iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IV **Month of publication:** April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4212

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Mobile Cloud Based Approach for Secure M-Health Application

Alekhya. J[1], P. Sowjanya[2], P. Abhi Tarun[3]
[1,2,3] *Department of IT, L.B.R.C.E., Krishna, A.P*

Abstract: ***Mobile cloud Computing is one of the major components of cloud computing that also deals with various issues of cloud services when is accessed by portable devices in the wireless environment. The Healthcare data which is stored in cloud computing is relatively sensitive compared to additional information which requires the majority management. While Cloud services are accessed by the mobile devices the extra confront like security arises. Providing the safety (security) and privacy for the healthcare information is a motivating topic to deal with. In this paper, we are implementing the health Prediction application, which is an end user support and online consultation project. Here we propose an android application that allows users to get immediate response on their health issues through an intelligent health care application online.***
Keywords: Mobile Cloud, M-Health, Data Security

I. INTRODUCTION

Usually, Hospitals and Clinics often use IT systems to store and process patient information, which is accessed by health professionals like the doctors and nurses to assist them to examine the physical condition and prescribe treatment. In a few 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 logic, cloud computing and mobile computing take part in vital roles since they represent a trend that has developed in recent years and offers high-quality knowledge to users who must control remote data. Cloud computing enables information to be stored and processed in shared environments accessed from end to end complicated communications structures(especially the Internet).Mobile computing provides access to data through portable devices and mobile communications technology, which assures user mobility[1].

The proposed application is fed with various symptoms and the disease/illness associated with those systems. It allows users to share their symptoms and issues and then processes user's symptoms to check for the health condition that could be associated with it. Here we use some intelligent data mining techniques to guess the patient's illness that could be associated with patient's symptoms. If the proposed application is not able to provide suitable results, it urges users to go for blood test, x-ray, CT scan or whichever report it feels user's symptoms are associated with, so next time user may be able to log in and upload an image of those reports. The application also has a doctor log 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].

II. MOBILE CLOUD COMPUTING IN HEALTH CARE

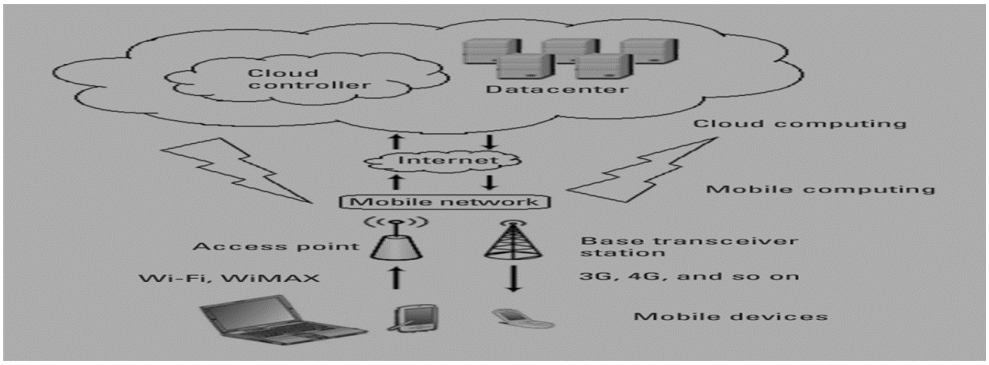


Figure 1.Mobile Cloud computing architecture. Mobile terminals access to cloud infrastructure through network operators.

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

This figure shows conservative cloud communications (cloud controllers, and so on) and a characteristic MCC architecture with mobile terminals that uses the structure provided by their network operators (including access points, base transceiver stations, and mobile network services) to access the Internet.

In the healthcare context, MCC is effective for remotely monitors sick persons and combines cloud and mobile equipment capabilities to help healthcare 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 healthcare systems in cloud computing. Next, we describe the system architecture of the proposed a framework. Later we discuss, what are the security issues related to the applications and finding the possible solutions for the application. The conclusion and final remarks present at the end of the paper.

III. M-HEALTH-CARE

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 aim of this project is to provide a secure and trustful m-healthcare so that users can use this application for their sensitive data without any doubt of security threat. It is also a user-friendly application, so users can easily use the application [3].

There are various advantages of using M-Healthcare.

They are:

A. Reduced hospitalization rates in hospitals and clinics;
B. Lower costs in general (reduced hospitalization costs);
C. Instant remote assistance (providing the right care at the right time);
D. Increases and improvements in patient monitoring process; and
E. Structured and centralized organization of patient health data.

