ISSN 1512-1232

RDBMS QUERY FOR AUTHENTICATING ACCESS TO PATIENT INFORMATION

[1]N.A Azeez, [2]A.P Dasylva, [3]O.M Omisore

[1,2]Department of Computer Sciences, University of Lagos, Nigeria
[3]Centre for Information Technology and Systems, University of Lagos, Nigeria

[1]nazeez@unilag.edu.ng, [2]sylvadeji@gmail.com, [3]ootsorewilly@gmail.com

ABSTRACT

The security of medical record is no doubt an issue of concern based on its importance and the required confidentiality. Electronic personal health records enable patients to access, manage, and share certain part of their own health information once it is available online. These capabilities establish the need for precise access-control mechanisms that should restrict the sharing of data to that authorized personnel. This research work explores the adoption of a relational database query for authentication as an access-control mechanism for restricting access to patient records. The project implemented the mechanism entirely in a relational database system using ANSI-standard SQL statements. Based on a set of access-control rules encoded as relational table rows, the mechanism determines via a single SQL query whether a user who accesses patient data from a specific application is authorized to perform a requested operation on a specified data object. The implementation was carried out with Microsoft Visual Studio 2010 – VB as the front-end. Testing of this query on a moderately large database has demonstrated execution times consistently below 100 milliseconds and only users who are authorized to perform specific operation are permitted by the system.

Keywords: *authentication, access, medical, patient information, query, database.*

1.0 INTRODUCTION

The rise in the security and privacy challenges of information related to Electronic Health Records (EHRs) is becoming worrisome across health institutions. Formerly, there was adequate privacy regarding the patient information since a consent form will be provided to any health practitioner who might be interested in getting any useful information from patient's details. The consent form was used to specify which part of the patient information should be used and which part should not be seen. However, with the advent of Information and Communication Technology, there has been limitless access to patient's information by illegal and unauthorized personnel.

The adoption of a relational database query for authentication as an access-control mechanism for restricting access to patient records will assist in determining who can access what medical information in an EHR environment. Studies show that less than 10 percent of patients had access to their health information. This implies that the greater percentage do not know what is contained in their EHR.

1.1 Brief Overview of Electronic Health Records

The main benefit of Electronic personal health record (EPHR) systems is that it allows individuals to manage and access part of their health information online. The feature also provides adequate mechanism for information privacy. EPHR provides adequate access privilege to specify

ISSN 1512-1232

unit a user may access thereby provides a detailed access control for the available information regarding patient information.

''Anyone whom I designate as a family member may view my medication list, except for one of my medications that I'd rather not share. . ."

The statement above could be likened to what is obtainable in a typical EPHR. Securing this kind of information requires technology which has rapidly evolved over the years ranging from manual restriction, encryption and other authentication procedures.

1.2 Justification

The idea of designing and implementing an RDBMS query for authentication is to restrict access to patient records and to specify with precision which users may access certain health record that will further provide the followings benefits:

- Controlled and reduced intrusion into patient personal medical record.
- Role profiling for users to scope their access.
- Faster processing of access based logic.
- Patient self-restriction setup on personal records.

1.3 Objectives of adopting RDBMS Query

The aim of this project is to use a relational database query for authentication as an access-control mechanism to patient records.

The objectives of this project are to:

a) Design a robust RDBMS query that will determine the kind of access to patient medical records.
b) Enable both patients and physicians to access records remotely in a secure and controlled manner.
c) implement the system

2.0 BACKGROUND INFORMATION

The main idea behind The Electronic Medical Record (EMR) was coined by Weed in 1969 when he introduced the oriented medical record in medical profession. As a result of his noble idea and innovation, the Institute of Medicine in the US made compulsory, the adoption of automated system in the practice of medical profession to enhance and improve the quality of service (Hersh1995).

Despite efforts made by researchers in this area since 1970, EMR adoption has not been effective. It has been established that there is just 20% and 5% adoption rate both in hospitals and clinics in the US. The case is a bit different in Canada where many clinics have already implemented EMR (Hersh1995). Various advances from recent work show adoption of various security models such Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC) for regulating access to patient information (Berhe et. al, 2009).

2.1 Paper-Based Medical Record

Despite the huge benefits currently being witnessed through the adoption of the EMR, most hospitals and clinics are still making use of paper for recording and storing their medical

ISSN 1512-1232

information (Dick and Steen1991). However, there are clear challenges and noticeable problems associated with paper-based medical records. Paper-based records are associated with haphazard and unorganized arrangement. The tendency of loosing vital documents during natural disasters is another big challenge (Hersh1995).

