Mobile Health Monitoring Privacy System based on Cloud

Deesha Vora
Pursuing Master Degree in computer engineering
Shree L. R. Tiwari College of Engineering, Mira Road, India

Amarja Adgoankar
Asst. Prof, HOD, Computer Technology
K.C. College of Engineering, Thane, India

Anil Chaturvedi
Asst. Prof, Information Technology
Shree L. R. Tiwari College of Engineering, Mira Road, India

ABSTRACT
In this paper it describe how tagstand writer is used to write patient unique id in NFC tag   and Doctors using NFC enabled smartphone to retrieve patient information when placed near NFC tag. Mobile devices use backend server to store and retrieve patient information. GCM is used to give notification to patients about their medicines. WEB MD is used to check patient disease by their own.

Keywords
Android platform, Near Field Communication (NFC), Google cloud messaging services (GCM), Web MD, 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, web MD is used.

2. 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 tagstand writer administrator can write unique tag id and application link in NFC tag.   To create patient application link administrator 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.

3. ADVANTAGES OF NFC TAG
There are many benefits of using NFC in healthcare, but the most potential advantages of using the NFC in health care are improve patient's identification by eliminating the paper based documentation work, provide a way to automation, increase efficiency and also decrease manual power.

 One can use this smart tag even when they go to other hospitals, so instead of carrying many files they need to simply carry this small smart tag that can be read using a reader at the respective hospital. So this even provides benefits to customer. And also during frequent checkups one need not carry heavy files but can simply carry their smart tag and update it every time the health checkup is performed. Through the use of this NFC in health care, doctors can reduce the time required to go through a patients profile by waiting for someone to bring it and also to go through a lot of papers.

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.

4. SYSTEM DESIGN OF NFC
Each NFC technology consists mainly of a low power smart tag and a reader. The tag is consists of a small antenna and a microchip. The NFC enabled Smartphone transmits radio-waves of about frequency of 13.56 MHz that are received by antenna in the smart tag and, which allows the reader to identify the information in the smart tag by converting the radio waves reflected by the smart tag in to digital information. This information is stored mainly in the Hospital backend server.
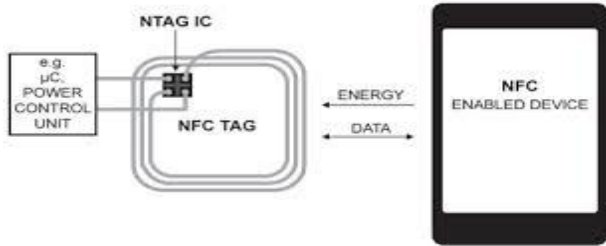
Fig 1: NFC Tag

5. GCM (GOOGLE CLOUD MESSANGING)

Google Cloud Messaging (GCM) for Android is a free service that helps developers send data from servers to their Android applications on Android devices, and upstream messages from the user's device back to the cloud. GCM is used to give notification to patient via SMS about their medicines according to prescribe time given by doctor. In this administrator is first fill the details of patient medicine online according to the prescribe time and server will be enable to that particular time and message will be sent to that particular patient by GCM and SMS gateway.

6. SYSTEM DESIGN OF GCM
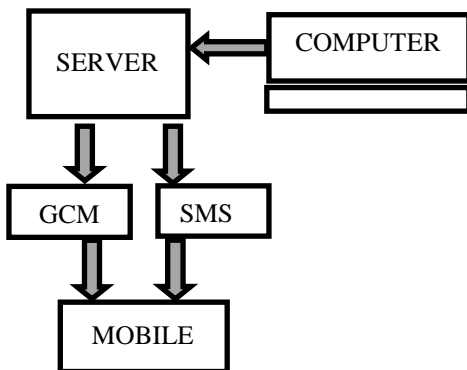
Fig 2: Notification of medicines via SMS AND GCM

7. WEB MD

It is used by patients to check their disease or prediction of diseases by their own. It maintains health conditions of individual and their life.
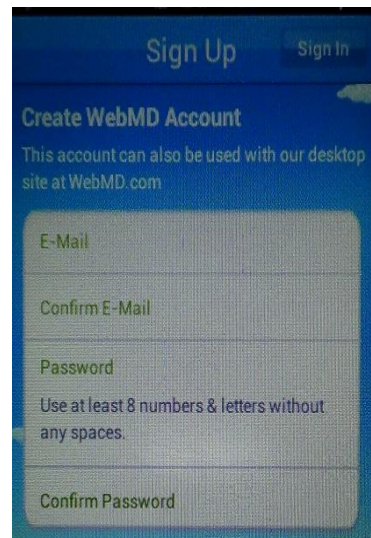

