MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

NEAR FIELD COMMUNICATION BASED ANDROID API HEALTHCARE SYSTEM

Bankar Kartik, Joshi Bhargav, Mungal Mahajan, Subhash Rathod
Computer Engineering Dept., MMIT lohegaon,
Pune, India
kartik.bankar@mmit.edu.in, ninad.joshi090@gmail.com,
mahajanmungal62@gmail.com

Abstract: *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.*

The main contribution of this paper is of applications for i) Secure Medical Tags for reducing medical errors and ii) Secure health card for storing Electronic Health Record) based on secure NFC tags, mobile device using NFC P2P mode or card emulation mode.
We have also briefly mentioned a basic security framework requirement for the applications. Since NFC NDEF format is prone to security attacks, we have utilized low level APIs on android based mobile devices, to securely access NFC tags such as MIFARE, classic tags with NFC properties 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, Secure Element, Graphical User Interface, NFC Data Exchange Format, EHR Electronic Health Record*

1. INTRODUCTION

One of the largest IT challenges in the health and medical fields is the ability to track large numbers of patients and materials. As mobile phone availability becomes ubiquitous around the world, the use of Near Field Communication (NFC) with mobile phones is emerging as a promising solution to this challenge. The decreasing price and increasing availability of mobile phones and NFC allows us to to apply these to developing countries in order to overcome patient identification and disease surveillance limitations, and permit

improvements in data quality,patient referral and emergency response. Benefit of NFC in this project is NFC Card Allows People to Enjoy the Pleasant Payment with NFC-enable for Hospitalality services.The purpose of the project entitled as NFC BASED SECURE MOBILE HEALTHCARE SYSTEM is to computerize the front office management of hospital to develop software which is user friendly, simple, fast, and cost effective. It deals with the collection data of patient's information, diagnosis details etc. Traditionally, it was done manually. The main function of the system is to register and store patient details and doctor details and retrieve these details as and when required and also to manipulate these details meaningfully. System input contains patient details, diagnosis details; while system output is to provide proper treatment details.

2. RELATED WORK

The Limitations of the existing system is that it is very difficult to retrieve data from case files. It is difficult to handle the whole system manually and it is less accurate and to keep the data in case files for future reference because it may get destroyed. Moreover it is very difficult to retrieve data. Redundancy of data may occur and this may lead to the inconsistency. The manual system is so time-consuming. The proposed system is very easy to operate with NFC card. Speed and accuracy are the main advantages of proposed system. There is no redundancy of data. The data are stored in the computer's secondary memories like hard disk, etc. it can be easily receive and used at any time. The proposed system will easily handle all the data and the work done by the existing systems. The proposed systems eliminate the drawbacks of the existing system to a great extent and it provides tight security to data.

3. TECHNOLOGY

NFC is an upcoming wireless technology which provides simple interfaces for device to device communication as well as access to NFC, RFID and smartcard tags. NFC enabled mobile device can operate in three modes: i) Reader mode: in which device can read and write to NFC based passive tags. ii) Peer to Peer (P2P) mode in which NFC devices can interact and exchange information with each other iii) Card emulation mode: in which NFC device can operate as a contactless card.NFC enabled mobile devices have a secure element (SE) which is a secure microprocessor (a smart card chip) that includes a cryptographic processor to facilitate transaction with authentication and security, and provides secure memory for storing applications and credentials. It comes in different form factors such as embedded, micro SD card or a UICC (SIM) card [9]. Due to simplicity of accessibility we have used SWP enabled micro SD card as a SE to manage cryptographic keys as well as patient medical records. SWP is a contact based protocol between Contactless frontend (CLF) and UICC. It is Java Card 2.2.2 compliant.

