ISSN 2395-1621

Real Time Applications by Using Near Field Communication Based on Security

[#1]Vrushali Bhand, [#2]Chaitali Ghadage, [#3]Sonam Khade

[1]chaitu.ghadage1994@gmail.com
[2]vrushalibhand@gmail.com
[3]khadesonam124@gmail.com

[#123]Dept. of Information Technology, AISSMS Institute of Information Technology, Pune.

ABSTRACT

Mobile devices can be rapidly used for an efficient healthcare management, banking system etc. A architecture is used for improving health care system with the help of Android based mobile devices with NFC and Bluetooth interfaces, smartcard technology on tamper resistant secure element (SE) for storing credentials and secure data, and a different services on a hybrid cloud for security and record management. Medical tags provided by it are used for reducing medical errors and secure healthcard for storing Electronic Health Record(EHR) based on NFC tags, Mobile devices using NFC P2P mode or card Emulation mode in healthcare system. Also in banking system it provides flexible use of NFC card for accessing transaction of more than one bank account of single user. The main contribution of this applications for i) Secure Medical Tags for reducing medical errors and ii) Secure Healthcard for storing Electronic Health Record (EHR) based on Secure NFC Tags, mobile device using NFC P2P Mode or Card Emulation Mode. We can make use of NFC card for shopping for travelling purpose, in Hotels etc. Simple touch of NFC enabled mobile devices can benefit both the patient as well as the medical doctors by providing a robust and secure health flow.

ARTICLE INFO

Article History

Received :28th April 2016

Received in revised form :

30th April 2016

Accepted : 2nd May 2016

Published online :

4th May 2016

***Keywords*—** NFC device, cloud computing, Secure Element(SE), NFC tag, Advanced Encryption Standard (AES),Electronic Health Record(EHR).

I. INTRODUCTION

Robust healthcare is a requirement for both developed countries. Where in developing countries like India, where there is a mass population to handle in hospitals and robust healthcare procedures are required the cost of healthcare is high and security and privacy are critical issues. An efficient, reliable, robust and secure health flow is important to manage patients, their health records smoothly and for the right care to reach to the patient at the right time .The major requirement in banking system is security, if user have more than one account in different banks then he need to carry that many number of cards and there is more possibility loosing card or damage , so to overcome this problem. we can use NFC enabled mobile for users as well as banking authorities.

The survey related to NFC based secure mobile healthcare system:

1.VedatCoskun, Busra Ozdenizci and Kerem Ok, "A Survey on Near Field Communication (NFC) Technology",2013
Near Field Communication (NFC) as a promising short range wireless communication technology facilitates mobile phone usage of billions of people throughout the world that offers diverse services ranging from payment and loyalty applications to access keys for offices and houses. Eventually NFC technology integrates all such services into one single mobile phone. NFC technology has emerged lately, and consequently not much academic source is available yet. On the contrary, due to its promising business case options, there will be an increasing amount of work to be studied in the very close future. Present the concept of NFC technology in a holistic approach with different perspectives, including communication essentials with standards, ecosystem and business issues, applications, and security issues. Open research areas and further

recommended studies in terms of academic and business point of view are also explored and discussed at the end of each major subject's subsection.

2.DivyashikhaSethial ,Daya Gupta I , Tanuj Mittal, UjjwalArora," NFC Based Secure Mobile Healthcare System", 978-1-4799-3635-9/14/$31.00 ©2014 IEEE.
Robust healthcare is a requirement for both developed countries, where the cost of healthcare is high and security and privacy are critical issues and developing countries like India, where there is a mass population to handle in hospitals and robust healthcare procedures are required. An efficient, reliable, robust and secure health flow is important to manage patients, their health records smoothly and for the right care to reach to the patient at the right time.

3.M. Roland and .I. Langer, "Digital Signature Records for the NFC Data Exchange Fonnat",2010
With the recent increase in usage of mobile devices especially in developing countries, they can be used for an efficient healthcare management. In this work, we have proposed a novel architecture for improving health care system with the help of android based mobile devices with Near Field Communication(NFC) and Bluetooth interfaces, smartcard technology on tamper resistant Secure Element (SE) for storing credentials and secure data, and a secure health service on a server for security and health record management.