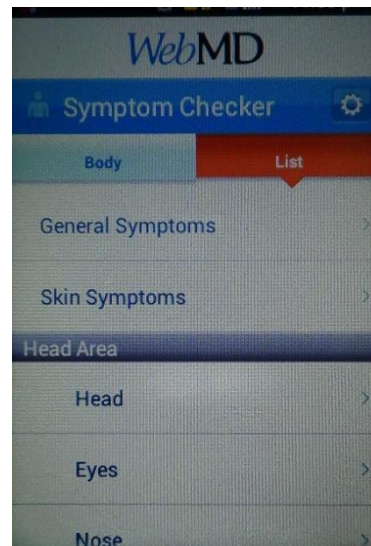**Fig 3: Main screen of Web MD For Sign up**
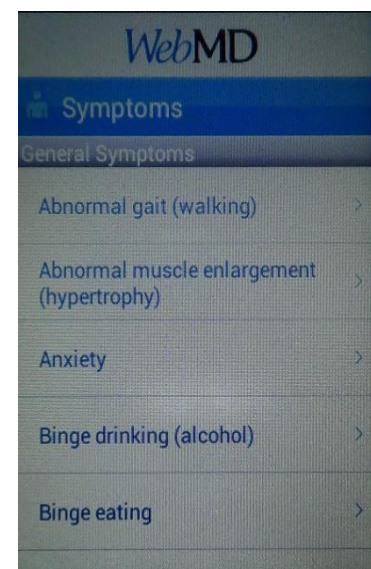

Fig 4: Create Web MD Account

Fig 5: List of Symtoms
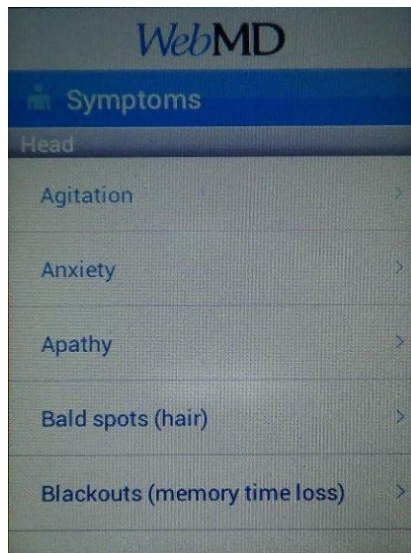

Fig 6: General Symptons
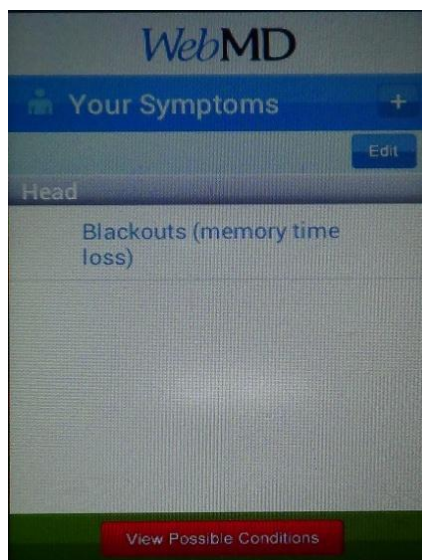
Fig 7: List of Head symptoms

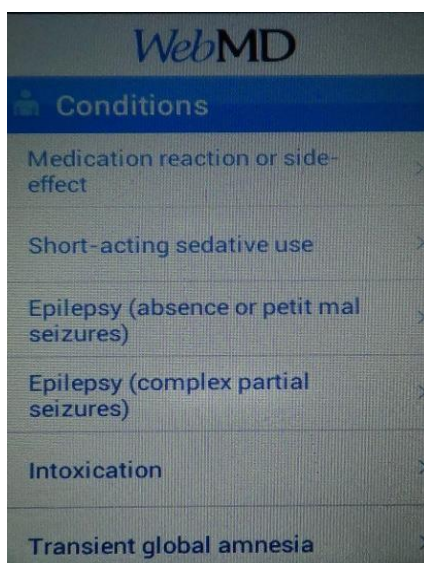**Fig 8: View possible conditions of Head Symptons**

Fig 9: Conditions of Head Symptons

8. AES ALGORITHM AND ECC ALGORITHM

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.

Advanced Encryption Standard is a symmetric- key block cipher published as FIPS-197 in the Federal Register in December 2001 by the National Institute of Standards and Technology (NIST). AES is a non-Feistel cipher. AES encrypts data with block size of 128-bits. It uses 10, 12, or fourteen rounds. Depending on the number of rounds, the key size may be 128, 192, or 256 bits. AES operates on a 4×4 column-major order matrix of bytes, known as the state.