In an analysis of U.S. Army outpatient clinics, (Tufo and Speidel, 1971) observed that many as 20% of charts had missing information, such as laboratory data and radiology reports, a finding consistent with more recent observations (Korpman&Lincoln1988).

2.2 Electronic Medical Record

An Electronic Medical Record (EMR) is an effective mean of capturing, disseminating, and analyzing medical and health related information of a patient. All professionals in the health care delivery system have a stake in efficient information flows. Thus the term EMR has a slightly different meaning depending on one's perspective. Indeed, Electronic Medical Records managed by individuals are termed Personal Health Records (PHRs). PHRs capture all relevant and useful personal health details. This may include diagnoses, X-Rays, and related items into a single repository (Hersh, 1995).

2.2.1 Problems of Electronic Medical Records

The main challenge of Electronic Medical Records is the difficulty in adequately securing records and preventing identity theft. Key security and privacy concerns for EMR systems include:

Hacking incidents on EMR systems that lead to altering of patient data or destruction of clinical systems

- Misuse and misinterpretation of health information records by authorized users of EMR systems
- Data mismanagement concerns
- intrusion of government or corporate into private health care matters

(Gelogo & Park, 2013).

Existing Access Control Models for Medical Information

2.3 Security of Personal Medical Records

Security of personal medical records does not just refer to access control. It also refers to the storage and management of medical records. Part of the regulatory control over medical records is that they must be stored securely in pre-defined locations. In some cases the organization in charge of storing those records must be able to point to the exact device that retains the records.

A system for remote access to medical records must be secure. However, the system must enable patients and their physicians to access those records as quickly and painlessly as possible; it must be usable. A few possible measures that is built into EHR systems include:

- **Access control:** this applies tools like passwords and PIN numbers, to help limit access to patient information to authorized individuals.
- **Encrypting your stored information:** This is when patient health information cannot be read or understood except by those using a system that can “decrypt” it with a “key.”
- **An audit trail feature:** This records who accessed your information, what changes were made and when (Gelogo& Park2013).

2.3.1 Traditional Access Control for EHRs

Access control in electronic health records (EHRs) often places full trust on the health care providers where the EHR data are often resided in, and the access policies are implemented and enforced by the health providers. Various access control models have been proposed and applied,

ISSN 1512-1232

including role-based (RBAC) and attribute-based access control (ABAC) (Chadwick & Otenko, 2002).

In RBAC, each user's access right is determined based on his/her roles and the role-specific privileges associated with them (Herath & Rao, 2009). The ABAC extends the role concept in RBAC to attributes, such as properties of the resource, entities, and the environment. Compared with RBAC, the ABAC is more favorable in the context of health care due to its potential flexibility in policy descriptions (Azeez et. al 2011). A line of research aims at improving the expressiveness and flexibility of the access control policies (Imine, Cherif, & Rusinowitch, 2009).

However, for personal health records (PHRs) in cloud computing environments, the PHR service providers may not be in the same trust domains with the patients'. Thus patient-centric privacy is hard to guarantee when full trust is placed on the cloud servers, since the patients lose physical control to their sensitive data. Therefore, the PHR needs to be encrypted in a way that enforces each patient's personalized privacy policy.

2.3.2 Cryptographically Enforced Access Control for Outsourced Data

This is basically for access control of outsourced data, partially trusted servers are often assumed. With cryptographic techniques, the goal is trying to enforce who has (read) access to which parts of a patient's PHR documents in a fine-grained way.

2.3.2.1 Symmetric key cryptography (SKC) based solutions.

A solution for securing outsourced data on semi-trusted servers based on symmetric key derivation methods, which can achieve fine-grained access control was proposed (Gunter &Terry2005). Unfortunately, the complexities of file creation and user grant/revocation operations are linear to the number of authorized users, which is less scalable. Files in a PHR are organized by hierarchical categories in order to make key distribution more efficient. However, user revocation is not supported. An owner's data is encrypted block-by-block, and a binary key tree is constructed over the block keys to reduce the number of keys given to each user (Gunter &Terry2005).

