ISSN No:-2456-2165

A Secure Cloud-Based Patient Electronic Medical Records System Using Two-Factor Authentication

Chigoziri B. Marcus[1]; Prince O. Asagba[2]
[1]Department of Computer Science
Faculty of Natural and Applied Science
Ignatius Ajuru University of Education,
Rivers State, Nigeria.

Abstract:- This work demonstrates a model that enhances security and predictive analytics of cloud-based clinical and patients' medical records for hospital management systems with adequate storage capacity, access to data for only authorized users, low cost medical services and implementation. The enhanced system uses Two-Factor Authentication (Password and Token) to grant access to authorized users in the system. Specifically aiming at providing greater security for sensitive information transmission, thereby enhancing the level of security in hospital management systems. The application was built with Python programming language, Django framework and machine learning algorithm with the capability to handle analytics. The efficiency of the model developed was tested and observed to be higher than previous models in terms of Security, Stakeholders' Participation, Access Control, Data Privacy and Flexibility. The token authentication and verification time were performed and an average of 10.95 seconds is required to access a patient's medical record which is not significant enough to compromise security.

Keywords:- *Cloud Computing, Electronic Medical Record, Data Mining, Two-Factor Authentication.*

I. INTRODUCTION

Cloud computing generally is referred to as the delivery of technological services over the web [1].It offers a simple on-demand network access model to an easily distribution, reduced management efforts, interaction between service providers and a communal pool of configurable computing resources[2].Cloud Computing and its business models have impacted immensely on developments in the twenty-first century, not only in the computing industry but in many other sectors [7].Cloud computing delivers computing and storage capacity as a service to a community of end recipients [6].

Cloud computing is the advancement of dispersed Computing, Parallel Computing, and Grid Computing, and the coordinates advancement result of Virtualization, Utility Computing, IaaS (infrastructure as a service), PaaS (platform as a service), and SaaS (Software as a service) [8].

In cloud computing, individual users and companies are allowed to oversee the communications of files, information, and applications without specific software installed on their devices; only internet access is required [9]. Figure 1 shows a typical cloud computing environment.

Fig 1:- Cloud computing environment (Source: Mansor et al. 2013)

Data mining is simply the process of extracting and analyzing a large set of information in order to discern trends and patterns. Data mining depends on effective data collection, warehousing, and computer processing. The method of retrieving and processing data efficiently has been a major problem for many years of data management, given the exponential growth of data generated ranging from Petabytes to Exabytes.

A medical record is a confidential record maintained by a medical practitioner or agency for a patient. This includes a description of the patient's medical history and information about each of the cases, including symptoms, diagnosis, care, and results, such as the patient's name, address, birth date. The primary aim of the medical record is to document the interaction and treatment of the patient with a health care provider to ensure sufficient healthcare for future references.

The integration of cloud storage and automated data mining promises easy technological connectivity and agility.As a consequence of the convergence, vast amount of data from different data warehouse can be easily retrieved [6]. With this approach, patient's records such as blood sugar, high blood pressure will be stored in the cloud first. The user of the system can be the patient or the health officer. Patient's details can be stored in the form of text, x-ray images or scan in a secured manner. Registered patient's do not need to carry their medical report on the go as the medical records are stored in the cloud and mining algorithm will be used to retrieve their data wherever, whenever it is required by a nearby licensed medical practitioner.

II. LITERATURE REVIEW

A. Electronic Health Record

Electronic health (medical) records (EHRs) are digitalized health records of patients collected from various health care settings. An electronic health record gathers, creates, and stores the health record electronically. With this system, medical information can be stored and shared conveniently through the cloud or other servers. Healthcare providers have been embracing the electronic health record cautiously.

Electronic health records can enhance clinical documentation reliability, tracking, billing, and coding for health use, and make health records portable. A typical electronic healthcare record comprises patients' bio-data, Medications, Allergies, Vital Signs, previous lab tests and results, Doctors' appointments and administration. EHR systems can be accessed by physicians from authorized healthcare facilities or individual organizations, as interoperating systems in affiliated health care units such as laboratories, medical imaging facilities, pharmacies, schools, and workplace clinics on a regional, or nationwide level.

