Implementation of a Secured Access Control Model in Legal Information Systems

Ekong[1] U.O. & Sambo, E.
Department of Computer Science
University of Uyo
Uyo, Akwa Ibom State, Nigeria
uyinomenekong@uniuyo.edu.ng, emem4mbo@yahoo.com

ABSTRACT

Current trends in Information Technology consider security as one of the most paramount area in effective dissemination of information and development of information systems. A secured system means a reliable system and a breach in security brings about lack of trust on that information. Role Based Access Control (RBAC) over the years has been used to control mechanism that gives permission to users by assigning roles and privileges. Legal information on the other hand, has to do with activities involved in managing all aspects of the corporate legal practice environment including; tracking of cases and documents using information technology. There is a significant increase and popularity of the use of information technology in the legal domain. This has brought about changes in the methods of capturing, storing, accessing, maintaining, distributing, securing and preservation of legal information. However, the vast deployment of new technologies to automate the filing, acceptance, and retrieval of litigation documents coupled with the flow of information among litigants has brought about threat on data and information as they pass through the internet , which has led to data falsification, modification, interception, fabrication and interruption. In this paper, an RBAC-LIS model is developed and implemented to prevent and control unauthorized access to legal information. RBAC provides flexible control and management by assigning users to roles and roles to permission. The Dynamic RBAC model is adopted in modeling the Legal Information System. UML is used for designing the system while, PHP and HTML were used to develop the source codes for the middle and front end. Finally MYSQL was employed at the backend. The Dynamic RBAC-LIS model was created with an embedded Blowfish encryption scheme that encrypts information stored in the database, which are only made available to authorized users. Implementation of the system reveals improvement on access control for the legal information system.

Keywords: Security, Access, Control, Model,Information, Law, legal & Systems,

CISDI Journal Reference Format
Ekong, U.O. & Sambo, E. (2017): Implementation of a Secured Access Control Model in Legal Information Systems. Computing, Information Systems & Development Informatics Journal. Vol 8 No 1. Pp 177-184

1. INTRODUCTION

Security is one of the major problems in any information system. Database security on the other hand, is considered to be a complex issue for a networked and internet connected system especially with internal employees who intentionally access and disclose sensitive information of an organization. Access control has been a major issue, mainly in database management systems and in operating systems. It aims at protecting system resources against undesired or inappropriate user access, whilst permitting authorized access. Access control is a mechanism that grant, denies or restricts user from having access to a system. It decides which system resources and applications can be used by whom. Although some information should be accessible by everyone, access to some sensitive information needs to be restricted. It is the process of deciding who can use specific system, resources and applications (Abhishek, et al., 2014). Access control gives support to both the confidentiality and the integrity properties of a secured system. The confidentiality does the protection of information from unauthorized disclosure while integrity protects information from unauthorized modification. Access control gives you the ability to dictate what information a user can both view and modify.

Access control models are usually seen as frameworks for implementing and ensuring the integrity of security policies that mandate how information can be accessed and shared on a system. It gives relationships among permissions, operations, objects, and subjects by distinguishing the difference between users, the people who use the computer system, and subjects, computer processes acting on behalf of users. Several intermediate concepts have been introduced over the past decades to organize these relationships. Access Control Model (ACM) gives security to the resources or data by controlling access to the resources and the system itself. However, access control is more than just controlling which users can access a computing or a network resource. In addition, access control manages users, files and other resources. It controls user's privileges to files or resources or data. There are different types of access control models but this paper will widely concentrate on the RBAC.

Early research on access control was dominated by two approaches: Mandatory Access Control (MAC) and Discretionary Access Control (DAC). DAC allows users to delegate their own rights to other users. It denies or allows access control based on the identity of the accessing user or group (Thion, 2008). Users are considered to be the owner of the objects under their control. A user can give his access control rights to another user belonging to the same group. This model however, in most information systems, the end users do not own the information to which they have access to but rather owned by the organization. So accesses are to be granted by the organization and not otherwise. This approach therefore, does not support large numbers of subjects and objects. MAC model restricts access to objects based on the sensitivity of information contained in the objects and authorization of persons (users) that accesses such information. In MAC, security is on objects and subjects while limiting access and consolidating all classification and access controls into the system through the system administrator who defines the usage and access policies which cannot be modified by any user.

This implies when a subject attempts to access an object, an authorization rule enforced by the administrator examines the security attributes and decides whether the access to the object can be granted (Abhishek, et al., 2014). MAC facilitates the multilevel security but delicate more power on the system administrator which further denies fine grained least privilege and dynamic separation of duty and validation on trusted components. Because of the rigid nature of MAC, where users had little or no control over the access control policy, and the problems associated with policy changes in DAC, early access control models could not meet practical requirements of commercial organizations. It was also realized that in large organizations data is not owned by individual users, but by the organization itself, thus access to data should consider one's position in the organizational hierarchy. This resulted to Role-Based Access Control (RBAC) (Andras, 2004).