The SKC-based solutions have several key limitations. First, the key management overhead is high when there are a large number of users and owners, which is the case in a PHR system. The key distribution can be very inconvenient when there are multiple owners, since it requires each owner to always be online. Second, user revocation is inefficient, since upon revocation of one user, all the remaining users will be affected and the data need to be re-encrypted. Furthermore, users' write and read rights are not separable (Gunter &Terry2005).

2.3.2.2 Public key cryptography (PKC) based solutions

PKC based solutions were proposed due to its ability to separate write and read privileges. Securing Personal Health Records in Cloud Computing is a scheme based on hierarchical identity based encryption (HIBE), where each category label is regarded as an identity (Gelogo& Park 2013). However, it still has potentially high key management overhead. In order to deal with the multi-user scenarios in encrypted search, a solution based on proxy encryption. Access control can be enforced if every write and read operation involves a proxy server. However, it does not support fine-grained access control, and is also not collusion-safe (Gelogo& Park 2013).

2.3.3 Attribute-Based Encryption (ABE)

The SKC and traditional PKC based solutions all suffer from low scalability in a large PHR system, since file encryption is done in a one-to-one manner, while each PHR may have an unpredictable large number of users. To avoid such inconveniences, novel one-to-many encryption methods such as attribute-based encryption can be used. Note that, a single authority for all users and patients is adopted. However, this suffers from the key escrow problem, and patients' privacy still cannot be guaranteed since the authority has keys for all owners.

ISSN 1512-1232

(Gelogo& Park 2013) applied cipher-text policy ABE (CP-ABE) to manage the sharing of PHRs. However, they still assume a single public authority, while the challenging key-management issues remain largely unsolved.

Though, some of these access control models have performed excellently well but weaknesses currently identified have made the adoption of RDBMS query inevitable.

3.0 RDBMS QUERY FOR AUTHENTICATION.

The idea of designing and implementing an RDBMS query for authentication is to restrict access to patient records and specify with precision which users may access certain health record. Doing this will provide controlled and reduced intrusion into patient personal medical record and role profiling for users to scope their access.

Security of personal medical records does not just refer to access control. It also refers to the storage and management of medical records. Part of the regulatory control over medical records is that they must be stored securely in pre-defined locations (Gelogo & Park 2013).

3.1 Data Element for RDBMS Query

Considering the database that is needed, each data element will be refined into a set of data objects as well as the characteristic or attributes of each.The hierarchy tables in the database are **RoleHierarchy**, **OperationHierarchy**, **ResourceTypeHierarchy**, and **ContextHierarchy**. The schema for all of these hierarchy tables consisted of the fields

- AncestorsID (AncsID)
- DecendantsID (DescsID)

The representation of these hierarchies as materialized transitive closures allows an SQL query to test for subsumption between a request attribute and the corresponding value in an access-control policy via a simple (non-recursive) join. All fields within all these tables were indexed.

3.0.1 Role Relationships

Role Relationships associate specific user with specific patient and designate a specific role for the user in each of relationship. Each valid role is represented by a unique RoleID, such as ‘‘Family- Member,” ‘‘Physician,” or ‘‘RecordSubject” (the latter indicates that the user is the patient). The users are assigned roles in the context of specific patient relationships, rather than as general attributes of their user accounts (in contrast to traditional role-based access-control models). This specificity, for example, allows patients to grant access to their designated physician only, rather than to all users who are physicians. The feature also allows individual users to have different roles with respect to different patients.

RoleIDs are organized into a subsumption hierarchy such that each descendant RoleID may inherit the permissions assigned to its ancestor RoleIDs. The fields are

- UserID
- PatientID
- RoleID

Access Rule: Access Rules determines and dictates the policies that permit or prohibit various data-access operations with respect to a specific patient record

PatientID and RoleID: represent the patient and the user role to which the access rule applies. Note that all access rules are specified with respect to roles rather than individual users.

OperationID: this specifies the permitted or prohibited operation that is specified by the rule. These identifiers are pre-defined within a hierarchy of operations that is common to the data repository and the PDP.

ISSN 1512-1232

ResourceTypeID: represents the semantic type of the resource to which the access rule applies (such as ‘‘Prescription,” ‘‘SignOr-Symptom,” or ‘‘PhysicalActivity”). These identifiers are pre-defined within a hierarchy of resource types that is common to the datarepository.

ResourceID: represents the specific data object to which the access rule applies (if specified). Note that each access rule may specify either a ResourceTypeID or a ResourceID, but not both. For example, one rule may permit access to all data of the type ‘‘Prescription” whereas a different rule may deny access to a specific instance of Prescription if a patient wishes not to share it (the rule for reconciling such conflicts has been expalined).

