International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 15th Nov 2018. Link :http://www.ijiemr.org/downloads.php?vol=Volume-07&issue=ISSUE-12

Title: A MOBILE CLOUD-BASED APPROACH FOR SECURE M-HEALTH PREDICTION APPLICATION

Volume 07, Issue 12, Pages: 236–244.

Paper Authors

[1]S.NAGAMANI, [2]DR.C.NAGARAJU

[1]L.B.R.College of Engineering- Mylavaram
[2]Yogi vemana University

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A MOBILE CLOUD-BASED APPROACH FOR SECURE M-HEALTH PREDICTION APPLICATION

[1]S.NAGAMANI, [2]DR.C.NAGARAJU
[1]Asst. professor L.B.R.College of Engineering- Mylavaram,
[2]Associate Professor, Yogi vemana University
[1]sikhinamnagamani@lbrce.ac.in, [2]nagaraju.c@yogivemanauniversity.ac.in

Abstract
In today's world Mobile cloud computing most essential technology in mobile environment. Mobile cloud computing means it is combined withmobile technology and Cloud technology. However, a direct combination of these two technologies can overawed a several stake races related to the performance, flexibility, security, and dynamic management deliberated in mobile Computing. This paper describes the Healthcare records which are stored in cloud computing is comparatively sensitive related to other information which requires the majority management. Although the data stored in cloud computing can be accessed by various mobile devices, all those transactions goes over the network. So security issues are raised. This paper describes safety and security for the healthcare information is innovating topic to deal with. In this paper, we are implementing the health Prediction presentation, which is a customer support and online talk session. Finally it intend an innovative android application which permits the users to get faster response through the online health care application.

General Terms
Mobile communication, Cloud computing, cryptography, Computer security, pervasive computing, computer architecture, Medical services m-health, mobile cloud computing, information security, distributed systems

Keywords
Mobile Cloud, M-Health, Data Security, Mobile cloud computing

1. Introduction
IT systems are used by clinics and hospitals to store and process patient's information and that can be accessed by professionals like doctors to examine the patient and prescribe the medicine. In some cases, the professionals who offer information to IT systems are not those who view and examine the data. The healthcare professionals are accountable for patients (as well as patients themselves) may not be actually there in the hospital environments where IT systems works and accesses resources for remotely of information are basic for healthcare services to work correctly.In this rationale, distributed computing and versatile registering partake in crucial jobs since they speak to a pattern that has created lately and offers top notch

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

learning to clients who must control remote information. Distributed computing empowers data to be put away and prepared in shared conditions got to from end to end confused correspondences structures(especially the Internet).Mobile figuring gives access to information through versatile gadgets and portable interchanges innovation, which guarantees client mobility[1]. The proposed application is encouraged with different side effects and the sickness/disease related with those frameworks. It enables clients to share their indications and issues and after that procedures client's side effects to check for the wellbeing condition that could be related with it. Here we utilize some keen information mining systems to figure the patient's disease that could be related with patient's manifestations. On the off chance that the proposed application can't give appropriate outcomes, it urges clients to go for blood test, x-beam, CT scan or whichever report it feels client's manifestations are related with, so next time client might have the capacity to sign in and transfer a picture of those reports. The frameworks. It enables clients to share their indications and issues and after that procedures client's side effects to check for the wellbeing condition that could be related with it. Here we utilize some keen information mining systems to figure the patient's disease that could be related with patient's manifestations. application additionally has a specialist sign in;

These scanned images (uploaded images) are now sent to the related specialized doctor along with patient contact details. Now, the doctors may contact the patient for further process [2].

2 MOBILE CLOUD COMPUTING IN HEALTH CARE

2. Mobile Cloud computing in Health Care

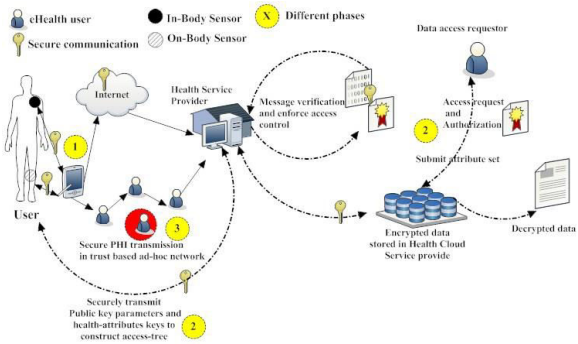


Figure1: Mobile Cloud computing architecture

(Mobile terminals access to cloud infrastructure through network operators.)