B. Two-Factor Authentication

Two-Factor Authentication (2FA) is a security mechanism which requires two authentication method from the independent categories of identifications to verify the identity of the user for a login or other transaction. Two-factor authentication uses the combination of two independent authorization technique: what the user knows (Password) Knowledge Base Authentication, what the user has (Token) Possession Base Authentication or what the user is (Biometric Verification) Inherence Based Authentication [10]. 2FA seeks to create a layered defense and to make access to a destination like a physical location, a computer system, the network or a database for an unauthorized person more difficult. If one layer is compromised or breached, at least one more barrier must also be ruptured before the target is successfully accessed.

C. Related Work

B. Kamala (2013) claimed that with the integration of data mining services in cloud computing (IDMCC) with case studies such: Hospital-based electronic health records (EHRs), Community-based health information sharing, Personal Health Records (PHRs), Patient accounting, financial and billing systems, the user is permitted to retrieve meaningful information from virtually integrated data warehouse that reduces the cost of infrastructure and storage. By Kamala's approach, small companies will benefit by using IDMCC.

In order, to ensure that the challenges facing Healthcare Delivery Organizations in developing countries in terms of securing medical data and its lack of adequate data mining tools, Samuel et al (2013) proposed an enhanced model integrating Healthcare Delivery Organizations (HDOs) in developing countries into the cloud. Their proposed model was intended to provide Data Security and User Authentication Engine (DSUAE) which prevents unauthorized access to patient medical records and as well employs standard encryption/decryption techniques to guarantee the confidentiality of such records. In conclusion, Samuel et al (2013) claimed that with the information provided from the proposed model, effective decisions could be made by the management of Health Delivery Organizations or other concerned stakeholders and as well lead to social/economic stability of nations of the developing countries.

With no doubt that security and privacy have been a major hindrance to the growth of the electronic health system since inception. Therefore, Gajanayake et al. (2016) came up with an access control architecture for the electronic health system. This system was attainable via the combination of three security models: Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role Based Access Control (RBAC). Their system provides healthcare practitioners and patients the privilege to detect and set access to electronic health records. The major setback to this system is its inability to be used elsewhere other than in attaining electronic health record requirements.

With the adoption of cloud computing into the healthcare sector, vital health information is now stored remotely in a third party server. Kester et al. (2015) considered guaranteeing the privacy, safety, and security of information by engaging the encryption to ensure confidentiality and authentication methods in the sector. In order, to achieve this, encryption and watermarking techniques of digital image data in the domain were reversed and they further proposed a recoverable watermarked and encrypted image processing technique for security and privacy of medical images. This scheme is been used in securing electronic health images. However, the framework is limited to images only and not voice or text.

Since the existing e-health system failed to preserve patients' private attribute information while maintaining original functionalities of medical services, Guo et al. (2012) proposed a framework called PAAS (Privacy-Preserving Attribute-Based Authentication System) which they claim leverages users' verifiable attributes to authenticate users and preserve the private issues. They developed a two-way administrative system that involves the patient and the doctor to handle authentication and authorization procedures instead of the traditional centralized process. By so doing,

users are provided access based on their privileges without revealing their identities and health conditions. Their approach addresses the issue of security, privacy, and the variability of all users' attributes. However, the possibilities of different domains seamlessly sharing medical data are slim. This framework might be good on paper but, the implementation to prove its efficiency in reality as claimed by the authors would be a lot difficult.

The need for security enhancement in the e-health system once again arises as Fan et al. (2014) carried out investigative research on the Data Capture and Auto Identification Reference (DACAR) and came up with the design and implementation of a core component of the DACAR platform named Single Point of Contact (SPoC). This component they claimed provides claims-based authentication and authorization functionalities that Deploy reliable e-health service to be hosted in the cloud domain. The results of this system are a bit fair. However, their proposed system is limited to a small number of users access.

Revisiting the Attribute Based Encryption (ABE) Technique as Kumar et al. (2013) proposed a new framework for electronic health. Here, they designed a system where users are divided into domains: the Public and Private Domains. In this design, a private user can encrypt / access information only in its personal domain attributes while the public domain permits the user to use multi-authority ABE to improve security measures in these domains. This approach is commendable. However, it presents a great challenge of scalability and flexibility because the integration of attribute based encryption in the Electronic Health Record system is a major and serious management task.

