Centralized Healthcare Management using RFID and One Time Password

[1]Kushagra Saxena, [2]Hitiksha Moily, [3]Sreyas Pillai, [4]Vedashree Mule, [5]Karan Rai

[1]Student, [2]Student, [3]Student, [4]Student, [5]Student
BE (Computer Engineering)
Department Of Computer Engineering,
Sandip Institute of Technology and Research Center, Nashik, India

Abstract: **In this research paper, we are proposing a Radio-frequency identification (RFID) based E-health card system where healthcare services can be delivered effectively to patients anytime and anywhere using it. We are developing an E-health card system through Information and Communication Technologies (ICT) that will involve RFID cards, mobiles, and web-based applications for the delivery of healthcare services and information. Reliable healthcare is a vital motive of the e-Health system. In the proposed model, the E-health system will include RFID card for easy access of information which will be secured by Secure Hash Algorithms and 2 Factor Authentication/OTP based system. Device interoperability along with its security is a challenging and important task in the healthcare sector that needs research attention which is covered in this paper.**

Keywords: **RFID, OTP, Secure Hash Algorithm-256, Healthcare management.**

I. INTRODUCTION

The Health care sector is one of the fastest-growing sectors in the world and the Health Care System is the backbone of this sector. The growth and development of the health care system are of utmost importance and influence the economic growth of a country. The advent of Information and Communication Technologies (ICT) have contributed to this development and is the need of Medical Information Management.

Communication errors between the patient and the various departments of the healthcare is the root cause of the various mistakes in healthcare and proper treatment of the patient.
[9] A research shows that 2/3rd of the major problems and 4 of the 7 solutions are communication-related which has led to a major portion of the diagnostic errors. So the major question which arises here is: 'How can we support the Patients and the Health care management to reduce this humongous amount of errors in the treatment of a patient?'

A patient in his life-line goes through a various amount of treatments at different places from different doctors and thus collecting a huge amount of medical data. The patient needs to give his personal information every time he visits and a new doctor or a troublesome hospital. In this phase the patient becomes unable to convey all his medical history to the doctor for better understanding and treatment. Various reports, medical prescriptions, lab results are generated during a patient medical history which he/she is unable to secure and most of them are hardcopy which is easy to be stolen or get into the wrong hands. The security and privacy of the medical data of a person is also a vital part that draws attention. [8]Confidentiality and security of protected health information (PHI), which is included in a patient's electronic health record, is addressed in the Health Insurance Portability and Accountability Act (HIPAA).
Hence, we propose to use RFID based E-health card which will be a one-time solution to all the above-discussed issues. All the various health information and the patient history such as reports, medical prescriptions, laboratory results will be stored under this health card with proper authentication and privacy maintained. The encryption methodology is used for keeping the data secured and the access is only given by One Time Password (OTP). The emergency situation is also provided under it. All these things are covered under a common framework in a secured manner which is technically briefed in the below sections.

II. RELATED WORK

In order to allow the healthcare system to be more reliable, more effective in promoting medical science we have prepared a survey on the most probable security as well as healthcare-related privacy problems that need to be taken into account. We face a lot of privacy issue in the health care system example Patient does not carry their medical document every time along with them; patient confidential data is not secure. To solve this privacy issue we proposed a new system, for that we study multiple papers, the literature study of this paper is as follows.
O. Par proposed security standards for taking actions against the unauthorized users. The approach used for the security concerns is the HIPAA Act, ISO 20000, ISO 27000, and laws. The security issues in the modern E-health system as these standards are less technical and more risk-focused for organizations of all shapes and sizes [1]. N. M. Shrestha, the author proposed Multi Authority Attribute-Based Encryption (MA-ABE) technique for securing the Patient Health Record (PHR). The technique has been made for access control of user's data in cloud computing. Though cloud computing is distributed computing some major security issues still exist [2].

