International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 2 (March '2017)
Proceeding of - National Conference on Recent Trends in Information Technology and Communication,
Conference held at Velammal Engineering College,Chennai,India.

PATIENT RECORD GENERALISATION USING CLOUD AND BIOMETRIC SENSORS WITH BLOWFISH ENCRYPTION

Aakash L,
Department of CSE,
Rajalakshmi Engineering College,
Chennai.

Deepak P.L,
Department of CSE,
Rajalakshmi Engineering College,
Chennai.

Abstract: As far as medical field is concerned one of the biggest problems faced by the illiterate patients is maintaining proper medical records. As most of them can't afford a well equipped hospital, or because of the instability in work ,they tend to keep changing the doctors and the hospital they visit and fail to maintain a proper medical record which leads to wrong diagnosis, improper treatment , worse side effects and much more. In order to overcome these issues, In this project an application is developed and only the properly qualified doctors are provided the access. Each doctor is provided with an individual login where the doctor can store and retrieve the patient records after the patient's authorization, which can be provided by the patients by placing their finger print in the biometric sensor integrated with the application. These data are completely stored in cloud so that any amount of data can be accommodated with total ease. There is also a separate option for the user to login to the application to just view and edit his/her medical record. This application is completely secure as the doctor can access the patient's record only after his/her authentication. And when it comes to the patient's module only his/ her record can be viewed. In order to secure the data in the cloud , the data is encrypted using the blowfish algorithm. A clear layout of the application is attached below.

Keywords: Biometric sensor, cloud, encryption, blowfish algorithm.

I.INTRODUCTION

As mentioned earlier in the abstract the sole purpose of this project is to take the advancement of medical technology to the lowest level of public.This app allows the illiterate people to keep complete records of their entire medical history without even having to own a mobile phone and yet with high security as well. All they have to do is approach any doctor at any place and just provide their fingerprint which brings in all the medical history of the patient so far. Some of the existing applications available in playstore related to health care maintenance are IBLUEBUTTON, TRACK MY MEDICAL RECORDS,CAPSULE PHR,MY MEDICAL etc.,

It is observed that over 17 million consumers access personalised applications related to health care in the survey taken in 2015.
This application stands aside of those application due to following reasons:

- It mainly targets on the poor people who cannot even afford a smartphone.
- The application is completely secure as the patient records can be viewed by the doctor only after the fingerprint authorisation of the patient
- A doctor can handle only one patient at a time as only one session is allocated per patient.This increases the personal attention to a patient and also only the doctor who has the authorisation of the patient can view the patient history.
- The data in the cloud is highly secure as the entire records are encrypted using blowfish algorithm.

II.ARCHITECTURE DIAGRAM

The figure 2.1 is the architecture diagram for the process that takes place when the patient approaches the doctor.

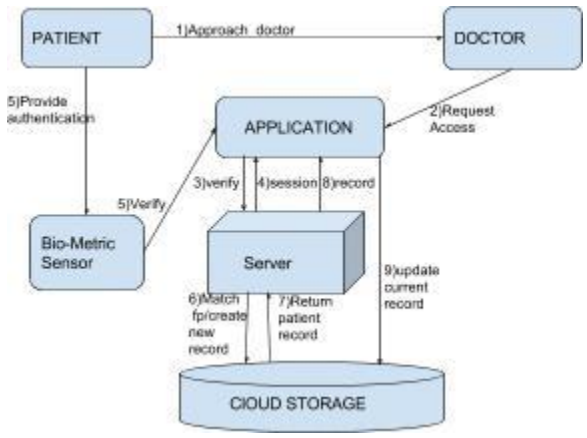


Figure 1: Doctor login

Doctor Login:

1. User interface:

When a patient approaches the doctor, the doctor logs into the application .Once the doctor's credentials are verified the doctor is allocated with a session within which the doctor can analyse one patient.