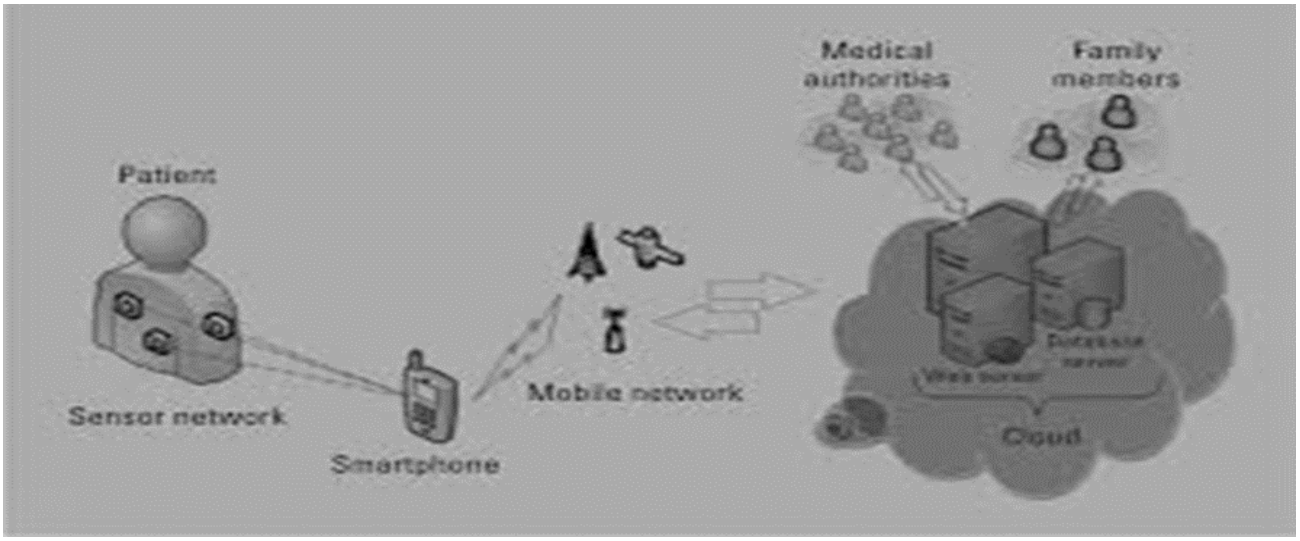


Figure 2. Typical Mobile Health Architecture.

Communications occur among sensors, the mobile environment, the cloud, healthcare professionals, and patient's family members [4].Sensor networks are used to capture biometric patient data through wireless body area sensor networks (WBASNs) remotely, and it allows early detection of chronic diseases for effective treatment, close monitoring of patients already diagnosed with chronic diseases, and prevention of chronic diseases.

IV. 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, Data security and User Authentication components. The Patient Records are encrypted by Data security and User Authentication. These encrypted records are stored and managed in the

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Cloud Service Provider which is the server end. These records are retrieved from cloud storage when requested by a user and displayed on the mobile device after decryption.

The User Application is designed in such a way that the health records and prescriptions of patients are made available to them on their mobile devices. The application is designed to provide different access to the users based on their roles:

