Journal of Computer Science and Information Technology
June 2014, Vol. 2, No. 2, pp. 21-36
ISSN: 2334-2366 (Print), 2334-2374 (Online)

Published by American Research Institute for Policy Development

An Enterprise Cloud-Based Electronic Health Records System

Adebayo A. Abayomi-Alli[1], Aderonke J. Ikuomola[2], Ifeoluwa S. Robert[3] and Olusola O. Abayomi-Alli[4]

Abstract

Electronic Health Record systems (EHR) are increasingly being deployed within healthcare institutions to reduce the problems and limitations of the paper-based approach but its deployment has been slow due to high investment and maintenance cost. Cloud Computing has been widely recognized as the next generation's computing infrastructure and it offers several advantages to its users. In this study, an Enterprise Electronic Cloud-Based Health Record System (E2CHRS) was designed, implemented and tested for recording, retrieving, archiving and updating of patients and other medical records. The Cloud database acts as the unified data bank for all the collaborating hospitals, the middleware provides a common platform for all the EHR systems between remote hospitals while an authentication server grants access to authorized users and denies unauthorized users access to records or resources on the system. An e-web portal serves as the front end of the system and it links the application with the cloud. Netbean IDE, Java development kit (JAD), WAMP server, Mysql, web browsers and other tools were used in developing the system. E2CHRS was deployed on twenty PC's and one server to simulate the enterprise network environment using different attack scenarios. The system performance was found to be satisfactory when tested.

Keywords: Cloud, Electronic, Enterprise, Health, Records, System

[1] Sound, System and Structures Laboratory, University of Pittsburgh, Pittsburgh, USA on leave from Department of Computer Science, Federal University of Agriculture, Abeokuta, Nigeria.
Phone: +14126141116 or +2347030672420, E-mail:ada44@pitt.edu
[2] Department of Mathematical Science, Ondo State University of Technology, Okitipupa, Nigeria.
[3] Department of Computer Science, Federal University of Agriculture, Abeokuta, Nigeria.

1. Introduction

An Electronic Health Record (EHR) is an evolving concept defined as a systematic collection of electronic health information about individual patients or populations (Saif, Wani, & Khan, 2010). It is a record in digital format that is theoretically capable of being shared across different health care settings and it include a range of data like demographics, medical history, medication and allergies, immunization status, laboratory test results, radiology images, vital signs, personal statistics like age and weight, and more. In many cases this sharing can occur by way of network-connected enterprise-wide information systems and other information networks or exchanges. The healthcare community generally agrees that improved use of accurate, current, and clearly understood health information is essential to the delivery of high-quality, cost-effective healthcare.

The benefits of this include improved clinical documentation and customer service, more efficient clinical workflows, improved medication management, and reduced transcription and labor costs (Burk, 2010).The healthcare industry has traditionally underutilized technology as a means of improving the delivery of patient care. Even today, organizations still rely on paper medical records and handwritten notes to inform and make decisions. Digital information is collated and kept between departments and applications, making access to a patient's longitudinal record difficult, if not impossible (Hitachi, 2012).

Patients in developing countries or in rural areas have to travel to larger hospitals carrying their paper-based medical records and in cases where they cannot they open new files without reference to the previous records. Patients registered in independent electronic health records systems also suffer from transferring their files from one hospital to another (McDaniel,2006) but with the electronic health records (EHR) system patients will have improved diagnosis and treatment, significantly fewer errors within personal health records, faster care and decision making responses from assigned medical professionals. Realization of these benefits is problematic in the health sector because healthcare is delivered by a highly fragmented “system” of private, public and nonprofit entities that exchange information within organizations to meet patient/business needs. This system makes it difficult to share information beyond organizational boundaries. The typical patient dealing with a single illness, for example, might consume healthcare products and services from many sources including primary care physicians, specialists, hospitals, pharmacies, medical laboratories and outpatient clinics.

To provide consistent, coordinated care at a reasonable cost, these organizations must be able to share patient's medical information freely while maintaining privacy and information security (Burk, 2010).

