International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT20634

A Security Framework for Electronic Medical Record

Obaloje Nkem Daniel
Department of Computer Science, Babcock University, Illishan-Remo, Nigeria

ABSTRACT

Electronic Medical Record (EMR) is basically the digital equivalent of paper records, or charts at a clinician's office. EMR assist and make easier the services rendered by a wide range of medical practitioners such as physicians, nurses, pharmacists and many others, hence, increasing the safety of patients. It's importance in the health sector cannot be overemphasized. The designed framework aims at identifying security challenges in the use and adoption of EMR, to design and implement a framework that will address issues identified in the use and adoption of EMR. This study presented a security framework to improve the security and privacy issues of EMRs by adopting Role Based Access Control and RSA cryptography. Role Based Access Control (RBAC) model was used because of its flexibility to support minimal functionality and its simplistic mode of assigning roles and permissions to users. In conclusion, this research was able to improve the security of EMRs and hence will increase its acceptance by health institutions which will bring about improved health services, especially in developing countries were manual record system are still prominent.

Keywords : Electronic Medical Record, Role-Based Access Control, RSA, Cryptography

I. INTRODUCTION

The term e-health, which emerged in the early twenty-first century, pertains to applying the utilization of modern information and communication technology to the conveyance of medical services in the health sector (Albahri, Albahri, Mohammed, Zaidan, Zaidan, & Salaman, 2018). E-health needs multidisciplinary advancements, such as telecommunication, computer science and instrumentation, to exchange medical data across expansive geographic regions. (Hussain, Al-Haiqi, Abdulnabi, Zaidan, Bahaa, & Kiah, 2015). Electronic medical record (EMR) and Electronic health record (EHR) are terms that are distinct from each other and are separately used, although both records contain the health-related information of patients and form the main factor of e-health applications. EMR is basically the digital equivalent of paper records, and typically contains general information such as treatment and medical history about a patient and is collected by the individual medical practice. EHR on the other hand is a more comprehensive report of the patients' medical history across systems and practices. All groups of healthcare providers, such as physicians, nurses and pharmacists, can utilize EHR and EMR (Abdulnabi, Kiah, Zaidan, Zaidan, & Alam, 2010). This study focuses on EMR (i.e. the legal record created in medical centres and ambulatory environments), which serves as the data source for EHR. Healthcare providers, patients, employers or insurers/payers are regarded as stakeholders, along with the government (Abdul-Talib, Zaidan, Zaidan, & Naji, 2009). EMR also performs a number of functions for non-care organizations. In order to justify payment for healthcare services rendered and to improve security, records are sent to insurance companies (government and private). These are used to monitor the

commercial aspects of health care for quality reviews, organizational reviews, and application studies. And they are used for general reasons, such as medical research, public health administration, management of social services and welfare systems, enforcement of the law, technical training and certification, and qualification for life insurance (Liu & Park, 2012). EMR systems can enhance the data collection process if well designed and implemented, leading to improved quality and reliability of health information. These systems help make sure that information on patients is easily accessible for continuity of care across health care facilities (Nzioka *et al.*, 2010).

1.1 Problem Statement

Electronic Medical Records (EMRs) are becoming both a popular and vital method of tracking and storing a patient's medical history, particularly in developing countries. EMRs are prone to risk of possible misuse and unauthorized access, hence, there is need to ensure that data is well scrutinized and protected to ensure that information are divulged to the right person as well as the need for a more secure process. In developing countries, patients are often responsible for the storage and transportation of their own medical records as these do not reside in one centralized location but are often distributed amongst different clinics. This creates a challenge for medical professionals who require the complete medical record in order to make a sound diagnosis and treatment plan. EMR use in medical institutions has many advantages for doctors, patients, and health care services. Unresolved privacy and security issues about patient information, however, are among the primary causes of its low adoption by medical institutions, especially in developing countries. Several approaches and methods, some of which are cryptography and access control, have been proposed in addressing the privacy and security issues so as to prevent hacking, misuse and abuse of patient's medical information. However, these techniques enhance security but do not seem sufficient to maintain the privacy and security of patient's record. Technical support and lack of adequate security culture also pose a challenge on the adoption of EMR especially in developing countries. In providing efficient security and privacy for EMR, there is need for a security framework that can promote security policies that is capable of adequately protecting patient's information and keep the privacy under the healthcare organization.

