International Journal of Computer Applications Technology and Research
Volume 13–Issue 11, 25 – 29, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1311.1004

Enhancing the Security of Patients' Records for Privacy and Integrity

Ononiwu Chamberlyn C.,[1]
[1]Dept of Computer Science, School of Applied Sciences, Imo State Polytechnic Omuma, Nigeria

Mgbeafulike Ike J.[2]
[2]Dept. of Computer Science, Faculty of Physical Sciences, Chukwuemeka Odumegwu Ojukwu University Uli, Anambra State, Nigeria.

Abstract: Data management and data protection is a burning issue across the globe. Security and authenticity of information are the major fears that keep organizations away from cloud computing as they are scared of losing information to unauthorized persons. In healthcare system, the amount of patient oriented data is constantly growing and the existing medical systems are faced with security challenges including vulnerabilities in access control, data breaches or unauthorized disclosure, inadequate authentication and authorization. In this work, an Enhanced Security Model for securing and protecting Electronic Health Records was developed using National Identity Number (NIN) serving as identity management in the cloud, One Time Password (OTP) served as means of authentication and Advanced Encryption Standard (AES) was used to encrypt the records for security and privacy. Object Oriented Analysis and Design Methodology (OOADM) were adopted in the design of the system. The New System enhanced the security of patients' records using NIN to serve as identity management in the cloud, the OTP served as means of authentication while AES ensured protection and privacy. The system was programmed using HTML, CSS, Php and JavaScript while the database was implemented with MySQL server. The results from the performance evaluation analysis based on the evaluation metrics of security, user friendliness, encryption time, reliability and privacy demonstrates that the new system is secured, reliable and user-friendly when compared with the existing system.

Keywords: EHR, NIN, OTP, AES, Cloud Computing, OOADM, CSS.

I. INTRODUCTION

During patients visit to hospital, physician records patient's medical encounter in a paper or electronic media and transmitted the record to nurses and other medical units for processing. These records forms part of the medical information processing for the healthcare sector and should be secured because as more of medical records are stored electronically, the threats to security and privacy increase. Electronic health records form an integral part of the healthcare system and it is imperative that EHRs are safe because there is evidence that breaches in security have an impact on patient's health care. This calls for an enhanced data management and data protection in clinics and hospitals.

The global trend now is that technology is taking over every aspect of human lives more especially information dissemination. A lot of data manipulations are witnessed in transmitting records manually or semi-automated way. Agencies, hospitals, ministries and individuals are looking for a more secured way of transmitting data. For example ministry of health in Nigeria is having daunting challenges linking up patient's medical records in all hospitals across Nigeria. This can be attributed to lack of confidence in transmitting patient's records electronically. With the latest development in technology, patient's medical records can be stored in the cloud. This will make it accessible from any internet access point and it will result to having all the hospital records stored in the cloud and integrated for easy sharing of data.
Looking at the trend of events in the developed countries, cloud computing tends to offer a more secured way of information dissemination electronically. Cloud computing includes a group of computers that are jointly used to provide different computations and tasks. Cloud computing is one of the most important IT paradigms in the last few years. One of the key benefits that is offered from this IT technology for the companies is reduced time and costs on the market. Cloud computing is providing companies and organizations to use shared storage and computing resources. It is better than to develop and operate with their own infrastructure. Cloud computing also provides organizations and companies to have a flexible, secure, and cost-effective IT infrastructure. It can be compared with the national electric grids that permit organizations and homes to plug into a centrally managed, efficient and cost-effective energy source. Main corporations including Google, Amazon, Cisco, IBM, Sun, Dell, Intel, HP, Oracle, and Novell have invested in cloud computing and propose a range of cloud-based solutions to individuals and businesses. There are different types and models in cloud computing regarding the different provided services. Cloud computing could be usually classified by two ways: by cloud computing location, and by the offered types of services. By the location of the cloud, cloud computing is typically classified in: public cloud (where the computing infrastructure is hosted by the cloud vendor); private cloud (where the computing infrastructure is assigned to a specific organization and not shared with other organizations); hybrid cloud (the usage of private and public clouds together); and community cloud (it involves sharing of IT infrastructure in between organizations of the same community). If the classification is based on type of offered services, clouds are classified in these ways: IaaS (Infrastructure as a service), PaaS (Platform as a Service), and Software as a Service (SaaS) [11].
When we utilize cloud computing we run our software on hard disks and CPUs that are not in front of us. That is why users are having more doubts about the security issues when they are using this technology. So, a lot of