RBAC is one of the access control mechanisms that give permission to the user by introducing roles (Lim, et al., 2001). It uses the concept of roles to manage permission to users. It serves as an alternative to traditional access control to simplify administration. In large systems, the amount of permissions assigned to a user may become high. It may become hard to keep track of all permissions. When a user moves between positions in the company, her permissions are changed according to her new tasks because administrators do not have a clear view over the user's permissions. They may fail to revoke all permissions that are no longer needed (Peter, 2005). Role-Based Access Control (RBAC), is a policy neutral access control mechanism that is widely known as being an inherently easier and less error-prone way of administrating access control policies. The basic principle of RBAC is the separation of Permission Assignments (PA) and User Assignments (UA). With RBAC, permissions are assigned to roles and roles are assigned to users. A user thereby acquires the permissions assigned to that specific role (Zhou, et al., 2013, Matulevicius and Lakk, 2015). A user's permissions are limited to the roles in which he or she is authorized to function. The separation facilitates the administration of security policy, where each process can then be administered independently. Since permissions are de-coupled from users, changes to permission or user assignments have minimal isolated impact on administration.

The legal system is essential to maintain stability and order in the society. Lawyers in any civilized society settle fundamental human rights, disputes and clashes. A legal practitioner in Nigeria is a barrister as well as a solicitor whose primary duties are; advocacy, litigation, counseling, preparation of legal document, etc. A lawyer defends his client (s) in the court of law by applying the principles of law to the evidence available, by providing relevant facts. Lawyers enlighten the public of their constitutional rights and ensure that people are not deprived of their fundamental human rights such as freedom of association, speech, opinion, religion etc., (Owoeye, 2011). Legal Information System (LIS) is defined as a system in which legal information is transformed, transferred, consolidated, received and feed back in such a manner that these processes function synergistically to underpin knowledge utilization by legal practitioners and their clients (Kamran, 2015).

Legal Information System also has to do with the activities involved in managing all aspects of the corporate legal practice. This includes the tracking of such items as the attorneys and other workers on the case, type of legal work, industry of the matter or client, witnesses, judges, courts, opposing counsel, issues, documents, budgets and invoices associated with each particular legal matter. This system can provide excellent communication and collaboration platforms to organize and distribute information. The system allows law firms, businessmen, creditors, bank officers and members of the public to search for relevant case information online.

Traditionally, lawyers request and seek approval to inspect documents at the court's registry counters. Once approval is given, the lawyers will obtain the extracts of the paper copy over the court registry counters. With this system, the process of requesting and obtaining copies of extracts of documents can be done on the legal information system. Lawyers can search for the relevant cases by examining the system index and can electronically request for an extract of the document from the court. The electronic copy will be sent to the law firm/s once the juridical officer approves the request. As these systems entail the processing and storage of confidential corporate and insurance carrier financial data, sensitive claims information, and privileged legal matter data, major considerations in the deployment of these systems are: availability of matter-level security.

2. METHODOLOGY

The framework of the proposed RBAC-LIS model based on Dynamic RBAC is depicted in Figure 1. Due to the sensitivity of legal information an additional constraints (cryptographic technique and access time) has been integrated to further protect the data stored in the database and take account of who accesses the information, at what time and duration of access for tracking purposes. RBAC-LIS model defines a set of users U, a set of roles R, a set of permissions P, a user-role assignment relation UA ⊆ U×R and a permission-role assignment relation PA ⊆ P×R which refers to such sets and relations as components of RBAC. Roles (u) for the set of roles to which a user u is explicitly assigned by the UA relation; that is, Roles (u) = {r ∈ R: (u, r) ∈ UA}. Similarly, Roles (p) for the set of roles to which a permission p is explicitly assigned by the PA relation; that is, Roles (p) = {r ∈ R: (p, r) ∈ PA}. Given r ∈ R, Prms(r) to denote the set of permissions for which r is explicitly assigned, and for R0 ⊆ R, Prms (R0) to denote the set of permissions for which the roles in R0 are explicitly assigned. That is, Prms(r) = {p ∈ P: (p, r) ∈ PA} and Prms (R0) [r ∈ R0 Prms(r).