III. CHALLENGES FACING CLOUD-BASED MEDICAL RECORD SYSTEMS

Whether the system is automated or manual, the objectives of all medical record systems are the same. Nevertheless, from a user's perspective, both methods vary profoundly in how data is entered and retrieved from the record, and the mechanisms for achieving these objectives differ. Although, electronic health records are embraced as an opportunity to rationalize and overcome problems in a broken healthcare system, EHRs often pose a range of important, emerging obstacles to resolve. Since patients often change physicians and see several physicians and specialists for primary healthcare, EHRs have the potential to improve the quality of healthcare, to allow multiple physician coordination, to improve medicinal safety, and to enhance healthcare assessment speed. However, many have feared for the inadequate safety and integrity measures of their records being put out in the open. High profile patients' will disagree with this technique despite its enormous benefit. For the sake of getting everyone to accept this trend, it is important to incorporate patient's participation as a key stakeholder to the system. Using the 2FA mechanism, a health officer is mandated to be authorized by the patient of choice before accessing his/her medical record.

IV. MATERIALS AND METHODS

A. *Methodology*

For this study, Object Oriented Methodology (OOM) was adopted to develop an all-inclusive stakeholder participation cloud-based electronic hospital management system.OOM is an approach to system architecture that encourages and enables the reuse to software components (architecture). This methodology allows the development of a computer system based on components to permit the efficient reusability of existing components and facilitate their component sharing with other components. These components can be combined in various ways to meet the new requirements specified by the user.

B. *Design*

The motive behind this architecture was to build a secured, dynamic, and dependable electronic health records (EHR) system. The architectural framework is controlled by authorized health officers and patients who are considered as major stakeholders in the EHR system. A patient will obtain his full access through authentication into a designated medical institution (hospital). At this point, he chooses who his medical personnel is. A health officer (HO) can also have access to patient's information that is available in the cloud through the patients' Token Verification security scheme.

Figure 2 shows a secured cloud-based hospital management system architecture.

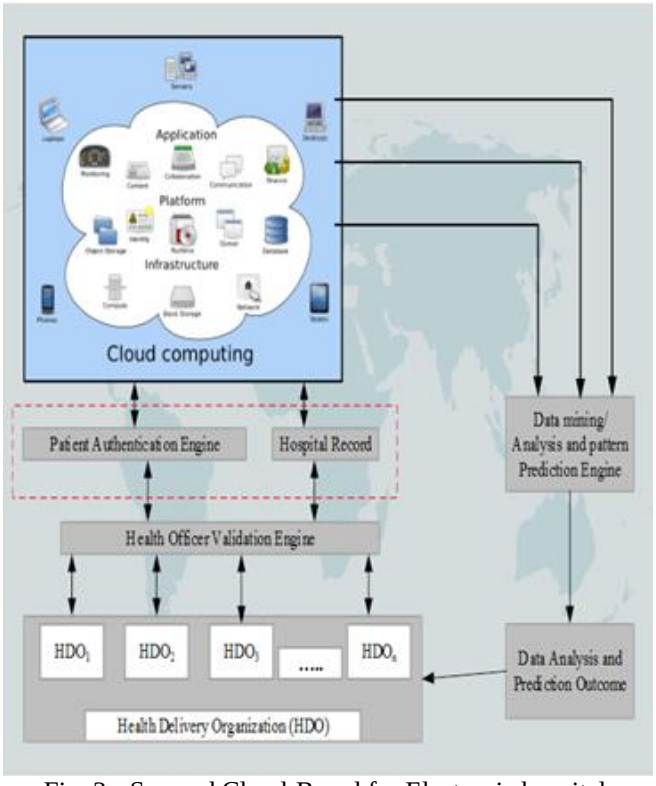

Fig. 2:- Secured Cloud-Based for Electronic hospital management system.