4. PROPOSED APPLICATION MODELS

4.1 Secure Medical Object Identification using NFC Tags

Reliable medical object identifiers are important for reducing errors in the hospital workflow, like giving correct medicine to a patient. We propose architecture of an application for issuing secure identifiers to reduce the error and also to prevent security attacks like modification, repudiation and masquerading. The secure NFC passive tags have been used for identifiers, specifically MIF ARE Classic. Bluetooth Low Energy (BTLE) stickers have lately been used to identify objects. But since they require a dedicated battery to operate, NFC passive tags are cheaper for identifiers to be used in healthcare. As discussed in section II, NFC tags with NDEF format are prone to security flaws [2]. Hence basic NFC-A interface can be used to access smartcards from a mobile device. A valid mobile reader must have security key for read access and a valid writer must have security key for update access. The tag is issued by a healthcare admin mobile device. It retains security keys in its SE for issuing tags. To enhance security, the access keys of the tag could be updated on a periodic basis for retaining secure IDs on the medical objects.

4.2 E-Health Card using NFC Tags

The secure tags used for application in III-A, are used for a different application for storing EHR on Health card of a patient. This is similar to a smartcard based Health card. But, here we suggest smartcards that can be securely and easily be accessed using mobile devices. The tag could retain patient 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. Similar to the secure tag application, this card can be issued and updated by an authorized health admin mobile device mobile admin patient can register at the mobile admin and then later show to an authorized doctor with mobile doc 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 Health Secure 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 patients 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.

5. IMPLEMENTATION

We have developed applications for both Android devices, using Android APIs, and administrative server, using PHP and MySQL, for secure, reliable and robust healthcare system. Mobile applications have been tested on Google Nexus 7 and Samsung Galaxy S3 devices. We have used MIFARE Classic IK tags for reading and writing data using APIs in Android framework (Android 2.3.3 and above). The Android framework provides android. NFC. Tech package, which contains necessary classes and methods to enable interaction with tags. We have used a SWP Secure microSD card (by GO-Trust), which provides a microSD based Java Card 2.2.2 solution. The card supports running Java Card applets on a hardware-backed SE. It also provides a contactless interface (ISO 14443) via SWP which can be used to interact with compliant PC/SC readers. We have tested it using a Samsung Galaxy S3 (i9300,by Samsung) mobile device with Android 4.1.2. The card can be accessed from an authorized Android application developed using Go-Trust library. Since the card

supports Global Platform 2.1.1 [\5], the installation can be done using custom Global Platform APDUs.

