ISSN 2395-1621

Real time applications by Using Near Field Communication Based on Security

[#1]Vrushali Bhand, [#2]Chaitali Ghadage, [#3]Sonam Khade, [#4]prof. R.Y.Totare

[#1234]Dept. of Information Technology, AISSMS Institute of Information Technology, Pune.

ABSTRACT

M**obile devices can be rapidly used for an efficient healthcare management, banking system, in hotel, bus etc. A architecture is used for improving health care system with the help of smartcard which is NFC (Near Field Communication) card 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 health card for storing Electronic Health Record(EHR) based on NFC tags. Also in banking system it provides flexible use of NFC card for accessing transaction of bank account which has account of hospital and users. The main contribution of this applications for i) Secure Medical Tags for reducing medical errors and ii) Secure Health card for storing Electronic Health Record (EHR) based on Secure NFC Tags. NFC card has one particular ID of every user which is used for authentication. 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.**

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

ARTICLE INFO

Article History

Received :30th April 2016

Received in revised form :

2nd May 2016

A0ccepted : 4th May 2016

Published online :

6th May 2016

I. INTRODUCTION

Robust healthcare system is a requirement for both developed and developing 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 here one bank has account of hospital and users so whenever user get treatment and make payment he can do transaction with one card only. This system is very useful in any real time use.

II. LITERATURE SURVEY

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.

III.METHODOLOGY

NFC tag:

When a patient is admitted in hospital for the first time a unique id is provided to patient which is enabled in card. Patient will be equipped with NFC tag. NFC tag reader is used to read the content from NFC card and shows it on receptionist computer. By using NFC tag stand writer we can write unique tag id and application link in NFC tag. NFC reader which is available from market, TTL logic which has one serialize cable to transfer data to computer which is also available from market and one microcontroller kit which has power supply, capacitors, registers, LED etc. is used in hardware part for detecting NFC card of authorized user. Whenever NFC card is placed near NFC reader the patient data is retrieve directly from the backend server. Doctor can get information of patient directly after authorization of paitient.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 form a backend server. Patients will equipped with NFC card, 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.

IV.HARDWARE

3.1 NFC card (Near Field Communication):

Near field communication is a technology for high frequency wireless short distance point to point communication. The operational range for NFC is less than 20cm, which is good from a security perspective, because it diminishes the threat of eves dropping. The other reasons to use NFC are the low cost of necessary components and that the connecting time is negligible. It is a small circuit attached to small antennae, capable of transmitting data to a distance of several meters.

3.2.1 PCB design:

a. Power supply:

1. DC Socket:
   Input for DC socket is 5v.Stepdown transformer(12v) or adapter is used to convert alternate current (AC) to Direct Current (DC)
2. Rectifier:
   To remove the impurities from signal and send signal.
3. Capacitor:
   Electrolytic capacitor of 7.8.9.v is used to store charge.
4. Regulator:IC7805
   Regulator is used to voltage conversion. In IC7805, 78 indicates positive charge and 05 indicates Voltage.
5. Electrolytic capacitor:
   To maintain supply constant and adjust noise.
6. Register:(330ohm):
   It is current limiting register.
7. Disk capacitor:
   It is used to reduce noise.
8. Crystal oscillator:
   It is 20mHZ oscillator

b. Microcontrolller:

1. Pullup and pulldown register for pic.
2. Pic IC 16F877A.
3. Male connector:
   It is used for flow of program and program dumping.
4. Priset(10kohm):
   It is variable register and used to control brightness of LCD(16*2).

3.2.2 NFC reader:

It is used to generate electromotive force(EMF).and used to detect NFC card which is magnetic strip.

3.2.3 TTL logic:

It is used for transmission of data serially.