This figure shows conservative cloud communications (cloud controllers, and soon) and a characteristic MCC architecture with mobile terminals that uses the structure provided by their network operators (including access points, base transceiver In the healthcare context, MCC is effective for remotely monitors sick persons and combines cloud and mobile equipment capabilities to assistancehealth care professionals observe and evaluate clinical situations during their daily activities (at home, work, and so on).The paper is further organized as follows. In Section III, we present the importance of stations, and mobile network services) to access the Internet. healthcare systems in cloud computing. Next, we describe the system architecture of the proposed a framework. Later we discuss, what are the security problemsrelated to the applications and finding the possible solutions for the

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

application. The conclusion and final remarks present at the end of the paper.

Using the mobile phone within the healthcare field is called m-healthcare. An m-healthcare request can be used by patients and as well as professionals. The purpose is to develop an m-healthcare application that makes our life easier and saves your time. People have a propensity to doubt the protection functionality power of m-healthcare applications and are bothered regarding it. The point of this undertaking is to give a protected and trustful m-social insurance so clients can utilize this application for their delicate information with no uncertainty of security risk. It is additionally an easy to use application, so clients can without much of a stretch utilize the application [3]. There are various advantages of using M-Healthcare. They are:

1) reduced hospitalization rates in hospitals and clinics;

2) Lower costs in general (reduced hospitalization costs);

3) Instant remote assistance (providing the right care at the right time);

4) Increases and improvements in patient monitoring process; and

5) Structured and centralized organization of patient health data

3. M-HealthCare

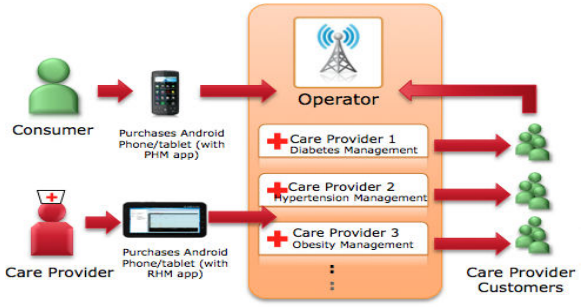


Figure2. Typical mobile health architecture.

Communications occur among sensors, the mobile environment, the cloud, healthcare professionals, and patient's family members [4]. Sensor systems are utilized to catch biometric quiet information through remote body territory sensor systems (WBASNs) remotely, and it permits early recognition of constant maladies for viable treatment, close monitoring of patients already diagnosed with chronic diseases, and prevention of chronic diseases.

4. System Architecture

The architecture of the proposed model of a cloud computing based Secure M-Health Prediction application is presented in Figure 3. The architecture consists of a Cloud Service Provider, User Application, User authentication components and Data security. The Patient Records are encrypted by data security and user authentication. These encrypted records are retained and achieved in the Cloud Service Provider which is the server end. These records are retrieved from cloud storage when requested by a user and exposed on the mobile device after decryption.The User Application is designed in such a way that the health records and prescriptions of patients are

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

made available to them on their mobile devices. The application is designed to provide different access to the users based on their roles:

(1) Doctors can edit update and view the medical record

(2) Patient can only View the record,

(3) Medical Data Management Administrator can create, delete, and update record

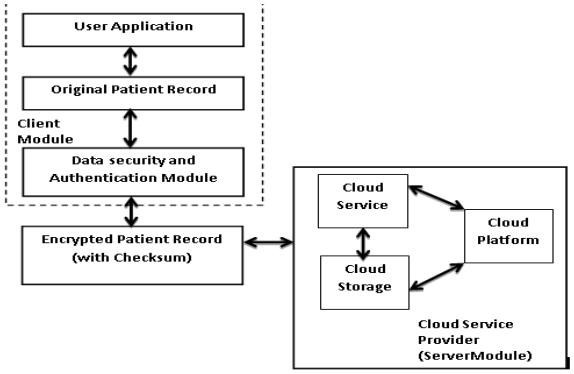


Figure 3.System architecture for secure mobile health application.