The integration of EHR between healthcare officers and exchanging them over the internet with other healthcare providers remains a challenge and a serious concern since it is exposed to theft, security violation and standardization difficulties (McDanaiel, 2006; Mirza&El-Masri, 2012). Authentication of user identity is therefore imperative in this form of distributed environments, without it; there can be little confidence in the developed system (Oracle, 2003). Common authentication methods and protocols are highlighted by (Duncan, 2002) as: Passwords, one-time passwords, public-key cryptography, zero-knowledge proofs, digital signatures, secure sockets layer, secure shell (SSH) and kerberos.

2. Literature Review

The traditional way of obtaining and gathering patient information is paper-based. Csiszar (2011)submitted that medical institutions would still rather use paper to gather information from their patients and also to record surgical procedures, observations and prescriptions. Some practitioners and physicians find accessing digital records somewhat complicated than obtaining a notepad and a pen. The thing that makes manual keeping of records very exhausting may be the mere undeniable fact that every day, a large number of new records are being stored in hospitals. It will be very complicated to sort medical records of all patients that keep increasing every minute. This complexity often arises to errors that will greatly get new daily happenings in hospitals, clinics and all sorts of other healthcare institutions. Aside from being time-consuming, collating records can be hard if you have no main paperback that may contain all information. The primary reasons for going to a "paperless" environment might be any or all of the following: proved medical documentation, increasing staff and/or instrumentation efficiency, reduction in overhead and the growth in practice, maximum coding revenues, eliminating record keeping space, enhancing the standard of care, accumulating information for managed care contracting, improving inter and intra office communications, standardizing an information platform for a physician group.

The electronic health record (EHR) is increasingly being deployed within healthcare organizations to improve the safety and quality of care. However Poissant*Et al.* (2005) enumerated some factorsthat are influencing the achievement of these goals while Zhang & Patel (2006) list the major benefits EHR systems would offer if well implemented.

Cloud computing brings a new business model which enables several advantages that would benefit the general healthcare community (Ahuja, Sindhu, & Jesus, 2012). By adopting the cloud in medical services both patients and healthcare organizations would obtain a huge benefit in patient's quality of service, collaboration between healthcare organizations as well as reductions in IT cost in healthcare companies (Deng *Et al*., 2010). Human life is priceless and medical resources are limited therefore, healthcare services adopted in cloud providers match a cost-effective concept where patients and health organizations take advantages of this new technology by improving patients' quality of service through a distributed high-integrated platform, coordinating of medical process as well as reducing IT infrastructure investment or maintenance costs which leads to a better healthcare environment (Wang, 2010).

Cloud computing is taking the business world by storm, offering a cheaper and easier way to complete an increasing number of tasks (Cristina, 2010; Deng *Et al.,* 2010; Dinh *Et al.*, 2013). Services are accessed remotely and only when necessary, so users need only pay for the time they spend using them (pay-as-you-go basis). The cloud is infiltrating every industry, but the virtualization of some more conservative industries, like healthcare is lagging behind.The five essential characteristics of cloud computing are particularly appealing to the needs of healthcare providers. These characteristics include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service(Agfa, 2012).

A mechanism for building trust and ensuring communication between different health information systems was proposed in (Pekka, 2004). The system employed an evolutionary cross platform model that integrates regional and national security domains with the help of an inter-domain zone. This zone offers common security and interoperability services for all connecteddomains. The main task of the platform is to offer centrally managed security services for cross-organisational pre-defined communication. The basic security services of the cross-platform domain are security policy bridging, cross-domain identification and authentication, certification services, static privilege management and auditing services.

Public Key Infrastructure (PKI) services were used on the platform to enable external users to access any of the EHRs inside connected domains. However, Pekka's model lacks harmonized legal and ethical framework, security services for trans-border communication and common security standards.

An approach based on utility computing and Wireless Sensor Networks (WSN) was presented by (Rolim, Koch, &Westphall, 2010). Wireless Sensor Networks (WSN) uses wearable sensors to collect vital signals that facilitate the collection and distribution of information to and from mobile devices. These two computing features were combined to build a system that automates the collection, input and analyses patients' vital data via a network of sensors connected to legacy medical devices, and delivers this information to the medical center's cloud for storage, processing, and distribution. With this, medical specialists can monitor patients at any place through the web (on a computer or mobile phones) and the system utilizes micro controllers to analyze collected data. However, there was no provision for confidentiality, integrity and privacy of patient data in this design. Also, the system has a complex architecture which may be difficult to implement in developing societies due to lack of infrastructural facilities.