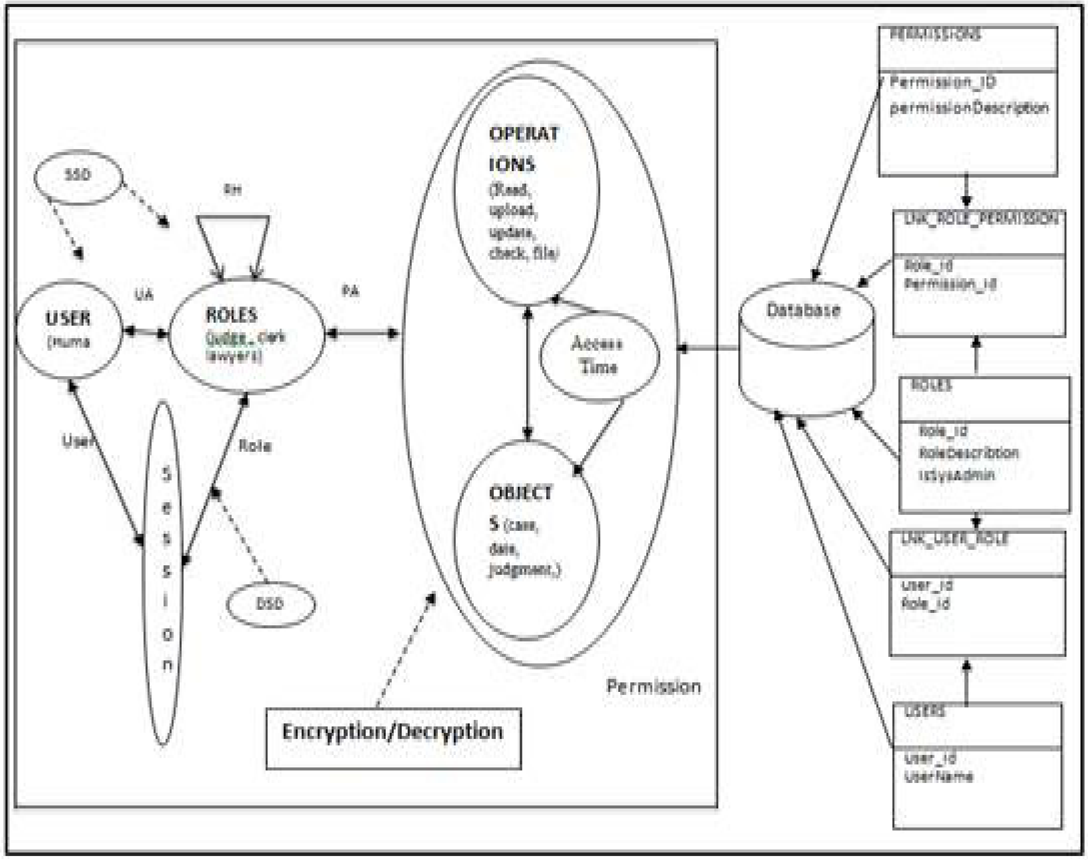


Figure 1: RBAC-LIS

The Unified Modelling Language (UML) use case and class diagram were employed in designing of the system. Figure 2 and Figure 3 represent the use case diagram and the class diagram respectively.

