NFC Based Secure Mobile Healthcare System

Divyashikha Sethia[1], Daya Gupta[1],
Tanuj Mittal, Ujjwal Arora
Department of Computer Engineering
Delhi Technological University
New Delhi, India
[1] (divyashikha@dce.edu, dgupta@dce.ac.in)

Huzur Saran[2]
Department of Computer Engineering
Indian Institute of Technology
New Delhi, India
[2](saran@iitd.cse.ac.in)

***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 healthcare system with the help of Android based mobile devices with NFC [1] and Bluetooth interfaces, smartcard technology on tamper resistant secure element (SE) for storing credentials and secure data, and a HealthSecure service on a hybrid cloud for security and health record management. The main contribution of this paper is proposal of 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 have also briefly mentioned a basic security framework requirement for the applications. Since NFC NDEF format is prone to security attacks [2], we have utilized low level APIs on Android based mobile devices, to securely access NFC tags such as MIFARE Classic tags with NFC-A (ISO 1443-3A) 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. It can also provide portability of devices and usability for health management in emergency situation, overpopulated hospitals and remote locations.**

Keywords— mobile based secure healthcare; NFC in healthcare; e-Health card; medical object identifier; RFID; MIFARE Classic; java card; secure element; patient health record

I. INTRODUCTION

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.

Identification of objects for secure medical procedures is very essential for a secure workflow. For example, secure identifiers on the medicines can help healthcare professional to administer correct medication to a patient to reduce errors.

Along with this issue the Patient Health Record management is important both for patients as well as hospital management. In developing countries like India, there is no centralized management of health records and records are mostly retained by patients in a paper format OPD (Out Patient Department) card, which is both cumbersome to maintain along with the paper based reports and also unreliable. Work is still being done for a secure, electronic patient record management as a Healthcard on a Smartcard in developing countries like India [3] and other nations [4]. Most of the public healthcare services issue a Healthcard on a Smartcard, which retains just the primary information of the patient. All other records are stored on a centralized medical storage server. In developing countries like India, there are challenges like costly infrastructure, connectivity problem for accessing centralized medical records and acceptability of the Healthcard uniformly across different hospitals.

With the recent advancements in mobile devices involving secure credential storage, larger storage capability, wireless communication interfaces and computational power, they can be used in healthcare for not only gathering vital health parameters, as in the Body Area Networks, but also for healthcare management. Privacy and security is a very important aspect of healthcare [5].We propose that the patient should retain all or major patient's EHR electronically, on a Healthcard that is either on a external Smartcard accessible by a mobile device or on the mobile device retained by a patient. A Healthcard retained on a mobile device can retain the entire EHR including reports and tests. Permitted portion can be accessed securely by an authorized medical provider by a simple tap of mobile device. Due to the computational capabilities the records can be summarized and organized for a quicker action to be taken.

Healthcard on a mobile device can be helpful in developed countries also, where healthcare cost is high and privacy and security are critical. The patient can retain all records and can manage the privacy concerns of which portion of the records are to be accessible. The records can occasionally be synced to the central server for backup or storing past history. EHR on Healthcards retained by people can also help in providing the right care in an emergency situation when the patient is unconscious. It can also help determine location of the patient in case of emergency through location service on recent mobile devices. The business logic of using Healthcard on mobile devices can be beneficial to a medical professional since it can securely identify patients using simple portable mobile devices and also get a concise health report. A simple tap of NFC enabled mobile device, will not only improve the workflow of medical professionals but also prove to be beneficial in emergency and chaotic conditions like mass populated

978-1-4799-3635-9/14/$31.00 ©2014 IEEE

hospitals. Simplified workflows will result in faster and more efficient patient-doctor interaction.

The main contribution of this paper is proposal of a robust secure healthcare architecture using Android based mobile device with Near Field Communication (NFC) [1] and Bluetooth interfaces and smartcard technology on Secure Element (SE) for retaining security credentials and EHR. NFC is already being used for applications related to financial payments and ticketing. We propose a novel usage of NFC enabled mobile devices to access secure external medical tags for identifying medical objects like medicines and patient Healthcards. The Healthcard could be on an external tag or retained on the patient mobile device using NFC P2P or card emulation modes. This can provide greater control of sharing personal records with any authorized doctor by a simple tap of mobile devices. Bluetooth can be used along with NFC to provide faster access of bulky data from mobile device.

