Secure sharing of Personal Health Record

Amit Ranjan[1], Abhishek Trivedi[2], Abhijeet Shukla[3], Akhil[4]
[1,2,3,4]Student, IMS Engineering College, Ghaziabad, Uttar Pradesh

ABSTRACT

The application is mainly used to solve problems for people in today's world. The health record is the major concern for the people in today's world. Hospitals have to keep a lot of records and data of the patient with them. So sometimes this becomes very difficult to store this huge amount of data. So as to make this easy for the hospitals and for patient's point of concern. All the data will be stored on the cloud and from their patient can access his data. Also, hospitals and doctors can also access the data. Basically, there are several modules are used in this project i.e. patient, admin, path labs, doctor. For the privacy purpose, we have used AES encryption to encode the data of the patient. Data will be sent in an encrypted manner so that the privacy must be maintained. Initially, the patient needs to register themselves and login credentials will be provided to them once they are registered. All the previous data will be recorded and all the reports will be uploaded on the portal. It is accessed by the patient at any time and anywhere. The objective is to provide a global application which is accepted by all the hospitals, doctors and patient where doctors can update the medical records on a regular basis so that patient needs not to carry the previous records while switching the hospitals and this will also increase the efficiency of treatment.

Keywords— *PHR (Personal Health Record), AES encryption, Access control*

1. INTRODUCTION

Today, patient health record (PHR) has lifted as common term of exchanging the health status. Due to the giant rate of record, maintaining peculiar data stations including many health record facility are sub-contract to third-party facility suppliers. [1]. Here each patient is allowed to take the whole control of medical records and can share health information with the doctor, including medical report during their treatment. But while it is easier to have PHR facility for everyone, but there can be many securities and privacy risks which could slow down its acceptance. The only cause to get panic is whether the patients could manage the sharing of their health information (PHI), specifically when they are stored on external stations where patients may not all-encompassing assurance [3]. For the security purpose the basic idea to encrypt to data before storing and patient will able to decide who would see their medical reports by giving authorization. AES encryption approach is used for encryption and decryption. Another module Doctor will give the prescriptions to the patient. He can update the medicine and reports. Path lab module can upload the reports of the patient. Admin has the authority to add the data of new patient and can also update the data. Doctor has also the authority to view the patient's PHR during the treatment which would increase the efficiency of treatment because pervious report and health condition helps the doctor to analyze for the better treatment .This will minimize the paperwork as all activities will be done electronically on the portal and data will be stored. The aim of the project is to provide all previous medical reports on the portal this help the patient not to carry reports while switching the hospitals including maintain the privacy[2]. Some of the important features of our projects are: all the data and information will go paperless, it will provide a platform to communicate with patient and doctors, privacy will be maintained through AES encryption, doctors can also view the previous medical history this would increase the efficiency of treatment, path lab can upload the details of the reports.
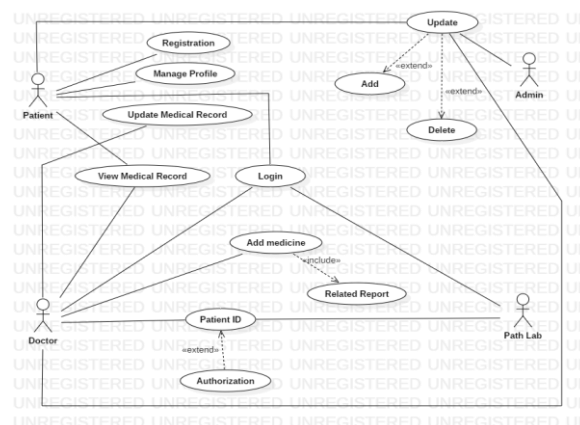
2. Use case diagram

Fig. 1: Case diagram

3. PROPOSED WORK

Web application can be installed in any system with Pentium IV processor, 512 MB RAM, 1 GB storage. Android application can also be installed on any android phone. It represents all the five modules i.e., doctor module, patient module, hospital module, admin module and path lab module. It shows the relationship between them.

4. RELATED WORK

Web application and android application is adequate to provide facility to the hospitals. Major problem related to this project is that when we will connect all the hospitals together. A huge amount of data has to be stored and we need a faster database and systems. Many applications are still in the market are providing the android application as well as the web application on paid basis but we are providing this facility free of cost. So that maximum number hospital can use this facility and can make their work more advance and technology based. AES encryption technique using SHA-1 and RSA algorithms [5].
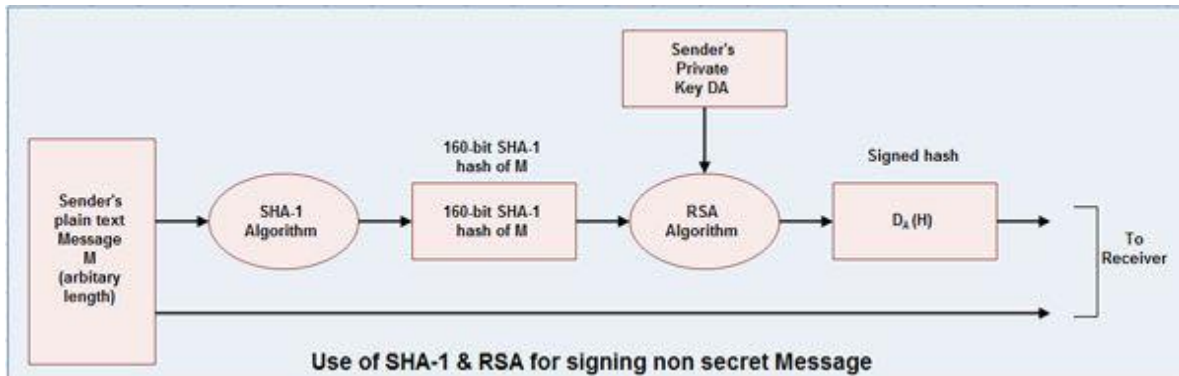

Fig. 2: Use of SHA-1 and RSA for signaling non secret message

5. CONCLUSION

This project will help to remove the traditional way of registering the patient i.e., through paper. Also the storage on the cloud through firebase will help the data to store on the cloud[4]. Privacy is the major concern for the hospitals. So through this project privacy can also be maintained. AES encryption technique is the primary feature of the project which will provide secrecy and privacy to the patient. Only patient can allow anyone to see his data. In future different proposals can also be introduced for the betterment of the project. New updates will also be available time to time for the web application as well as for the android application. So that bugs can be resolved and application can be made faster and easy to run on the systems.

6. REFERENCES

[1] V. Jagdale, D. Kekan, and IJCSMC, "Secure Sharing of Personal Health records in Cloud using Attribute based Encryption," vol. Vol. 4, no. Issue. 4,

[2] April 2015. [Online]. Available: https://ijcsmc.com/docs/papers/April2015/V4I4201577.pdf

[3] J. Foreman, "At risk of exposure," June 2006. [Online]. Available: https://www.latimes.com/archives/la-xpm-2006-jun-26-he-privacy26-story.html

[4] "The health insurance portability and accountability act of 1996," 1996. [Online]. Available: http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp

[5] What is SHA?" ecomputernotes.com/computernetworkingnotes/security/sha-1".