2. ***Biometric sensor***

Now in order to view the patient's records the application requests for the patient's fingerprint sensor.

3. Server

Once the fingerprint is provided by the user the server matches the fingerprint with the cloud and checks if any previous records exists .

4. ***Cloud***:

If yes the server retrieves the data from the cloud decrypts it after verification of the fingerprint and displays it in the application. If not new record is created and displayed in the application.Now the doctor can diagnose the patient using after verifying the previous records and update the current status of diagnosis,which will be encrypted and stored in the cloud.Once the patient is attended the session can be ended by the doctor.

The figure 2 is the architecture when the patient uses the application directly.

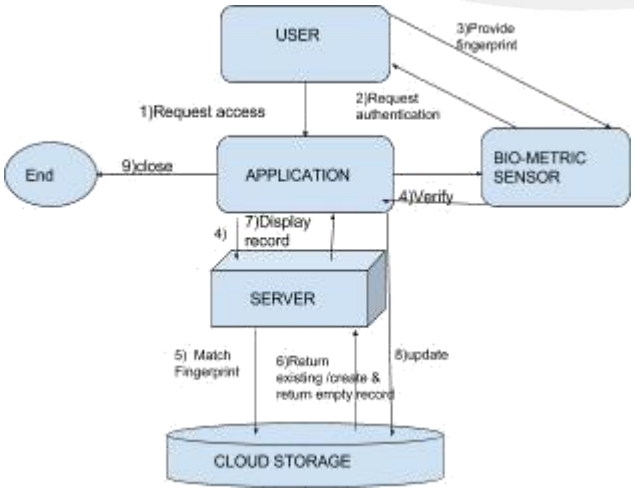


Figure 2: User login

Patient login :

1. User interface

If a patient wants to check his/her medical records in the mobile all he has to do is to open the application and select patient login

2. Biometric sensor:

Place the fingerprint.

3. Server:

The server checks for the records in cloud and matches it with the fingerprint. If the match is found the corresponding record is displayed in the application. If not found new record is created where the user can update the records.

4. Cloud:

The server retrieves the data from the cloud decrypts it after verification of the fingerprint and displays it in the application. After the record is updated it is again encrypted and stored in the cloud.

Cloud data encryption:

The user records in the cloud is encrypted using BlowFish algorithm.This is a symmetric block cipher encryption algorithm. It executes rapidly and is a Feistel algorithm with a simple encryption function. It uses a single key to encrypt and decrypt information. The process divides the data stream into blocks of a specified length (64 bits) and encrypts and decrypts the block. Wherever the block length is inadequate padding is inserted to make the encryption viable. Since the key used is of a variable length the algorithm is ideal for securing data. Since the data encryption algorithms are available in android studio library it can be integrated with application with single line of the code.