AppContextID: represents the application from which the data access request is submitted. The value may designate the unique ID of a specific application, indicating that the access rule pertains only to requests originating from that application, or it may designate the special value ‘‘AllApps”.

Effect: simply indicates whether the rule allows (“Permit”) or prohibits (‘‘Deny”) the specified operation.

(1) At least one combination of Role Relationship and Access Rule exists that PERMITS the requested operation AND

(2) No combination of Role Relationship and Access Rule exists that DENIES the requested operation.

3.0.2 Human Element

This refers to the users of the system; Patient, Users (Physician, Family member) who are very important element of the system. Human Element (HE) injects instruction to the system in the form of search requests to which the system must respond. The information/output of the system then aids Human Element (HE) in decision-making.

3.0.3 Input Interface Design

“Anyone whom I designate as a family member may view my current medication list, with the exception of one medication that I’d rather not share…”

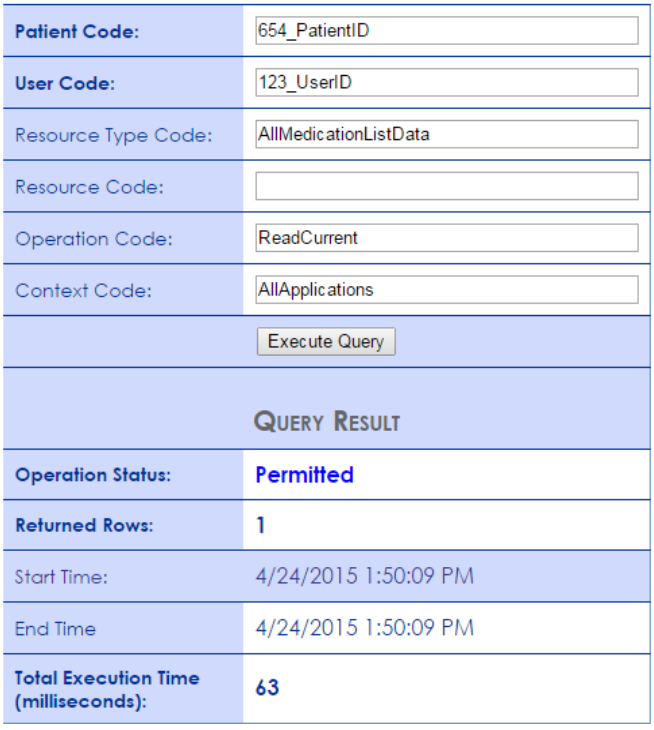

Figure 1. Execute Query: User Type Spouse

ISSN 1512-1232

Access Rules 1 specifies the general case, whereas AccessRules 2 specifies the exception by listing the specific medication record that should not be shared with family member users.

Users assigned the "Spouse" or "Child" role will inherit all the rights assigned to the "FamilyMember" role (by virtue of the Role hierarchy), except for the ability to view the specified medication list item. Note that by designating the OperationID "ReadCurrent", AccessRule1 allows the reading of the current values of data only, rather than historic (i.e., previously changed or deleted) values as shown Figures 1 and 2

