NFC-Based Secure Mobile Healthcare System

Madhura PM, Palash Jain, Harini Shankar
Department of Information Science, Visveswaraya Technical University, Bangalore-60
madhura.manjunath7@gmail.com, palashjain2801@gmail.com, harini_27oct1994@hotmail.com

ABSTRACT-Near Field Communication (NFC) is a wireless communication standard which enables two devices in a short range to establish a communication channel within a short period of time through radio waves in the 13.56 MHz frequency range. A secured and an efficient architecture for improving healthcare system, uses Android based mobile devices with NFC smartcard technology on tamper resistant Secure Element (SE) and a Health Secure service on a hybrid cloud for security and health record management. In this work, we propose NFC cards (MIFARE classic cards) that are equipped with internal memory, which provide the potential advantage of improving patient's identification by eliminating the paper based documentation work. 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.

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. The advancement of science and technology in the field of healthcare has improved the quality of people's lives. At the same time mobile phones are gradually adopted for solving some tough healthcare issues. The purpose of this project entitled 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 using NFC's promising features. As NFC cards are equipped with internal memory, patients can have critical information stored on their NFC card for fast access in critical situations. This information can vary and can be configurable. Information such as blood type and allergies can be stored as critical fast access data. This paper proposes a novel usage of NFC enabled mobile devices to access secure external medical tags for identifying medical objects like medicines and patient Health cards. The Health card could be on an external tag or retained on the patient mobile device using NFC Peer to Peer(P2P) or card emulation modes. The business logic of using Health card 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. Simplified workflows will result in faster and more efficient patient-doctor interaction.

II. NFC TECHNOLOGY

NFC is an upcoming wireless technology which provides simple interfaces for device to device communication as well as access to NFC, Radio Frequency Identification(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 tags are of different types and use NDEF (NFC Data Exchange Format) for storing and sending data. We utilize MIFARE Classic 1K tags, 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) properties for improved security. The MIFARE Classic IK 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 is Java Card 2.2.2 compliant. Java Card 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[1]. The smart card specification standards, 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). It is compliant to work on Android 2.3.3 and above.

III. PROPOSED ARCHITECTURE

We have proposed an architecture for NFC based secure health care as illustrated in Fig. 1 for i) secure medical identifiers as in flow steps 1.1 to 1.5 and ii) Health card retaining EHR using Android mobile devices as in flow steps 2.1 to 2.5. We have proposed a secure healthcare service like Health Secure on a hybrid cloud to which all hospitals can subscribe. The Health Secure 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 Health card 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 Health cards, we use patient's and doctor's set of public and private keys, which are Kp_{UBPAT}, Kp_{RIPAT} and Kp_{UBDOC}, Kp_{RJDOC} 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 and the details of the implementation in section IV.

A. NFC Tags Utilization for Secure Medical Object Identification

It is important to reduce errors in the hospital workflow using Reliable medical object identifiers, such as giving correct medicine to a patient. We propose architecture of an application for issuing secure identifiers to reduce the error

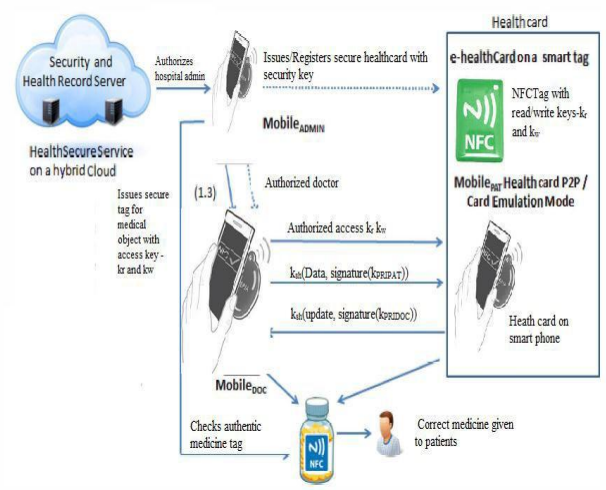

Fig.1: Architecture of NFC based mobile healthcare system

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 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. 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. NFC Tags in e-Health Cards

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. 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 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.

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 Kp_{UBPAT}. Kp_{RJPAT} and doctor's public and private keys Kp_{UBDOC}, Kp_{RIDoc} 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 information.

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 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. 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.

IV. IMPLEMENTATION

Applications have been developed 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 latest android phones. We have used MIFARE Classic for reading and writing data using APIs in Android framework (Android 2.3.3 and above).The memory of this card is 1Kb. 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, which provides a microSD based Java Card 2.2.2 solution. The card supports 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 an ASUS Zenfone 2 mobile device with Android 4.1.2. The card can be accessed from an authorized Android application. Since the card supports Global Platform 2.1.1, 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.