3.2.4 Design:

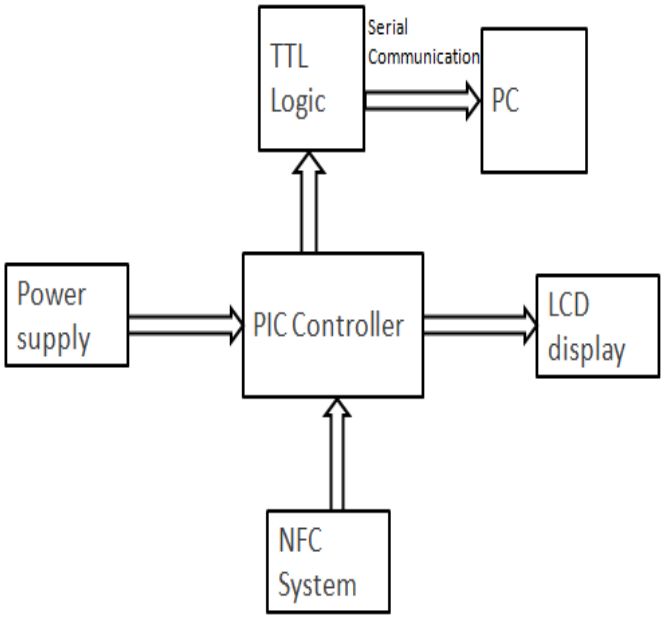


Fig:Block digram for hardware

V. PROPOSED SYSTEM

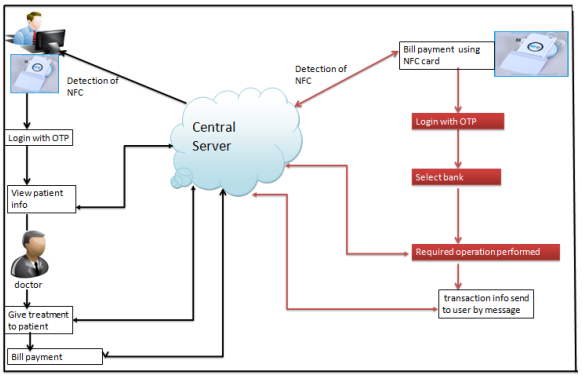
1. Working of Proposed System:

In Hospital: For secure identification as well as for retrieving previous information about patient & patient Health card. When a patient is admitted in hospital for the first time a unique id is provided to patient. Patient will be equipped with NFC card. Doctors and other staff will also has NFC card and they have NFC device for detection of NFC card instead of NFC enabled smart phone. NFC tag reader is used to read the content from NFC card and send to computer through TTL logic. 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.

In this process when user goes to the hospital for treatment he has one NFC card. Admin logged in itself then he himself fill all the information of patient after successful identification of patient. when admin click to view patient details new page will open that time user has to put his NFC card near NFC device and id will automatically displayed on computer and user's name will displayed on LED. After that admin is able to see user history and he can add new treatment.

Bank site: At bank side there is new website for bank which is NFC bank. User has to open his account in that bank where already hospitals account is existing.

User can add balance change password through that banking website.



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.

VI. 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.

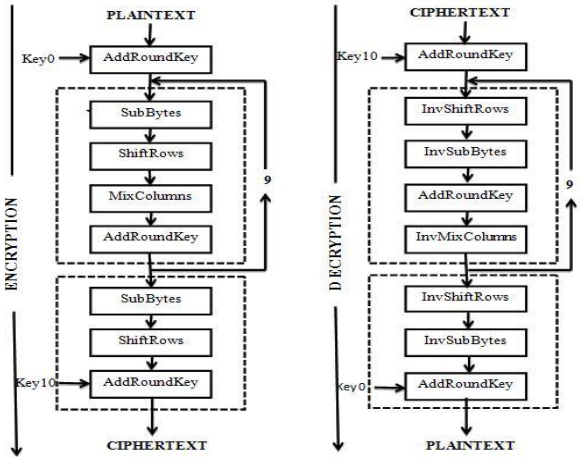
4 Add Round Key: Add Round Key proceeds one column at a time. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition. The last step consists of XO Ring the output of the previous three steps with four words from the key schedule. And the last round for encryption does not involve the "Mix columns" step.

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

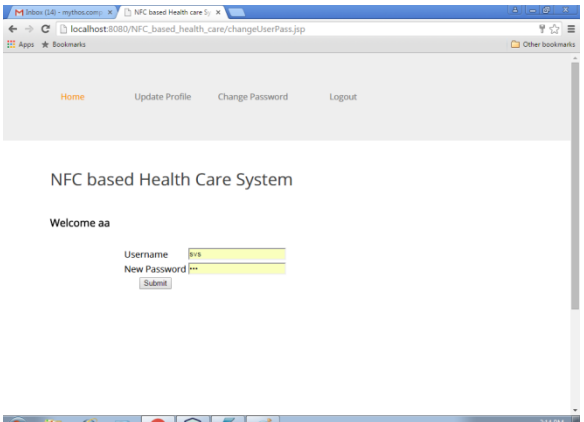
a) Inverse shift rows
b) Inverse substitute bytes
c) Add round key
d) Inverse mix columns.