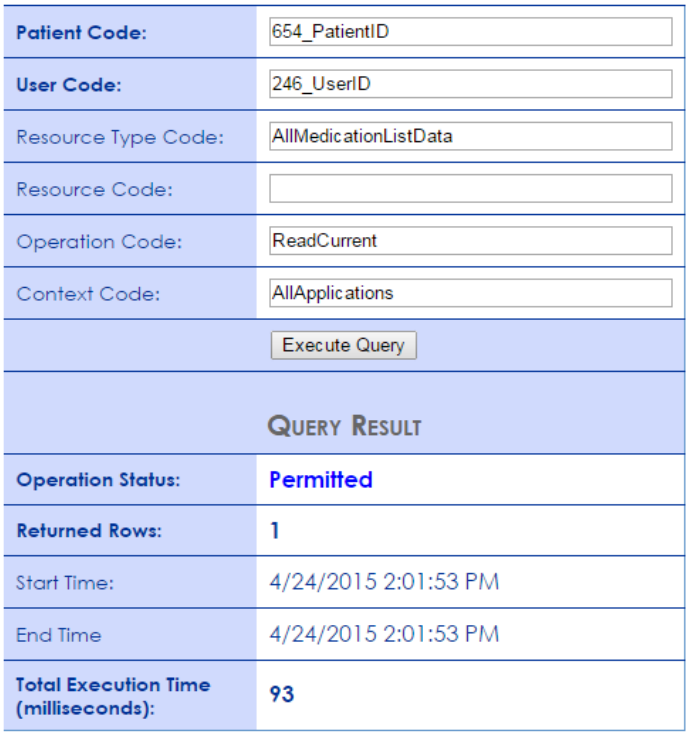

Figure 2. Execute Query: User Type Child

Sample RDBMS Query **1**

```
SELECT @No_Of_Rows =Count(ar.PatientID)---AS [No_Of_Rows]
FROM RoleRelationships AS rr,
AccessRules AS ar,
dbo.RoleHierarchy AS rh,
ResourceTypeHierarchy AS rth,
OperationHierarchy AS oh,
ContextHierarchy AS ch
WHERE ( rr.PatientID = @PatientNo AND
      rr.UserID =   @UserNo AND
      rr.PatientID = ar.PatientID AND
      rr.RoleID = rh.DescID AND
      rh.AncID = ar.RoleID AND
(( rth.DescID = @ResourceTypeNo  AND rth.AncID = ar.ResourceTypeID)OR
ar.ResourceID = @ResourceNo)
                  AND  oh.DescID=@OperationNo
                  AND oh.AncID = ar.OperationID
                  AND   ch.DescID = @ContextNo
                  AND ch.AncID = ar.ContextID AND ar.Effect ='Permit')
ANDNOTEXISTS
```

ISSN 1512-1232

Sample RDBMS Query **2**

```
(SELECT*
FROM RoleRelationships rr_1,
 AccessRules ar_1,
dbo.RoleHierarchy  rh_1,
 ResourceTypeHierarchy rth_1,
 OperationHierarchy oh_1,
 ContextHierarchy ch_1
WHERE @PatientNo = rr_1.PatientID AND
      @UserNo = rr_1.UserID AND
          rr_1.PatientID = ar_1.PatientID AND
          rr_1.RoleID = rh_1.DescID AND
          rh_1.AncID = ar_1.RoleID AND
(((@ResourceTypeNo = rth_1.DescID AND
          rth_1.AncID = ar_1.ResourceTypeID)OR  @ResourceNo = ar_1.ResourceID)AND
           @OperationNo = oh_1.DescID AND
          oh_1.AncID = ar_1.OperationID AND
         @ContextNo = ch_1.DescID AND
          ch_1.AncID = ar_1.ContextID AND
          ar_1.Effect ='Deny')
--Initioalize End Time
set @EndTime=Getdate()
set @ExecTime =DATEDIFF(ms,@StartTime,@EndTime)--(Datepart(second,@EndTime)-
Datepart(second,@StartTime))
select @No_Of_Rows AS'No_Of_Rows',@ExecTime as'Execution_Time',@StartTime
as'Start_Time',@EndTime as'End_Time'
```

"Anyone whom I designate as a health care provider may view my medication list and my history of office visits and hospitalizations…"

Patient Code:	654_PatientID
User Code:	357_UserID
Resource Type Code:	AllMedicationListData
Resource Code:	
Operation Code:	RecordViewing
Context Code:	AllApplications
	Execute Query
	QUERY RESULT
Operation Status:	**Permitted**
Returned Rows:	**2**
Start Time:	4/24/2015 2:11:58 PM
End Time	4/24/2015 2:11:58 PM
Total Execution Time (milliseconds):	**76**

Figure 3. Execute Query: Operation Code: RecordViewing

ISSN 1512-1232

The Start Time is the time when a query was issued while the End Time is when the query was executed. The difference between the Start Time and the End Time indicates the time it takes the query to be executed. This is otherwise known as the Total Execution Time. What is observed is that it takes a very short time, which is evaluated in milliseconds for a query to be executed. By designating the OperationID "RecordViewing", the rules allow the viewing of current and historical records, given the relationship of "RecordViewing" to "ReadCurrent" and"ReadHistorical" in the Operation hierarchy as shown in Figure 3.