4.SasikanthAvancha, AmitBaxi, and David Kotz, "Privacy in mobile technology for personal healthcare",2012
Information technology can improve the quality, efficiency, and cost of healthcare. In this survey, we examine the privacy requirements of mobile computing technologies that have the potential to transform healthcare. Such *mHealth* technology enables physicians to remotely monitor patients' health and enables individuals to manage their own health more easily. Despite these advantages, privacy is essential for any personal monitoring technology. Through an extensive survey of the literature, we
develop a conceptual privacy framework for mHealth, itemize the privacy properties needed in mHealth systems, and discuss the technologies that could support privacy-sensitive mHealth systems.

5.Smart Card Technology in U.S. Healthcare: Frequently Asked Questions,2012
The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America.

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.

Patient Identification using NFC Tags:

We have developed a NFC based Identification and hospital management system using NFC card to identify, store and query data for patients from a backend server. Patients will equipped with NFC tag, and doctors and other staffs will be provide with NFC devices. When NFC card are placed near the NFC device data will be read and 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.

Working Modes of NFC:

1.e-Health Card using NFC Tags:

The secure tags are very important point to concern. Those tags are used for application, are used for a different application for storing EHR on Healthcard of a patient. This is similar to a smartcard based Healthcard. But here we suggest smartcards that can be securely and easily be accessed using mobile devices. The tag is able to retain patient and bank authorities and customers identification information along with emergency information, insurance

information and health records. The tag could be organized into different sections, each administered separately by different set of security access keys. This is like secure tag application, this card can be issued and updated by an authorized health admin mobile device MobileADMIN'.A patient can register at the MobileADMIN and then later show to an authorized doctor with MobileDoc in an OPD which would have the required access keys KR and Kw for reading and updating the health records respectively. All NFC information can be retained with a timestamp. Due to limitation of space on the card, it can only retain recent health records. Detailed health records can be retained on a storage server of the HealthSecure service on hybrid cloud. At the end of the visit the patient can present the tag back to the administrator to tap and store his visit detail on the hybrid cloud. At any point of time if patient's past records are required, they can be retrieved over secure wireless interface (like HTTPS) from the hybrid cloud, using the patient ID on the tag. This application will help the patient to retain the recent health records on a cheap yet secure tag equivalent to a smartcard.

2. e-Health Card based on P2P NFC mode:

In this application architecture NFC P2P mode is used to retaining a Healthcard on a mobile device. The EHR is retained on the mobile device in a secure region instead of NFC tag. The patient can tap his mobile device onto the doctor's mobile device to exchange his records using NFC NDEF format. The doctor can read and update the records and tap them back onto the patient's mobile device. Both patient and doctor register for the OPD session with the health admin, MobileADMIN, to get secure keys. The patient's public and private keys KpUBPAT. KpRJPAT and doctor's public and private keys KpUBDOC, KpRIDoc get stored on the SE of their respective mobile devices for the OPD session, This Healthcard offers more storage space as compared to what a smartcard based tag can provide as in application III-B. It also ensures that only the permitted records of the patient are accessed by an authorized doctor, thus retaining security and privacy of the patient. NFC P2P mode can be utilized for information exchange, But very large health records exchanged over NFC can be slow due to the low data rate of NFC. Bluetooth can be used along with NFC for exchange of larger health record data. A basic security framework requirement.

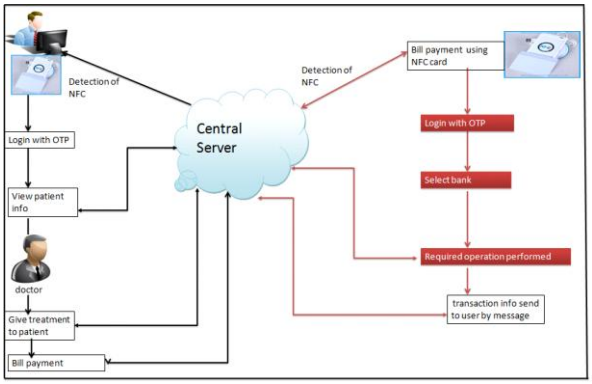
3. e-Health Card based on NFC card emulation:

In this application architecture, card emulation and Java card applets installed on the SE is used for retaining healthcard on a mobile device. We propose usage of a SE in the form of an SWP enabled microSD card as provided by GoTrust, which can be issued to the patient by HealthSecure service. Java Card applet is used to authenticate and authorize the reader and writer to access and update the health records using NFC SWP protocol. SE has limited space that is why it can only retain part of the health records. The remaining health records can be retained outside the SE region on the SD card in a secure manner. The Card on the MobilepAT can be accessed externally by a PC/SC reader that is attached to Mobileooc. Since the SE has limited space, an extended card consisting of past records and other health information, like images and reports, can be stored in encrypted format on an insecure region. Hence this Healthcard is different from a standard plastic smartcard used for Healthcard in the previous scenario. Since NFC has lower data rate, Bluetooth can be used to access the extended card. The Java card applet can be used to initiate Bluetooth pairing between mobile devices. This Healthcard is most secure and can also be used to retain larger information on the mobile device and is similar in idea to the Wireless Medical Card.

II. PROPOSED SYSTEM

- *Working of Proposed System:*

In Hospital: For secure identification as well as for retrieving previous information about patient & patient Healthcard. 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 also has NFC card instead of NFC enabled smart phone. NFC tag writer is used to read the content from mobile to NFC tag. Whenever NFC card of patient is placed near NFC device the patient data is retrieve directly from the backend server .Then Doctor is able to read the contents by using NFC tag. By getting previous data about patient doctor gives treatment as per required. Then add new prescription & Download test report of patients.



Doctor: Doctor is able to login with his id and password. After successful authentication of doctor he can be able to view patient's details. He can also able to view patient's previous prescription and can be able to add new prescription. At the end he can download test reports of patients.

Reception: receptionist who can be admin is able to add new patients. also after receptionist successful authentication is able to update patients information. also uploading patients test reports and viewing patients log is done by receptionist.

In Banking system :For customer and banking authority identification and secure transaction. User with NFC enabled mobile goes to ATM. Then ATM with RFID machine can makes OTP the RFID machine will directly makes authentication through bank server through sending request. By using this information & authentication

User is allowed to perform operations as per required then after successful transaction receipt is being provided.

III.ALGORITHM

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.

3 MixColumns: 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.

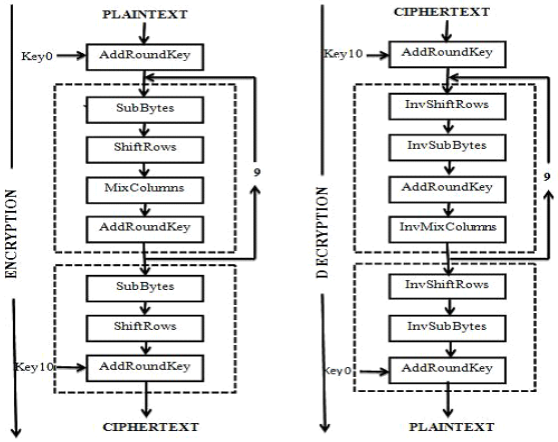
Decryption:
Decryption involves reversing all the steps taken in encryption using inverse functions like

- Inverse shift rows

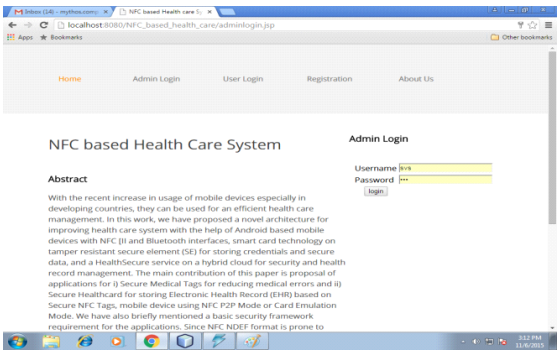
b) Inverse substitute bytes
c) Add round key
d) Inverse mix columns.

