Design and Implementation of a Cloud-Based Healthcare Information System

[1]Bashir MainaSaleh
[2]Nasiru Sani
[3]Suleiman Hussaini
[4]Ibrahim Ahmad Tsafe

ABSTRACT

The healthcare is a critical institution that constantly requires available information at the right time and with high accuracy. Right information at the right time save lives, which is the main rationale behind healthcare services (saving lives). Electronic Health Record systems (EHR) are increasingly being deployed within healthcare institutions to reduce the problems and limitations of the paper-based approach.The deployment of the EHRhas been slow due to high investment and maintenance cost. Cloud Computing is an emerging technology that can be integrated with traditional health management to provide better health services. This work proposes a Cloud-Based Healthcare Information System (CBHIS) for recording, retrieving, archiving and updating of patients' information and other medical records to have a better management, high speed and increased quality for the medical processes keeping in mind the major issues of security, privacy and confidentiality of the patient information related to cloud computing.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.Netbeans 8.1 IDE was used to design the system

KEYWORDS
Cloud, Computing, Healthcare,Information, System, Electronic

INTRODUCTION

Cloud computing, also **on-demand computing**, is a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources.[1]

Cloud computing is one of the emerging technologies that has an increasing impact on both private and public sectors. It represents an on-demand service model for delivering resources ranging from storage and data access, via computation to software provisioning. Typical categories of cloud computing include Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) & Security as a Service (SecaaS).

Modern information technology is increasingly used in healthcare with the goal to improve and enhance medical services and to reduce costs. In this context, the outsourcing of computation and storage resources to general IT providers (cloud computing) has become very appealing. E-health clouds offer new possibilities, such as easy and ubiquitous access to medical data, and opportunities for new business models.

Compared to other industries, the healthcare industry has significantly underutilized technology to improve operational efficiency. Most healthcare systems still rely on paper medical records. Information that is digitized is typically not portable, inhibiting information sharing amongst the different healthcare actors. Use of technology to facilitate collaboration and to coordinate care between patients and physicians, and amongst the medical community is limited.

Around the globe, healthcare reform has mandated that it is time for healthcare information technology (HIT) to be modernized and cloud computing is at the center of this transformation. The healthcare industry is shifting toward an information-centric care delivery model, enabled in part by open standards that support cooperation, collaborative workflows and informationsharing. Cloud computing provides an infrastructure that allows hospitals, medical practices, insurance companies, and research facilities to tap improved computing resources at lower initial capital outlays. Additionally, cloud environments will lower the barriers for innovation and modernization of HIT systems and applications. Cloud computing caters to the key technology requirements of the healthcare industry:

- ✓ Enables on-demand access to computing and large storage facilities which are not provided in traditional IT environments.
- ✓ Supports big data sets for electronic health records (EHR), radiology images and genomic data offloading, a burdensome task, from hospital IT departments.
- ✓ Facilitates the sharing of EHRs among authorized physicians and hospitals in various geographic areas, providing more timely access to life-saving information and reducing the need for duplicate testing.
- ✓ Improves the ability to analyze and track information (with the proper information governance) so that data on

[1]*Postgraduate Student, MSc Computer Science, Department of Computer Science, NIMS University Jaipur, Rajasthan, India*
[1]*Email: bashir.maina2@gmail.com*
[2]*Univeristy Health Services, Federal University Dutse, Jigawa State, Nigeria*
[2]*Email: nasirusanimusa@gmail.com*
[3]*Kashim Ibrahim Library, Ahmadu Bello University Zaria Kaduna State, Nigeria*
[3]*Email: hsuleiman@abu.edu.ng*
[4]*Postgraduate Student, MSc Computer Science, Department of Computer Science, NIMS University Jaipur, Rajasthan, India*
[4]*Email: abbatsafe99@yahoo.com*

Copyright ©IJICCT-2016.

treatments, costs, performance, and effectiveness studies can be analyzed and acted upon.

Healthcare data has stringent requirements for security, confidentiality, availability to authorized users, traceability of access, reversibility of data, and long-term preservation. Hence, cloud vendors need to account for all these while conforming to government and industry regulations. Problems in making IT systems interoperable have delayed cloud computing growth in the health care industry.