Saif, Wani, & Khan (2010) proposed a network engineering solution for data sharing across healthcare providers for protecting patients' health data privacy in an EHR system. The system implemented a role-based and signature-based delegation. The role based delegation yields dynamics in the face of delegates' status, availability and change. The signature-based delegation provides a secure avenue for basic delegation and revocation. In addition to this, basic access control based on public key encryption techniques was implemented. This ensures that sharing of data is enabled and privacy of patients' data is protected across all collaborating healthcare centers but the introduction of proxy sign-in in the system exposes it to another high security risk.

Padhy, Patra, &Satapathy (2012)designed and presented the implementation of a cloud based rural healthcare information system model. The system employs a cloud central server that accepts virtual machines as tenants. The tenants are secure individual state-of-the-art facilities that store information in different healthcare centres. The connectivity and configuration of the cloud rural healthcare information is based on the service provider policy and location of the cloud data centre.

Internet is the main communication link between the service provider and rural healthcare centre. It also maintains the network traffic between the physical resources and the cloud. The authentication server uses the authentication and authorization mechanisms. With this model, patients can view their health records and prescriptions on their mobile phones on a request basis. The system can be used to share information seamlessly and in near real-time across devices and other applications. However, there is no fail-safe mechanism in the model to ensure system reliability and availability. Also, small hospitals and private physician do not have the IT requirements to support the technologies employed in the system.

3. Design Methodology

This section introduces the proposed design of the cloud based electronic medical record system.

3.1 Design Considerations

i. Cloud-based EHR: Pooling various healthcare IT resources into large clouds so as to facilitate ease of record sharing.
ii. Authentication: Security is achieved through the use of passwords.

3.2 Architecture of the System

The architecture of the cloud-based enterprise electronic health record system is presented in Figure 1. The system consists of two major components which are: the cloud-based system and the e-health web portal.

3.2.1Cloud-Based System

The cloud-based system consists of a central database server, Unifier Interface Middleware (UIM) and anAuthentication Server.

3.2.1.1 Cloud Central Database Server

This acts as the unified data bank for all the collaborating hospitals. The Infrastructure as a Service (IaaS) cloud datacenter contains the central database server as the data repository for storing electronic medical records and retrieving patient information.

The information is stored in a unified standard format which can be retrieved via query commands sent and resaved from the sharing hospitals' Web Portal system passing through the Unifier Interface Middleware (UIM).

3.2.1.2 Middleware

This part of the cloud provides a common platform for all the EHR systems of the sharing hospitals. It has an interface that masks the heterogeneity of all collaborating hospitals EHR standards, to facilitate the communication transactions between the Central Database and hospitals' systems. It recognizes any type of EHR standard it communicates with. This middleware remains in the cloud and communicates with the sharing hospitals via network connections. In this regard, each hospital does not need to have its own separate mask interface in order to benefit from the cloud; just an interface is enough to handle the job.