5.1 System Implementation

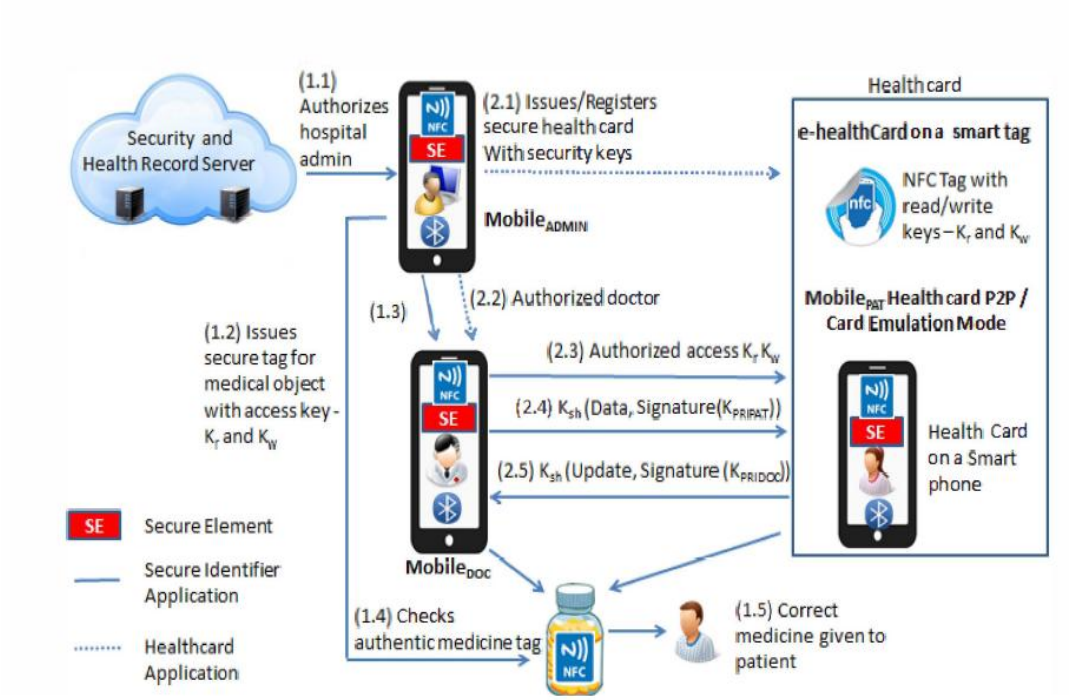

Fig.1: System Implementation

5.2 e-Healths Card based on P2P NFC mode

This application architecture is based on retaining a Health card on a mobile device using NFC P2P mode. The HER is retained on the mobile device in a secure region instead of NFC tag as in III-B. The patient can tap his mobile device onto the doctor's mobile device to exchange his records using NFCNDEF 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, Mobile ADMIN, 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 Health card 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 record sex changed 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.

6. SECURITY FRAMEWORK REQUIREMENT

There is a strong security framework required for the health care management. It is different from the financial data security which is small in size and is handled by a set of trained professionals with standardized models. The health care data can be large in size as in a

Health card with entire EHR. Also the health card could be accessed by various persons: patient, medical professional, emergency person and insurance. The patient should be able to securely manage the access control of the EHR. We provide a brief overview of a basic security framework requirement for the application of Health card on a patient mobile device using NFC P2P or Card Emulation mode. There is a requirement of confidentiality, integrity, mutual authentication, access control of EHR, privacy threats leading to identity thefts and insurance security breach .The security framework involves various entities. A cryptographic server is used to generate, verify and store security keys. An administrator is present to issue Health cards /tags and register patients/doctors. Mobile devices used by doctors are equipped with a Doctor App and a secure element (Doctor SE). Health card used by patients is called Patient card which in this case is using a NFC P2P or card emulation mode. The SEs involved, like Doctor SE, run a Java Card applet to manage cryptographic keys as well as patient medical records. Since the health card could be accessed by various persons: patient, medical professional and emergency person, they could use the concept of shared key based on Attribute Based Encryption. The patient could access the card using combination of Patient key in the form of a PIN and Biometrics. There could be a separate Doctor PIN for doctor and a super key for emergency team when patient is unconscious. In case of loss of mobile devices the keys which are maintained by the HealthSecure service can be invalidated.