II. REVIEW OF LITERATURE

The focus of related work is to study the possible ways in which privacy of Electronic Medical Records can be improved and the existing tools and techniques employed in improving Electronic Medical Records privacy. Other studies also support the conclusion that, with the rapid adoption of Electronic Medical Records and the need to share these records between healthcare practitioners and patients, the privacy of these records need to be optimized for a better security of the records. To explore the challenge of preserving patients' privacy in electronic health record systems; a Patient Controlled Encryption scheme was proposed by Josh, Melissa, Eric, & Kristin (2009) that allows the patient to use their decryption key to generate subkeys which will allow their delegates to search and access only certain parts of their record. Yu-Chi, Gwoboa, Yi-Jheng, & Kuo-Chang (2013) proposed a new secure index scheme for keyword-search over encrypted ERMs, referred to as P-index. Kiah, Abdulnabi, Zaidan & Zaidan (2013) proposed a hybrid of simple object access protocol/extensible markup language (SOAP/XML) with advanced encryption standard and secure hash algorithm version 1 was used to achieve the security requirements with the capability of integrating with other systems through the design of XML messages. Alanazi, Zaidan, Zaidan, Mat Kiah, and Al-Bakri (2014) developed a hybrid system (AES and NTRU) with a highly cured approach to transmitting electronic medical records (EMRs) and identifying entities that transmit private patient information without permission. Lixian, Junzuo,

Robert, and Yingjiu (2016) proposed a new model for Ciphertext-policy attribute-based encryption (CP-ABE) with partially hidden access structure. Yilun, Xicheng, Jinshu, & Peixin (2016) proposed a cost-efficient secure channel free searchable encryption (SCF-PEKS) scheme for sharable EMRs. Yang & Jiguo (2018) proposed a novel Secure Channel Free Public key encryption without designated server (SCF-wdPEKS) scheme, that provides the resistance to the existing known three types of keyword guessing attacks, but also has the merit of no designated server. Mikhael, Kuspriyantoa, Noor, & Edi (2017) applied the Advanced Encryption Standard (AES) process that does disturb and hinder the speed of data transmission. Kai, Shangyang, Yanhui, Hui, & Yintang (2018) proposed a blockchain-based information management system, MedBlock, to handle patients' information. Ahmed, Sahar, & Tarek (2018) proposed a secure multiparty computation protocols which allows a group of distrustful data owners to jointly cooperate in executing analytical queries against their data while revealing nothing about the entire dataset.

III. METHODOLOGY

3.1 Design of Proposed Framework

In designing the framework, the study will use dribble v4, WireFrame Sketch and Toad Modeller. Components of the framework will be designed in line with the EMR standard based on the issues identified.

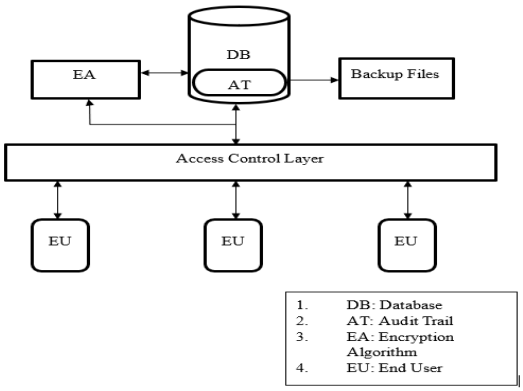

Figure 1: Proposed Security Framework for EMR
Source: Authors Model

In the proposed framework, EU can be patient, nurses, doctors, laboratory scientist or any other personnel resting access to the EMR system. These EU are onboarded onto the system during a registration stage. At the registration stage, important and basic information such as age, date of birth, next of kin, contact details, email address, etc. are captured. At this level the user role is defined and requirements/functionalities if each role is defined using a set of rules as defined by the organization. Upon accessing the EMR system, an authentication phase is required. This allows the system identify what role a user belong to. The authentication will be based on username/user id and unique password. For this framework, the Role Based Access Control (RBAC) model is used because of its flexibility to support minimal functionality and the secure but simplistic mode of assigning roles and permissions to users. After successful authentication, based on the user role, access will be given to user. For roles and functionalities that do not involve sensitive information such as chronic diseases, last date of surgery, mental status, etc. the user can have access to them without passing through the encryption layer. On the other hand, request for sensitive information pass through the EA layer. The EA layer is responsible for encrypting and decrypting information going into and coming out of the DB. At the EA layer, the RSA algorithm will be implemented. The DB is the data repository where all information is stored. On the DB, there is an audit trail (AT) mechanism implemented. The AT keeps track of every event that happens on the system by every user. This gives a visibility of user attempts to access unauthorized data as well as actions performed by authorized users on the system. In addition to the AT, a backup mechanism was also implemented and the DB snapshots are taken and kept in the backup files segment. This backup allows for data availability should in case there is any compromise on the data in the DB. The backup will be performed at regular intervals by the EMR system.