Doctors can edit update and view the medical record

Patient can only View the record,

Medical Data Management Administrator can create, delete, and update record

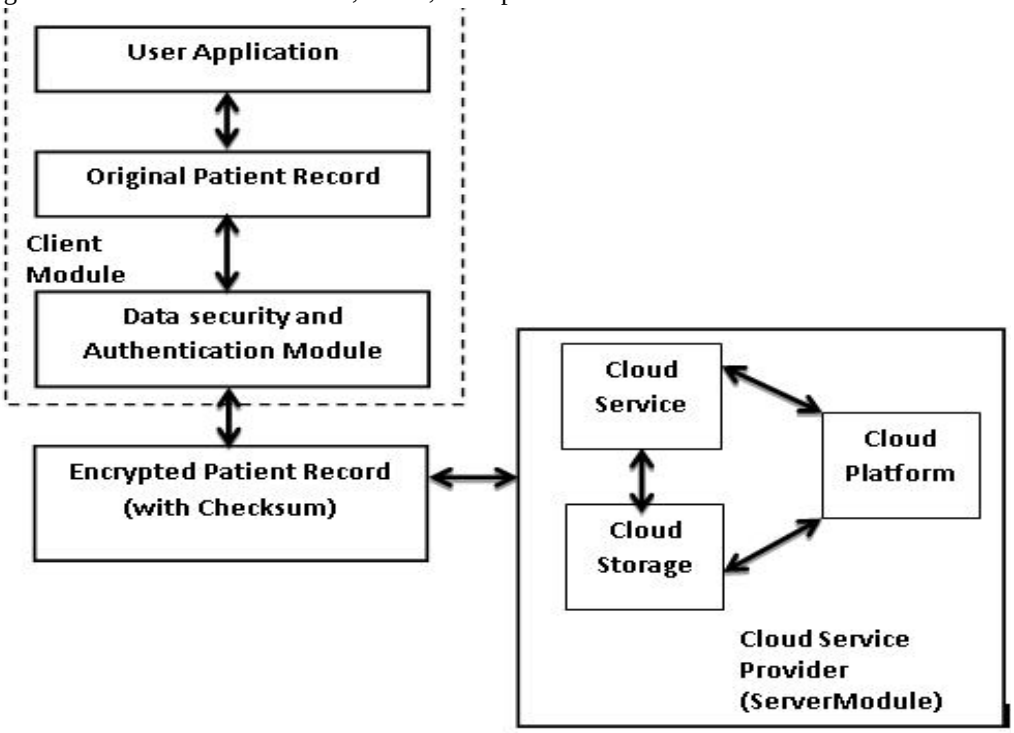


Figure 3. System Architecture for Secure Mobile Health Application.

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. In order to make the task of getting from password to key very time-consuming for an attacker, implementation can mix in a random number, known as a salt, to create the key.

V. 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.

A. 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 [5].

B. 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. If any integrity of data is changed/ modified by the unauthorized person in an illegal way, the prevention mechanism blocks the illegal attempt of modifying data. Detection mechanisms do not prevent unauthorized modification of data, but it only reports that the data integrity is no longer reliable [5].

C. 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.

Encryption and decryption are performed by a key. 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 different keys for encryption and decryption [5].

D. Authentication

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

The three general ways for authentication factors is described below:

1) Something the participant has, example tokens, ID card
2) Something the participant knows, example password, PIN
3) Something the participant is, example voice, Bio-metric

VI. 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.

VII. MCC APPLICATION SECURITY ISSUES

Ensuring information confidentiality and privacy in a distributed computing architecture such as a cloud is a great challenge[8], and it is important 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:

A. 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].

B. 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.

C. 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 necessary to 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

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

VIII. M-HEALTH CARE 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.

IX. 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

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

sender to a receiver. Cryptography uses the mechanism to encryption and decrypts data. Confidentiality, integrity, and authenticity 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.

Symmetric cryptography: In symmetric cryptography sender and receiver both uses the same key for the process of encryption and decryption. This key is known as 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.

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 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

X. 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 favour 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 verify users' identity, particularly for patients being monitored.