Another study proposed by V. Krishna, an international health card that is USB based and with data encryption technique. SQLite database is used for the security of the data. The SQLite database faces a problem when the memory requirements get larger and the performance optimization is harder when using SQLite [3].M. T. Alam, proposed a model of a secured smart E-Health System which uses Near Field Communication (NFC) based smart card and used role-based access control for security concerns and while exchanging information encryption techniques have been considered [5].

III. PROPOSED METHODOLOGY

A. SYSTEM ARCHITECTURE:

The proposed system consists of hardware and software which will be OTP based on authentication and security. The hardware consists of an RFID card and RFID reader.
The software part consists of five modules:

1. Patient module: In this module patient will register himself by adding mandatory details, can schedule appointments, and view his test reports, history. Patient will also receive notifications regarding further appointments and when the medicines will be getting over. The Patient's Information/Medical History can be accessed without harming its privacy.

2. Doctor module: In this module doctors will register themselves, they will be able to accept and reject appointments, upload prescriptions, and inform if any tests need to be done.

3. Pharmacy module: In this module pharmacist will register himself and will be able to see only the prescription of the patient. And will give medicines as per the prescription.

4. Laboratory Module: In this module the lab person will register himself and will perform the tests mentioned by the doctors. He can also upload the results of the tests of the patient.

5. Insurance: This will include basic information regarding the insurance policy of the patient. Like the policy number, Policy name, Duration of the policy.

Emergency Login: This module is provided in case of any emergencies.

The data is made secure with Encryption using the SHA algorithm.

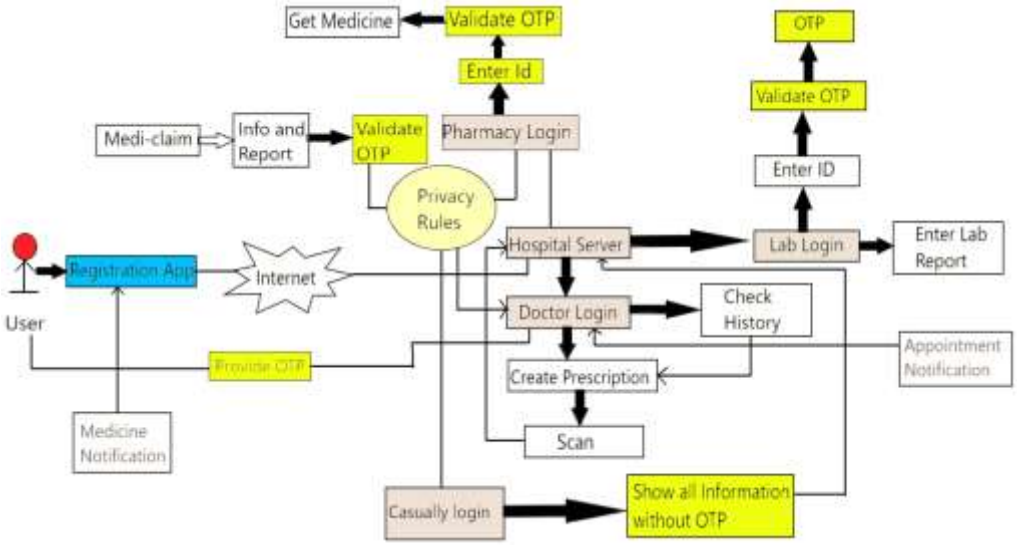

Figure 1. System Architecture

B. HARDWARE ARCHITECTURE:

Each patient will be having an RFID card which will be given by the central authority. It is troublesome for patients to carry medical reports wherever they go. So to solve this problem we proposed a new system that includes cloud-based health monitoring privacy preservation to protect the patient's confidential data. Also, the medical reports and all medical-related data are stored on the cloud which is accessible everywhere in the world using an RFID card.
To authenticate the RFID card the RFID reader will be installed in the Hospitals, Pharmacy, and Laboratories.
The RFID RC522 is a low-cost RFID reader and writer which is based on the MFRC522 microcontroller. They work on 13.56MHz frequency.

