queries issued using SQL Express Dbase Sever

QUERY NUMBER	RBAC	BLP
1	10	12.6
2	15	18
3	17	23
4	20	26
5	22	29
6	24	32
7	27	38
8	30	41

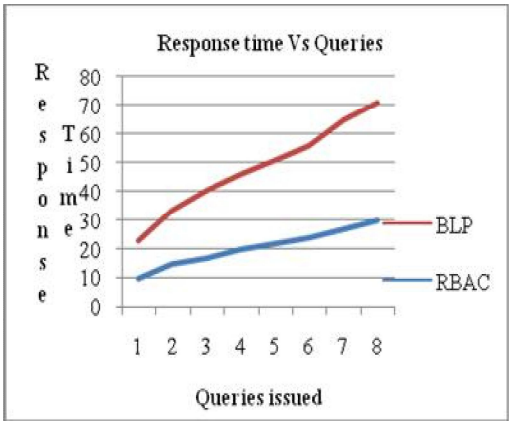

Figure 12: Response time Vs Queries Issued with SQL Express Dbase Sever

Table 5: Effect of the response time on the queries issued using PostgreSQL Dbase Sever

QUERY NUMBER	RBAC	BLP
1	7	10
2	13	16
3	15	19
4	18	22
5	19.6	25
6	22	30
7	24	34
8	27	37.8

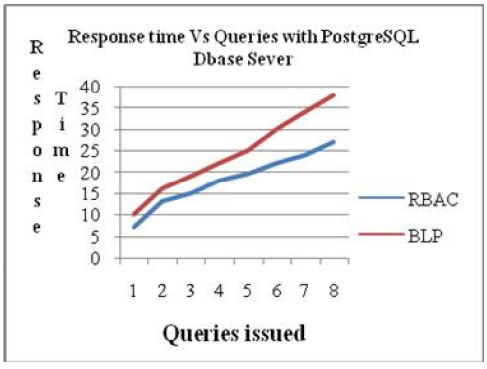

Figure 13: Response time Vs Queries Issued with PostgreSQL Dbase Sever

CONCLUSION

From Figure 12 and Figure 13, it is clearly shown that the RBAC security model is more efficient than BLP. This is more evident when queries were issued to both the SQL Express Dbase Sever and PostgreSQL Dbase Sever. The efficiency of RBAC was noticed when the response time was lower compared to the response time obtained for BLP under the same conditions.

From previous discussions and the latest observation stated above, it has been clearly established that the Role Based access control model is best fit for implementation reliable access control to medical-based information.

REFERENCES

He, C., Cao, C., & Bao, S. (2011). An Enhanced Role-Based Access Control Mechanism for Hospital Information Systems. *2011 Seventh International Conference on Computational Intelligence and Security* (pp. 1001-1005). USA: IEEE Computerc Society.

Hue, P. T., & Wohlgemuth, S. (2011). An Experimental Evaluation for a New Column – Level Access Control Mechanism for Electronic Health Record Systems. *International Journal of u- and e- Service, Science and Technology, 4*(3), 73-86.

NSF. (2000). *Federal Cyber Service:Scholarships forService (SFS) A Federal Cyber Service Training and Education Initiative Program Solicitation.* National ScienceFoundation Solicitation NSF 01-11.

Zhang, X., Li, Q., & Seifert, J. (2007). Flexible Authorization with Decentralized Access Control Model for Grid Computing. *10th IEEE High Assurance Systems Engineering* (pp. 156-165). London: IEEE Computer Society.

Akinsanya, A. K., Zhang, X., Li, Q., & Seifert, J. (2007). Flexible Authorization with Decentralized Access Control Model for Grid Computing. *10th IEEE High Assurance Systems Engineering Symposium* (pp. 156-165). USA: IEEE Computer Society.

Azeez, N. A., Venter, I. M., Iyamu, T., & Oyewole, A. S. (2013). An investigation into five grid security models: their implementation, strengths and weaknesses: An overview of five security models. *International Journal of Applied Computing, 5* (2), 73-86.