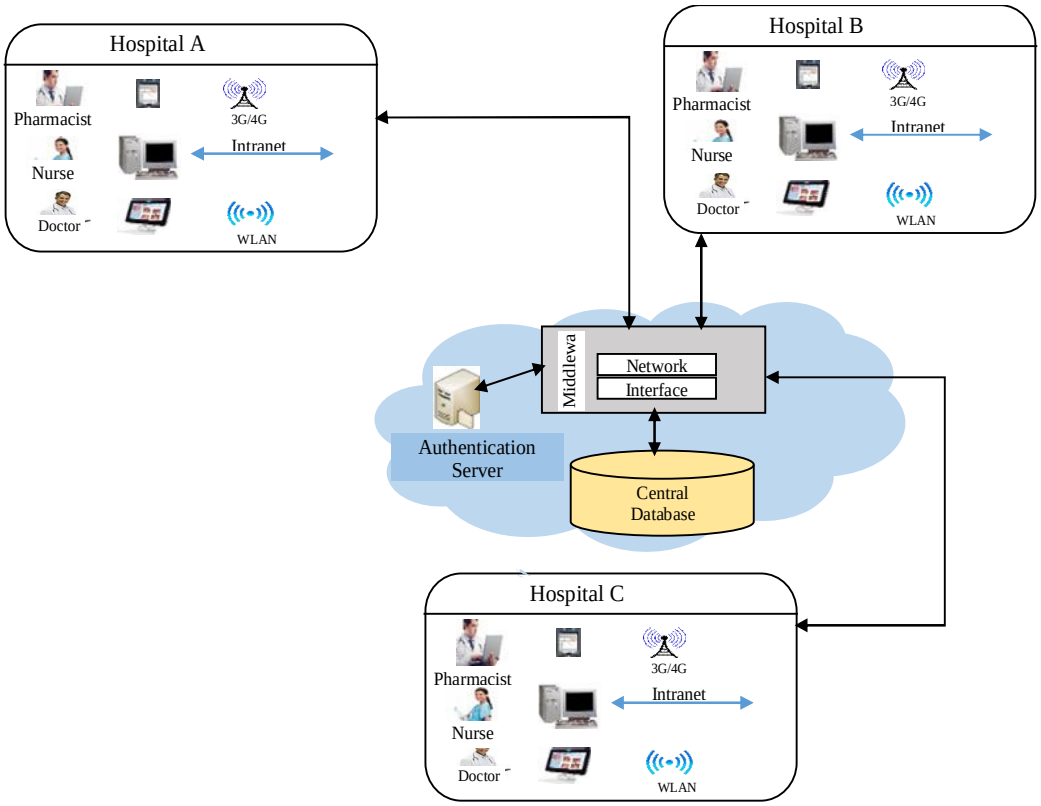

Figure 1: A Cloud-Based Enterprise Electronic Health Records System

3.2.1.3 Authentication Server

This is the part of the system that handles authentication and authorization. It verifies if an entity using the system has the right to perform the intended action such as (updating, retrieving, transferring,etc) on the health information provided. The authentication server grants access to authorized users and denies unauthorized users access to records or resources on the system. This is achieved through the generation of usernames and passwords for doctors (or other members of staff) of the sharing hospitals who will serve as part of the admin. Any member of the admin is expected to log in to the system with their username and password. The system compares the username and password with those in the local database and grants access to the user if they match, otherwise, the user is denied access.

3.2.2E-Health Web Portal

This is the front end of the whole cloud system. It is the third part of the cloud (top layer) that provides an application - Software as a service (SaaS) for the EHR system. The proposed health cloud system presents for end users (authorized doctors and clinicians) a configurable web portal to navigate through the central database and the whole EHR system. The web portal can send messages and receive response messages between the middleware and the hospital system. For each sharing hospital in the cloud, the web portal offers the user two tabs, one for accessing the hospital's local EHR system, and another for joining the cloud central database. Through this web page, every authorized user can retrieve, update and receive health information from the cloud's central database with limited access depending on the end user's privileges. The user can also, know from the retrieved information displayed on the web portal, if the requested EHR for a specific patient from a specific hospital exists inside the cloud or on the target hospital's local system and can choose to view EHR information about the patient even from locally independent hospitals connected to the cloud.Algorithm for retrieving and creating a patient's record is below:

Suppose $D_{1...}D_k$ are EHR systems of k hospitals all having a central location, C, where $k \geq 1$

Suppose for each EHR system, D_n, there exists, P_i for $1 \leq i \leq m$ for m number of patients.

To retrieve the e-health records of any patient P_i;
Step 1: Start
Step2: Input X, which is the identity of the patient P_i
Step 3: Check if $X \in D_n$
Step 4: If $X \in D_n$, goto 11
ELSE goto 5
Step 5: Join cloud
Step 6: Check if $X \in D_{n+1}$, where $1 \leq n \leq (k - 1)$
Step 7: if $X \in D_{n+1}$, goto 11
ELSE display "NO RECORD WAS FOUND"
Step 9: Create patient's record
Step 10: Add record to the database D_n
Step 11: Display patient's record
Step 12: End

The flowchart below describes the authentication procedure for the doctor's login is shown on Figure 2 while the algorithm for authentication is shown below:

Suppose DS is the status of the doctor.
At start up, *DS = False*

Step 1: Accept doctor's username and password from the medical record manager.
Step 2: Open the local database of the hospital.
Step 3: Search for the doctor's details.
Step 4: If doctor's username and password exist in the database, change DS = True
Step 5: Grant access to the user.
ELSE
Step6: Print "ACCESS DENIED: PLEASE CONTACT ADMINISTRATOR"
Step 7: Stop.

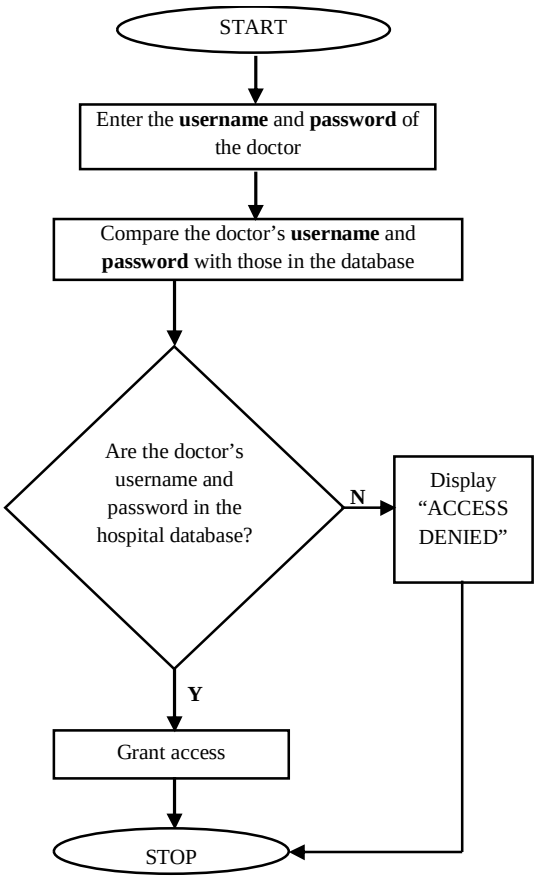

Figure 2*:* Flow Chart for Authentication

4. Implementation and Testing

The system was implemented and tested on twenty personal computers and one server meeting the minimum software and hardware requirements with Internet facilities. When the application is launched, the login or authorization interface pops up. The doctor seeking authorization inputs his username and password in order to gain access into the system. When an authorized doctor's correct login details are entered in the username and password columns, the system compares the details with those registered for the doctor in the database and the system grants access to the doctor as shown in Figure 3.

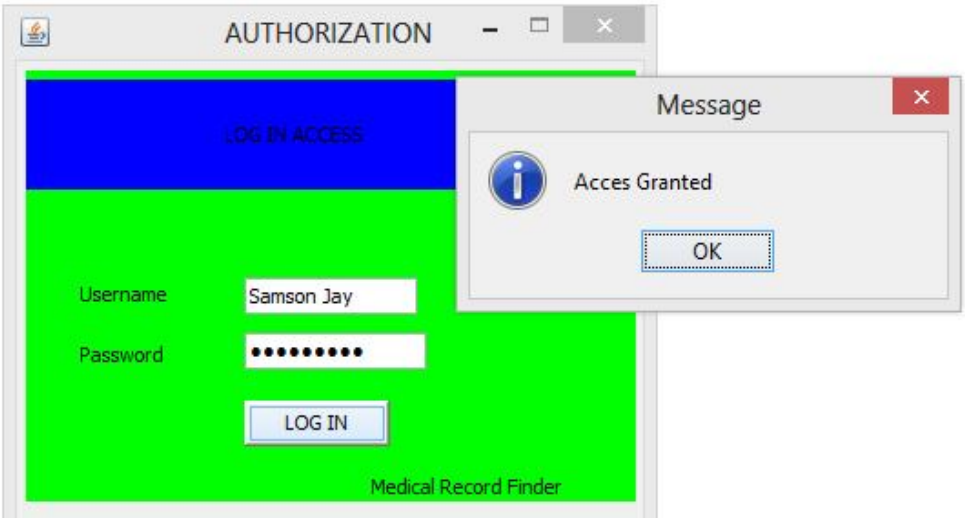

Figure 3*:* Login Access for an Authorized Doctor

After a successful login by a doctor, the home screen granting access to continue is displayed as shown in Figure 5.When you click to continue, a dialog box appears where you can search for the record of a patient directly from the database of the hospital by typing the first name in the search bar and clicking on search.

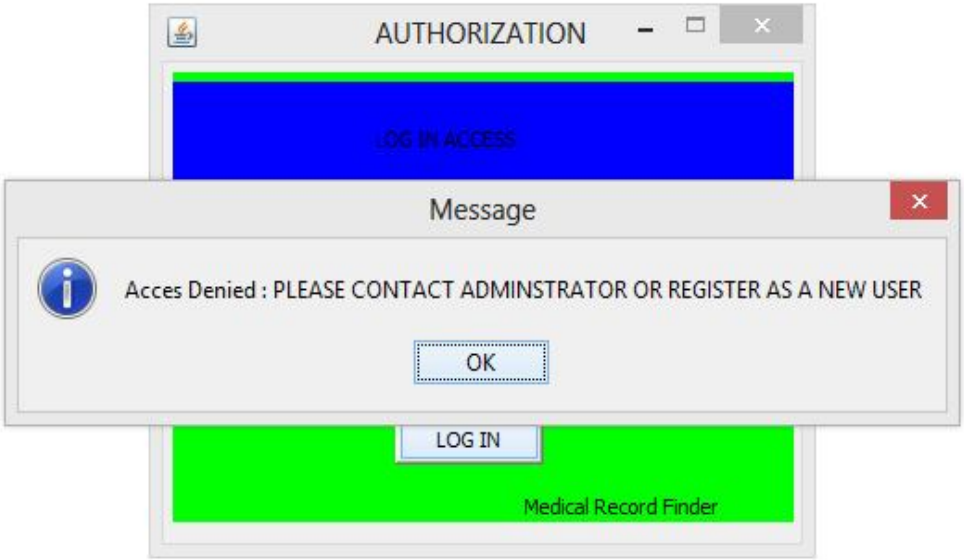

Figure 4*:* Unauthorized User Denied Access

However, if there is an attempt by an unauthorized user to gain access into the system by inputting incorrect details (i.e. incorrect username and password), the system denies such a user the access as shown in Figure 4.

Figure 5: Screenshot Showing Home Page

Figure 6: Shows the Search Result for a Particular Patient

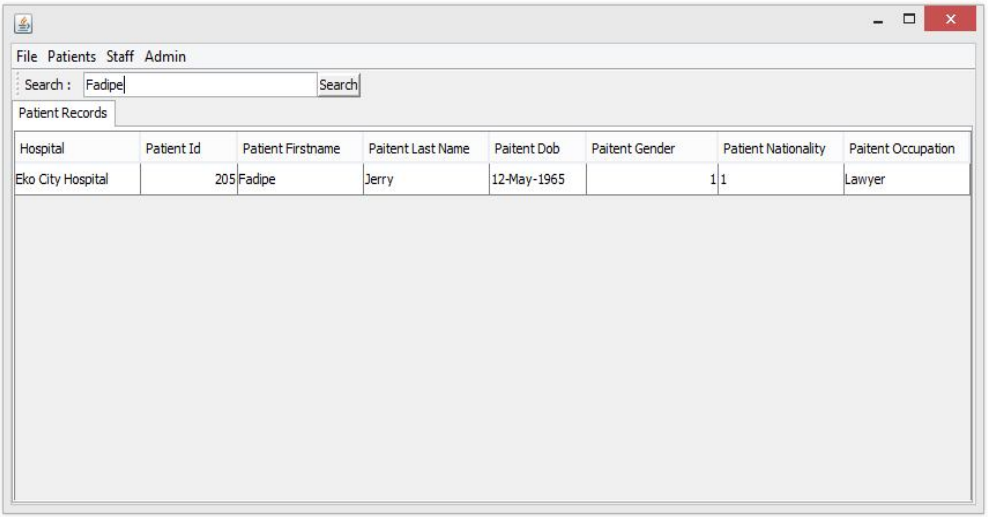

Figure 6: Search Result for a Patient

However, if the patient does not have a record with the hospital, the application displays a 'No Result Found' message as shown in Figure 7.