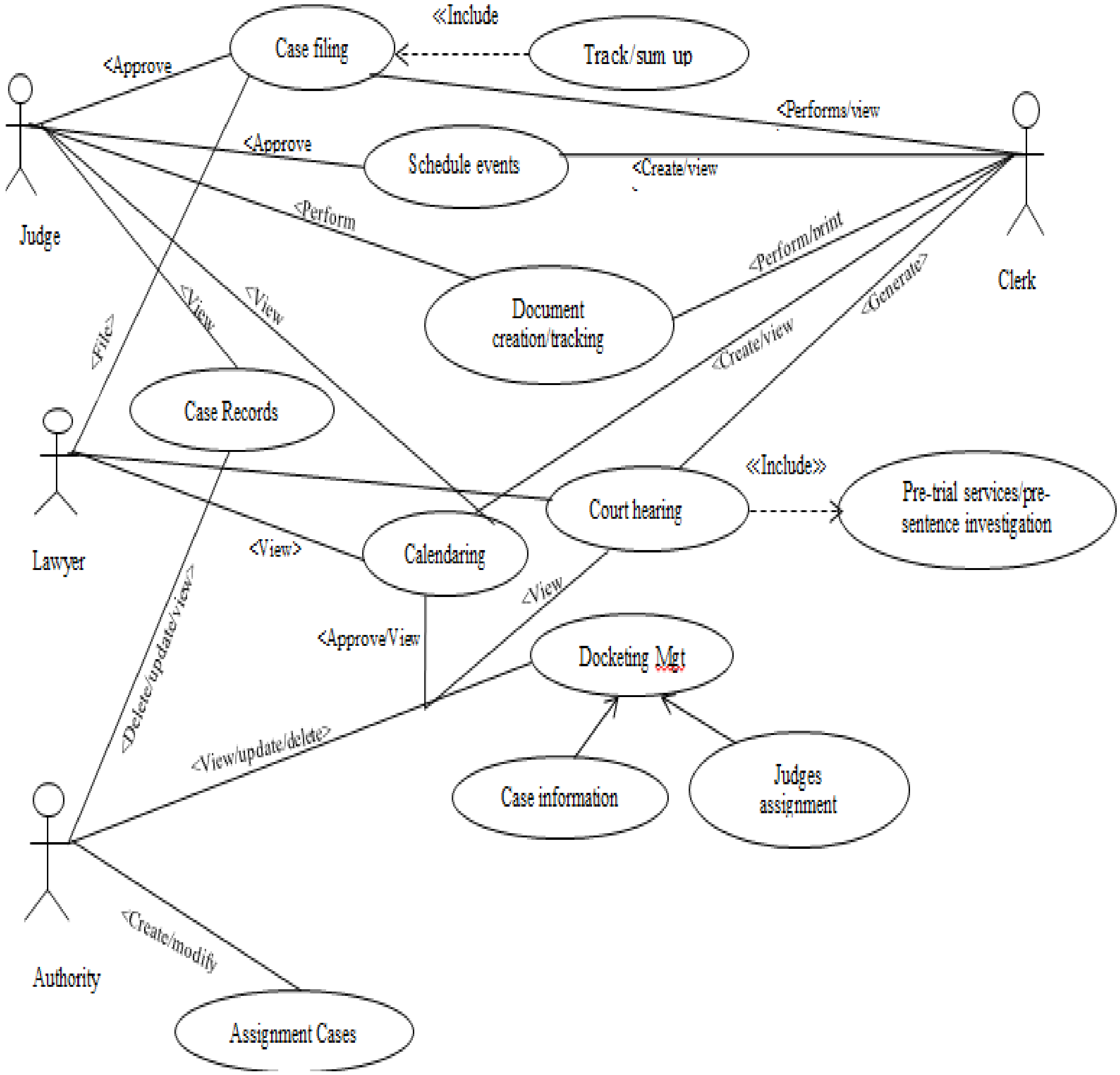


Figure 2: RBAC-LIS Use case diagram

The RBAC-LIS Class diagram depicts the static structure of the system. The class diagram is made up of 10 major classes which include; user, administrator, judge, role, LNK userRole, LNK Role-Permission, permission, clerk, lawyer and authority classes with their associated attributes and methods respectively.