For Hardware we need the following components:

1. Raspberry Pi
2. Micro SD Card
3. Power Supply
4. RC522 RFID Reader
5. Breadboard
6. Breadboard Wire

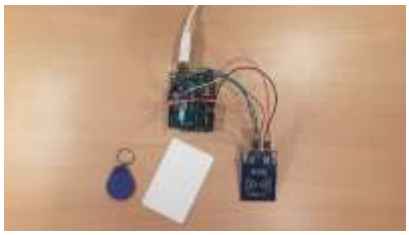

Figure 2. RFID Module

The authentication will be OTP based. The patient will simply scan the RFID card and will receive the OTP. If the OTP is correct he will be able to enter into the system otherwise, access to the system will be denied.

C. SOFTWARE ARCHITECTURE:

The software consists of five modules through which the Patients, Doctors, Pharmacists, Lab person will be able to communicate with the system. We will also be providing an android application for the same.

The patient will have an RFID card. He will scan the card at the places where the reader will be installed. After scanning the card he will receive an OTP. If the OTP is correct the authorities will be able to see the data.

The proposed system is designed in such a way that patient's privacy will be maintained.

Doctors will be able to see only the data they are supposed to see.

Pharmacists can only see the prescription and medicine related data.

Laboratory person can view only the patient's reports and upload newly generated reports.

MySQL is used for storing the information of the patient. For core web development Java and android are used.

D. SECURITY METHODOLOGY:

Our E-Health Card stores the cluster of data about patients. As the whole data or information is stored in the E-Health Card which is a portable like an ATM Card. Because of which it creates a chance of threat of mishappening to the privacy of any patient. Keeping this in focus we have used the two-way authentication system to protect the data from an unknown person. This is a very efficacious approach commonly known as OTP (One Time Password) system. In this approach when the patient will swipe his/her card at respective place, firstly he will get an OTP on his registered mobile number. After the confirmation of OTP only, the respective sever (doctor, pharmacist, laboratory, etc.) will have access to the patient's details. So, at every place there is a requirement of the patient to give access to its data through OTP.

OTP generation algorithm typically makes use of Cryptographic hash function i.e. SHA-1, which can be used to acquire a value but are difficult to reverse, and therefore it is complicated for the attacker to gain the data that was used for the hash.

Also, the data of the patient is being stored on the cloud which should be safe there because the cloud is a large cluster of different kinds of data. So for the privacy of data or information, we have used the SHA-256 algorithm. SHA stands for Secure Hash Algorithm, which is a cryptographic hash function with a digest length of 256-bits. It was first proposed by the United States National Security Agency (NSA).

The SHA-256 algorithm is predicated on the Merkle-Damgard construction method consistent with which the initial index is split into blocks immediately after the change is formed, and people successively into 16 words.

It is a one-way function that converts a text of any length into a string of 256 bits. This is known as a hashing function. In this case, it is a cryptographically secure hashing function, in that knowing the output tells you very little about the output.

The SHA-256 contains the following parameters-

Block size indicator (byte): 64

Maximum allowed message length (bytes):33

Characteristics of the message digest size (bytes): 32

The standard word size (bytes): 4

Internal position length parameter (bytes):32

The number of iterations in one cycle:64

The speed attained by the protocol (MiB/s): approx. 140

We can understand by taking a simple example of hashing,

Suppose we write a word and after hashing it will provide a coded cluster of word,

Normal: abc

Hash : ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad

Here hash doesn't mean 'encryption' of the words, it cannot be decrypted back to the original text because it is a 'one-way' cryptographic function, and is a fixed size for any size of the source text. This makes it suitable when it's appropriate to match 'hashed' versions of texts, as against decrypting the text to get the first version.

IV. RESULT AND DEVELOPMENT

E-health card system is developed in a very user-friendly manner. The usability of the health card system is been examined and make sure that it meets the requirement of the patient. Its actions are just like a banking card which can be made handy in any means of travel. The working and presentation of the E-health card is proposed in the following paragraphs.