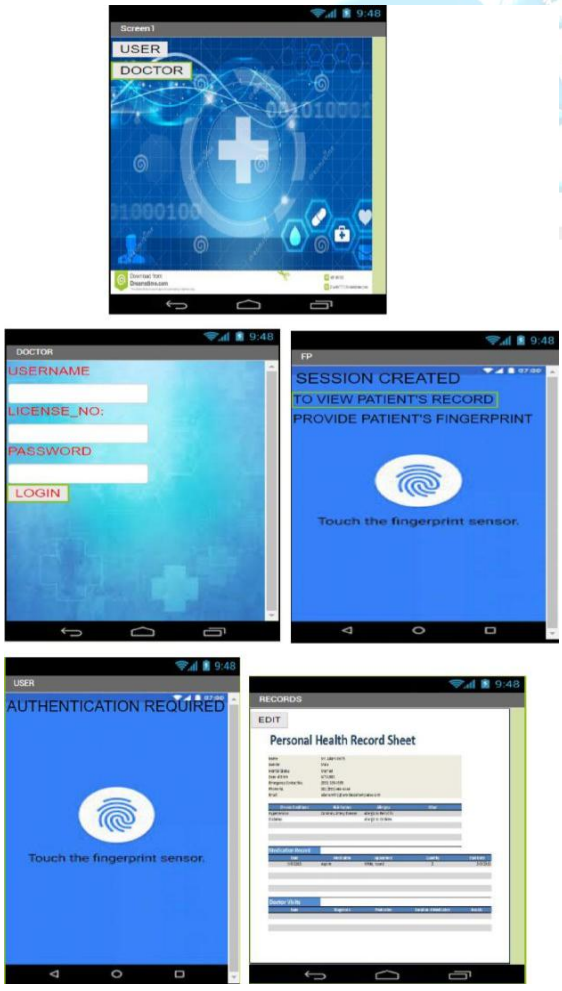
Blowfish in pseudocode

```
uint32_t P[18];
uint32_t S[4][256];
uint32_t f (uint32_t x) {
uint32_t h = S[0][x >> 24] + S[1][x >> 16
& 0xff];
return ( h ^ S[2][x >> 8 & 0xff] ) + S[3][x
& 0xff];
}
void encrypt (uint32_t & L, uint32_t & R) {
for (int i=0 ; i<16 ; i += 2) {
L ^= P[i];
R ^= f(L);
R ^= P[i+1];
L ^= f(R);          }
L ^= P[16]; R ^= P[17]; swap (L, R);
}
void decrypt (uint32_t & L, uint32_t & R) { for (int i=16 ; i >
0 ; i -= 2) {
L ^= P[i+1]; R ^= f(L); R ^= P[i]; L ^= f(R);
}
L ^= P[1];
R ^= P[0];
swap (L, R);
```

```
}
{
for (int i=0 ; i<18 ; ++i)
P[i] ^= key[i % keylen];
uint32_t L = 0, R = 0;
for (int i=0 ; i<18 ; i+=2) {
encrypt (L, R);
P[i] = L; P[i+1] = R;
}
for (int i=0 ; i<4 ; ++i)
for (int j=0 ; j<256; j+=2) {
encrypt (L, R);
S[i][j] = L; S[i][j+1] = R;
}
}
```

Softwares used:

Application is created using android studio, biometric sensor can be integrated with the application using the fingerprint api, The google cloud can also be integrated into the application using the google cloud api available in the android studio.



III. PROCESS:

The application consists of two separate modules one which is accessed by the doctor and other is accessed by the user, which is to be selected from the homescreen of the application. When the doctor access the application the application requests for the complete login credentials such as username , password , license id , which is to eliminate the fake doctors from accessing the details. Once the server grants access into the application doctor is provided with a session where the patient has to provide his/her fingerprint to view or create the medical record. The record is encrypted using blowfish algorithm for cloud security, After the session the record is updated and . encrypted again before storing into the cloud. The user can access the application as well. As the application targets on rural users,the UI is completely simplified for the patient's end.The user just has to open the application place the fingerprint and the record is displayed where in the backend mechanisms are same as in previous module. After viewing the record the user can close the application

IV. CONCLUSION

Though this project is a research level project,once it is implemented would surely have a huge impact in the medical field. As this application mainly focuses upon the less fortune and rural community which comprises of almost one-fourth of the entire population. This application is also highly secure as it uses blowfish encryption technique for security of data in the cloud, which ensures the privacy of every individual who uses this app . Though any doctor with a proper license and authorisation can access the application ,the patient records cannot be viewed with his/her authentication through fingerprint. And this application also provides a separate login module for the user where he/she can check their record with the fingerprint. Thus with this application totally removes the necessity of users to maintain a separate medical record and helps doctors to diagnose the patients in a much efficient manner.

VI. REFERENCE

[1]. http://www.securstore.com/blog/popular-c loud-encryption-algorithms/

[2]. http://mymedicalapp.com/

[3]. https://en.wikipedia.org/wiki/Blowfish_(ci pher)