different types of attacks could happen in the cloud technology. Besides the above mentioned, most known attacks involve phishing, IP spoofing, message modification, traffic analysis, IP ports, etc. There are a lot of security techniques for data protection that are accepted from the cloud computing providers, and they all provide authentication, confidentiality, access control and authorization.

Authentication in Cloud Computing ensures that the proper entity or person is getting access to the provided data from the cloud technology provider. When authentication is ensured in the cloud computing, it means that the user's identity is proved to the cloud service provider when accessing the stored information in the cloud. Public and private types of cloud are using various designs for authentication with RSA. RSA cryptosystem accepted different models for authentication like two factor authentication, knowledge based authentication, and adaptive authentication. AWS (Amazon Web Services) is concentrated on the confidential information transfer between the web server and the browser including virtual private cloud [13]. In this context different authentication schemes are implemented, such as multifactor authentication, access management, AWS identity. There is also a technique for authentication that is allowing users to use just one password in order to authenticate themselves to multiple services [1].

II. REVIEW OF RELATED LITERATURES

A medical record is defined as any document that explains all detail about a patient's history, clinical findings, diagnostic test results, pre and postoperative care, patient's progress, and medication [3]. It can also be described as a chronologically written account of a patient's examination and treatment that includes the patient's medical history and complaints, the physician's physical findings, the results of diagnostic tests and procedures, and medications and therapeutic procedures. It comprises a chronologically written account that includes a patient's initial complaint(s) and medical history, physical findings, results of diagnostic tests and procedures, any therapeutic medicines or procedures, and subsequent developments during the illness [5]. Medical records cover an array of documents that are generated because of patient care.

[10] stated that at a minimum, a medical record must include the patient's identifying information, including name, date of birth, Social Security number, address, contact information, insurance information, emergency contact information, etc. She added that beyond those basics, the medical record must also include adequate clinical documentation that substantiates medical necessity.

[6] moreover noted that all medical records contain common information as identified as:

a. Personal identification information: each medical record must have specific personal identification information, such as social security, state or government issued identification number to tie record to the correct patient.
b. Medical History: everyone has a medical history, even if they have never been to a hospital.
c. Family Medical History: information about family member's health is an important part of your medical records because some health concerns are genetic.
d. Medication History: what we ingest, whether it is prescribed, over the counter, herbal or illegal is an important piece of our medical puzzle. A medical professional need to know about herbal, over the counter, home remedies, prescription medicines and even illegal drug use because of the way these can affect our health not only immediately, but over time, some drugs, medicines, or other ingestible materials are water soluble, some are fat soluble; some have short half-lives, while others stay in our bodies for longer periods.
e. Treatment History: knowing what treatment has been given, whether they worked, and which have failed is significant information for the provider to have.

[4] stated that patient records constitute the bulk of the medical records of almost all the health care centers all over the world. The existing system of medical record keeping used in Clinics is predominantly paper-based and it is associated with problems such as misplacement of patients' record, unnecessary duplication of patients' record as well as lack of effective back up facilities. In an attempt to address the problems associated with paper-based medical record, the project aimed at automating the whole processes by designing a web-based application to minimize the cost of procuring stationery materials needed for paper-based record keeping and enhancing the integrity and security of the patients' medical records.

[8] proposed an open data integration platform for patient, clinical, medical, and historical data across multiple health information systems. As an open platform, it can accommodate and integrate further heterogeneous data sources such as data streams generated by wearable Internet of Things (IoT) devices. As an integration platform, it facilitates centralization of data assets. This centralization empowers every stakeholder in a patient-centered care setting to actively participate in decision-making. A range of analytics and reporting solutions, such as data warehouse, interactive dashboards, and predictive analytics tools, can be deployed upon this open data integration platform. The proposed platform is currently being adapted and implemented to address patient-centered healthcare and clinical decision support requirements in a sports injury clinic at a not-for-profit private hospital in Melbourne, Australia.