Patients in developing countries or in rural areas have to travel to largerhospitals carrying their paper-based medical records and in cases where they cannotthey open new files without reference to the previous records. Patients registered inindependent electronic health records systems also suffer from transferring their filesfrom one hospital to another [2] but with the electronic health records(EHR) system patients will have improved diagnosis and treatment, significantly fewererrors within personal health records, faster care and decision making responses fromassigned medical professionals. Realization of these benefits is problematic in thehealth sector because healthcare is delivered by a highly fragmented "system" ofprivate, public and nonprofit entities that exchange information within organizationsto meet patient/business needs. This system makes it difficult to share informationbeyond organizational boundaries. The typical patient dealing with a single illness, forexample, might consume healthcare products and services from many sourcesincluding primary care physicians, specialists, hospitals, pharmacies, medicallaboratories and outpatient clinics.

To provide consistent, coordinated care at a reasonable cost, theseorganizations must be able to share patient's medical information freely whilemaintaining privacy and information security. [3]

The integration of EHR between healthcare officers and exchanging themover the internet with other healthcare providers remains a challenge and a seriousconcern since it is exposed to theft, security violation and standardization difficulties.[4] Authentication of user identity is thereforeimperative in this form of distributed environments, without it; there can be littleconfidence in the developed system [5]. Common authentication methodsand protocols are highlighted by Duncan [6] as: Passwords, one-time passwords,public-key cryptography, zero-knowledge proofs, digital signatures, secure socketslayer, secure shell (SSH) and kerberos.

LITERATURE REVIEW

The traditional way of obtaining and gathering patient information is paper-based. Csiszar[7] 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.

Cloud computing brings a new business model which enables severaladvantages that would benefit the general healthcare community [8]. By adopting the cloud in medical services both patients and healthcareorganizations would obtain a huge benefit in patient's quality of service, collaborationbetween healthcare organizations as well as reductions in IT cost in healthcarecompanies [9]. Human life is priceless and medical resources arelimited therefore, healthcare services adopted in cloud providers match a costeffectiveconcept where patients and health organizations take advantages of this newtechnology by improving patients' quality of service through a distributed highintegratedplatform, coordinating of medical process as well as reducing ITinfrastructure investment or maintenance costs which leads to a better healthcareenvironment [10].

Cloud computing is taking the business world by storm, offering a cheaperand easier way to complete an increasing number of tasks [11]. Services are accessed remotely and only when necessary, sousers need only pay for the time they spend using them (pay-as-you-go basis). Thecloud is infiltrating every industry, but the virtualization of some more conservativeindustries, like healthcare is lagging behind.The five essential characteristics of cloudcomputing are particularly appealing to the needs of healthcare providers. Thesecharacteristics include on-demand self-service, broad network access, resourcepooling, rapid elasticity, and measured service[3].

Saifet al [14] proposed a network engineering solution for datasharing across healthcare providers for protecting patients' health data privacy in anEHR system. The system implemented a role-based and signature-based delegation.The role based delegation yields dynamics in the face of delegates' status, availabilityand change. The signature-based delegation provides a secure avenue for basicdelegation and revocation. In addition to this, basic access control based on publickey encryption techniques was implemented. This ensures that sharing of data isenabled and privacy of patients' data is protected across all collaborating healthcarecenters but the introduction of proxy sign-in in the system exposes it to another highsecurity risk.

Padhy et al[15]designed and presented the implementationof a cloud based rural healthcare information system model. The system employs acloud central server that accepts virtual

Copyright ©IJICCT-2016.

machines as tenants. The tenants are secureindividual state-of-the-art facilities that store information in different healthcarecenters. The connectivity and configuration of the cloud rural healthcare informationis based on the service provider policy and location of the cloud data center.

Issues Related to the existing system

- Huge Investment
- Legacy Systems
- More IT Staff for management
- Not possible to adopt for all healthcare organizations including rural healthcare centers

PROPOSED SYSTEM

We present a cloud based healthcare information system. In the past, health care providers (such as the family doctor) have stored medical records of their patients on paper locally. This allowed a controlled environment with easy management of data privacy and security: keeping the paper records in a locked cabin at the doctor's practice. Even the increasing use of personal computers and modern information technology in medical institutions allowed for a moderate effort to manage privacy and confidentiality of individual medical records. This was due to the decentralized and locally managed infrastructure of each healthcare organization. But nowadays outsourcing of IT infrastructure (e.g., cloud computing) and other services (e.g., billing processing and accounting for medical practices) leads to a complex system where privacy-sensitive data are stored and processed at many different places. Hence, it becomes attractive to store and process healthcare data "in the cloud" (at outsourced data providers that can be accessed via the Internet). While such information processing systems promise improved service quality, the complexity to manage data security and increases privacy.