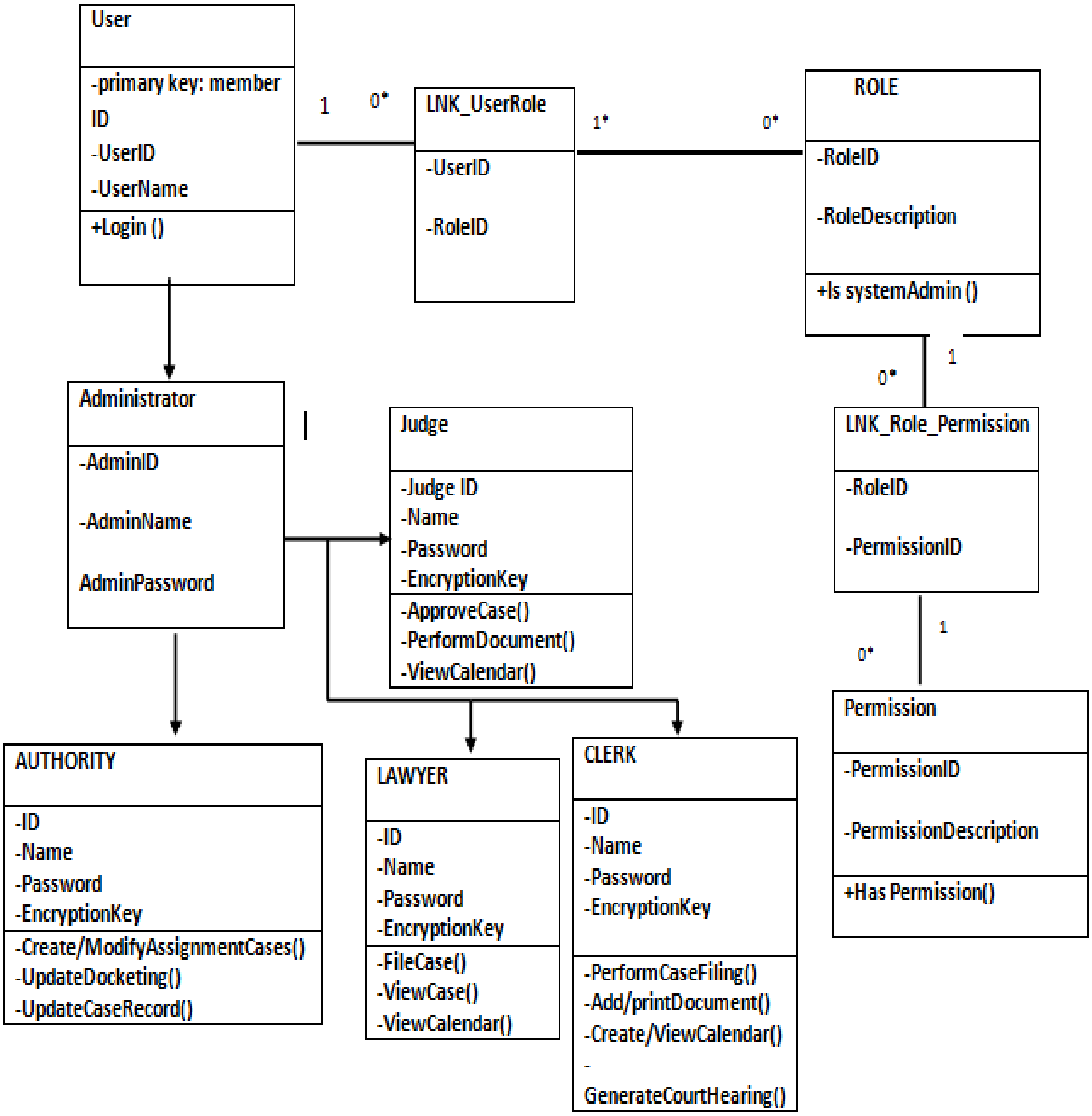
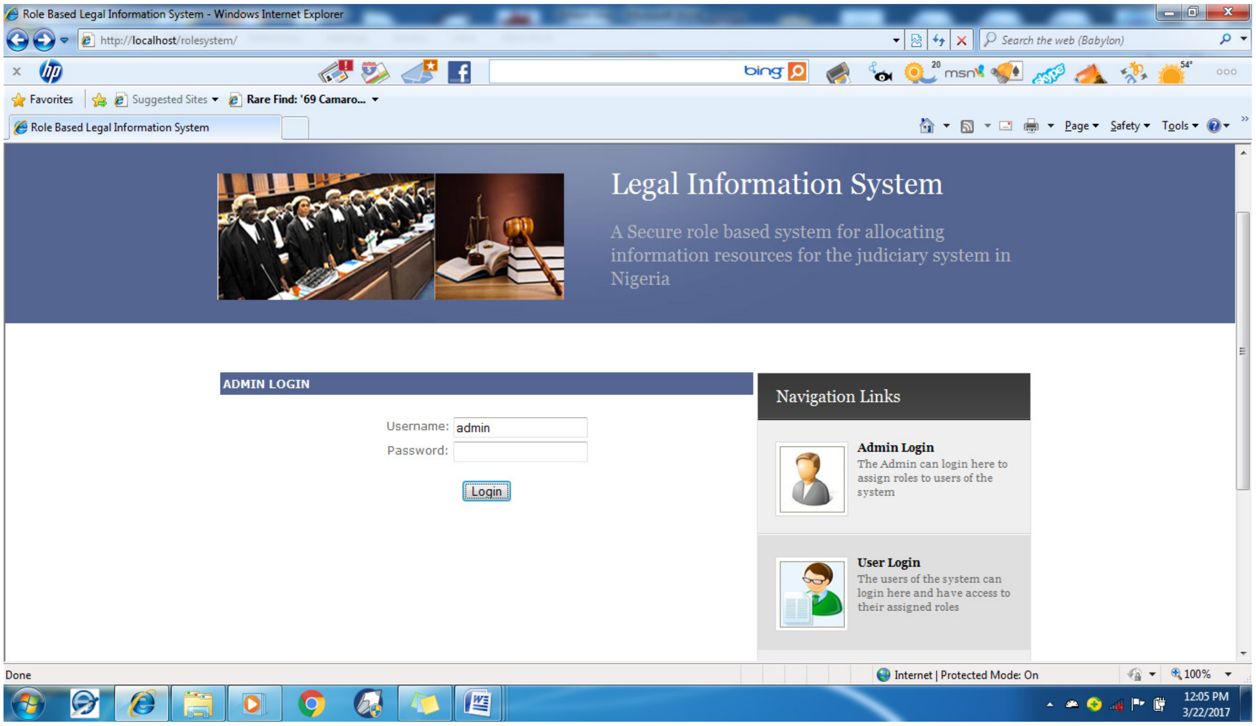


Figure 3: RBAC-LIS Class diagram

3. RESULT AND DISCUSSION

The implementation of RBAC is based on two navigational links; the Administrator's portal and the Users' Portal. The administrator's portal as depicted in Figure 4 displays the login page of the administrator. A correct entry gives him the control of the whole system. Figure 5 shows the interface where the administrator add new user by assigning role and grants some privileges to the user. Once a user is added to the system the user can have access to the information that is being assigned to the role.