[9] stated that several recent works proposed and implemented cryptography as a means to preserve privacy and security of patient's health data. Nevertheless, the weakest point of electronic health record (EHR) systems that relied on these cryptographic schemes is key management. Thus, the paper presents the development of privacy and security system for cryptography-based-EHR by taking advantage of the uniqueness of fingerprint and iris characteristic features to secure cryptographic keys in a bio-cryptography framework. The results of the system evaluation showed significant improvements in terms of time efficiency of this approach to cryptographic-based-EHR. Both the fuzzy vault and fuzzy commitment demonstrated false acceptance rate (FAR) of 0%, which reduces the likelihood of imposters gaining successful

access to the keys protecting patients' protected health information. The result also justifies the feasibility of implementing fuzzy key binding scheme in real applications, especially fuzzy vault which demonstrated a better performance during key reconstruction. It is important that future work considers the experimentation of the time cost that it will take patients to generate their confidential keys.

[2] maintained that measures such as encryption and password for data protection have loopholes and hackers know how to get their way through them. Encryption outputs (Cipher text) usually do have patterns with which to recognize the algorithm that produced it and quickly they design a reverse algorithm to decrypt and read the data. In the course of Passwords too, it was found out that passwords can be guessed, copied or hijacked. This research therefore provided a solution by designing an encryption model that can generate inconsistent cipher text with no pattern. Since illegal decryption is hinged on pattern matching, this encryption is therefore hack-proof. The research also designed a system of authentication that uses Biometrics instead of Password for access control. The advantages of having Biometric Systems in the cloud were given, such as reduction of cost and ubiquitous access. These designs are simulated using a web-system developed with PHP, MySQL, JavaScript and other Programs.
The result obtained from the system shows that the system's encryption's cipher text is unique and cannot be decrypted with the conventional and contemporary illegal decryption systems. The system does not decrypt without additional input (Salt_key) from the user. This distinguishes the cryptosystem from others. The research gap in this work is that the key for salting the encryption is user dependent. A user having different keys for different data may forget or confuse the keys, since it is not stored in the database for security sake, there is need therefore to find out how to manage/retrieve these keys in case of user forgetfulness.

III. ANALYSIS OF THE NEW SYSTEM

The enhanced security model for protecting electronic health records presents an authentication technique that made use of three-tier authentication which includes authentication factor for verifying the intended user to overcome the insider attack and providing single-sign on access of the registered services. The proposed authentication technique works on three phases. In the first phase, the users register themselves with the first-tier and second-tier authentication credentials. The first-tier authentication credentials are simple like username and password whereas the second-tier authentication credential is the National Identity Number (NIN). For the third-tier authentication, the user does not need to provide the authentication credentials like first-tier and second-tier authentication. The system is using the mobile secret code as the third-tier authentication code (One Time Password – OTP). This secret code is valid for some amount of time to access the requested service. We provide the time limit with the secret code. After the time limit expires, the user cannot access the requested service with that secret code.
The proposed scheme follows the following steps to authenticate the user for accessing the requested services.

1. For accessing the electronic health records, the user provides the URL of the electronic health records service provider in the web browser which sends the request to the server for loading the Login GUI of the service provider.
2. The user provides the registered username and password (first-tier authentication credentials) at the login GUI for verifying themselves to the server.
3. If the username and password provided by the user to the server is correct, then the server sends the reply of validation at the user side. The application program or server gets this validation reply at the user side.
4. The validation reply validates the user for the further authentication. If the server sends the positive reply for validation, then the system request for the users NIN for further authentication.
5. Once the user supplies his/her NIN, the system links up the NIN database to authenticate the users identity
6. Once the user enters the NIN and submits this information to the application program, the system extracts his/her phone number from NIN database and sends the secret code (OTP) on the registered contact number of the user. This secret code has some time limit which is set by the cloud service provider. After the time limit, the code will be expired and no more use of that code.
7. The users provide the OTP which they got on their mobile number to the secret code submission screen for authenticating themselves.
8. Once the user provides the secret code to the system, it will match the code which it sends to the user and also checks the time limit of that code. If the user provides the correct secret code within the time limit, then the system initiates the code for loading the requested service in the web browser.
9. After initiating the code of requested service, the system loads the electronic health records software in the user's web browser.
10. Once the requested service is loaded into the web browser of the user, direct communication has been established between the user's web browser and the electronic health records server.