In the proposed model, the components of Data security, User authentication protects the medical records and prevents unauthorized access which is powered by the MD5 Hash Algorithm. This algorithm can be used for storing the passwords of each user which is used for user authentication. The Original Patient Record file can be appended with a checksum generated by MD5 which helps in confidentiality along with authentication. A Password-Based Encryption (PBE) is used to encrypt patient record which derives an encryption key from a password for each user. So as to make the assignment of getting from secret phrase to key extremely tedious for an assailant, execution can blend in an irregular number, known as a salt, to make the key.

5. Security Problems

There are several security concerns in the field of m-healthcare. In this system, every data is very private and sensitive. So trust should be set up in every step between each participant. The assurance of information security (availability, integrity, confidentiality, and authenticity).Security can be provided by using general cryptography ideas. Below the cryptographic concepts are described.

Availability:

Availability is a system that refers to use of resources or information by intended users. The unavailable system is as no system type. So availability is the very important side of reliability and also for system design

Integrity:

Integrity is another important mechanism of data security. It ensures preventing data from modification or unauthorized change when data/ messages transferred between sender and receivers. The recipient can verify integrity by the attached hash value of the original message. Prevention and detection mechanism are two classes of integrity. In the event that any trustworthiness of information is changed/altered by the unapproved individual in an illicit way, the anticipation instrument hinders the unlawful endeavor of adjusting information. Location systems don't anticipate unapproved change of information, yet it just reports that the information uprightness is never again dependable [5].

Confidentiality:

During communication process, data can be eavesdrops by the third party. The eavesdropper can do any illegal action against the data. Confidentiality makes sure that only intended receiver reads data without attacking the third party. It gives secure communication between sender and receivers. Encryption and decryption protect data against reading by the third party.

Decryption and Encryption are performed by a key. Based on keys there are two types of cryptographic systems based on keys: Symmetric key and Asymmetric Key. In Symmetric key cryptography encryption and decryption share the same key, but in Asymmetric key crypto, they use dissimilar keys fordecryption and Encryption. [5].

Authentication:

Authentication is a process that performs identity verification [6]. There are three categories of authentication protocols: client authentication (here server confirms client credentials), server authentication (here client verifies server identification), and mutual authentication (here client and server togetherverify each other identity).

The three general ways for authentication factors is described below [5]:

a. Something the participant has, example tokens, ID card

b. Something the participant knows, example password, PIN

c. Something the participant is, example voice, Bio-metric

6 Challenges in the Mobile Environment

There are three main challenges in the mobile environment. The first aspect to be considered concerns the use of mobile devices, which are subject to the same security issues as conventional computers (infection by malware, application bugs, operating system vulnerabilities, and so on). However such devices' portability characteristics and wireless networks can cause new threats.The second interesting aspect is namely, bring your own device (BYOD) [6], which suggest using employees' private mobile equipment for professional purposes. This practice brings more convenience to users because it unifies professional and personal data and applications on the same equipment; however, numerous security problems arise. Such equipment has been the target of many attacks because private-use devices do not receive the same treatment and care regarding security as business equipment that is used strictly for professional activities and whose reliability is almost always the responsibility of IT teams.Another problem related to the mobile environment is the uncontrolled proliferation of m-health applications of diverse origins and purposes. Several such applications do not follow any formal software development methodology (even because no methodology is targeted specifically to m-health segment)and prioritize functionality over information security. Although some strategy contains privacy and safety measures policies (such as the US National Institute of Values and Technology's Strategies for Managing the retreat of mobile devices in the Enterprise[7]), no prescriptive or legal obligation has been established in most cases.

7. MCC Application Security Issues

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Guaranteeing data classification and protection in a dispersed registering engineering, for example, a cloud is an extraordinary challenge[8], and it is vital to establish and maintain the trust of mobile users in relation to the processing of processing of applications based on cloud computing.

There are three aspects related to the security of the information used in various applications stand out:

1) The Security of the mobile equipment: This aspect concerns the prevention of attack through malware happening or the misuse of application or operating system vulnerabilities [9].