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements, i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key – e.g., a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key. For current cryptographic purposes, an *elliptic curve* is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation, y2=x3+ax+b, along with a distinguished point at infinity, denoted ∞. (The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation will be somewhat more complicated.).
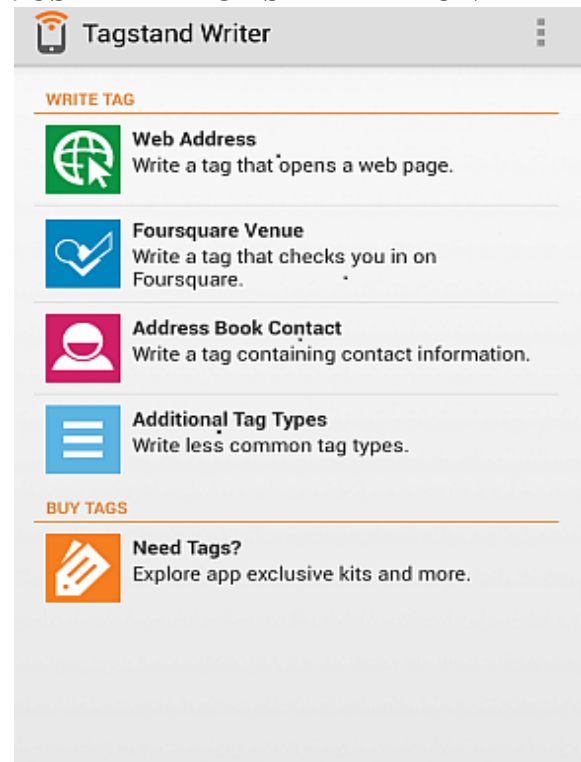
9. USABILITY OF SMART PHONE
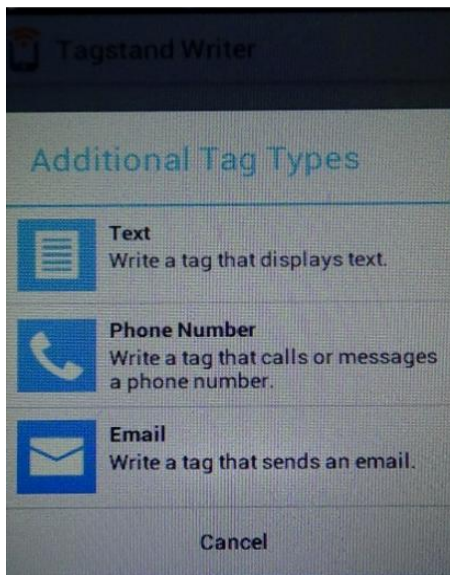

Fig 10: Main screen of Tagstand Writer
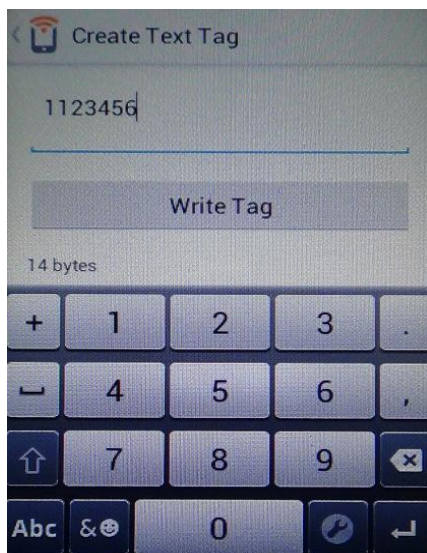
Fig 11: Main screen to write tag that display text

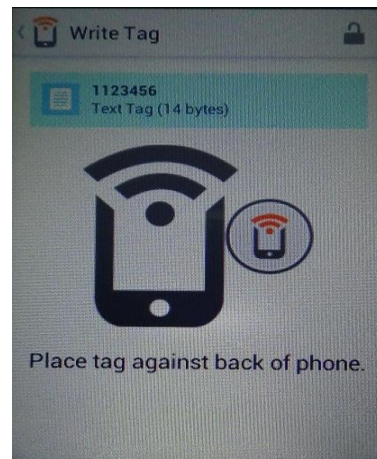**Fig 12: Main screen to write Unique ID of Patient**

Fig 13: Main screen to place NFC tag against NFC enabled phone

10. CONCLUSION

Trial to improve the health system by different technological means and providing a better communication and secure way to transform Patient information in globalised manner. In future it can develop for many hospitals as it has described for single hospital.

11. 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] Cloud Security Solutions Comparison among Various Cryptographic Algorithms, Volume 4, Issue 4, April 2014.

[4] Mobile Cloud for Assistive Healthcare (MoCAsH), 2010 IEEE Asia-Pacific Services Computing Conference.

[5] CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 6, JUNE 2013

[6] NFC-based Hospital Real-time Patient Management System, Volume4 Issue4- April 2013

[7] Mobile Healthcare System using NFC Technology, Vol.9, Issue 3, No 3, May 2012