The healthcare data can be large in size as in a Health card with entire EHR in section. 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. 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 and authenticate Healthcards / tags and register patients/doctors. Mobile devices used by doctors are equipped with a Doctor App and a secure element. Healthcard used by patients is called Patient card which in this case is using a NFC P2P or card emulation mode. Since the health card could be accessed by various persons: patient, medical professional and emergency person. There could be a separate Doctor PIN for doctor and a super key for emergency team when patient is unconscious. 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 get a unique identification ID (UID_{pat} and UID_{doc}) and a set of public and private keys (K_{pUBPAT}, K_{pRIPAT} and K_{pUBOOC}, K_{pRIDoc}) which are stored locally in the security server based on the respective card ID and/or secure element ID. An encrypted and signed data communications ensures confidentiality and integrity.

V. MEDICAL USE CASES OF NFC

There are a lot of use cases for NFC in medical devices and healthcare. The possible areas include monitoring and management of home based care. The application includes monitoring systems for a variety of chronic diseases, including but not limited to diabetes, hypertension, cardiac diseases (infarctions, heart failure, arrhythmias and other rhythm abnormalities), pulmonary diseases like asthma and COPD, and neurological abnormalities like seizures, chronic renal failure, etc. For example, a biometric device called ―MiniME‖ developed by Ergonomidesign monitors various vital parameters like ECG, blood pressure, heart rate, pulse oximetry, body temperature, blood glucose, cholesterol, haemoglobin and prothrombin time, and transmits the data using NFC to the cloud.

Another company working on medical devices with NFC embedded in them is Impak Health. They are involved in home-based cardiac, pulmonary and sleep monitoring. They have incorporated NFC in devices such as ―RhythmTrack‖ that tracks a person's ECG, and ―SleepTrack,‖ which tracks the sleep cycle and duration. Similarly, FITBIT – a fitness monitoring company – has incorporated NFC for transferring details like calories burned, number of steps taken and other details from a wristband to the user‘s smart phone which houses a user-friendly application. Gentag, a company specializing in mobile health, is using NFC to transfer data from devices ranging from diagnostic assays to skin patches. Nedap, a Netherlands-based security and identification specialist, has rolled out 50,000 NFC phones for nurses. They are used for recording home visits for the elderly. NFC is becoming widely accepted for medical devices in some markets specifically in the developed countries. Sony Corporation has developed an NFC Healthcare Library which enables communication between healthcare products embedded with the NFC Dynamic Tag (FeliCa Plug) and healthcare applications installed on smart phones. This library is available free of charge for a number of OS, including Windows, Linux and Android. Companies like Omron, Terumo and A&D are incorporating Sony‘s solution into their devices like BP monitors, pedometers, blood glucose meters, etc. Various other companies like Qolpac and Identive WPG have brought NFC into the mainstream with uses ranging from medication compliance to X-ray image sharing.

CONCLUSION

Near field communication can be extremely beneficial in the modern era of technology. It is interactive and secure which does not require any special software to run on. It is also more intuitive, making it a good candidate for use in the home-based monitoring and management domain, particularly among the elderly. 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 system has improved access to patients' medical history and improved medical checkups by automatically updating information and access to the entire patient's medical records. This will improve the health flow in crowded hospitals of developing countries as well as of developed nations. While it is still at the fringes and is waiting for its big break, NFC is being increasingly adopted by a number of organizations. Certain security-related concerns need to be allayed and the solutions developed around NFC have to be demonstrably secure. Taking all these factors into consideration, it is reasonable to conclude that NFC is a promising technology. Adoption of NFC in medical devices will help increase the security and ease of data transfer between medical devices and also provide personalized healthcare.

REFERENCES

[1] Divyashikha Sethia, Huzur Saran, **"NFC Based Secure Mobile Healthcare System",** IEEE Transactions on Communication Systems and Network(COMSNETS), Jan 2014.

[2] A Devendran, Dr. T Bhuvaneshwari, Arun Kumar Krishnan, **"Mobile Healthcare System using NFC technology",** International Journal of Computer Science Issues(IJCSI), May 2012.

[3] Ketan Bhadoriya, Rajshekar Humbe, Yogesh Kodgire, S.G. Phule, **"NFC Based Healthcare System",** International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 6, 2015.

[4] Bankar Karthik, Joshi Bhargav, Mungal Mahajan, Subhash Rathod, **"NFC Based Android API Healthcare System",** Multidisciplinary Journal of Research in Engineering and Technology, March 2015.

[5] Prasad S. Halgoankar, Vijay M. Wadhai, **"NFC based Healthcare System for Mobile Prescription",** International Journal on emerging trends in Technology(IJETT), September 2015, Volume 2, Issue 2.

[6] Divyashikha Sethia, Daya Gupta, Tanuj Mittal, Ujjwal Arora, Huzur Saran, **"NFC Based Secure Mobile Healthcare System",** IEEE Transactions on Communication System and Network(COMSNETS), Jan 2014.

[7] Sanjana H.D, Gopika Priyadarshini, Yamini Gadidam, Shruthi B, Vikranth B.M, **"NFC Based Secure Mobile Healthcare System",** Journal of Emerging Technologies and Innovative Research(JETIR), April 2015, Volume 2, Issue 4.

[8] Danco Davcev, Goran Jakimovski, **"Ergonomics design of Healthcare NFC-based System",** International Conference on Applied Human Factors and Ergonomics (AHFE 2015).