ISSN No:-2456-2165

The framework as seen in figure 3 consists of components such as Health Delivery organization (HDOs), Cloud, Data Mining/ Analysis and Pattern Prediction Engine (DMAPPE), and Patients and Health Officials (Users) Two-Factor Verification Engine.

i. Each HDO maintains EHRs, and all the information in EHRs is collected from several HDO units such as hospitals, radiology, laboratory, pharmacy, billing and so forth. It is also important to note that users are connected to the cloud through HDOs across the platform.
ii. The cloud system hosts patients and general hospital information and provides different services to authorized users. Also, its computing part supplies the necessary services over the network.
iii. User Verification: Users here are usually the patients, doctors, nurses, specialists, technicians, researchers, or other individuals, or groups. Due to the fact that several users are assumed to be connected to the cloud, privacy and security of data are an obvious concern to lookout. This is why the Multi-Factor scheme has been put in place as individual users have a unique identification.
iv. DMAPPE analyses requests to match them with stored data for similarities before coming up with an outcome.

Figure 4 shows the step by step breakdown of the operations of the system using a sequence diagram.

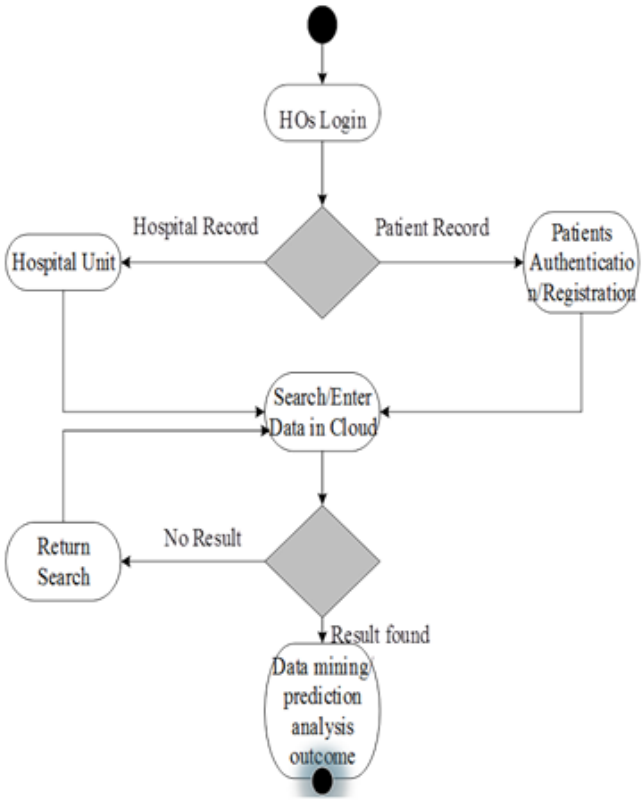

Fig.3.Use Case Diagram for the developed system

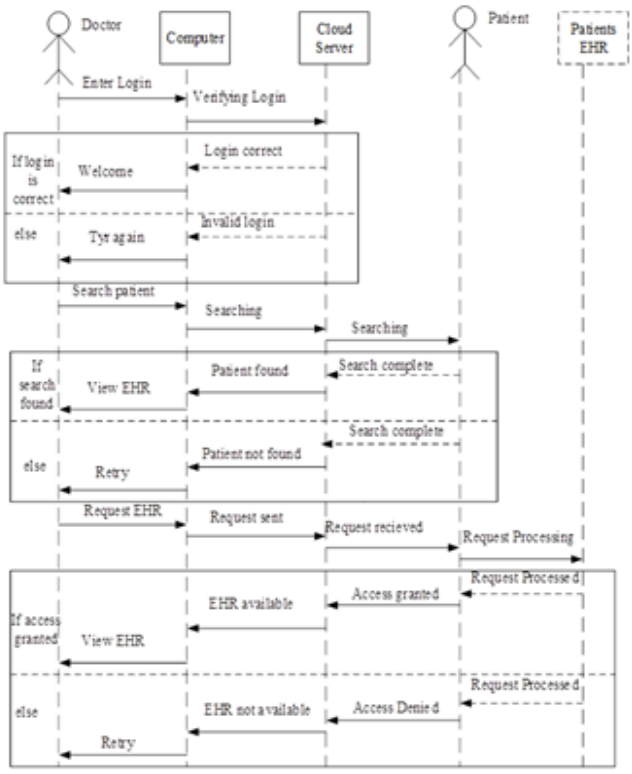

Fig.4.Sequence Diagram for the developed system.