There is a strong cryptographic framework required for healthcare data. We have briefly mentioned the security requirement in section VII. However the detailed design, threat analysis, implementation and testing of the framework is still in progress and is beyond the scope of this paper.

The mobile devices and Healthcards can be authorized by a HealthSecure service on a hybrid cloud, to provide services for enhanced security and extended storage for health records. We plan to work on the architecture of the Healthsecure service in the future.

The paper is broadly divided into seven sections. Section II provides an overview of technologies for NFC, NFC tags, SE and Java Card. In section III we discuss about the proposed architecture. Section IV illustrates the implementation part followed by a brief overview of the security framework requirement in section V. In section VI we discuss briefly about some related work, followed by section VII which presents the conclusion and future work.

II. TECHNOLOGY

NFC [1] is an upcoming wireless technology which provides simple interfaces for device to device communication as well as access to NFC, RFID and smartcard tags [6]. 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 tags are of different types and use NDEF (NFC Data Exchange Format) [6] for storing and sending data. NFC tags must have a secure read and write access for critical applications such as those related to healthcare. NDEF provides no protection against data manipulation, overwrite protections and digital signature records cannot avoid malicious modification of tags [2]. Hence we utilize MIFARE Classic 1 K tags [7], which employ a proprietary protocol compliant to parts of ISO/IEC 14443-3 Type A, and write raw data using NFC-A (ISO 14443-3A) [8] properties for improved security. The MIFARE Classic 1K tag offers 1024 bytes of data storage, split into 16 sectors. Each sector is protected by two different keys, called key A and key B for secure access.

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, microSD card or a UICC (SIM) card [9]. Due to simplicity of accessibility we have used SWP enabled microSD card (by GO-Trust [10]) 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.

Java Card [11] is a technology which enables Java based applets to run on smartcards with very limited memory and processing capabilities and provides data encapsulation, firewall and cryptography. The smart card specification standards [12], ISO/IEC 7816 for contact and ISO/IEC 14443 for contactless, specify that communication between a host application and a smart card is done through Application Protocol Data Units (APDUs).

III. PROPOSED APPLICATION MODELS

We have proposed an architecture for NFC based secure healthcare as illustrated in Fig. 1 for i) secure medical identifiers as in flow steps 1.1 to 1.5 and ii) Healthcard retaining EHR using Android mobile devices as in flow steps 2.1 to 2.5. We have proposed a secure healthcare service like HealthSecure on a hybrid cloud to which all hospitals can subscribe. The HealthSecure hybrid cloud provides service for maintaining Cryptographic servers for secure framework and Storage server to provide backup as well as space for extended EHR. $Mobile_{ADMIN}$ is a mobile device of an authorized medical admin. $Mobile_{PAT}$ is the patient's mobile device with the Healthcard and $Mobile_{DOC}$ is the doctor's mobile device. Since a larger screen would be better suited to view and update the health records, $Mobile_{DOC}$ could either be an NFC enabled tablet, for portability, or a laptop with external smartcard reader. K_A and K_B are the read and write access keys respectively for a secure tag based on MIFARE Classic. For NFC P2P based and card emulation based Healthcards, we use patient's and doctor's set of public and private keys, which are K_{PUBPAT}, K_{PRIPAT} and K_{PUBDOC},K_{PRIDOC} respectively. A symmetrical shared key K_{SH} is used for encrypting data.

Hospital administration has an application for securely reading/writing with a mobile device, $Mobile_{ADMIN}$, to manage smartcard based tags and patient Healthcards. $Mobile_{ADMIN}$ can register with the proposed HealthSecure cloud service on a hybrid cloud, which can issue security keys for our architecture. The mobiles use SE and simple interfaces of NFC and Bluetooth for credential storage and communication. We discuss the architecture of the applications briefly in the following subsections and give the details of the implementation in section IV and security framework requirement in section V.

A. Secure Medical Object Identification using NFC Tags

Reliable medical object identifiers are important for reducing errors in the hospital workflow, like giving correct

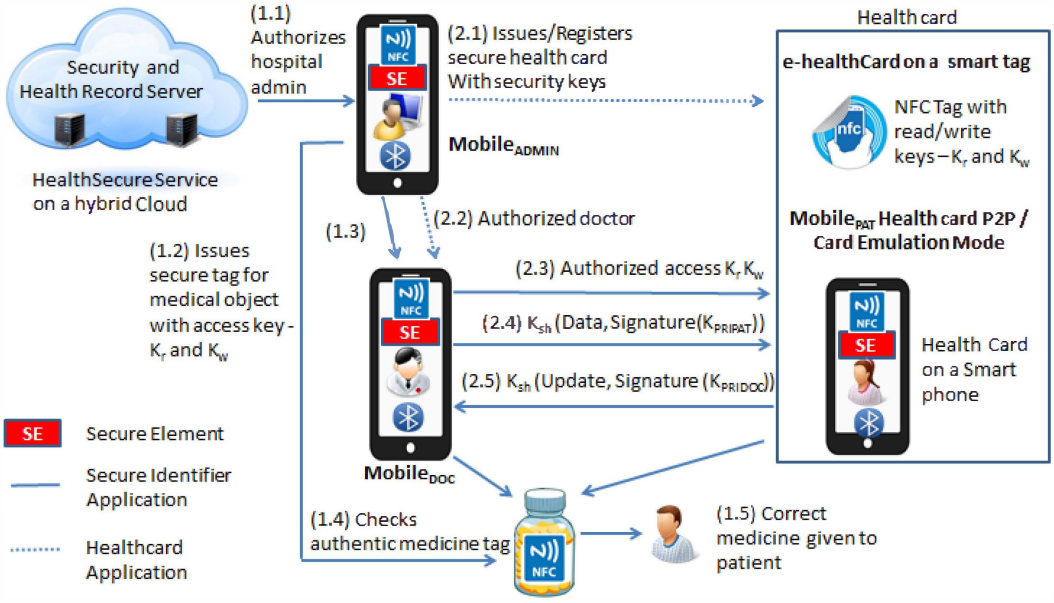

Fig. 1. NFC Based Secure Healthcare Architecture

medicine to a patient [13]. 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 MIFARE Classic. Bluetooth Low Energy (BTLE) stickers [14] 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 K_R for read access and a valid writer must have security key K_W for update access. The tag is issued by a healthcare admin mobile device, $Mobile_{ADMIN}$, which has registered to a HealthSecure service. 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. Fig. 1, steps 1.1 to 1.5, shows the workflow of secure tag identifiers in bold. Along with medical identification records, information related to timestamp can also be updated.

B. 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 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 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 $Mobile_{ADMIN}$. A 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 K_R and K_W 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.

C. e-Health Card based on P2P NFC mode

This application architecture is based on retaining a Healthcard on a mobile device using NFC P2P mode. The EHR 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 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, $Mobile_{ADMIN}$, to get secure keys. The patient's public and private keys K_{PUBPAT}, K_{PRIPAT} and doctor's public and private keys K_{PUBDOC}, K_{PRIDOC} 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

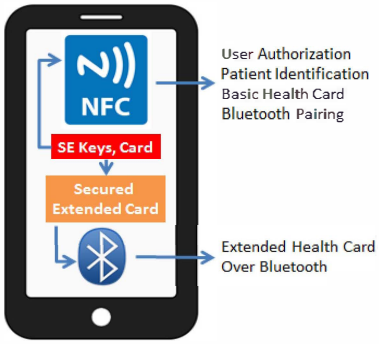

Fig. 2. Proposed Card emulation architecture

health record data. A basic security framework requirement is discussed in section V.

D. e-Health Card based on NFC card emulation

In this application architecture, Healthcard is retained on a mobile device using card emulation and Java card applets installed on the SE. We propose usage of a SE in the form of an SWP enabled microSD card as provided by GoTrust [10], which can be issued to the patient by HealthSecure service. Java Card applet can be used to authenticate and authorize the reader to access and update the health records using NFC SWP protocol. Since the SE has limited space, 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 $Mobile_{PAT}$ can be accessed externally by a PC/SC reader that is attached to $Mobile_{DOC}$. 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 [17]. Fig. 2 shows the proposed card emulation architecture. A basic security framework requirement is discussed in section V.

IV. 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 1K 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 [15], the installation can be done using custom Global Platform APDUs. Java card applets have been developed to store credentials for security framework and for card emulation mode.

Implementation of Security framework and hybrid cloud service is in progress and will be tested and deployed in the field in our future work.

V. SECURITY FRAMEWORK REQUIREMENT

There is a strong security framework required for the healthcare 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 [16]. The healthcare data can be large in size as in a Healthcard with entire HER in section III.D. 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 as in Figure 3. There is a requirement of confidentiality, integrity, mutual authentication, access control of EHR, privacy threats leading to identity thefts and insurance security breach [5].

The security framework involves various entities. A cryptographic server is used to generate, verify and store security keys. An administrator is present to issue Healthcards / tags and register patients/doctors. Mobile devices used by doctors are equipped with a Doctor App and a secure element (Doctor SE). Healthcard 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 [18]. 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.

We have suggested usage of Public Key Infrastructure (PKI) for the security framework. The security flow consists of 1. Healthcard personalization 2. Mutual Authentication between the patient and the medical doctor to assure the correct patient is appearing before an authorized doctor and there is no relay attack 3. Access control for data viewable by the doctor 4. Secure healthcard retrieval and updation.

There is an initial phase of personalization in which the Patient Card and the Doctor SE get a unique identification ID (UID_{PAT} and UID_{DOC}) and a set of public and private keys (K_{PUBPAT}, K_{PRIPAT} and K_{PUBDOC}, K_{PRIDOC}) from the security server based on the respective card ID and/or secure element ID. This phase ensures that both the Patient Card and the

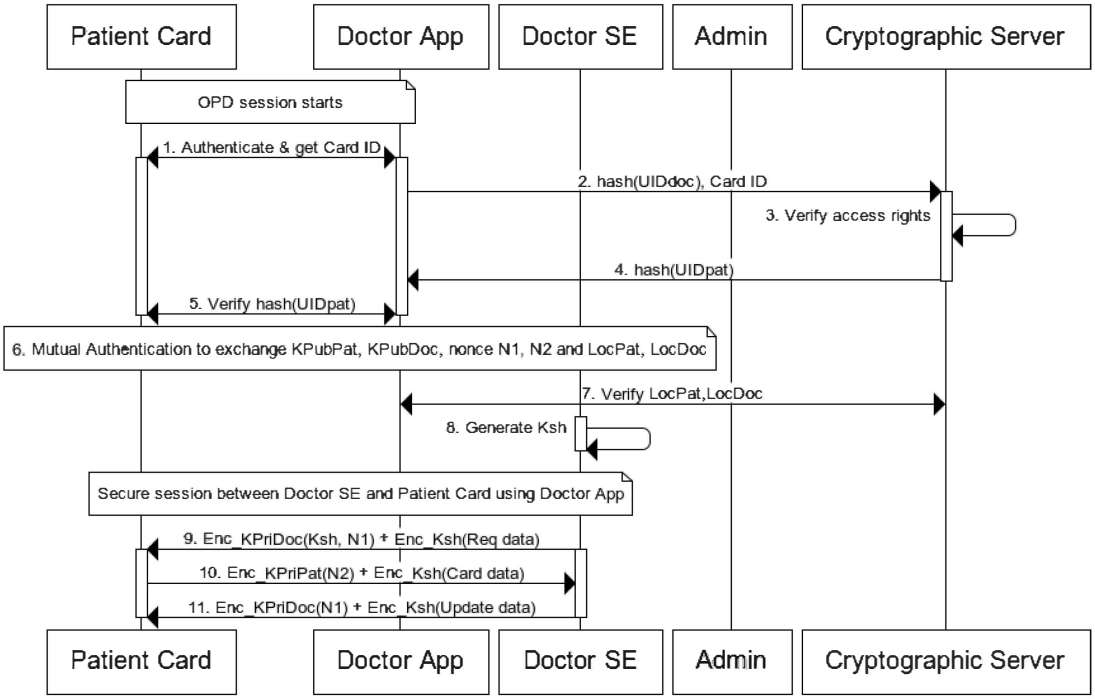

Fig. 3. Sequence diagram of basic security framework

Doctor SE have their respective UIDs and keys securely stored locally.