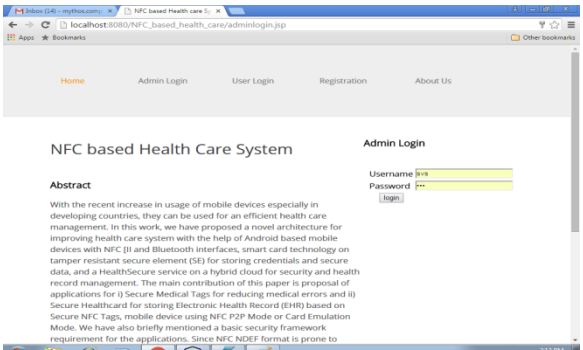
The third step consists of XO Ring the output of the previous two steps with four words from the key schedule. And the

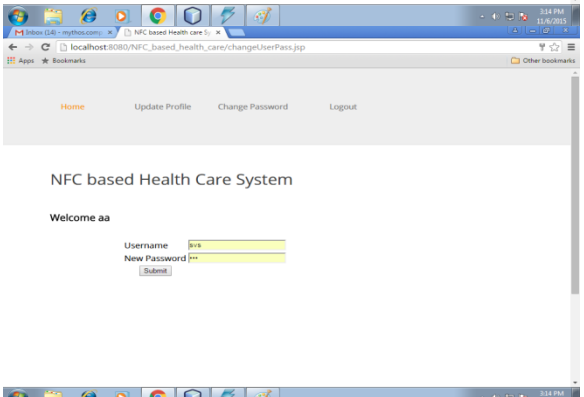
a) last round for decryption does not involve the "Inverse mix columns" step.

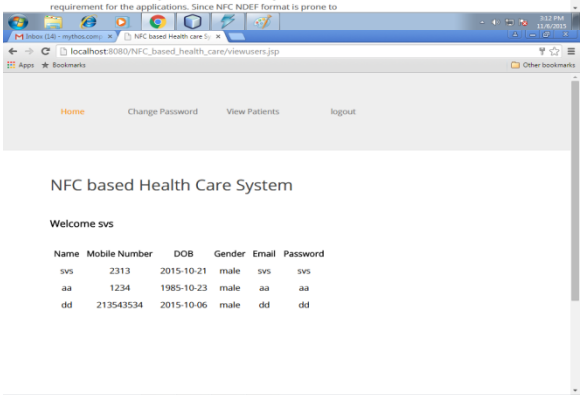


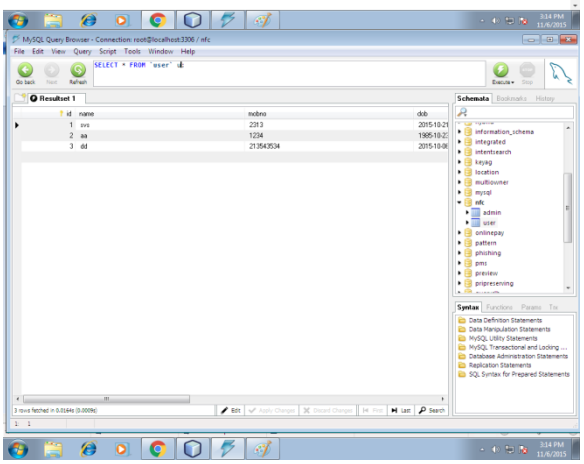
VII. RESULT ANALYSIS

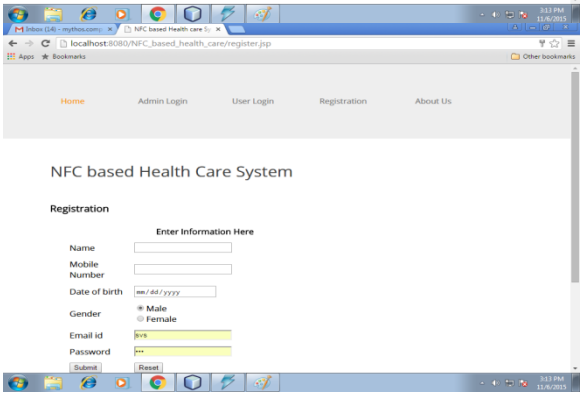












VIII. CONCLUSION AND FUTURE WORK

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