PROPOSED SYSTEM DESIGN AND ARCHITECTURE

The requirement of the Cloud based information system is to create secure, state-of-art facility to store the data / information available in different healthcare centers and to provide access to users in a secured manner, as per their roles and privileges.

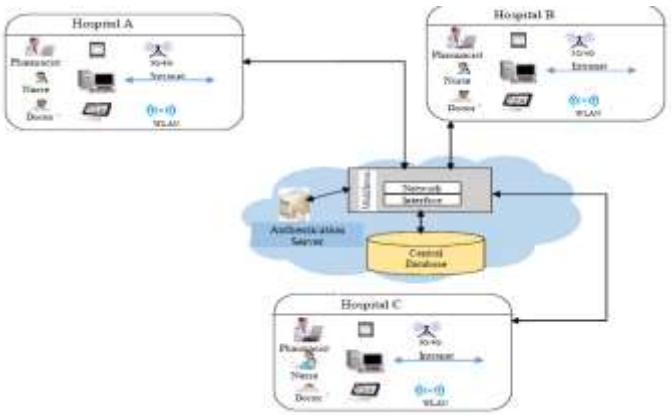


Figure 1: A Cloud-Based Enterprise Electronic Health Records System

Cloud Central Database Server

This acts as the unified data bank for all the collaborating hospitals. TheInfrastructure as a Service (IaaS) cloud datacenter contains the central database serveras the data repository for storing electronic medical records and retrieving patientinformation.

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

Middleware

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

Authentication Server

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

Copyright ©IJICCT-2016.

E-Health Web Portal

This is the front end of the whole cloud system. It is the third part of thecloud (top layer) that provides an application - Software as a service (SaaS) for theEHR system. The proposed health cloud system presents for end users (authorizeddoctors and clinicians) a configurable web portal to navigate through the centraldatabase and the whole EHR system. The web portal can send messages and receiveresponse messages between the middleware and the hospital system. For each sharinghospital in the cloud, the web portal offers the user two tabs, one for accessing thehospital's local EHR system, and another for joining the cloud central database.Through this web page, every authorized user can retrieve, update and receive healthinformation from the cloud's central database with limited access depending on theend user's privileges. The user can also, know from the retrieved informationdisplayed on the web portal, if the requested EHR for a specific patient from aspecific hospital exists inside the cloud or on the target hospital's local system and canchoose to view EHR information about the patient even from locally independenthospitals connected to the cloud.

Suppose D1…Dk are EHR systems of k hospitals all having a central location, C, wherek ≥ 1

Suppose for each EHR system, Dn, there exists, Pi for $1 \leq i \leq m$ for m number ofpatients.