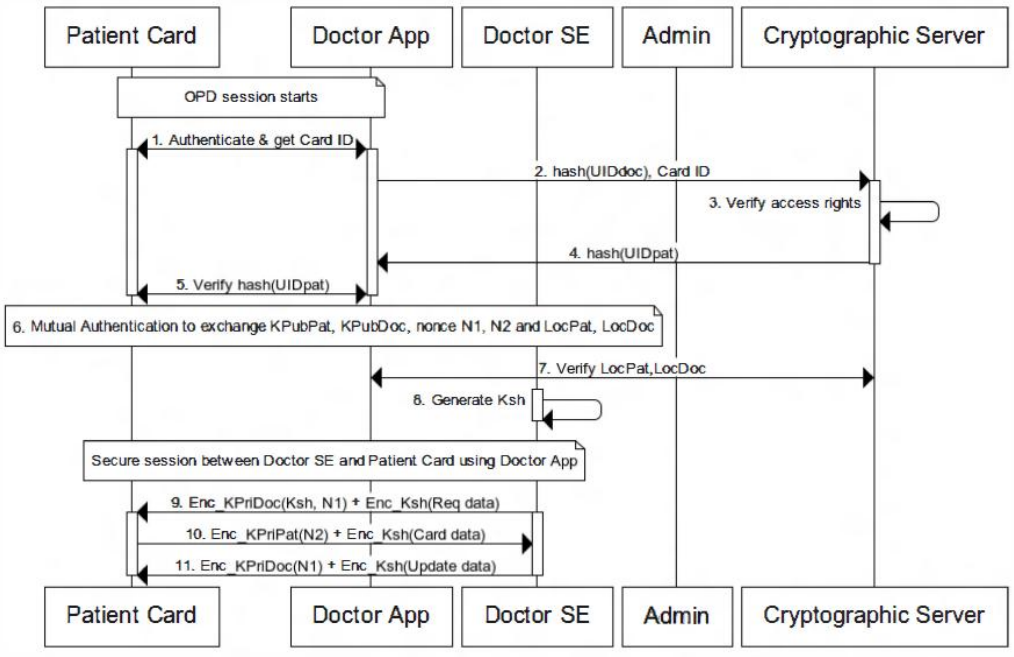

Fig.2: Security Framework.

7. CONCLUSION AND FUTURE SCOPE

In this work, we have proposed applications based on NFC enabled Android mobile devices for improving healthcare process for secure medical object identification and patient Health card on an external tag or mobile device itself. The applications are simple to use with a simple touch of NFC for secure communication. This will improve the health flow in crowded hospitals of developing countries like India as well as of developed nations. The business

model will benefit the patients as well as medical professional since.These techniques can be developed as NFC enabled mobile phone application to connect the application to a database.

ACKNOWLEGEMENT

We would like to thank our guide for his timely support and useful suggestions and all our colleagues who have helped us.We also extend sincere thanks to all the staff members of Department of Computer Engineering and Information Technology of our college.

REFERENCES

[1]. Vedat Coskun, Busra Ozdenizciand Kerem Ok, "A Survey on Near Field Communication (NFC) Technology", J. Wireless Personal Communications: An International Journal, vol. 71, pp. 2259-2294, 2013.

[2]. 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.

[3]. Ryan W. Gardner, SujataGarera, Matthew W. Pagano, Matthew Green, and Aviel D. Rubin, "Securing medical records on smart phones", Proceedings of the first ACM workshop on Security and privacy in medical and home-care systems, pp. 31-40,2009.

[4]. Lahtela, A., Hassinen, M.and .Iylha, V., "RFID and NFC in healthcare: Safety of hospitals medication care", IEEE proceedings on Pervasive Computing Technologies for Healthcare, pp. 241-244, 2008.

[5]. Saroj Kumar Panigrahy, Sanjay Kumar .lena, and Ashok Kumar Turuk, "Security in Bluetooth, RPID and wireless sensor networks", ACM Proceedings on 2011 International Conference on Communication, Computing Security, pp. 628-633,2011.

[6]. Sebastian Dunnebeil, Felix Kobler, Philip Koene, .Ian Marco Leimeister, and Helmut Krcmar, "Encrypted NFC Emergency Tags Based on the German Telematics Infrastructure", IEEE proceedings on Near Field Communication (NFC), 2011 3rd International Workshop, pp. 50- 55.IEEE Press, 2011.

[7]. Adam Marcusˆo Guido Davidzony, Denise Law, NamrataVenna, Rich Fletcher, AamirKhanz and Luis Sannenta, "Using NFC-enabled Mobile Phones for Public Health in Developing Countries", IEEE Proceedings on First International Workshop.

[8]. DivyashikhaSethia, Shantanu .lain and HimadriKakkar, "Automated NFC enabled Rural Healthcare for reliable patient record maintenance", Proceedings of Global Telehealth Conference, vol. 182, pp. 104-113, 2012.

[9]. Sasikanth Avancha, Amit Baxi, and David Kotz, "Privacy in mobile technology for personal healthcare", ACM Computing Surveys (CSUR), vol. 45 Issue I, article 3, 2012.