XI. EXPERIMENTAL RESULTS

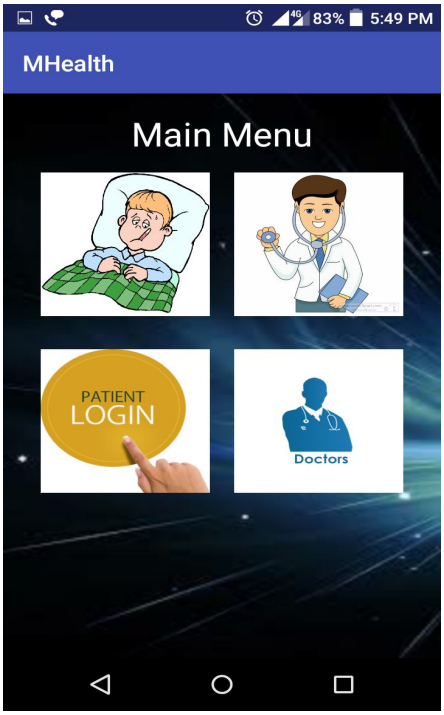


FIGURE 4*:* HOME PAGE

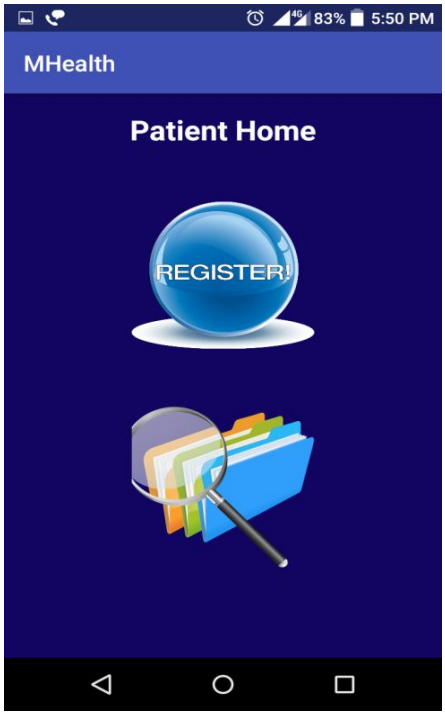


FIGURE 5: PATIENT'S HOME PAGE

Figure 4 shows the home page of the MHealth app. It shows four icons. First icon is used for patient registration. Second icon is used for patient's login. Third icon is used for doctor registration. Fourth registration is used for doctor login. During the registration phase of the patient, the details of the patient is taken like name, id, password, mail id, etc., During the login phase of the patient, his user id and password is taken. If he gives correct user id and password he gets logged in and is shown in figure 5.

