TECHNEX | SVPCET- Hackathon

Team Hackk

Digital Medical Record (DMR) Using NFC

Team Members- -Harshal Dawande -Arpit Dalal
-Avish Rangari -Tushar Mankar

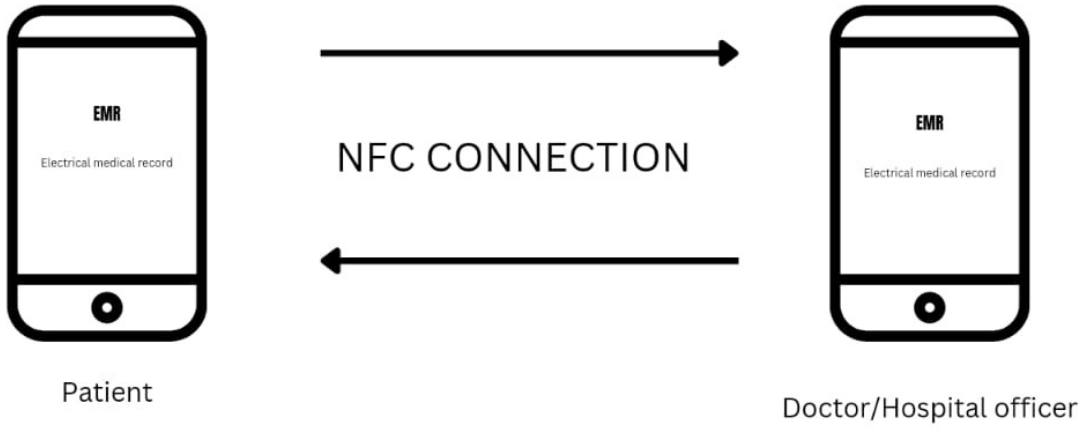


Fig 1- NFC based DMR Architecture

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. NFC technology allows off-line data transfer between mobile phones. In addition NFC also has a secure element section that allows it to store data securely. Through special applications the data can be modified by the authorized party using an authentication system. In this hackathon a Digital Medical Record was developed by our team using NFC technologies.

I. Introduction

Robust healthcare is required in both developed countries, where healthcare costs are high and security and privacy are critical concerns, and developing countries such as India where despite of affordable services the quality of service provide provided is low. Science and technology advancements in the field of healthcare have improved people's lives. Simultaneously, mobile phones are gradually being used to solve some difficult healthcare issues. The goal of this project, DIGITAL MEDICAL RECORD USING NFC, is to computerize the front office management of a hospital in order to develop software that is user friendly, simple, fast, and cost effective by utilizing the promising features of NFC. Because NFC cards have internal memory, patients can store critical information on their NFC card for quick access in emergency situations. This information can change and is customizable. As critical fast access data, information such as blood type and allergies can be stored. This paper suggests a novel application of NFC-enabled mobile devices to access secure external medical tags for identifying medical objects such as medicines and patient health cards. The Health card could be stored on an external tag or on the patient's mobile device via NFC Peer to Peer (P2P) or card emulation modes. The business logic of using a Health card on mobile devices can be advantageous to a medical professional because it can securely identify patients using simple identification methods.

Medical Record

A Medical Record is a file containing records and documents about the patient containing identity, examination, medication, other medical treatment in health care facilities for outpatients, hospitalized by both government and private. The benefits of medical records include medicinal purposes, improvement of service quality, education and research, financing, health statistics, as well as legal, discipline, and ethical proofs. The need for a practical, complete, and accurate medical record becomes an urgent need in today's healthcare services. The practicality of medical records, among others, can be seen from the media used in storing medical record data, the process of updating medical record data, and the process of reading medical records. Medical records are also required to contain complete information about the patient's medical history. Data on medical records is used as a reference of medical personnel in dealing with patients therefore this data must be accurate. Three properties of medical records are difficult to meet by conventional medical records by using paper as the medium.

II. 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. MobileADMIN is a mobile device of an authorized medical admin. “Mobile-P” is the patient's mobile device with the Health card and “Mobile-D” is the doctor's mobile device. Since a larger screen would be better suited to view and update the health records, MobileDoc could either be an NFC enabled tablet, for portability, or a laptop with external smartcard reader. KA and KB 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 KpUBPAT, KpRlPAT and KpUBDOC, KpRJDOC respectively. A symmetrical shared key KSH is used for encrypting data. Hospital administration has an application for securely reading/writing with a mobile device, MobileADMIN, to manage smartcard based tags and patient Health Cards. MobileADMIN 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’

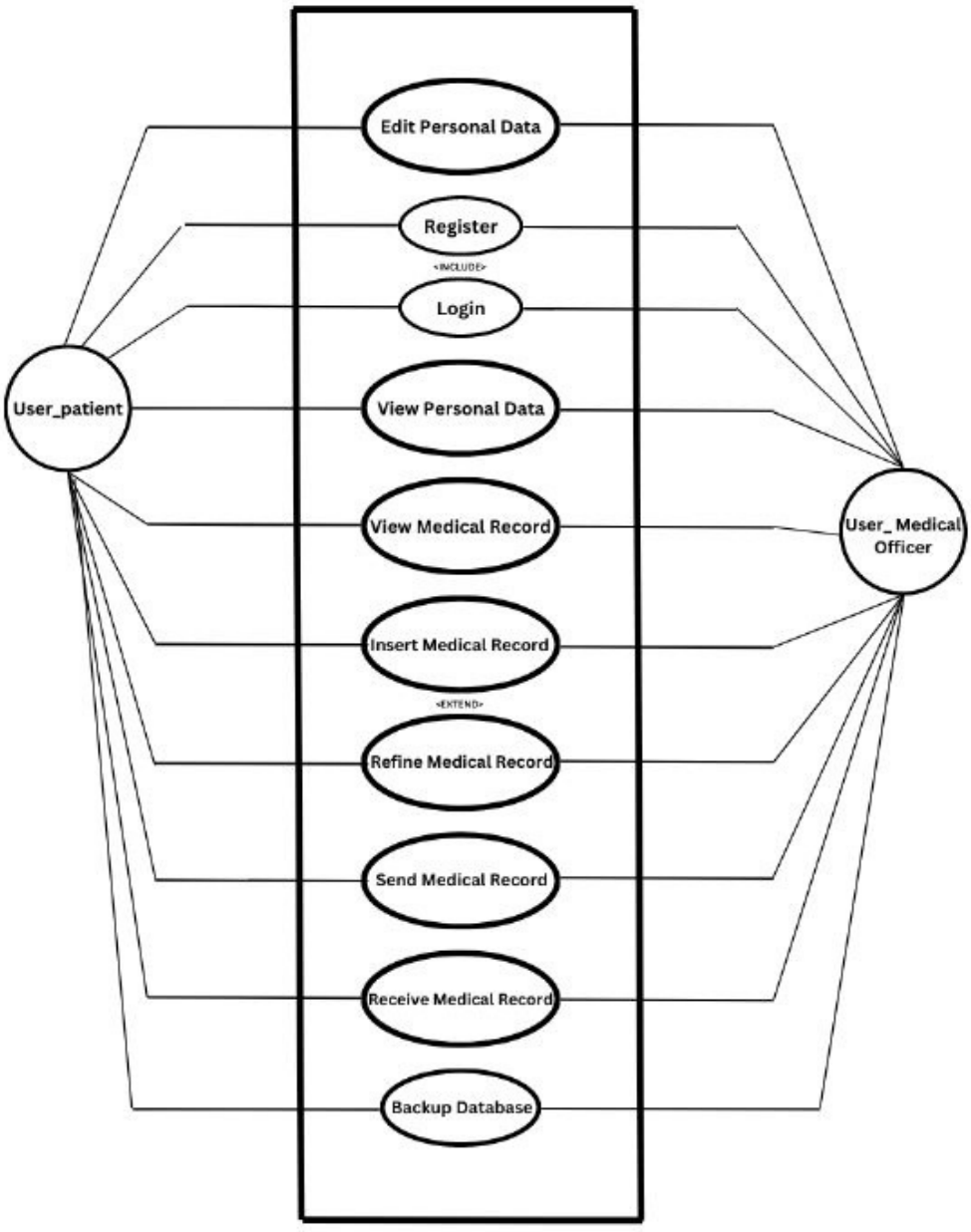
A. NFC Tags Utilization for Secure Medical Object Identification It is important to reduce errors in the hospital workflow using Reliable medical object identifiers, such as giving correct medicine to a patient. We propose architecture of an application for issuing secure identifiers to reduce the error 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 KR for read access and a valid writer must have security key KW for update access. The tag is issued by a healthcare

admin mobile device, MobileADMIN, 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 showing 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 the 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 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 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. 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 a 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 Health Card on a mobile device using NFC P2P mode. The EHR is retained on the mobile device in a secure region instead of the 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, MobileADMIN, to get secure keys. The patient's public and private keys are 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. 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 MobilePAT can be accessed externally by a PC/SC reader that is attached to MobileDOC. Since the SE has limited space, an extended card consisting of past records and other health information, like images and documents.



III. Implementation

Applications can be developed for both Android devices using Android APIs, and administrative servers, using PHP and MySQL, for secure, reliable and robust healthcare systems. Implementation of the 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 the 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 can be used to generate, verify and store security keys. An administrator bot will be present to issue and authenticate Health Cards / tags and register patients/doctors. Mobile devices used by doctors are equipped with a Doctor App and a secure element. A Health Card used by patients can be called a 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 the doctor and a super key for the emergency team when the patient is unconscious.

The security flow consists of

1. Health Card 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 health card retrieval and updation.

There is an initial phase of personalization in which the Patient Card and the Doctor get a unique identification ID (UIDpat and UIDdoc) and a set of public and private keys (KpUBPAT, KpRlPAT and KpUBOOC, KpRIDoc) 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.

IV. 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 —MiniMEll developed by Ergonomidesign monitors various vital parameters like ECG, blood pressure, heart rate, pulse oximetry, body temperature, blood glucose, cholesterol, hemoglobin 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 —RhythmTrackll that tracks a person's ECG, and —SleepTrack,ll 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 smartphone 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. 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 and healthcare applications installed on smartphones. 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.

We plan to make use of this library provided by Sony in our device and enable native access and reporting of results directly in the form of Near Field Communication.