Azeez, N. A., & Venter, I. M. (2012). Towards achieving, scalability and interoperability in a Triple-Domain Grid-Based Environment. *11th Annual Information Security South Africa Conference ISSA 2012 , 15 – 17 August 2012* (pp. 1-10). Johannesburg , South Africa: IEEE.

Azeez, N. A., Venter, I. M., & Tiko, I. (2011, 26-28 September). Grid Security Loopholes with proposed countermeasures. *26th International Symposium on Computer and Information Sciences* (pp. 411-418). Imperial College, London: Springer Verlag, London.

Cassell, C., & Symon, G. (1994). Qualitative research in work contexts. *Qualitative methods in organizational research*, pp. 1-13.

Cassell, C., & Symon, G. (1994). *Qualitative research in work contexts.* Qualitative methods in organizational research.

Chris , C., Alana , M., David , V., & Peter, v. (2011). *An Overview of International Cyber-Security Awareness Raising and Educational Initiatives.* Research report commissioned by the Australian Communications and Media Authority.

Copeland, W., & Chiang, C. C. (2012). Securing Enterprise Mobile Information. *International Symposium on Computer, Consumer and Control* (pp. 1-4). IEEE Computer Society.

Furnell , S. M., Gennatou, M., & Dowland , P. S. (2002). A prototype tool for informationsecurity awareness and training. *Logistics InformationManagement, 15*(5-6), 352–357.

Hansche , S. (2001, January/February). Designing a security awareness program. *Part 1, information.Systems Security*, pp. 14–22.

He, C., Cao, C., & Bao, S. (2011). An Enhanced Role-Based Access Control Mechanism for Hospital Information Systems. *2011 Seventh International Conference on Computational Intelligence and Security* (pp. 1001-1005). USA: IEEE Computer Society.

INFOSEC. (2003). http://www.infosecisland.com/blogview/22611-On-the-Cyber-Security-Landscape-in-Africa.html.

INTER. (2011). http://www.internetworldstats.com/asia/sg.htm .

ISF. (2003). *The standard of good practice for information security*. Retrieved from Information Security Forum.

ISO17799. (2000). *Information technology, code of practice for informationsecurity management.* International Standards Organisation.

Kruger, H. A., & Kearney, W. D. (2 0 0 6). A prototype for assessing information security awareness. *Computers & Security*, 289 – 296.

Leach , J. (2003). Improving user security behaviour. *Computers and Security*, 685–692.

Martins , A., & Eloff, J. H. (2004, August). Measuring information security. Retrieved from <http://philby.ucsd.edu/wcse291_IDVA/papers/rating-position/Martins.pdf>;2001

Taylor, B. W. (2002). *Introduction to management science* (7th ed. ed.). Prentice Hall;.

Teare, G., & Da Veiga , A. (2003). Information security culture and awareness. *2003 ISSA Conference.* Sandton Convention, South Africa: IEEE.

Xu, L., & Liu, G. (2012). Analyzing algorithms of information security. *International Conference on Computer Science and Electronics Engineering* (pp. 1-4). IEEE Computer Society

Matveev, A. V. (2002). The Advantages of Employing Quantitative and Quantitative Methods in Intercultural Research. *Bulletin of Russian Communication Association THEORY OF COMMUNICATION AND APPLIED COMMUNICATION*, pp. 59-67.

Sandhu, R. S. (1993). Lattice-Based Access Control Models. *Journal of Computer, 26*(11), 9-19.

Schein , E. H. (1985). *Organizational Culture and Leadership: A Dynamic View.* San Francisco,Jossey-Bass.

Schlienger , T., & Teufel, S. (2003). Information security culture – from analysis to change. *South African Computer Journal, 31*, 46–52.

Schlienger, T., & Teufel, S. (2002). Information Security Culture - The Socio-Cultural Dimension in Information Security Management. In M. T.-H. In: M. A. Ghonaimy (Ed.), *IFIP TC11 International Conference on Information Security (Sec2002).* Cairo, Egypt, Kluwer Academic Publishers.

Spurling, P. (1995). Promoting security awareness and commitment. *Information Management and Computer Security , 3(2)*, 20–6.

Stanton , J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviours. *Computers and Security , 24(2)*, 124–133.