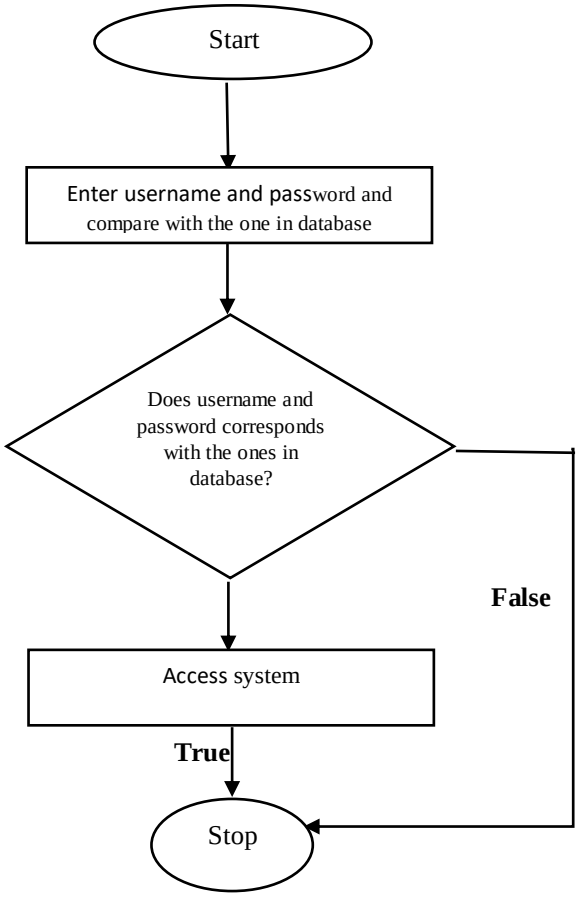


Figure 2: Flow Chart for Authentication

The flowchart above describes the authentication procedure for the doctor's login. Algorithm for retrieving and creating a patient's record is below:

To retrieve the e-health records of any patient Pi;

Step 1: Start

Step2: Input X, which is the identity of the patient Pi

Step 3: Check if X ∈Dn

Step 4: If X ∈Dn, goto 11

ELSE goto 5

Step 5: Join cloud

Step 6: Check if X ∈ Dn+1, where $1 \leq n \leq (k - 1)$

Step 7: if X ∈ Dn+1, goto 11

ELSE display "Patient Pi Record doesn't exist"

Step 9: Create patient's record

Step 10: Add record to the database Dn

Step 11: Display patient's record

Step 12: End

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 (the doctor).

ELSE

Step6: Print "ACCESS DENIED: PLEASE CONTACT ADMINISTRATOR"

Step 7: Stop.

IMPLEMENTATION AND TESTING

Copyright ©IJICCT-2016.

The system was implemented and tested. When the application is launched, the login or authorization interface pops up, where the user selects his/her category from the available categories (i.e. patient, staff, doctor and admin). Each category of user has a username and password required to access the system and work based on his/her privilege. The doctor for example seeking authorization inputs his username and password in order togain access into the system. When an authorized doctor's correct login details areentered in the username and password columns, the system compares the details withthose registered for the doctor in the database and the system grants access to thedoctor as shown below.



Figure 3: User Login

The doctor selects the doctor category and provide valid username and password to access the doctor form to perform certain operations as shown below:



Figure4: Doctor Form

The doctor after successful login can search the local database to find the record of a patient or directly connect to the cloud where all the databases are stored. On click of the search database, a window pops-up which enables the user to search for a patient providing the patient's ID. In case where the patient record is not found, the doctor is giving a chance to connect to the cloud to check the record of the patient in the cloud as shown below:

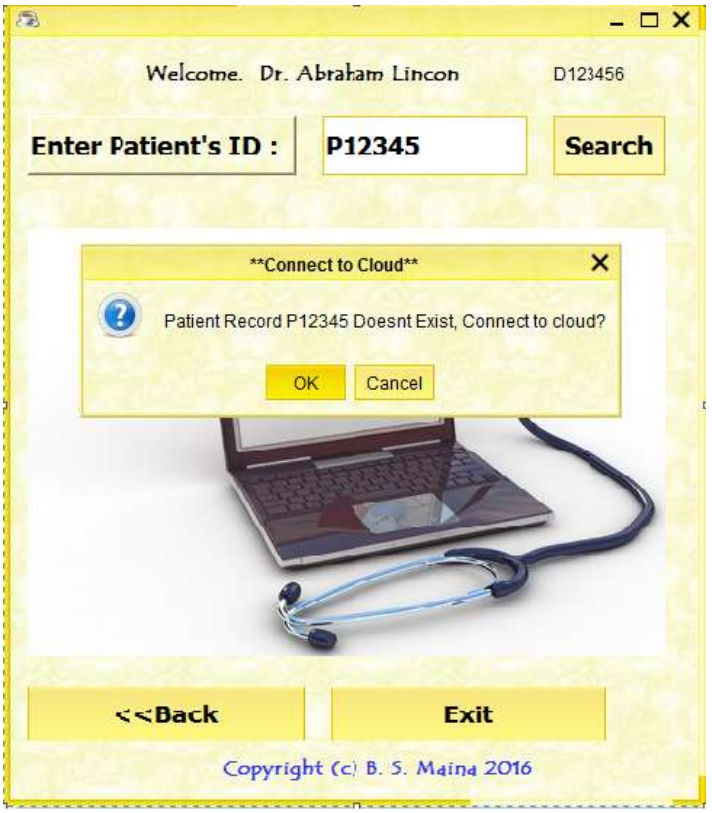


Figure 5: No patient record scenario

The doctor on click of the OK button connects to the cloud server in order to look forthe patient's record in the cloud database. In case where the record exists in the cloud database, the doctors view the record together with previous prescription to enable him know the health status of the patient and make further prescription when required with the help of the information he viewed in the patients record.The system performance was found to be satisfactory when tested.Records of new patientsvisiting the hospital for the first time can be created.For example, the contactinformation of a new patient can be added by the admin as one of the privileges of the admin.

CONCLUSION

In order to realize the sharing of medical information, coordination of medical, as well as the efficient and cost-effective health information system through the construction of a distributed and high-integrated platform, the medical and health information system infrastructure based on the cloud computing

Copyright ©IJICCT-2016.

is proposed and three kinds of application mode, SaaS, PaaS and IaaS, are applied in this architecture.

In this paper, a cloud-based health information system hasbeen designed and implemented. Cloud computing (CC) has been widely recognizedas the next generation's computing infrastructure and it offers some advantages byallowing users to use infrastructures like servers, networks, and storages, platformslike middleware services and operating systems, and software such as applicationprograms. By adapting the cloud technology to medical record management, lowerthe cost of healthcare delivery is achieved through reduce administrative bottlenecks.
High accessibility, availability and reliability make cloud computing a better solution for healthcare interoperability problems.

FUTURE WORK

It is expected that in future,as smartphones are increasingly becoming essential part of human life as the mosteffective and convenient communication tools,cloud-based health information systemwill be incorporated into the mobile devicesin order to enhance the level of access of the service and further reduce maintenance cost.

REFERENCES

[1] A. Qusay, "*Demystifying Cloud Computing"*,The Journal of Defense Software Engineering *(CrossTalk)*, vol. 1, pp. 16–21, 2011.

[2] A. Agfa, "*Moving Digital Imaging into the Clouds"*, Agfa HealthCare, Mortsel-Belgium, 2012.

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

[4] D. Burk, "*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, 2014

[5] C. Cristina,*"Electronic Health Record Adoption: Perceived Barriers and Facilitators"*-A Literature Review, Centre for Military and Veterans' Health, University of Queensland. 1-53, 2010.

[6] M. Deng, N. Nalin, M. Schlehahn, and E. Abbadi,*"Trust Model for Cloud Applications and First Application Architecture"*, Seventh Framework Programme, Technical report D3.1.1/1.0, 1-152, 2010.

[7] H. Dinh, T. Lee, C.Niyato, andP. Wang, *"A survey of mobile cloud computing: architecture, applications, and approaches, Wireless Communications and mobile computing,"* 13(18), 1587-1611, Dec. 2013.

[8] R. Duncan, "*An Overview of Different Authentication Methods and Protocols"*,SANS Institute InfoSec Reading room.Retrieved fromhttp://www.sans.org, 2014.

[9] J. Csiszar,"*Paper-Based Medical Records vs. Electronic Medical Records*," Retrieved fromhttp://www.voices.yahoo.com/paper-based-medical-records-vs-electronic-medical-8591569.html, 2011.

[10] P. McDaniel, *"Authentication, the Internet Encyclopedia*", John Wiley Publishers. 2006.

[11] H. Mirza, andS. El-Masri, "*Cloud Computing System for Integrated Electronic Health Records,"* Department of Information Systems, College of Computer and Information Sciences, King Saud University. 2012.

[12] Oracle, "*Security Overview"*, 10g Release 1 (10.1).Part No. B10777-01, 2003.

[13] R. Padhy, M. Patra, andS. Satapathy, *"Design and Implementation of a Cloud based Rural Healthcare Information System Model"*, UNIASCIT, 2 (1), 149-157, 2012.

[14] S. Saif, S. Wani, andS. Khan, "*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), 2010.

[15] X. Wang, *"Application of Cloud Computing in the Health Information System, Computer Application and System Modeling (ICCASM)"*, 2010.

Copyright ©IJICCT-2016.