V. RESULTS ANDDISCUSSION

Features	Rate	Scale
Access Control	XXX	30
Security Analysis	XXXX	40
Data Privacy	XXXX	40
Data Integrity	XXXX	40
Flexibility	XXX	30
Data Sharing	XXX	30

Table 1:- System Metrics Indicator

Figure 5 illustrates the performance metrics of the developed system.

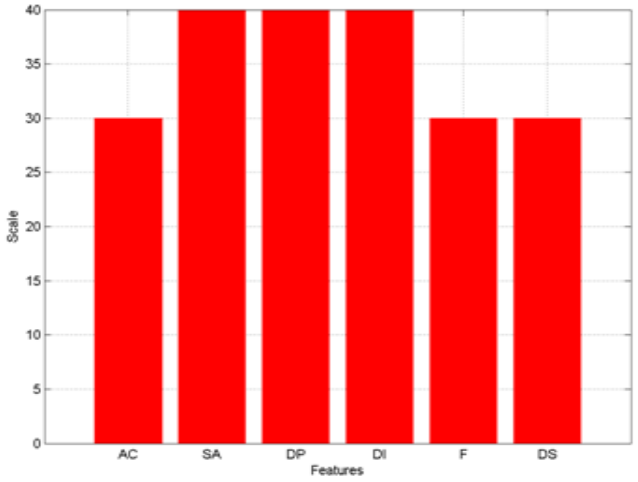

Fig. 5. System Performance Indicator Chart

The system was examined using three analysis tools (Use Case, UML and Sequence Diagram), the data collected were analyzed to create a quantitative understanding of systems security level and general performance. A specific level of performance metrics are required to quantify the security exposure. These metrics expresses the current level of security in the system. The key performance indexes are: Access Control, Security Analysis, Data Privacy, Data Integrity, Flexibility and Data Sharing.

In order to attain a quantifiable measurement of the system, a unit point scale of X = 10 is allocated to each metric assuming if true. Table 1 and Figure 5 illustrates the table and graphical representation of the systems security level respectively.

Patients	Time Sec	Patients	Time Sec
1	9	11	10
2	11	12	7
3	5	13	5
4	7	14	10
5	15	15	13
6	8	16	15
7	20	17	6
8	15	18	7
9	10	19	16
10	18	20	12

Table 2: Token Time Interval

Figure 6 shows demonstrates the token time interval
.

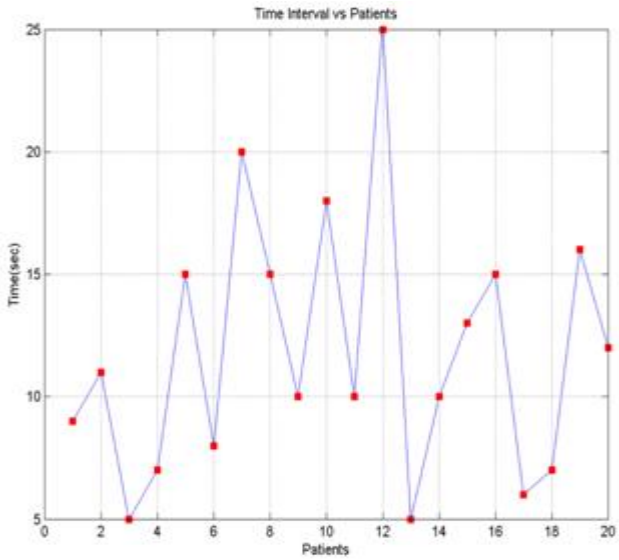

Fig. 6. Token Time Interval

A salient aspect of this system is the time taken to gain access to the patient's EMR, in other words, the time interval in sending the token, receiving and verifying the token in order to access the medical record is negligible. Although, there are several factors that affects the time interval in delivering the token on the patient's device, such as internet speed and mobile phone capability. An experiment of 20 persons from different locations were assumed as patients and registered into the EHR system. Then the token authentication and verification were performed to obtain the time interval in sending, receiving the OTP and logging into a patient's EMR. From Table 2 and figure 6, it is calculated that an **average of 10.95 seconds** is required to access a patient's medical record and in a security settings, a 10.95 seconds' waiting time is not significant enough to compromise security.