3.2 Design Model

The software process model may be defined as a simplified description of a software process which, provides process frameworks that may be extended and adapted to create more specific software engineering processes. The variants of the model accommodate the generic framework activities which defines a workflow that invokes each activity in a different manner.

The analysis and design, which entails the creation of models for proper understanding of the requirements and how to best achieve them, are illustrated below. Since the specification requirements of the application are well defined, the Water Fall Development Model of implementation is adopted. This model prescribes a systematic approach to software development, which starts with a well-defined, understood specification of requirements and moves through to it been deployment in a linear form.

3.3 Development Analysis

This involves a number of steps which ought to be followed which includes the design such as the entity relationship diagram which represents the relationship between the participating entities. The step-wise sets of activities include:

i. **Requirements identification**: This entails ensuring that needed tools and an outline of all other requirements are established and acquired from the onset.

ii. **The design**: After the Platform requirements and tools are in place, the project team must know all entities and how the Platform should look and how it should function.

iii. **The implementation**: After the design analysis, the project team can now implement the design of the system.

iv. **Validation:** After designing the platform, the team must test the designed Platform for bugs or errors and ensure that the Platform meets all the requirements and functionalities needed by the end users

v. **Maintenance:** The Platform must be maintained from time to time. For instance, adding new contents, removing old contents.

3.4 Model and Use Case Diagrams

A use case diagram is used to show the functionality provided by the Platform in terms of actors, their goals-represented as use cases, and any dependencies between them. It depicts every functionality that an end user can do on the Platform to be developed. In other words, it represents every case of use / action. A use case is an abstraction of the dialogue between an actor and a system. It states the possible interaction without giving the detail of each scenario.

Meanwhile, scenarios specify behavior of use case by description, not modelling. A sequence of steps describes a possible interaction between the Platform and the actor or user. The Interface designs are meant to give a feel of what the proposed Platform should look like; in terms of basic features and functionality. The designs are also meant to further explain the use case diagrams. In Figure 2, it shows the used case diagram for the proposed platform dashboard. This interface is what would be encountered when logged into the system. Different items in various dialogue boxes would have several extensions that would give further in-depth information about the patient and other operations that are to be carried out. Figure 3 shows the use case and interface design for the welcome page or the main menu. This interface shows the basic activities that can be carried out by any user on the dashboard and various extensions to search options linked to the nodes. While Figure 4 displays a diagram showing more in-depth in the dialogue extension to search options linked and the EMR Adaptors