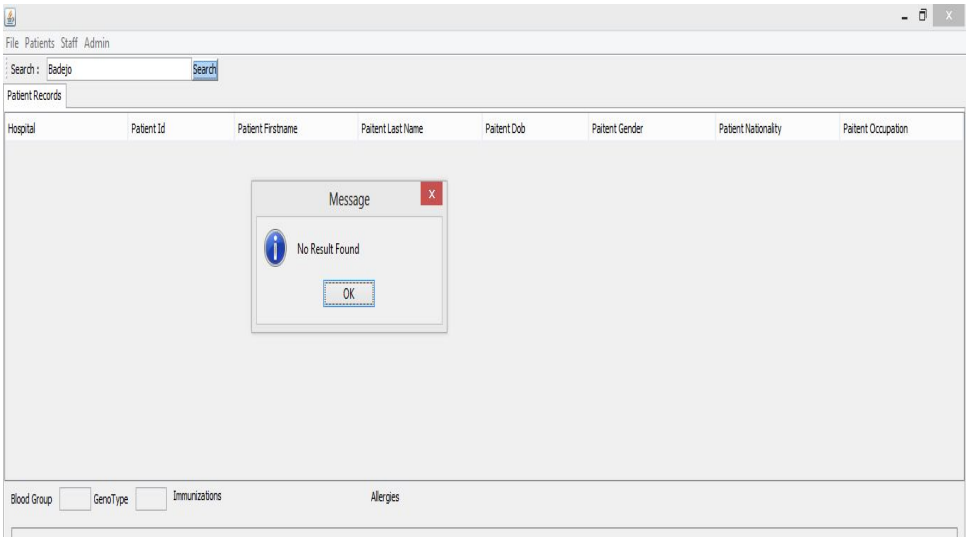

Figure 7*:* Screenshot Showing no Result

When searching for a patient's record in the cloud database and a 'No Record Found' message is displayed, it means that the patient does not have a record with Hospital A. The doctor can connect to the Cloud Server in order to look up the patient's record in Hospital B. To do this, the doctor clicks on File and then clicks on Connect to Cloud. A Connect to Cloud dialogue box pops up and the doctor enters the connection details for the destination hospital as shown in Figure 8.

The system performance was found to be satisfactory when tested using different attack scenarios by the twenty users on the PC's.Records of new patients visiting the hospital for the first time can be created.For example, the contact information of a new patient can be added by clicking on the Add Patient option in the Patient menu. Then the Add Contact Information option is clicked.

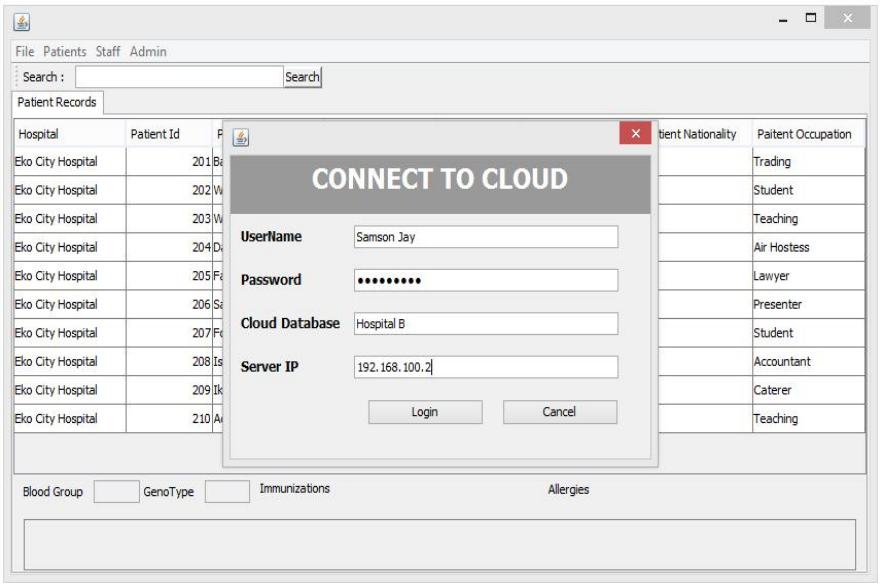

Figure 8*:* Screenshot Showing Connection to the Cloud Database

To add new information, click on New and then Save to add the new record you created to the database of the hospital. The medical information of a new patient can be added by clicking on Patients, Add Patient, Add Medical Information and New. Then, you click on ***Save*** to add the record to the database of the hospital.