Now the OPD session can start between the patient and the doctor as detailed under Fig. 3. The Doctor App authenticates the Patient Card and retrieves the card ID. The card ID along with hash (UID_{DOC}) is sent to the server to verify access rights of doctor. Once verified, the server returns hash (UID_{PAT}), which is used to verify the authenticity of doctor by the patient. Now, as given in step 6, the patient and doctor mutually authenticate to exchange respective public keys, K_{PUBPAT}, K_{PUBDOC} and randomly generated nonce, N1 and N2 by patient and doctor SE respectively using algorithm suggested in [19], to prevent man in the middle attack. The location of patient is also shared with doctor, and with the help of server, validation is done to make sure both are same to avoid relay attacks. Loc_{PAT} and Loc_{DOC} could be GPS location or a related parameter in the ambience gathered from audio or light sensors on the mobile devices [20]. Now a symmetric key K_{SH} is generated by the Doctor SE for efficient encryption of health data and secure communication is held (steps 9 to 11). The doctor sends K_{SH} along with its request securely and receives the data. Similarly, an update, like a prescription, can be sent back securely to the Patient Card. A encrypted and signed data communications ensures confidentiality and integrity. This a basic framework requirement and we are working on designing a stronger framework as mentioned in section VII.

VI. Related Work

Emergency NFC tags [21] retain patient medical emergency information. But the work does not consider write protection and reusable NFC tags. NFC mobile devices have been used for storing credentials to be used for billing and identity [22]. We propose using it for healthcare applications with credentials and a much stronger security requirement since it is accessed by number of people and the quantity of data could be large. Smart poster [23] proposes using secure NFC tags since "NFC tags are vulnerable to spoofing as well as cloning", with a web server to securely retain the details of the poster. An application using NFC to track patients with pneumonia has been deployed in Karachi [24]. NFC based tags have also been used to tag medicines to reduce medical errors [13]. None of this work takes care of NFC tag security. We have suggested a novel manner of secure tags based on NFC-A protocol for our applications based on secure NFC tags. In our previous work [25] we have used NFC tags for reliable patient records and automating the health flow with Body Sensors. We have further expanded the work for new applications of NFC enabled devices for health flow data management with medical identifiers and Healthcards. The applications suggested in this paper for the improved workflow management with NFC enable mobile devices are unique to the best of our knowledge. Secure records can be stored on a mobile device for emergency purpose [18] using concept of shared keys. But they do not use any hardware tamper resistant device. Work has been done [17] for a wireless medical card with NFC and high speed interface with bulk memory card. Our work is different since we have proposed a similar larger card as in section III.D using a hardware tamper resistant SE based on a microSD card on a mobile device with NFC and Bluetooth interface.

VII. Conclusion and Future Work

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

Healthcard 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 they can use the commonly retained mobile devices conveniently. The cost of the architecture can be reduced by using microSD cards or UICC cards with inbuilt NFC antenna. These forms of SEs can be issued as Healthcards on mass scale to reduce the cost and to be operational on non NFC mobile devices. The proposed architecture can be used for applications other than healthcare with secure identifiers and secure transfer of large data between devices.

Although MIFARE Classic security algorithm Crypto1 has been broken [26], any other secure smartcard based tags like MIFARE DESIRE could be used in future based on the availability of the APIs. We have suggested a basic security framework requirement in this paper. A detailed design, implementation, testing and field deployment of the he security framework is in progress and will be addressed in our future work. We also plan to enhance the security framework using identity encryption using zero knowledge proofs and attribute based encryption for shared key management, access control of health data, and delegation of rights by patient to other trusted person for collection of health data. The current security framework is based on Public Key Infrastructure. Identity based Encryption and Attribute Based Encryption techniques can also be compared in future. We need to work on the security issues of NFC and Bluetooth for accessing secure Healthcard in future for security threats of theft, cloning, man in the middle and relay attacks and loss of a mobile device.

We plan to design architecture of the HealthSecure service on a hybrid cloud in the future with replicated Kerberos cryptographic servers and a Hospital Information System for backup of EHR. We also need to compare NFC and BTLE for card emulation. NFC has higher energy requirement, compared to BTLE, when it is in a reader mode to activate the passive tag. But NFC has an advantage of smoother interfaces and getting initiated by a simple tap, while BTLE requires pairing.