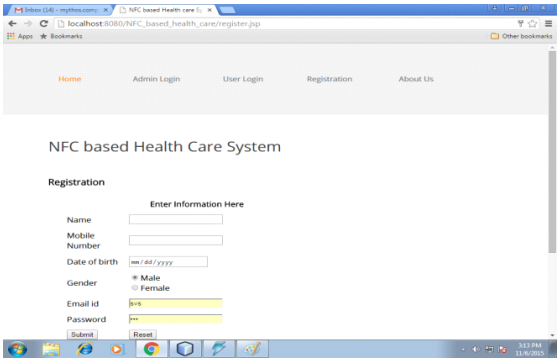
The third step consists of XO Ring the output of the previous two steps with four words from the key schedule. And the

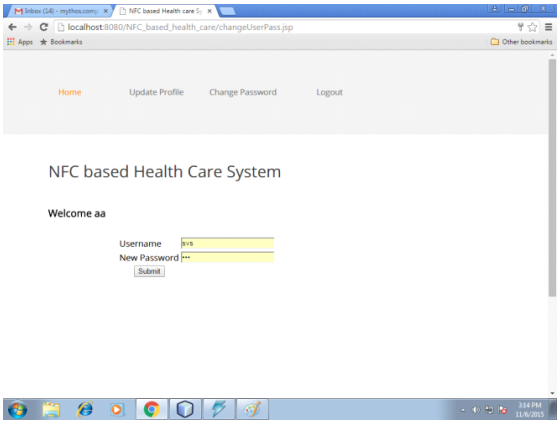
- last round for decryption does not involve the "Inverse mix columns" step.

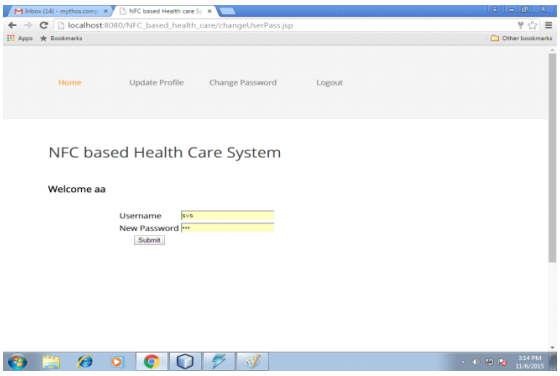


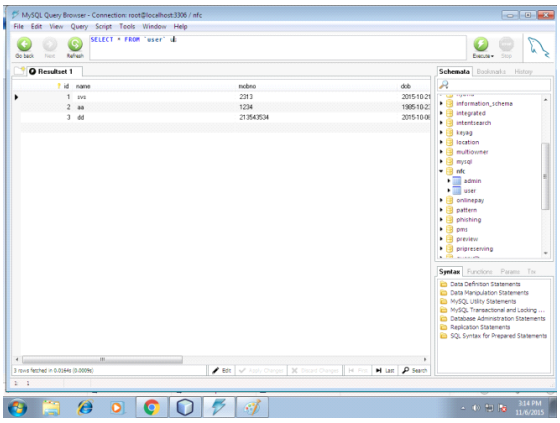
IV.RESULT ANALYSIS











V. CONCLUSION AND FUTURE WORK

NFC enabled devices can be connected to an existing web service enabled infrastructure using standard technologies. Cloud computing is used for information storage and NFC card for storing personal identification number and information is retrieved by using RFID. This improves the health flow in crowded hospitals, security in banking system and convenient for all other systems.

REFERENCES

[1]DivyashikhaSethial ,Daya Gupta I , Tanuj Mittal, UjjwalArora," NFC Based Secure Mobile Healthcare System", 2014 IEEE.

[2]VedatCoskun, BusraOzdenizci and Kerem Ok, "A Survey on Near Field Communication (NFC) Technology",2013

[3] M. Roland and .I. Langer, "Digital Signature Records for the NFC Data Exchange Fonnat", IEEE Proceedings of the Second International Workshop on Near Field Communication (NFC), pp, 71-76, 2010.

[4]SasikanthAvancha, AmitBaxi, and David Kotz, "Privacy in mobile technology for personal healthcare",2012