5. Conclusions

In this work, a cloud-based enterprise electronic health records system has been designed and implemented. Cloud computing (CC) has been widely recognized as the next generation's computing infrastructure and it offers some advantages by allowing users to use infrastructures like servers, networks, and storages, platforms like middleware services and operating systems, and software such as application programs. By adapting the cloud technology to medical record management, lower the cost of healthcare delivery is achieved through reduce administrative bottlenecks. The convenience this kind of system will give to patients especially in developing world cannot be quantified. In addition, electronic medical records, digital medical imaging, pharmacy records and doctor's notes are all consolidated and accessible in real time. The ability of researchers to run analytics on the now structured data in the cloud will lead to better treatment options, optimal insurance programs and the possibilities of truly personalized healthcare.

Finally it is expected that in future mobile devices (e.g., smartphone, tablet PC's, etc) which are increasingly becoming an essential part of human life as the most effective and convenient communication tools will be incorporated into the enterprise cloud-based health record system.

References

Agfa (2012).Moving Digital Imaging into the Clouds, Agfa HealthCare, Mortsel-Belgium, May 2012.

Ahuja, P., Sindhu, M. & Jesus, Z. (2012).A Survey of the State of Cloud Computing in Healthcare, Network and Communication Technologies, 1(2), 12-19.

Burk, D. (2010).(2014, May 5).A Framework for Sharing Personal Medical Information Securely and Efficiently Across Public / Private Institutions,Cisco Internet Business Solutions Group (IBSG).Retrieved fromhttp://tools.cisco.com

Cristina, C. (2010). Electronic Health Record Adoption: Perceived Barriers and Facilitators-A Literature Review, Centre for Military and Veterans' Health, University of Queensland. April, 2010, 1-53.

Deng, M., Nalin, M., Schlehahn, E. &Abbadi, I. (2010).Trust Model for Cloud Applications and First Application Architecture, Seventh Framework Programme,Technical report D3.1.1/1.0, 1-152.

Dinh, H. T., Lee, C., Niyato, D. & Wang, P. (2013).A survey of mobile cloud computing: architecture, applications, and approaches, Wireless Communications and mobile computing, 13(18), 1587-1611, Dec. 2013.

Duncan, R. (2002).(2014, May 14).An Overview of Different Authentication Methods and Protocols,SANS Institute InfoSec Reading room.Retrieved fromhttp://www.sans.org

Hitachi (2012). How to Improve Healthcare with Cloud Computing, Hitachi Data Systems, White Paper, May, 2012, 1-20.

Csiszar, J. (2011).(2014, February 8).Paper-Based Medical Records vs. Electronic Medical Records.Retrieved from http://www.voices.yahoo.com/paper-based-medical-records-vs-electronic-medical-8591569.html

McDaniel, P. (2006). Authentication, The Internet Encyclopedia, John Wiley Publishers.

Mirza, H. & El-Masri, S. (2012).Cloud Computing System for Integrated Electronic Health Records, Department of Information Systems, College of Computer and Information Sciences, King Saud University.

Oracle (2003).Security Overview, 10g Release 1 (10.1).Part No. B10777-01

Padhy, R., Patra, M. &Satapathy, S. (2012). Design and Implementation of a Cloud based Rural Healthcare Information System Model, UNIASCIT, 2 (1), 149-157.

Pekka, R. (2004).(December 9, 2013). A Cross Platform Model for Secure Electronic Health Record Communication, International Journal of Medical Informatics, pp291–295. Retrieved fromhttp://www.intl.elsevierhealth.com/journals/ijml

Poissant, L., Pereira, J., Tamblyn, R., &Kawasumi, Y. (2005).The Impact of Electronic Health Records on Time Efficiency of Physicians and Nurses: A Systematic Review, Journal of the American Medical Informatics Association, 12(5), 2-5.

Rolim, C., Koch F., & Westphall, C. (2010).A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions, Network and Management Laboratory.

Saif, S., Wani, S., & Khan, S. (2010). A Network Engineering Solution for Data Sharing Across Healthcare Providers and Protecting Patients' Health Data Privacy Using EHR System",Journal of Global Research in Computer Science,2 (8).

Wang, X. (2010).(January 15, 2014)Application of Cloud Computing in the Health Information System, Computer Application and System Modeling (ICCASM). Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5619051

Zhang, J. & Patel, V. (2006). Electronic Health Records - A Human Project, E-Health and Medical IT Solutions, 35-36.