REFERENCES

[1] Vedat Coskun, Busra Ozdenizci and 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 J. Langer, "Digital Signature Records for the NFC Data Exchange Format", IEEE Proceedings of the Second International Workshop on Near Field Communication (NFC), pp, 71-76, 2010.

[3] Rashtriya Bima Yojana, http://en.wikipedia.org/wiki/Rashtriya_Swasthya_Bima_Yojan

[4] Smart Card Technology in U.S. Healthcare: Frequently Asked Questions, http://www.smartcardalliance.org/resources/pdf/Smart_Card_Technology_in_Healthcare_FAQ_FINAL_096012.pdf, 2012

[5] Sasikanth Avancha, Amit Baxi, and David Kotz, "Privacy in mobile technology for personal healthcare", ACM Computing Surveys (CSUR), vol. 45 Issue 1, article 3, 2012.

[6] NFC Forum Tedchnical Specifications, http://www.nfc-forum.org/specs/spec_list/ndefts

[7] MIFARE Classic 1K specification document, http://www.nxp.com/documents/data_sheet/MF1S50YYX.pdf

[8] NFCA on Android, http://developer.android.com/reference/android/nfc/tech/NfcA.html

[9] Mobile/NFC Security Fundamentals Secure Elements 101, http://www.smartcardalliance.org/resources/webinars/Secure_Elements_101_FINAL3_032813.pdf, 2013

[10] GO-Trust® Secure microSD Java, http://www.go-trust.com/products/microsd-java/

[11] Java Card™ Platform Security, http://www.oracle.com/technetwork/java/javacard/documentation/javacardsecuritywhitepaper-149957.pdf

[12] Smart Card Standards for contact and contactless interfaces, http://www.smartcardalliance.org/pages/smart-cards-intro-standards

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

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

[15] Global Platform Specifications, http://www.globalplatform.org/specificationscard.asp

[16] Why healthcare IT security is harder than the rest, http://www.csoonline.com/article/print/693941

[17] Stefan Krone, Bjoern Almeroth, Falko Guderian and Gerhard Fettweis, "Towards A Wireless Medical Smart Card", IEEE Design, Automation & Test in Europe Conference & Exhibition,pp 1483 – 1488, 2012

[18] Ryan W. Gardner, Sujata Garera, 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.

[19] Yun-Seok Lee, Eun Kim, and Min-Soo Jung, "A NFC based Authentication method for defense of the Man in the Middle Attack", 3 rd International Conference on Computer Science and Information Technology (ICCSIT'2013) January 4-5, 2013 Bali, Indonesia

[20] Tzipora Halevi, Di Ma, Nitesh Saxena, and Tuo Xiang, "Secure Proximity Detection for NFC Devices Based on Ambient Sensor Data", Computer Security – ESORICS 2012. Lecture Notes in Computer Science, vol 7459, pp 379-396, 2012.

[21] Sebastian Dunnebeil, Felix Kobler, Philip Koene, Jan 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.

[22] Gergely Alp´ar, Lejla Batina, and Roel Verdult, "Using NFC phones for proving credentials", 16th Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance. LNCS, vol. 7201, pp. 317-330. Springer Verlag, 2012.

[23] Jason Wu, Lin Qi, Ram Shankar Siva Kumar, Nishant Kumar, and Patrick Tague, "S-SPAN: Secure Smart Posters in Android using NFC", IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks, pp. 1-3, IEEE Press, 2012

[24] Adam Marcus_, Guido Davidzony, Denise Law, Namrata Verma, Rich Fletcher, Aamir Khanz and Luis Sarnenta, "Using NFC-enabled Mobile Phones for Public Health in Developing Countries", IEEE Proceedings on First International Workshop on Near Field Communication, pp. 30-35. 2009.

[25] Divyashikha Sethia, Shantanu Jain and Himadri Kakkar, "Automated NFC enabled Rural Healthcare for reliable patient record maintenance", Proceedings of Global Telehealth Conference, vol. 182, pp. 104-113, 2012.

[26] Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia, " A Practical Attack on the MIFARE Classic", Smart Card Research and Advanced Applications. LNCS, vol. 5189, pp. 267—282, 2008.