VI. CONCLUSION

All in all, health delivery organizations (HDOs) are lacking in terms of data management. A significant number of deaths are been recorded annually due to mismanagement of clinical records. Some factors responsible for these are; high cost of medical services, inadequate access to quality healthcare personnel and infrastructure, inaccurate diagnostic and therapeutic procedures, and poor storage of medical/clinical data. This work provides a better and secured cloud-based Platform for Healthcare Delivery Organizations in the cloud to enable them to carry out their operations efficiently. The proposed system incorporates a one-time password (OTP) Scheme that guarantees the security and confidentiality of patients' electronic health records as well as prevents unauthorized access to such records. The platform also provides a means which useful information can be mined through its machine learning predictive support system.

REFERENCES

[1]. Srinivasa, R., Nageswara, R., and Ekusuma, K., 2009. "Cloud computing: An overview," Journal of Theoretical and Applied Information Technology (JATIT), Pp. 71-76.
[2]. IBM Corporate Marketing White paper, "Cloud computing: Building a new foundation for Healthcare,".ibm.com/cloud, 2011.
[3]. Zimmermann, H. J. (2006). Knowledge Management, Knowledge Discovery, and Dynamic Intelligent Data Mining. Cybernetics and Systems: An International Journal, 37(6), pp. 509- 531.
[4]. Becerra-Fernandez, I. &Sabherwal, R. (2010). Knowledge Management: Systems and processes... New York: ME Sharpe.
[5]. DU, H. 2010. Data Mining Techniques and Applications: An Introduction. Hampshire: Cengage.
[6]. K. ShanthaShalini, R. Shobana, S. Leelavathy andV. Sridevi.A Cloud Based Approach for Health CareManagement. Int. J. Chem. Sci.: 14(4), 2016, 2927-2932.
[7]. Sanjay, P. A., Sindhu, M., and Jesus, Z. 2012. "A Survey of the state of Cloud computing in Healthcare," in Canadian Center of Science and Education, Network and Communication Technologies; Vol. 1, No. 2; ISSN 1927-064X E.
[8]. Jun Zeng (2018). The Development and Application of Data Mining Based on Cloud Computing. *J. Phys.: Conf. Ser.* 1087032008
[9]. MansorZauir, Mohamad M. Al Rahhal, Abdullah Al-Faifi, Alaaeldin M. Hafez, Hassan Abdalla (Jan, 2013). Survey of Data Mining Usage in Cloud Computing

[10]. Tamara S Mohamed (2019) Security of Multifactor Authentication Model to Improve Authentication Systems. Cihan university Sulaimaniah, Iraq
[11]. B. Kamala, (2013) A Study on Integrated Approach of Data Mining and Cloud Mining. International Journal of Advances in Computer Science and Cloud Computing, ISSN: 2321-4058 Volume- 1, Issue- 2,
[12]. Samuel, O.W, Omisore, M.O, Ojokoh, B.A, Atajeromavwo, E.J, (2013) Enhanced Cloud based Model for Healthcare Delivery Organizations in Developing Countries. International Journal of Computer Applications (0975 – 8887) Volume 74– No.2, (July 2013)
[13]. Gajanayake R, Iannella R, Sahama T. Privacy oriented access control for electronic health records. e-J Health Inf (2014);8(2):175–86.
[14]. Kester, Q, Nana, L, Pascu, A, Gire, S, Eghan, J, Quaynor, N. A Security Technique for Authentication and Security of Medical Images in Health Information Systems. In: 2015 15th International Conference on Computational Science and Its Applications, Banff, AB, Canada, (2015), pp. 8–13.
[15]. Guo, L, Zhang, C, Sun, J, Fang, Y. PAAS: A Privacy-Preserving Attribute-based Authentication System for eHealth Networks. In: 2012 32nd IEEE International Conference on Distributed Computing Systems, Macau, China, (2012), pp. 224–233.
[16]. Fan, L, Lo, O, Buchanan, W, Ekonomou, E, Sharif, T, Sheridan, C., SPoC: Protecting Patient Privacy for e-Health Services in the Cloud. (2014), pp. 1–6.
[17]. Kumar M, Fathima M, Mahendran M. Personal health data storage protection on cloud using MA-ABE. Int J ComputAppl (2013); 75 (8):11–6.