"My primary physician, Dr. John, may view and modify my medication list and may view and annotate my log of meals and physical activities…"

Patient Code:	654_PatientID
User Code:	357_UserID
Resource Type Code:	PhysicalActivity
Resource Code:	
Operation Code:	WriteOwnAnnotation
Context Code:	AllApplications
	Execute Query
	QUERY RESULT
Operation Status:	**Permitted**
Returned Rows:	**2**
Start Time:	4/24/2015 2:21:49 PM
End Time	4/24/2015 2:21:49 PM
Total Execution Time (milliseconds):	**90**

Figure 4. Execute Query: User Type: Physician

The "Physician" role grants Dr. John the rights that have been assigned to all the health care providers of this patent (because "Physician" is subsumed by "HealthCareProvider" in the Role hierarchy). The role "PHADefined1" grants to Dr. John the additional rights specified in AccessRules. The current Role hierarchy allows up to 10 such "PHADefined" roles to be assigned to various individuals or group of individuals for each patient.

Although this method is not as flexible as allowing UserIDs to appear directly in access-control rules, it reduces the number of join operations required in the adjudication query. It also provides the ability to create patient-defined group of users with special rights or restrictions, when such groups are not among those already defined in the Role hierarchy as shown in Figure 4,no user except *myself* may view or change my access-control policies.

ISSN 1512-1232

Patient Code:	654_PatientID
User Code:	680_UserID
Resource Type Code:	AccessControl
Resource Code:	
Operation Code:	AllOperations
Context Code:	AllApplications
	Execute Query
	QUERY RESULT
Operation Status:	Permitted
Returned Rows:	1
Start Time:	4/24/2015 2:44:33 PM
End Time	4/24/2015 2:44:33 PM
Total Execution Time (milliseconds):	110

Figure 5. Execute Query: Resource Type Code for Access Control

The AccessRule grants to this user read and right operations against both the RoleRelationships and AccessRules objects for this patient (by virtue of the hierarchical relationships among "AccessControl," "Relationships," and "AccessRules" in the ResourceType hierarchy). The same ability to assign or change access controls could be assigned to other roles (such as "RecordCustodian" or "Spouse") or to individual users (via the "PHADefined" mechanism) as shown in Figure 5.

ISSN 1512-1232

Figure 6. Analysis of RDBMS Query users report graph

Figure 6 shows the number of users, total number of attempts made to gain access, the total number of denial as well as the percentage of permission and denials.

The figures further shows the number of times user 123_UserID tried to access the system. Number of times permitted and numbers of times denied with their percentages respectively. Similar reports were also obtained for other users and detailed analysis were conducted for better interpretation of access privileges provided when using RDBMS Query**.**