Role Based Legal Information System - Windows Internet Explorer
http://localhost/rolesystem/
Search the web (Babylon)
Favorites
Suggested Sites
Rare Find: '69 Camaro...
Role Based Legal Information System
Page
Safety
Tools
Done
Internet | Protected Mode: On
100%
12:05 PM
3/22/2017

Legal Information System

A Secure role based system for allocating information resources for the judiciary system in Nigeria

ADMIN LOGIN

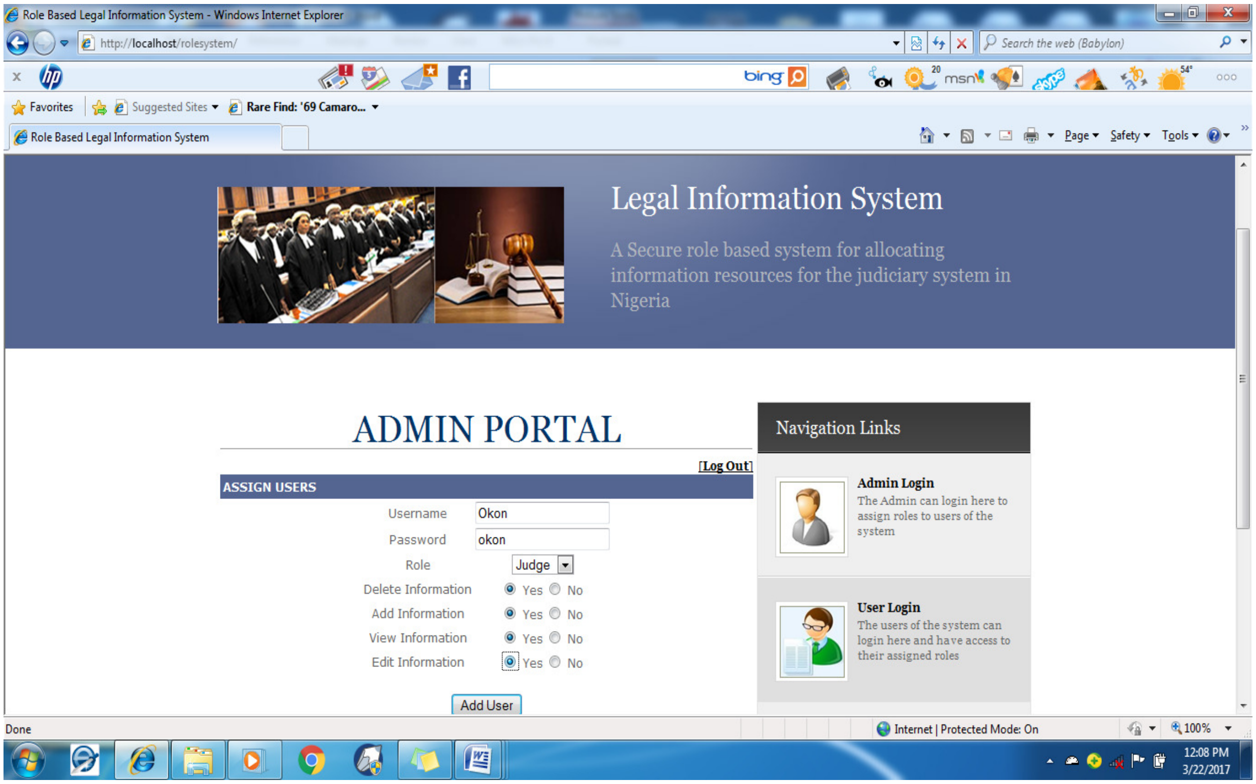
Username: admin
Password:

Navigation Links

Admin Login
The Admin can login here to assign roles to users of the system

User Login
The users of the system can login here and have access to their assigned roles

Figure 4: The Administrators portal


Role Based Legal Information System - Windows Internet Explorer
http://localhost/rolesystem/
Search the web (Babylon)
Favorites
Suggested Sites
Rare Find: '69 Camaro...
Role Based Legal Information System
Page
Safety
Tools
Done
Internet | Protected Mode: On
100%
12:08 PM
3/22/2017

Legal Information System

A Secure role based system for allocating information resources for the judiciary system in Nigeria

ADMIN PORTAL

[Log Out]

ASSIGN USERS

Username	Okon
Password	okon
Role	Judge
Delete Information	● Yes ○ No
Add Information	● Yes ○ No
View Information	● Yes ○ No
Edit Information	● Yes ○ No

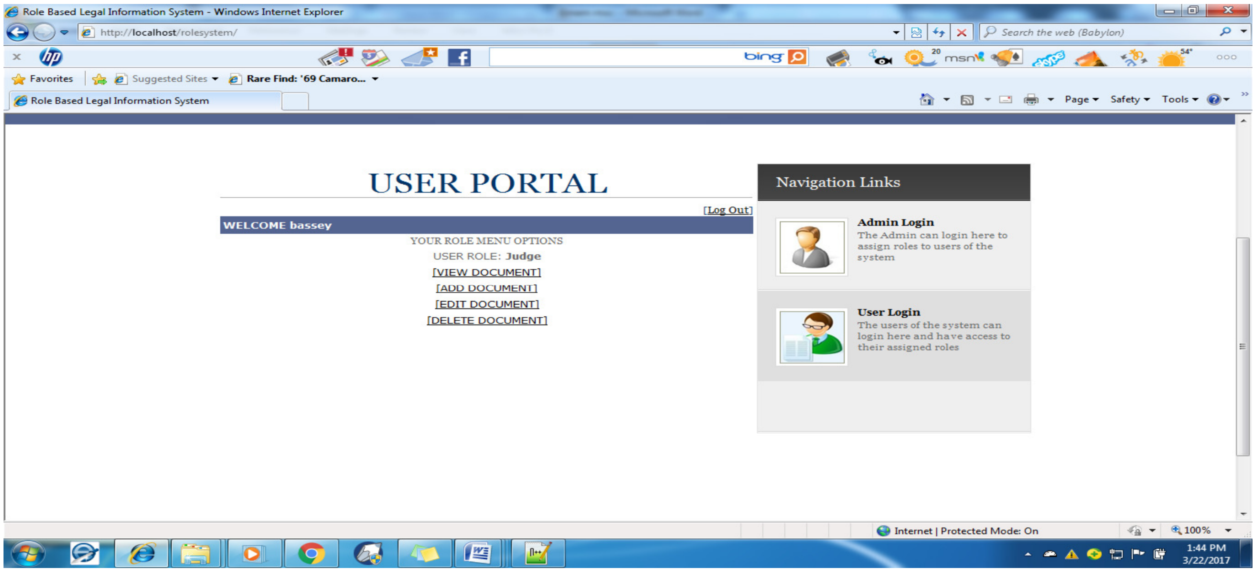
Navigation Links

Admin Login
The Admin can login here to assign roles to users of the system

User Login
The users of the system can login here and have access to their assigned roles

Figure 5: The Control Panel of the Administrator's portal

From the user portal, as depicted in Figure 6, new users that have been assigned a role have access to the privileges. Permissions are granted to the user based on the role assigned to that user. The user can login with the username and password assigned to the user. The login form allows the user registers cases with the case id and case title. Data are encrypted in such a way that only those users who possess appropriate access permission according to their role specified by Role Based Access Control Policies can decrypt the encrypted data before access can be granted.


Role Based Legal Information System - Windows Internet Explorer
http://localhost/rolesystem/
Search the web (Babylon)
Favorites
Suggested Sites
Rare Find: '69 Camaro...
Role Based Legal Information System
Page
Safety
Tools
Internet | Protected Mode: On
100%
1:44 PM
3/22/2017

USER PORTAL

[Log Out]

WELCOME bassey

YOUR ROLE MENU OPTIONS

USER ROLE: Judge

[VIEW DOCUMENT]
[ADD DOCUMENT]
[EDIT DOCUMENT]
[DELETE DOCUMENT]

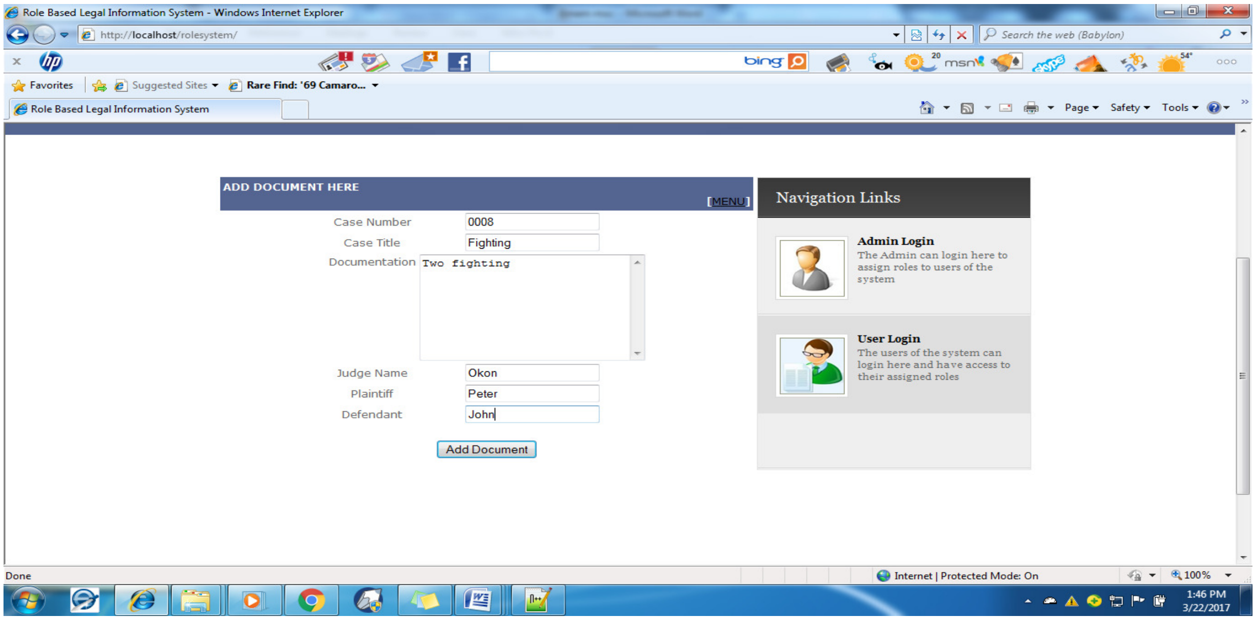
Navigation Links

Admin Login
The Admin can login here to assign roles to users of the system

User Login
The users of the system can login here and have access to their assigned roles

Figure 6: The User Portal for RBAC-LIS

The add document interface shown in figure 7, shows where the user registers cases with the case id and case title. The output screen displays all the cases registered in the system including the case number, case title, judge, plaintiff and defendant. Any case can be searched using case id.


Role Based Legal Information System - Windows Internet Explorer
http://localhost/rolesystem/
Search the web (Babylon)
Favorites
Suggested Sites
Rare Find: '69 Camaro...
Role Based Legal Information System
Page
Safety
Tools
Done
Internet | Protected Mode: On
100%
1:46 PM
3/22/2017

ADD DOCUMENT HERE

[MENU]

Case Number: 0008
Case Title: Fighting
Documentation: Two fighting
Judge Name: Okon
Plaintiff: Peter
Defendant: John

Add Document

Navigation Links

Admin Login
The Admin can login here to assign roles to users of the system

User Login
The users of the system can login here and have access to their assigned roles

Figure 7: Add Document Interface

4. CONCLUSION

In this paper, a role based access control model for legal information system has been demonstrated using Blowfish encryption, UML, PHP and MYSQL database for its main storage. Roles are assigned based on the responsibilities of the users of the system. The authorized user who satisfies the access policies will be able to decrypt the data using their private key. With the access time the system accountabilities are guaranteed. Role based access control for legal information system has showed that it is a really good solution for security purposes especially for legal information.

REFERENCES

1. Abhishek, M. Suyel, N. and Samir, N. (2014). "Taxonomy and Classification of Access Control Models for Cloud Environments", Department of Computer Science & Engineering, Tripura University, Suryamaninagar, Tripura West, Tripura, India, Retrieved 12-08-16 from: http://www.springer.com/978-1-4471-6451-7
2. Andras, B. (2004). "Role-based access control policy administration" Cambridge, United Kingdom, Retrieved 24-05-17 from: http://www.cl.cam.ac.uk/
3. Kamran, K. (2015). Legal Information System: A Model Framework for Indian High Courts, Junior professional assistant (central library), University of Kashmir (India).
4. Lim, B. P., Zakaria O. and Mustaffa K. M. (2001). Role Based Access Control in Kidney Dialysis Information System, *Malaysian Journal of Computer Science*, Vol 14, No. 2, pp 20-25.
5. Matulevicius R. and Lakk H. (2015) A Model Role-based Access Control for SQL Databases, Journal of Complex Systems informatics and modelling Quarterly (CSIMQ), Issue 3, pp 35-62, ISSN: 2255-9922.
6. Peter, G. (2005). "Role based access control in a telecommunications operations and maintenance network Performed for Ericsson" AB LITH-IDA-EX–05/012–SE
7. Thion R. (2008). "Access Control Models". University of Lyon, France, Available at http://liris.cnrs.fr/romuald.thion/files/RT_Papers/Thion07%3ACyber%3AAccess.pdf
8. Owoeye, J. (2011). Information Communication Technology (ICT) Use as a Predictor of Lawyers Productivity, Principal Librarian Nigerian Institute of Advanced Legal Studies Lagos, Nigeria, Retrieved 12-06-2016 from http://unllib.unl.edu/LPP/
9. Zhou, L., Varadlharajan V., and Hichens M. (2013). Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage, *IEEE Transaction on Information Forensics and Security*, pp. 1947-1960.