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

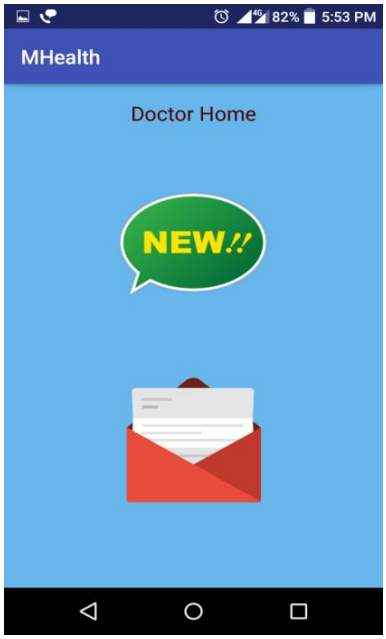


FIGURE 6: DOCTOR'S HOME PAGE

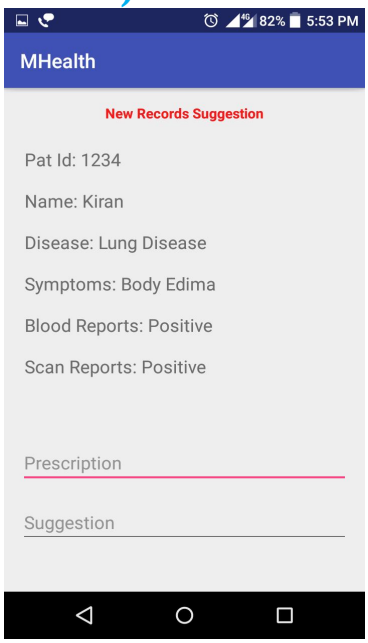


FIGURE 7:DOCTOR'S TREATMENT

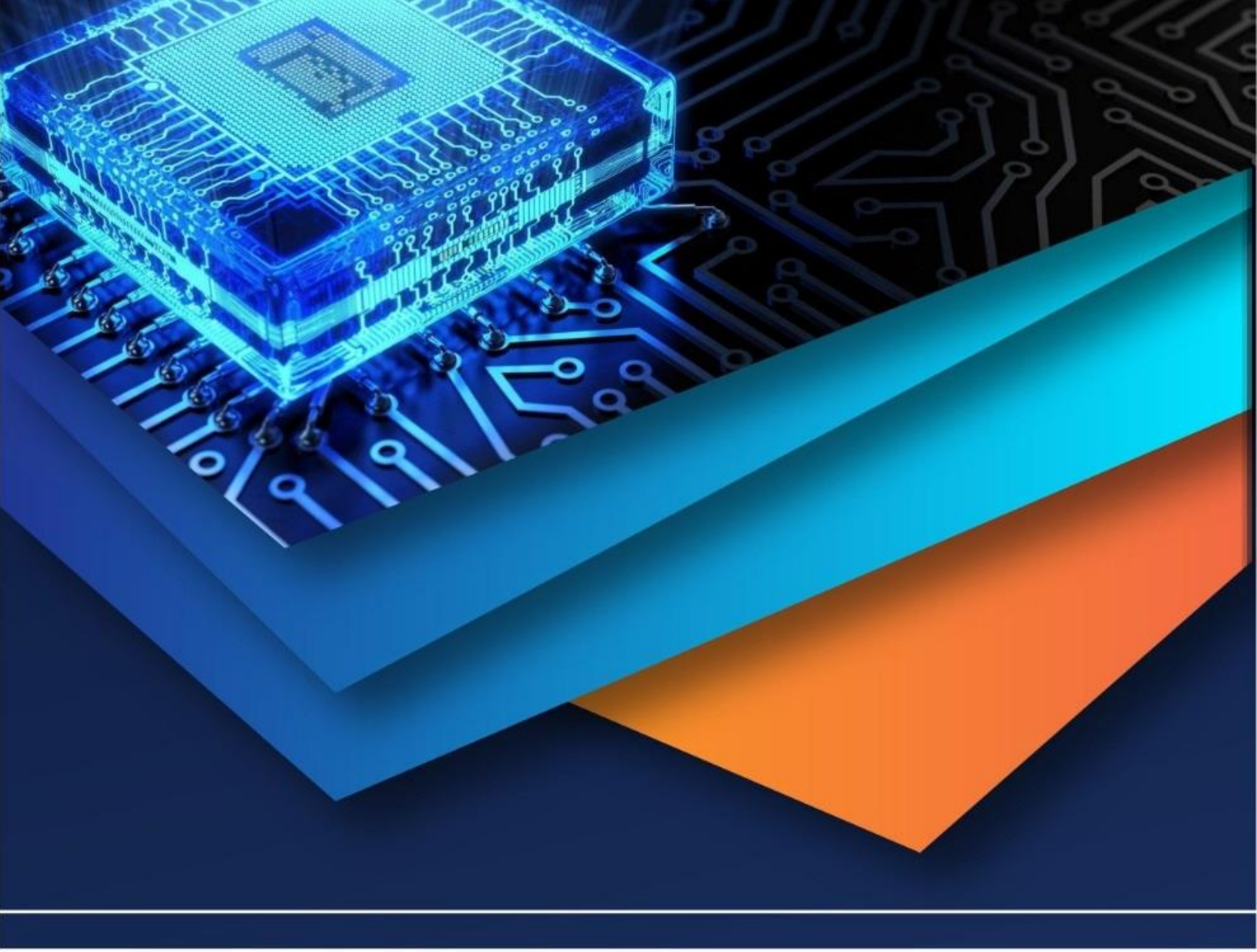
The patient tells about his disease after he logs in and that data is stored in the cloud. The doctor logs in by using his user id and password. He checks the patient records and prescribes the medicine to the patient. After that the total record is stored in the cloud.

XII. 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. A few years ago 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 at anytime and anywhere by using his/her mobile phone. The mobile healthcare communication between patient and healthcare professionals will increase efficiency and reliability significantly.

REFERENCES

[1] Silas L. Albuquerque and Paulo R.L. Gondim, "Security in cloud computing based m-health".
[2] www.nevonprojects.com/android-based-smart-health-prediction-application.html
[3] A. Benharref and M.A. Serhani, "Novel Cloud and SOA-Based Framework for E-Health Monitoring Using Wireless Biosensors", IEEE J. Biomedical and health Informatics, vol. 18, pp. 46-55
[4] S. Muftic, "Lecture Note of Network Security Course", Royal Institute of Technology (KTH), 201
[5] J. Burns and M.E. Johnson, "Securing Health Information", IT Professional, vol. 17, no. 1, 2015, pp. 23–29.
[6] M. Souppaya and K. Scarfone, NIST Special Publication 800-124 Revision 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise, June 2013; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP. 800-124r1.pd
[7] 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
[8] H. Suo et al., "Security and Privacy in Mobile Cloud Computing", Proc. 9th Int'l Wireless Comm. and Mobile Computing Conf. (IWCMC), 2013, pp. 655–65
[9] J. Meyer, "Potential Security Vulnerabilities of a Wireless Network Implementation in a Military Healthcare Environment", East Carolina University.http://www.infosecwriters.com/text_resources/pdf/Wireless_JMeyer.pd
[10] D. Weerasinghe, M. Rajarajan, V. Rakocevic and P. Kostkova, Security, "Protection on Trust Delegated Data in Public Mobile Networks", (Ed.): eHealth 2009.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY