International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 4, Issue 6, June 2015 **ISSN 2319 - 4847**

Mobile Health Monitoring Privacy System based on Cloud

[1]Deesha Vora , [2]Amarja Adgoankar , [3]Anil Chaturvedi

[1]Pursuing Master Degree in computer engineering
Shree L. R. Tiwari College of Engineering, Mira Road, India

[2] Asst. Prof, HOD, Computer Technology
K.C. College of Engineering, Thane, India

[3] Asst. Prof, Information Technology
Shree L. R. Tiwari College of Engineering, Mira Road, India

ABSTRACT

This paper presents the concept of how primary care physicians are increasingly interested in adopting electronic medical record (EMR) systems, few use such systems in practice. Mobile devices offer new ways for users to access health care data and services in a secure and user-friendly environment. Mobile healthcare (m-healthcare) systems are regarded as a solution to healthcare costs without reducing the quality of patient care and also how NFC Tag writer is used to write patient unique id in Near Field Communication (NFC) tag and Doctors using Near Field Communication (NFC) enabled smartphone to retrieve patient information when placed near NFC tag. Mobile devices use backend server to store and retrieve patient information. Google Cloud Messaging (GCM) is used to give notification to patients about their medicine. Advanced Encryption Standard (AES) and Elliptic curve cryptography (ECC) algorithms are combine together to provide security about patient information.

Keywords: Android platform, Near Field Communication (NFC), Google cloud messaging services (GCM), AES Algorithm, ECC algorithm.

1. INTRODUCTION

Cloud-assisted mobile health monitoring, which applies the prevailing mobile communications and cloud computing technologies to provide feedback decision support, has been considered as a revolutionary approach to improving the quality of healthcare service while lowering the healthcare cost. In current hospitals patient have to stand in a queue and fills forms manually.

There is no permanent records of patients and no global accessibility. In emergency doctor need to diagnose every time, test, report generation etc. There is no system to give notification to patients about their medicines .So patients can take their medicines on time. There is no system for the patients to check their disease by their own.

The doctors using website about patient information should be secure which is attached to the server and the android application fetching data from cloud should be secure so we are suing AES and ECC algorithm for security of data so it will not disclose patient information to others.

Health care is using different technologies approach for early detection, prevention of disease to improve quality of life. Proper documentation of patient record should be maintain. Patient should be aware of their disease and how to cure their diseases. Latest technologies like NFC, GCM is used.

2. METHODOLOGY

2.1 NFC Tags

When a patient is admitted in hospital for the first time a unique id is provided to patient. Patient will be equipped with NFC tag. Doctors and other staff will be equipped with NFC enabled smart phones. NFC tag writer is used to read the content from mobile to NFC tag. NFC tag writer can be downloaded from android mobile phone using play store. By using NFC tag stand writer we can write unique tag id and application link in NFC tag. To create patient application link we use ECLIPSE SDK online and then transfer to mobile by using USB cable. Whenever NFC tag is placed near NFC enable smartphones the patient data is retrieve directly from the backend server. Doctor uses hospital Wi-Fi to connect to internet to retrieve patient information directly from the server. The query processor handle the communication between mobile and server.

2.2 Advantages of NFC Tag

With NFC there is no need of a pairing of devices, physicians or staff just has to place the NFC reader next to the tag.
A secure communication between mobile and tag is ensured because of the short NFC communication distances of about 0-20 centimeters and the fact that NFC readers can only read one tag at a time.
Small size of tags (0.5mm²) makes it portable. The fact that the tag can be rewritten, makes is cost effective and best suitable for using for identification.
Their won't be a need of paper works any manual writing of reports or carrying reports or files.
Using NFC in health care, doctors can save the time and staff required to produce and maintain the patient records and fast treatment could be done.

2.3 Patient Identification using NFC Tags

We have developed a NFC based Identification and hospital management system using Android platform to identify, store and query data for patients form a backend server. Patients will equipped with NFC tag, and doctors and other staffs will be provide with NFC enabled Smartphone.
When Smartphone are placed near the NFC tag data will be read mobile and this unique ID will be sent to server to select the appropriate record.
This tag can be assigned to patient with a unique ID at the time of registration. NFC based Identification and hospital management system is developed for Android platform using the Android SDK that will be compatible with all versions and will run in all NFC enabled Android phones.
NFC technology will be used for identification wherein once a person is identified, the ID will be sent to Server to retrieve all the data about the patient. When brought near NFC tag, the mobile device extract the ID, and read other Android/NFC related information like parameters for automatic application execution, If ID is matched with the record the application get started otherwise display message of unidentified ID.
For successful identification it opens up the patient records and display information coming from the backend server system.

2.4 Algorithms

2.4.1 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size. It can be implemented on various platforms especially in small devices. It is carefully tested for many security applications.

Algorithm Steps: These steps used to encrypt 128-bit block
1. The set of round keys from the cipher key.
2. Initialize state array and add the initial round key to the starting state array.
3. Perform round = 1 to 9: Execute Usual Round.
4. Execute Final Round.
5. Corresponding cipher text chunk output of Final Round Step.

Usual Round: Execute the following operations which are described above.
1. Sub Bytes
2. Shift Rows
3. Mix Columns
4. Add Round Key, using K (round)

Final Round: Execute the following operations which are described:
1. Sub Bytes
2. Shift Rows
3. Add Round Key, using K (10)

Encryption: Each round consists of the following four steps:
1 Sub Bytes: The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.
2 Shift Rows: In the encryption, the transformation is called Shift Rows.
3MixColumns: The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.
4 Add Round Key: Add Round Key proceeds one column at a time. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition. The last step consists of XO Ring the output of the previous three steps with four words from the key schedule. And the last round for encryption does not involve the "Mix columns" step.

Decryption: Decryption involves reversing all the steps taken in encryption using inverse functions like
a) Inverse shift rows

b) Inverse substitute bytes
c) Add round key
d) Inverse mix columns.

The third step consists of XO Ring the output of the previous two steps with four words from the key schedule. And the last round for decryption does not involve the "Inverse mix columns" step.

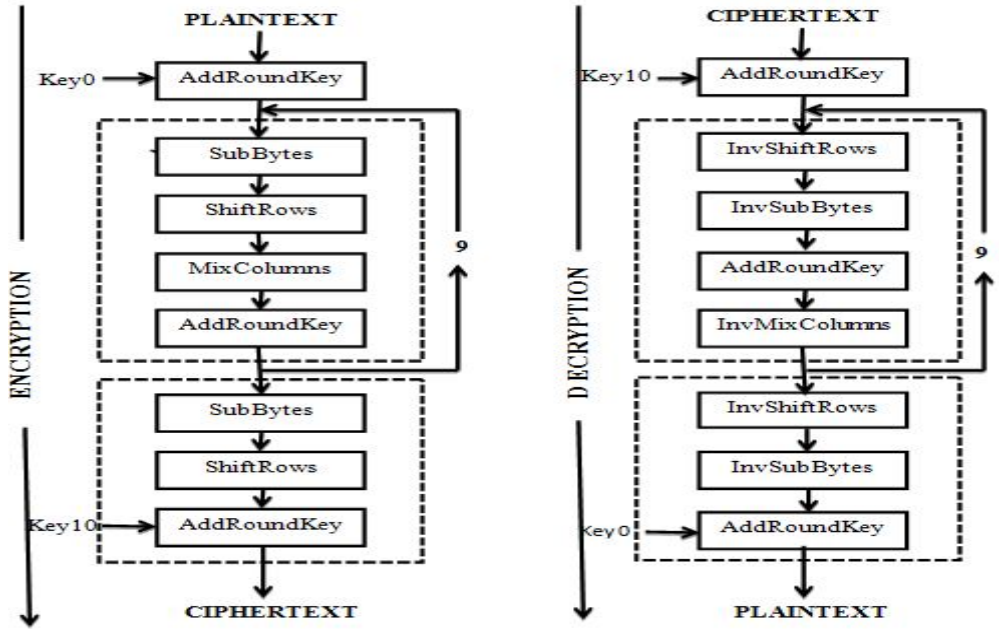

Fig.1 AES Algorithm

2.4.2 Data Encryption standard (DES)

Data Encryption standard (DES) mainly adopted by industry for security products. Algorithm design for encryption and decryption process has been done with same key. This algorithm processes the following steps.

[1] DES accepts an input of 64-bit long plaintext and 56-bit key (8 bits of parity) and produce output of 64 bit block.

[2] The plaintext block has to shift the bits around.

[3] The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.

[4] The plaintext and key will processed by following

a. The key is split into two 28 halves

b. Each half of the key is shifted (rotated) by one or two bits, depending on the round.

c. The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed keys used to encrypt this round's plaintext block. The rotated key halves from step 2 are used in next round.

e. The data block is split into two 32-bit halves.

f. One half is subject to an expansion permutation to increase its size to 48 bits.

g. Output of step 6 is exclusive-OR'ed with the 48-it compressed key from step 3.

h. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.

i. Output of step 8 is subject to a P-box to permute the bits.

j. The output from the P-box is exclusive-OR'ed with other half of the data block.

k. The two data halves are swapped and become the next round's input.

DES decryption

The decryption process with DES is essentially the same as the encryption process and is as follows:

• Use the cipher text as the input to the DES algorithm but use the keys Ki in reverse order. That is, use K16 on the first iteration, K15 on the second until K1which is used on the 16th and last iteration.

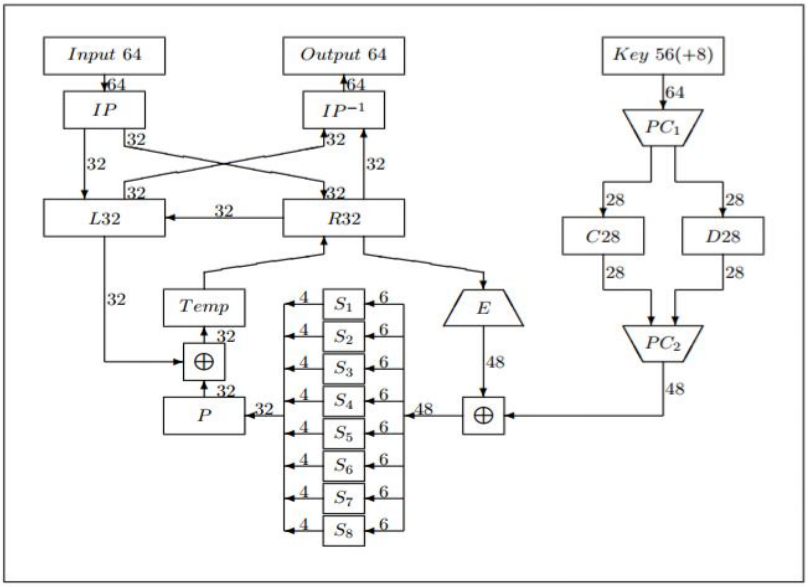

Fig.2 DES encryption/decryption algorithm

3. Results

Doctor: Android Application: Login - View Patients - View Patient Details - View patient previous Prescription - Add new prescription - Download test report of patients.
Reception: Admin :(Web Application): Add new patients - Login Update patients - Login Upload patients Test report - Login View patient log.