Once access is granted to the user, all data transmission will be encrypted using Advanced Encryption Standard (AES). It is based on two common techniques to encrypt and decrypt data known as substitution and permutation network (SPN). SPN is a number of mathematical operations that are carried out in block cipher algorithms. AES has the ability to deal with 128 bits (16 bytes) as a fixed plaintext block size. These 16 bytes are represented in 4x4 matrix and AES operates on a matrix of bytes. In addition, another crucial feature in AES is number of rounds. The number of rounds is relied on the length of key. The key sizes decide the number of rounds and AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. In this dissertation, 128 bits AES algorithm was used and it uses a particular structure to encrypt data to provide the best security.

International Journal of Computer Applications Technology and Research
Volume 13–Issue 11, 25 – 29, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1311.1004

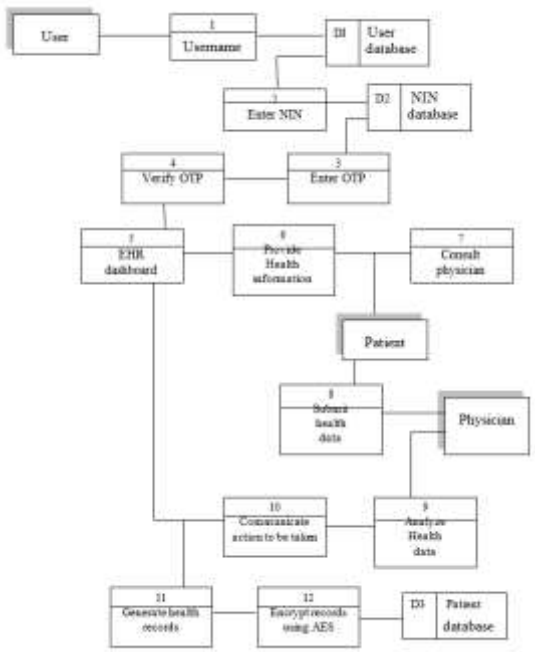

Figure 1: Data flow diagram of the new system

High Level Model of the Proposed System

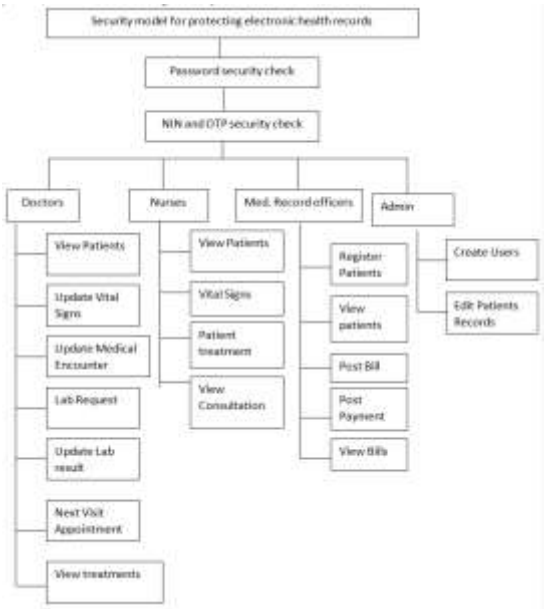

Figure 2: High-Level Model of the System

Activity Diagram for Security Model

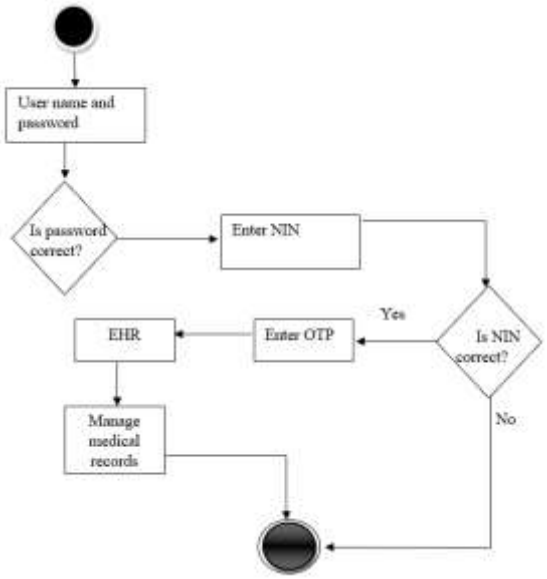

Figure 3: Activity Diagram of the security model

IV. CONCLUSION

Cloud based system faces a lot of security concerns and this scares organizations away from hosting their database in the cloud environment. Most security concerns centers on the privacy and validity of their data. This calls for more secured authentication system for cloud computing. Any authentication system's core strength depends upon the probability of success for breaking that system for accessing the services provided by the cloud service providers. In this thesis authentication scheme, the core strength is first-tier, second-tier and third-tier authentication user credentials. For getting the access of the requested service, the attacker has to break all the authentication layers. At the first tier, the username and password of the user is verified. At the second tier, the NIN is verified by linking the NIN database and verifying the number provided. At the third tier, OTP is sent to the user's phone number and the user is expected to enter the OTP for final identification. Also the AES algorithm was used to secure the data more by encrypting the data stored in the cloud based database. With the above security measures, the data security of the electronic health records is guaranteed.