2) The security of information transmission from a mobile device to the cloud (and vice versa):

This aspect should consider the various entities (including unreliable, such as cyber cafes or generic public networks) and technologies (Wi-Fi, 3G, 4G, and so on) that stand between the mobile device and the cloud and could present threats that affect information security.

3) The security of processing and storage in the cloud:

This environment is a great target for attackers because it concentrates several types of information from multiple users in a single infrastructure. It is essentialto consider resource sharing in the cloud- as is used during information processing- to ensure that a given user's information is protected in relation to other users and to cloud infrastructure administrators. This presents a significant challenge.

Table 1: Problems and solutions for cloud-computing-based mobile health systems.

Security problem	Possible solution
Vulnerabilities of User's Personal Equipment	Use of Antimalware software can reduce the security issues of local and cloud-based environments. Making the users aware of the secure use of mobile devices Imposition of policies that restrict the use of personal equipment for private content Supply of specific equipment by the organization (under the control of the organization's IT) for professional use
Confidentiality and integrity related issues in cloud environment	Encryption of the data sent to the cloud Security as a service
Providing System User's guarantee for access control and authenticity	Security credentials and bio-metric-based authentication Authentication, authorization, and accounting processes
Giving assurance of cloud computing service Availability	Providing Secure Network connection assurance Server redundancy Prevention of storage failures Adopting a new private cloud

Security problem possible solution Vulnerabilities of User's Personal Equipment use of Antimalware software can reduce the security issues of local and cloud-based environments. Making the users aware of the secure use of mobile devices Imposition of policies that restrict the use of personal equipment for private content Supply of specific equipment by the organization (under the control of the organization's IT) for professional useConfidentiality and integrity related issues in cloud environment Encryption of the data sent to the cloud Security as a serviceProviding System User's guarantee for access control and authenticitySecurity credentials and bio-metric-based authorization, authentication, and accounting processesGiving assurance of cloud computing service Availability Providing Secure Network connection assurance Serverredundancy Prevention of storage failures Adopting a new private

cloud Here is the list of the possible solutions to the security related problems.

8. m-healthcare Threats and Attacks

There are several threats and attacks involved with m-healthcare systems, like electronic data transactions security, mobile user authentication, and the security and privacy of data stored on mobile devices [10].Let us discuss a bit details about electronic data transactions security. Nowadays, almost every mobile device connects to the Internet through Wireless Access Point. It makes patient's data vulnerable to the attacker. The possible risk can be man-in-middle, spoofing, sniffing, or session hijacking[10].When a third person sits with a mobile device, connects to your wireless access point and listens to your network data and in the worst case captures your data, then modifies it and sends to the destination. If a patient data is modified before the diagnosis process, it will result in the improper diagnosis, which will lead to a wrong prescription that can be very harmful to the patient.Authentication of the mobile user is very important while accessing sensitive patient data. Patient's private data must not be accessible to the third person other than the patient itself or the authorized physicians. After the authentication, the user will get access to the data depending on his/her access limit. It means that after the authentication the user will be authorized to access data. And also the security of the authentication data during transmission is vital. Because if the user information is viewed by the third party, they may use it next time to access data [11].In some cases, the sensitive patient data are downloaded to the mobile device and if the device is lost then it may happen that the patient's data will be viewed by the third person. The authentication process can secure the mobile data in some sense, but if we store the data in the mobile device as a plain text format, it can be retrieved by other applications or specialized tools that can read or modify the data. So, it is also very important to secure data stored on a mobile device.

9. Encryption Options:

Cryptography is a mechanism that is used to prevent the messages from being read by the others when the message transfers from a sender to a receiver. Cryptography uses the mechanism to encryption and decrypts data. Authenticity, Confidentiality,integrity techniques are used to provide security to the end user's data. Encryption, its various types, and applications used as a framework to MCC and is one of the most effective methods for providing the guarantee to information security which is the requirement of mobile health. Several possibilities of encryptions exist for mobile cloud- based m-health.

A) **Symmetric cryptography:** In symmetric cryptography sender and receiver both uses the same key for the process of encryption and decryption. This key is identifiedas the secret key. This secret key is shared between sender and receiver. It can be used to guarantee the confidentiality of health data stored in public cloud environments.