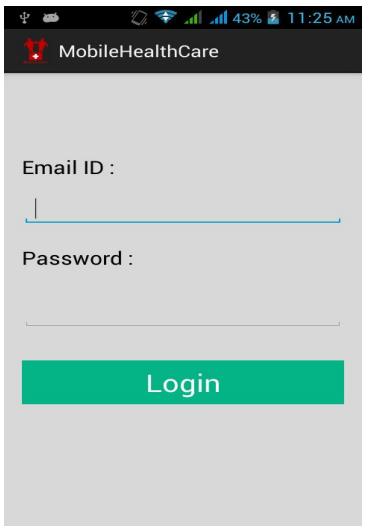

Fig.3 Doctor Login

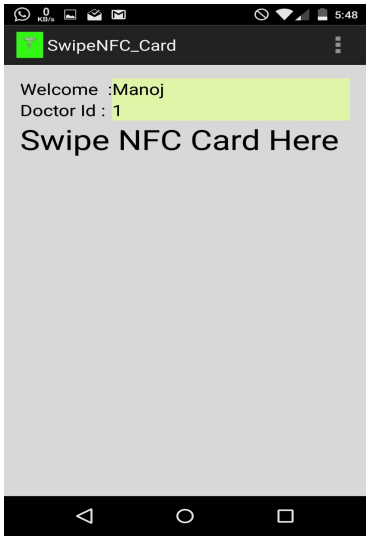

Fig.4 Swipe NFC Card

Fig.5 Patient detail screen

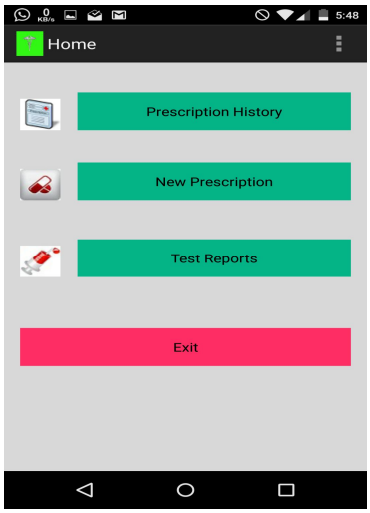

Fig.6 Select Option

Fig.7 Prescription History detail

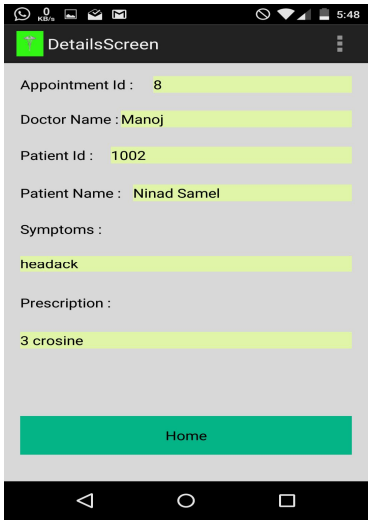

Fig.**8** Patient prescription detail

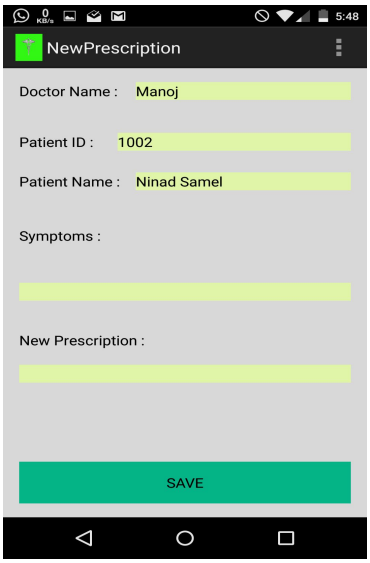

Fig.9 Change prescription

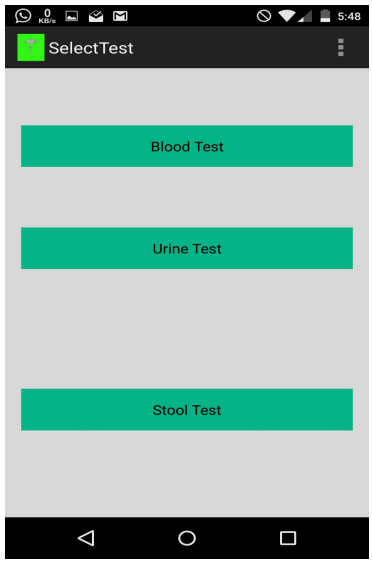

Fig.10 Select Test option

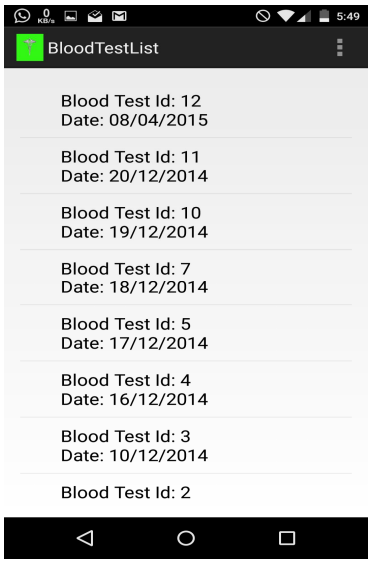

Fig.11 Blood test detail

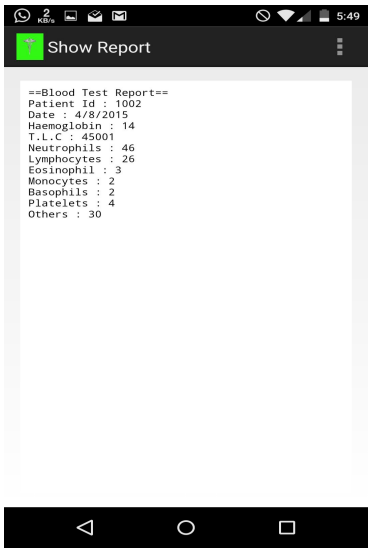

Fig.12 Blood report (Test report)

4. CONCLUSION

The Android Smartphone's having NFC application used in any Hospital, Clinic, Dispensary or Pathology labs .Here we tried to show how NFC enabled mobile can used for identification and be connected via the any network to exchange information across any device that is incompatible or does not have an NFC reader. Hence we can conclude that NFC technology appear to be credible for providing an efficient solution in many health care organization. Trial to improve the health system by different technological means and providing a better communication and secure way to transform Patient information in globalized manner.

REFERENCES

[1] Developing a NFC Based Patient Identification and Ward Round System for Mobile Devices using the Android Platform, 2013 IEEE Point-of-Care Healthcare Technologies (PHT) Bangalore, India, 16 - 18 January, 2013.
[2] NFC+ Android Application by using NFC technology for Hospital Management System, , Vol.2, No.2, April 2014
[3] NFC-based Hospital Real-time Patient Management System , International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue4- April 2013
[4] Mobile Healthcare System using NFC Technology, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 3, May 2012.