REFERENCES

[1]. Acar Tolga, Mira Belenkiy & Alptekin Kupcu (2013). Single password authentication. International Journal of Computer and Telecommunications Networking, 57(13), 2013/167.

[2]. Shevtekar Sumit, Gangurde Yadhnesh & Bulbule Ayush (2023). Ensuring data security in transit and rest in cloud environments. International Journal of Current Science Research and Review, 13(4), 2250 – 1770.

[3]. Bali A. (2017). Management of Medical Records: Facts and Figures for Surgeons. Journal of Maxillofacial Oral Surgery, 10(3), 199–202

[4]. Bitrus J., Wadzani A. G., Ngubdo M. A. & Agu, E. O. (2020). Design and Implementation of a Secured Web based Medical Record Management System: A Case Study of Federal University Wukari (FUW) Clinic. International Journal of Computer Applications 177(41), 27 – 33.

[5]. Farlex Partner Medical Dictionary (2012). https://medicaldictionary.thefreedictionary.com/DuBois+formular

[6].R&G Editorial Staff (2022). Component of a medical record. Retrieved from https://www.rngmedcons.com/components-of-a-medical-record/

[7]. Khalid A. & Shahbaz, M. (2013) Cloud computing technology: Service and Opportunities. Pakistan journal of Science, 65(3), 343 - 351

[8]. Madhura J., Dinithi N., Daswin S., Damminda A., Brian D. & Kate E .W. (2020). A data integration platform for patient-centered e-healthcare and clinical decision support. Research Center for Data Analytics and Cognition, La Trobe University, Victoria, Australia b School of Allied Health, La Trobe University. Victoria, Australia

[9]. Omotosho A., Emuoyibofarhe J. & Meinel, C. (2022). Ensuring patients' privacy in a cryptographic-based-electronic health records using bio-cryptography. International Journal of Electronic Healthcare, 9(4), pp. 227

[10]. Rose R. (2019). The differences among records and what's legally required to be in them.Retrieved from https://www.phyicianspractice.com/

[11]. Muhammed F. M, Urooj A., Irfan k. & Sundas k. (2017) Cloud computing environment and security challenges: A review; International Journal of Advanced Computer Science and Applications, 8(10), 183-195.