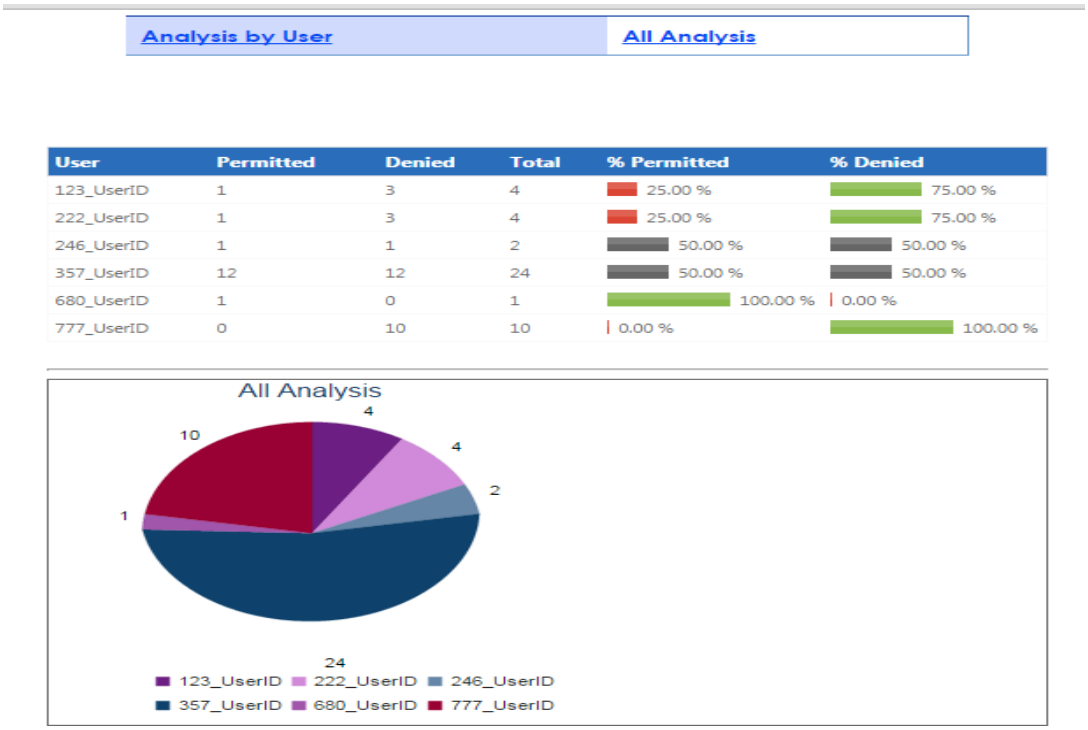

Figure 7. General analysis report graph

Figure 7 provides a comprehensive statistical summary of what is presented in Figure 6. It shows the number of times all the registered users have tried to access the system. Number of times permitted and the number of time access were denied with their percentages respectively.

4.0 CONCLUSION

There is no gain saying the fact that vulnerable nature of medical information is mainly due to inadequate access control measure to monitor, control and direct access to the authorized users. The idea of designing and implementing an RDBMS query for authentication therefore is to restrict access to patient records and to specify with precision which user may access certain health record with the aim of providing controlled and reduced intrusion into patient personal medical record. This mechanism will also assist in ensuring role profiling for users to scope their access, faster processing of access based logic and to further ensure patient self-restriction setup on personal records. It is the opinion of the authors that full scale implementation of **RDBMS Query** for accessing patient information will assist in no small measure at ensuring privacy and confidentiality of medical information in any health institution in the country.

ISSN 1512-1232

5.0 REFERENCES

1. Avison, D. and Fitzgerald, G. (1995), Information Systems Development: Methodologies, Techniques and Tools, 3rd Edition, McGraw-Hill, Berkshire.
2. Avison, D.E. and Shah, A. (1997), the Information System Development Life Cycle: A First Course in Information Systems, McGraw Hill International (UK), England.
3. Azeez, N. A., Iyamu, T., & Venter, I. M. (2011). Grid Security Loopholes with proposed countermeasures. In E. Gelenbe (Ed.), ISCIS2011, 26th International Symposium on Computer and Information Sciences 26-28 September 2011 (pp. 411-418). Imperial College, London, UK: Springer Verlag.
4. Berhe S, Demurjian S and Agresta T (2009), "Emerging Trends in Health Care Delivery:Towards Collaborative Security for NIST RBAC E. Gudes, J. Vaidya (Eds.): Data and Applications Security 2009, LNCS 5645, pp. 283–290, 2009.c IFIP International Federation for Information Processing 2009.
5. Chadwick, D., & Otenko, A. (2002). RBAC Policies in XML for X.509 Based Privilege Management. SEC '02 Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives. The Netherlands, The Netherlands ©2002: ACM, Computing.
6. Crowell, W.H., (2009) biomedical Instrumentation and Biometric Technology in Electronic Seminars.[online] http://www.seminartopics.com/seminar/biometric-technology
7. CS2 Software Engineering Note – SEN (2004) Software Requirements [Online], www.inf.ed.ac.uk/teaching/courses/cs2/LectureNotes/CS2Ah/SoftEng/se02
8. Dick, R., & Steen, E. (Eds.). (I991). The computer Based patient record: An Essential Technology for Patient Care. Washington, DC: National Academy Press.
9. Dunlop, L., (2007) Electronic Health Records: Interoperability Challenges and Patient's Right for Privacy. Shidler Journal of Computer and Technology, vol. 3, no.16 [online] http://www.law.washington.edu/WJLTA/Issues/3/3/8.
10. Gelogo, Y.E., & Park S.(2013). A Study on Secure Electronic Medical DB System in Hospital Environment.Catholic University of Daegu, Daegu, Korea.Department of Nursing.
11. Gunter, T. D., & Terry, N. P. (2005). The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions, in J. Med Internet Res., vol. 7, no. 1.
12. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18 n 2, 106-25.
13. Hersh, W. R. (1995). The Electronic Medical records: Promises and Problems. Biomedical Information Communication Center, Oregon Health Sciences University, BICC, 3181 S. W.
14. Imine, A., Cherif, A., & Rusinowitch, M. (2009). *An Optimistic Mandatory Access Control Model for Distributed Collaborative Editors.* INRIA: IEEE.
15. Korpman. R.,& Lincoln. T. (I988). The computer-stored medical record:For whom? Journal of the American Medical Association 259, 3454-3456.
16. Levingston, S. A. (2012). Opportunities in physician electronic health records: A road map for vendors. Bloomberg Government.[online], http://www.healthit.gov/providers-professionals/benefits-electronic-health-records-ehrs
17. Miller, R., Masarie., F., & Myers. J. (1986).Quick medical reference (QMR) for diagnostic assistance.MD Computing. 3, 34-48.
18. Microsoft (2015). Hardware requirements [online] technet.microsoft.com
19. Mohammed, S., &Fiaidhi, J., (2010). Ubiquitous Health and Medical Informatics: The Ubiquity 2.0 Trend and Beyond, Medical Information Science Reference, ISBN 978-1-61520-777-0.