The medical record of a patient contains a whole different type of report format. To store all this kind of information in a secured database and as well as to show the different reports in a well-structured manner involves adequate data conversion algorithms. To reduce the inconvenience between doctor and patient, we have introduced different functionalities in our smart E-health card, certain privacy algorithms, security measures, and a friendly user interface for our smart E-health card. We have used MySQL to store the patient data due to its high performance and data security. We have introduced an OTP verification system at the transaction of an RFID card Doctors of high positions or the priority given by the patient to a specific person can have access at the time of emergency due to the unconsciousness of the patient. Access of health card is strictly based on login authorization by the user. The security authorization on the smart E-health card is based on the Shah 256 algorithm which benefits the encryption credentials of the user. Plus also, the decryption is done by the same algorithm for validating the accessibility of the user. Smart view of the reports is shown in the medical history with the particular attachments of scanned images and documents.
At the time when the doctor tries to access the patient card by an RFID reader, an OTP is received on patient's mobile and then only a doctor can access patient credentials.
For laboratory, an adequate amount of information is displayed of the patient and medical technologists can see the pending test of the patient which is to be performed and simultaneously give the result according to it. For pharmacists, an adequate amount of information is displayed of the patient and what are the medicines prescribed by the doctor. For receptionist, we have added an appointment system, by which the assistant of the doctor can schedule or delete the appointment of the patient, according to the schedule of the doctor.

The proposed model has been developed at the Computer Lab of Sandip Institute of Technology and Research Center (SITRC) and tested a bunch of students and with the help of teachers at SITRC. Our project team has played the role of administration to verify the users and other medical staff and departments. Also our teachers handled the medical department (Doctor, laboratory, pharmacy, medi-claim department). The other students has played the role of patients with RFID card, our web module was tested by them and verified.

V. CONCLUSION

In this model we have proposed a neoteric model for the electronic health card in which all the different aspects of the healthcare system are covered. The proposed model is user friendly since all the healthcare-related challenges are covered under a common framework. The proposed RFID based card will improve the overall health system. We have also provided Two Factor Authentication in the form of OTP, which is an additional layer of protection used to ensure the security of Patient accounts beyond just a username and password. All the various health information and the patient history such as reports, medical prescriptions, and laboratory results will be stored under this health card with proper authentication and privacy maintained. In conclusion, the proposed model will be economical and makes sure that the holder of the card will receive high-quality medical aid.

REFERENCES

[1] O. Par, Ergin Soysal, " Security Standards For Electronic Health Records, " IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, pp. 815-817, 2012.

[2] N. M. Shrestha, A. Alsadoon, P.W.C. Prasad, L. Hourany, & A. Elchouemi, " Enhanced e-Health Framework for Security and Privacy in Healthcare System," Institute of Electrical and Electronics Engineers (IEEE), pp. 75-79, 2016.

[3] V. Krishna, " Introduction of an international health card in Healthcare Information systems," International Journal of Advances in Electronics and Computer Science, pp. 4-9, 2016.

[4] N. Thiranant, M. Sain, L. Hoon, "A design of security framework for data privacy in e-health system using web service," 16th International Conference on Advanced Communication Technology (ICACT), pp. 40-43, 2014.

[5] M. T. Alam, L. Ali, " A Model of a Secured Smart e-Health System," International Conference on Industrial Engineering and Operations Management Kuala Lumpur, Malaysia, pp. 2174-2181, 2016.

[6] A. Ivanovic, & P. Rakovic, " E-health Card Information System: Case Study Health Insurance Fund of Montenegro," Mediterranean Conference On Embedded Computing (MECO), pp. 10-14, 2019.

[7] C. Turcu, C. Turcu, & V Popa, " An RFID-based System for Emergency Health Care Services," International Conference on Advanced Information Networking and Applications Workshops, pp. 624-629, 2009.

[8] C. S. Kruse, B. Smith, H. Vanderlinden, & Alexandra Nealand, "Security Techniques for the Electronic Health Records," J Med Syst 41:127, 2017.

[9]Stephanie Sargent, “Communication Errors: A Leading Cause of Mistakes in Healthcare”, https://www.sehealthcarequalityconsulting.com/2017/09/05/communication-errors-a-leading-cause-of-mistakes-in-healthcare/