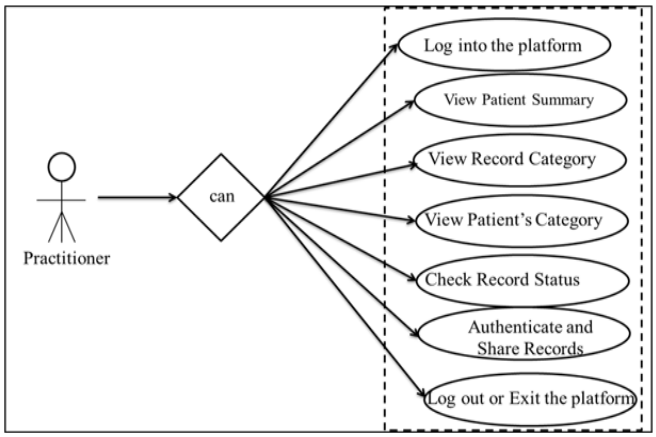

Figure 2. User Case Diagram for the proposed Platform Dashboard

Source: Authors Model

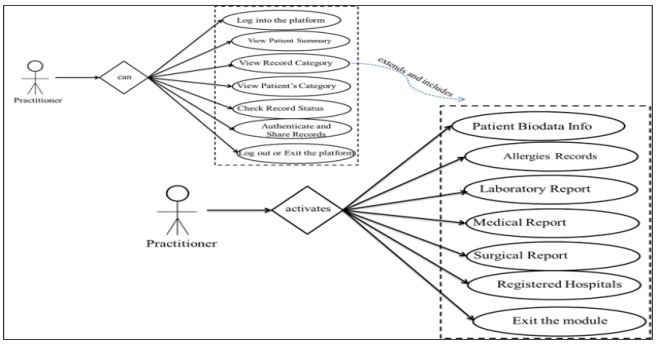

Figure 3. Diagram showing extension to search options linked from the nodes

Source: Authors Model

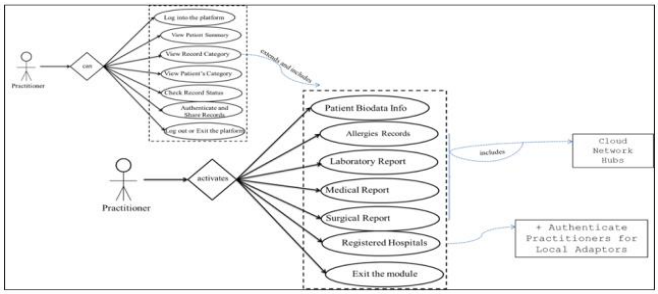

Figure 4 : Diagram showing extension to search options linked and EMR Adaptors

Source: Authors Model

3.5 Development Platforms

3.5.1 SIMUL8

Patients belonging to different record categories are individuals with conditions that vary and these conditions develop at different rates. When scheduled for appointments, they don't arrive quickly. Each appointment can take different amount of time, depending on the patient's need. SIMUL8 as a design tool will be used to model the real-life randomness and variation present in daily healthcare registration and routine systems.

3.5.2 Toad Modeler

Toad Modeler is a database design tool and modeling software that will be used for database design, maintenance and documentation. It will be used to show, visually create, maintain, and link EMRs, EHRs and network hub systems and Adaptors. It will also be of great assistance when changes are deployed to records' structure across different platforms. Toad Modeller will be used to construct logical and physical data models, compare and synchronize models, generate complex SQL/Data Definition Language (DDL), create and modify scripts, and reverse and forward engineer internal databases and health data warehouse systems.

3.5.3 Amazon RedShift and SaaS

As shown in figure 3.4, the volume of data being generated and collected and shared by various hospitals is in staggering level. These records' needs, will be encrypted and stored in the cloud network data warehouse that will allow effective medical data analytics strategy, and one cloud storage as service product in particular built for this big data revolution process is Amazon Redshift.

IV. RESULTS AND DISCUSSION

4.1 Practitioners Login Page

The practitioner page as presented in Figure 5 is the landing page of the developed system. On this page, the practitioner logs in by providing the authentication name (username) and the NHIS code. Once these values are provided, the system validates and performs an authentication process. This process authenticates the role of the practitioner to determine what access he/she has. Upon successful validation,

the system displays the access level practitioner has as shown in Figure 6 and Figure 7. The actions practitioner can perform is also listed on the login page. In addition to the validation of the practitioner and listing the access and role of the practitioner, a button to login also pops up. On this button, the practitioner clicks to finalize the login process. If practitioner had a revoked right, or is not registered, the button to login (enter the hub) does not appear and the status of the practitioner is displayed as shown in Figure 8.

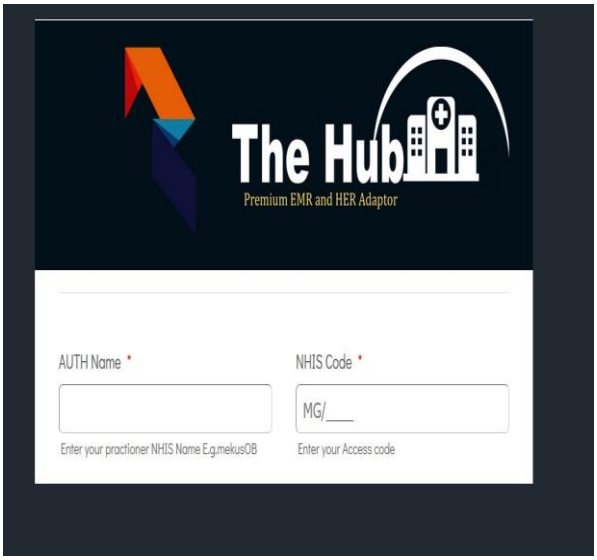

Figure 5 : The practitioner login page.

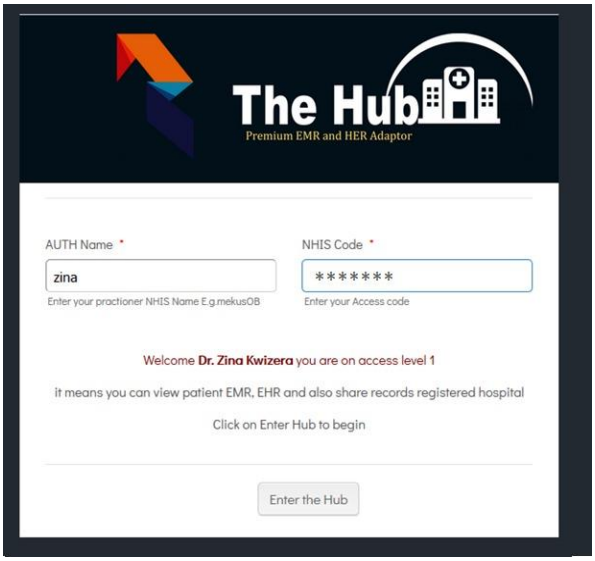

Figure 6 : The login process showing the access and role of the practitioner with access level 1, respectively

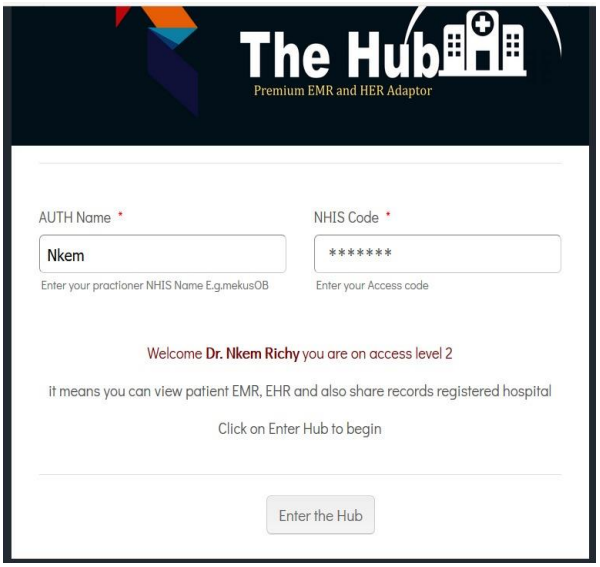

Figure 7: The login process showing the access and role of the practitioner with access level 2

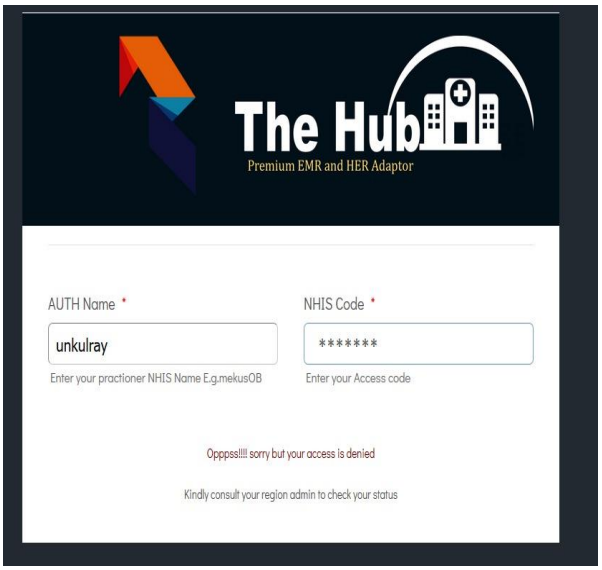

Figure 8: The login page for a practitioner with revoked access, respectively

4.2 Patient's Identification

Upon successful validation of the practitioner, the practitioner searches for patients and identifies patients either by National Identification Number (NIN) or the Patients Identification Number (PIN). As shown in Figure 9. An attempt to proceed without confirming an identification module throws an error. Even when the user has selected an identification option. The field must correspond with the patient's ID (RSA 128 level 3); As shown in Figure 10

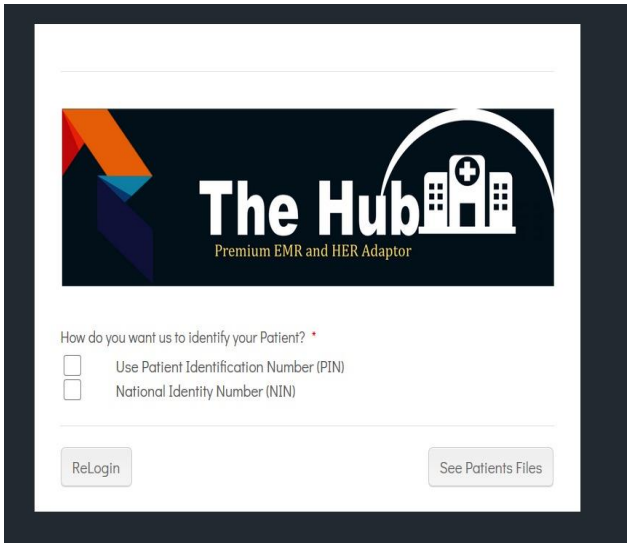

Figure 9: Patients Identification Page

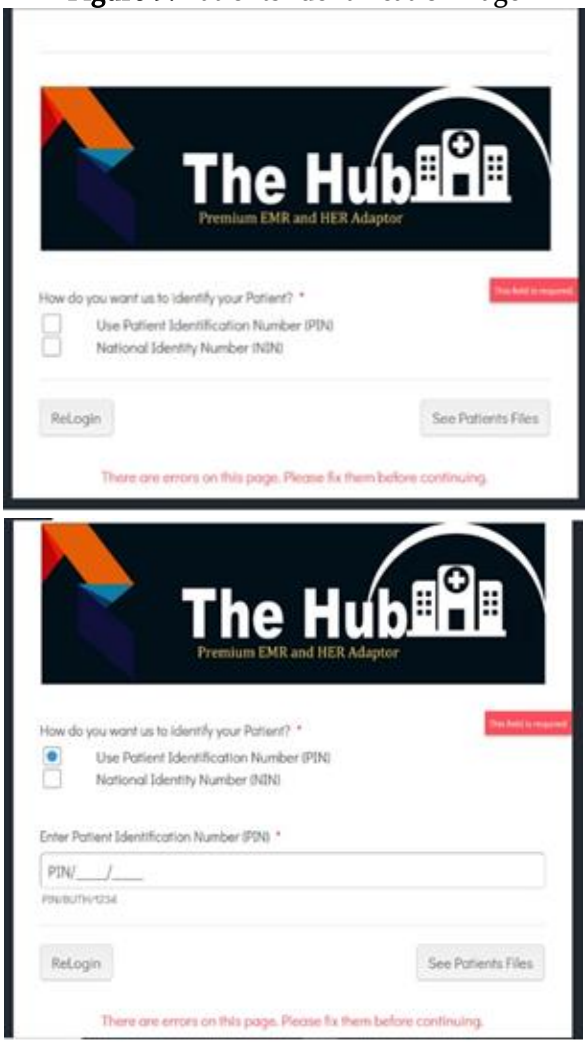

Figure 10 : Page Showing Error for Invalid Patient Identity

4.3 Viewing Patient's Records

Upon successful validation of the patient's identity, the system displays information based in the access level of the practitioner. An example as in Figure 11. shows summary, status (Abiola's authorized sharing as you can see a green icon) allergies are shown, registered hospitals and the last three major admission cases. Also, the page has categories of report which can be viewed upon a click. The report view of a patient can be viewed by the practitioner. As shown in Figure 12, laboratory category selected and the most recent report (pdf, png, txt, tables, mp4) is presented first and also can be attached and shared on from the window.

Figure 11: Page showing patient's results based on practitioner's access level.

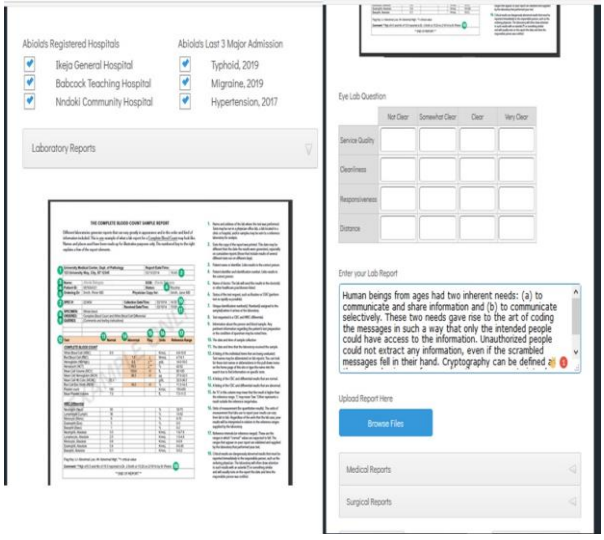

Figure 12: Sample of Laboratory Report for Patients, respectively.

4.4 Security Module of the System

Upon validation, of patient, the inputted identification has to tally with the owner code. As shown in Figure 13, the confirmation of the owner code allows access to view the records.

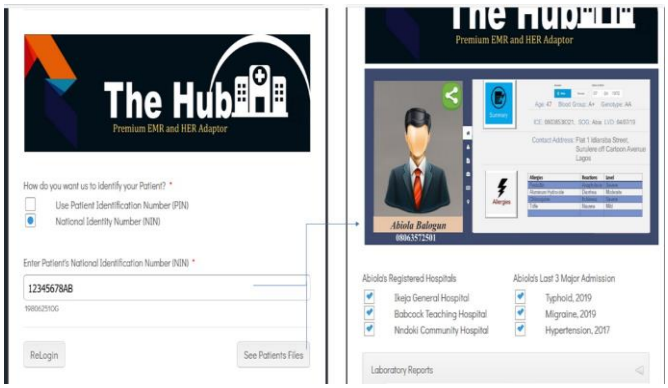

Figure 13: Checking owner code in line with patient's identification.

4.5 Sharing Patient's Records

Once the sharing code is entered, an encrypted token (AES256) is attached to the node of the report to keep integrity and audit trail of who sent and who received what. The encrypted code becomes visible once the sharing access code has been resolved by the interior server policy which holding the patient's preferences on whether to share or not to share. Figure 14 shows a sample of the sharing screen. Figure 15 shows the sharing ability disabled by the patients. With this, the practitioner is unable to share the report of patients.

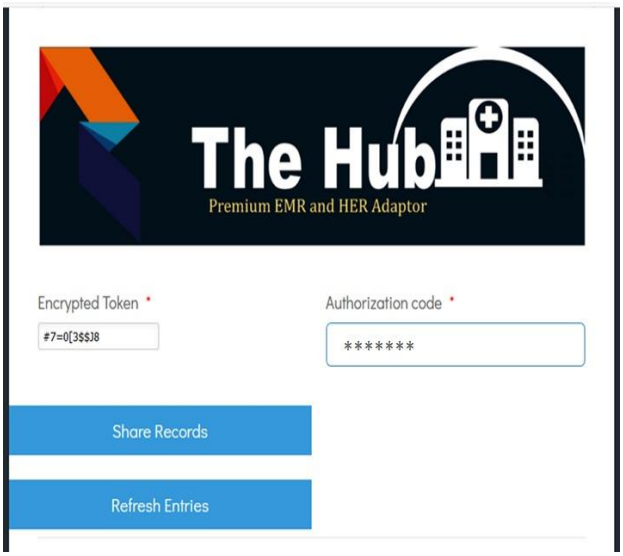

Figure 14: Patient's Record Sharing Screen.

Figure 15: Sharing record disabled by patients, respectively

V. SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Summary

EMR is basically the digital equivalent of paper records, or charts at a clinician's office. EMR assist and make easier the services rendered by a wide range of medical practitioners such as physicians, nurses, pharmacists and many others, hence, increasing the safety of patients. It's importance in the health sector cannot be overemphasized. Despite its significance in enhancing the health sector and increasing the safety of patients, its adoption has been slow due to some security and privacy issues identified in this research. This research

consulted and reviewed literatures so as to identify the security challenges faced by EMR and its adoption. This research designed and implemented a framework for EMR to mitigate the identified challenges.

The EMR system was developed using Toad Modeler, MySQL, PHP, HTML 5. AES 256 cryptography, authentication and different levels of abstraction for the practitioners were adopted to improve security for the developed EMR system. Due to the large volume of data generated, used and shared by health institutions, Amazon Redshift cloud services was used for storage. To also enhance security, data are encrypted before they are uploaded to the cloud and this makes the data useless if it falls into the hands of unauthorized users in the process of transmission. The authentication used in this study was based on username/user id and password. Role Based Access Control (RBAC) model was used because of its flexibility to support minimal functionality and its simplistic mode of assigning roles and permissions to users. The system was further evaluated using the Task Orientation evaluation approach with a validated questionnaire.

5.2 Conclusion

Many health-care centers in developing countries like Nigeria still depend on manual records of patients stored in paper and files. This manual storage of papers in files becomes a problem when the number of patients and clinical visits increases. It is a problem for medical practitioners and patients because sorting these files becomes a problem especially in emergency situations and when a patient record containing vital information is distributed in different health centers within a geographical location.

EMR have been able to solve many of these problems associated with the manual method of patient records and has been in use since 1972. Despite the solutions EMR presents to medical professionals, their adoption has not been encouraging and patients are still faced with the problems associated with manual record system. The low acceptance of EMR from literature has been attributed to security and privacy concerns related to EMRs. This study presented a security framework to improve the security and privacy issues of EMRs by adopting Role Based Access Control and RSA cryptography. This research was able to improve the security of EMRs and hence will increase its acceptance by health institutions which will bring about improved health services, especially in developing countries were manual record system are still prominent.

5.3 Recommendation

This study is recommended to hospitals, clinics, medical practitioners and other healthcare institutions that wants to improve their medical record system and also enhance the security and privacy of their client's confidential health data. Aside computerizing health records, it can be used to monitor the commercial aspects of health care for quality reviews, organizational reviews, and application studies. They also help to provide data used for medical research, public health administration, management of social services and welfare systems, enforcement of the law, technical training and certification, and qualification for life insurance. It recommended that further studies be conducted on EMRs in other to address other challenges such as lack of technical Support, interoperability, error in data entry, unavailability of infrastructures in developing countries, which has also militated against its slow adoption.

VI. REFERENCES

[1]. Abdulnabi M., Kiah M., Bahaa B., Zaidan A., Zaidan B., Alam M. (2010). Suitability of using SOAP protocol to secure electronic medical record databases transmission. Int J Pharmacol., 2010;6(6):959–64.

[2]. Abdul-Talib, Y., Zaidan, A., Zaidan, B., Naji, W. (2009). Optimizing security and flexibility by designing a high security system for e-government servers. ICOCI09, Univ., (pp. 355 - 358). Malaysia.

[3]. Ahmed, T., Sahar, S., & Tarek, S. (2018, March 12). Privacy-Preserving Secure Multiparty Computation on Electronic Medical Records for Star Exchange Topology. Arabian Journal for Science and Engineering, 1-10. doi:https://doi.org/10.1007/s13369-018-3122-5

[4]. Alanazi, O., Zaidan, A., Zaidan, B., Mat Kiah, L., & Al-Bakri, H. (2014). Meeting the Security Requirements of ElectronicMedical Records in the ERA of High-Speed Computing. Journal of Medical Systems, 165-178. doi:10.1007/s10916-014-0165-3

[5]. Albahri, S., Albahri, S., Mohammed, I., Zaidan, B., Zaidan, A., Hashim, M., & Salaman O. (2018). Systematic Review of Real-time Remote Health in Triage and Priority-Based Sensor Technology: Taxonomy, Open Challenges Motivation and Recommendations. J Med Syst., 2018;42(5):80.

[6]. Hussain M., Al-Haiqi A., Abdulnabi M., Zaidan A. A., Bahaa B., Anuar N. B., Kiah L. M. (2015). The landscape of research on smartphone medical apps: Coherent taxonomy, motivations, open challenges and recommendations. Comput Methods Prog Biomed., 2015;122(3):393–408.

[7]. Josh, B., Melissa, C., Eric, H., & Kristin, L. (2009). Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records. Microsoft Research, 103-114.

[8]. Kai, F., Shangyang, W., Yanhui, R., Hui, L., & Yintang, Y. (2018, June 12). MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. Journal of Medical Systems, 1-11. doi:https://doi.org/10.1007/s10916-018-0993-7

[9]. Kiah, M., Abdulnabi, S., Zaidan, B., & Zaidan, A. (2013, September 14). An Enhanced Security Solution for Electronic Medical Records Based on AES Hybrid Technique with SOAP/XML and SHA-1. Journal of Medical Systems, 1-18. doi:10.1007/s10916-013-9971-2

[10]. Lixian, L., Junzuo, L., Robert, H. D., & Yingjiu, L. (2016). Ciphertext-policy attribute-based encryption with partially hidden access structure and its application to privacy-preserving electronic medical record system in cloud environment. SECURITY AND COMMUNICATION NETWORKS, 1-17. doi:10.1002/sec.1663

[11]. Liu, W., & Park, E. K. (2012). e-Healthcare security solution framework. 2012 21st International Conference on Computer Communications and Networks, ICCCN 2012 - Proceedings. https://doi.org/10.1109/ICCCN.2012.6289239

[12]. Mikhael, B. R., Kuspriyantoa, Noor, C. B., & Edi, R. (2017). Securing electronic medical record in Near Field Communication using Advanced Encryption Standard (AES). Technology and Health Care, 1-6. doi:10.3233/THC-171140

[13]. Nzioka, C., Osumba, M., Cheburet, S., Barsigo, A., Kimanga, D., Vakil, S., … Siganga, W. (2010). Standards and guidelines for electronic medical record system in Kenya. Institutional Training & Education Centre for Health, 1–112. Retrieved from https://www.ghdonline.org/uploads/Standards_and_Guidelines_for_Electronic_Medical_Record_Systems.pdf

[14]. Yang, L., & Jiguo, L. (2018). Efficient searchable public key encryption against keyword guessing attacks for cloud-based EMR systems. Cluster Computing, 1-15. doi:https://doi.org/10.1007/s10586-018-2855-y

[15]. Yilun, W., Xicheng, L., Jinshu, S., & Peixin, C. (2016). An Efficient Searchable Encryption Against Keyword Guessing Attacks for Sharable Electronic Medical Records in Cloud-based System. Journal of Medical Systems, 1-9. doi:10.1007/s10916-016-0609-z

[16]. Yu-Chi, C., Gwoboa, H., Yi-Jheng, L., & Kuo-Chang, C. (2013, October 26). Privacy Preserving Index for Encrypted Electronic Medical Records. Journal of Medical System, 1-7. doi:10.1007/s10916-013-9992-x

Cite this article as :

Obaloje Nkem Daniel, "A Security Framework for Electronic Medical Record", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 3, pp. 01-11, May-June 2020. Available at doi : https://doi.org/10.32628/CSEIT20634
Journal URL : http://ijsrcseit.com/CSEIT20634