ISSN 1512-1232

20. Rothfeder. J. (1992). Privacy for sale: How Computerization has made everyone's private life an open secret. New York Simon and & Schuster.
21. Schadow G., Barnes M., McDonald C.J. (2001) Representing and querying conceptual graphs with relational database management systems is possible. In: Proceedings of the AMIA annual fall symposium, Washington DC; p. 598–602
22. Silverstein, S., (2009). 2009 a pivotal year in healthcare IT, Drexel University.
23. Tufo, H., &Speidel. J. (197I).Problems with medical records.Medical Care. 9, 509-517.
24. Walter V. S., Sam A. F., Ethan S., Patricia F, B. (2010). A method to implement fine-grained access control for personal health records through standard relational database queries. Journal of Biomedical informatics.
25. Ayofe, A.N, Adebayo, S.B, Ajetola, A.R, Abdulwahab, A.F (2010) "A framework for computer aided investigation of ATM fraud in Nigeria" International Journal of Soft Computing, Vol. 5, Issue 3 pp. 78-82
25. Azeez, N.A, Olayinka, A.F, Fasina, E.P, Venter, I.M. (2015) "Evaluation of a flexible column-based access control security model for medical-based information" Journal of Computer Science and Its Application. Vol. 22, Issue 1, Pages 14-25
26. Azeez, N. A., and Ademolu, O. (2016). CyberProtector: Identifying Compromised URLs in Electronic Mails with Bayesian Classification. 2016 International Conference Computational Science and Computational Intelligence (CSCI) (pp. 959-965). Las Vegas, NV, USA: IEEE.
27. Azeez, N. A., and Babatope, A. B. (2016). AANtID: an alternative approach to network intrusion detection. The Journal of Computer Science and its Applications. An International Journal of the Nigeria Computer Society, 129-143.
28. Azeez, N. A., and Iliyas, H. D. (2016). Implementation of a 4-tier cloud-based architecture for collaborative health care delivery. Nigerian Journal of Technological Development, 13 (1), 17-25.
29. Azeez, N. A., and Venter, I. M. (2013). Towards ensuring scalability, interoperability and efficient access control in a multi-domain grid-based environment. SAIEE Africa Research Journal, 104 (2), 54-68.
30. Azeez, N. A., Iyamu, T., and Venter, I. M. (2011). Grid security loopholes with proposed countermeasures. In E. Gelenbe, R. Lent, and G. Sakellari (Ed.), 26th International Symposium on Computer and Information Sciences (pp. 411-418). London: Springer.
31. Azeez, N.A., and Lasisi, A. A. (2016). Empirical and Statistical Evaluation of the Effectiveness of Four Lossless Data Compression Algorithms. Nigerian Journal of Technological Development, Vol. 13, NO. 2, December 2016, 64-73.
32. Nureni, A. A., and Irwin, B. (2010). Cyber security: Challenges and the way forward. Computer Science & Telecommunications, 29, 56-69.
33. Azeez, N.A and Venter, I.M (2012). Towards achieving scalability and interoperability in a triple-domain grid-based environment (3DGBE)- Information Security for South Africa (ISSA), 2012, pp 1-10.
34. Azeez N.A and Otudor A.E (2016) "Modelling and Simulating Access Control in Wireless Ad-Hoc Networks" Fountain Journal of Natural and Applied Sciences. Vol 5(2), pp 18-30
35. Azeez, N.A Abidoye, A.P Adesina, A.O Agbele, K.K Venter, I.M Oyewole, A.S(2013) "Statistical Interpretations of the Turnaround Time Values for a scalable 3-tier grid-based Computing architecture" Computer Science & Telecommunications, Vol 39 (3), pp 67-75.

Article received: 2018-03-31