B) **Asymmetric cryptography**: Message sender and receiver use different keys for message encryption and decryption process in an asymmetric key cryptography system. Here one key is used as private key and it is

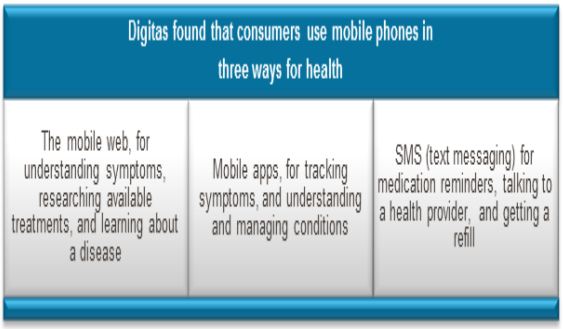
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

kept private which is only known to the owner of the key. Another key is used as public key and it is stored in a register or other accessible file. Public key cryptography is also applied for key management and signature applications: keys exchange for symmetric cryptography and digital signature

C) **Identity-based encryption (IBE):** It generates public keys for the use (with the asymmetric cryptography) from identity values, such as an email address and Social Security number.This asymmetric encryption scheme ensures that parties that must store data about a patient do not use the digital patient's certificate directly (it might not be available), but use only data based on the patient's identity to generate the encryption key (public key) to be used and that will ensure access control to data stored in shared environments (typically in the cloud).

10. Access Control

Access control is another problem of the m-health system. Here the difficulty is users like patients, family members, doctors, nurses, IT support staff, and so on) have a precise outline and they must have some appropriate privileges relative to their needs and as well as access registered for the purposes of subsequent accounting and for auditing. Therefore, the solution is implementing the reliable processes of, authentication, authorization and accounting for the users.In the specific context of authentication, biometrics is an option especially suitable in favor of m-health systems. It not only provides, in certain contexts, parameters measured from biological functions that can be used to create cryptographic keys, but such parameters can also be used to authenticate users' identity, particularly for patients being monitored.



11 EXPERIMENTAL RESULTS

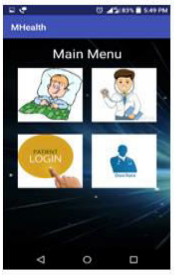


FIGURE 4: HOME PAGE

FIGURE 5:PATIENT'S HOME PAGE

11. Conclusion

An m-healthcare application has a set of services. Users of smart mobile devices can use those services by installing the application on their devices. In past m-healthcare didn't exist and the people need to go physically to the medical service center for getting each service and physician also provided paper base service. After introducing m-healthcare application, it makes people life easier and comfortable. The Patient can retrieve his/her medical information atanytime and anywhere by using his/her mobile phone. The mobile healthcare communication between patient and healthcare professionals will increase efficiency and reliability significantly.

12. References

1. Silas L.Albuquerque and Paulo R.L.Gondi,"Security in cloud computing based m-health".

2.www.nevonprojects.com/android-based – smart-health-prediction-application.html

3.Sabin a yesmin "Mobile Application for Secure healthcare System" www.divaporatl.se/smash/get/diva2:644378/FULLTEXT01.pdf

4. A.benharref and M.A.Serhani "Novel cloud and SOA Based Framework fro E-Health Monitoring using Wireless Biosensors",IEEE J.Biomedical and health Informatics,vol.18,pp.46-55

5.S.Muftic "lecture Note of Network Security course",royal Institute of Technology(KTH),2012

6.J.Burns and M.E.Johnson,"Seccuring Health Information",IT professional,vol.17,no.1,2015,pp.23-29.

7.M.Souppaya and K.Scarfone ,NIST Special publication 800-124 Revisipn1:Guidelines for Managing the security of Mobile devices in the enterprise,une 2013;hhtp://nvlpubs.nist.gov/SpecialPublications/NIST.SP.800-124rl.pdf.

8.M.Shiraz et al .,"A review on distributed application Processing Frameworks in Smart Mobile Devices For Mobile Cloud computing ",IEEE comm.surveys& tutorials, vol 15,no.3,2013,pp.1294-1313.