IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 3, March 2016.
www.ijiset.com
ISSN 2348 – 7968

NFC Based Health Care System

Prof. Rupali Chopade[1], Punam Deshmukh[2], Kavita Kamble[2], and Dhanashri Nazarkar[2]

[1]Information Technology Department, MMCOE,
Pune, Maharashtra, India.
[2]Information Technology Engineering, MMCOE, Savitribai Phule Pune University,
Pune, Maharashtra, India.

Abstract

Mobile devices are largely used in almost every aspect now-a-days as they are easy to carry and access. Considering this large use of mobile phones, it will be helpful to use it in healthcare system to make the medical data easy to carry, accessible, manageable and will increase the efficiency. For this android based mobile device with NFC smartcard technology can be used for storing credentials and securing the data, to create Health Secure service on a hybrid cloud. This can be achieved using the system including -
i) Secure Medical Tags for reducing medical errors and
ii) Secure Health card for storing Electronic Health Record.
This system can benefit both the patient and the 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: Digitized record, Electronic Medical Record (EMR), Near Field Communication (NFC), NFC reader, Patient health record, secure medical tags.

1. Introduction

Mobile phones now-a-days are largely used in almost every part of our life as they are easy to carry and are easily accessible [16]. They can always be available with the patient and are location aware. Considering this large functionality of mobile phones, it will be helpful to use it in healthcare system to make the medical data easy to carry, efficient, accessible, and manageable. So that the patients can use mobile phones for self-help or communication with a doctors. Or doctors can use it to monitor the health of the patient with the use of portability of health records.

For this NFC (Near Field Communication), which is an upcoming technology that has proven to be reliable and secure can be used for storing health credentials and securing the data [11]. This can be achieved using the system which includes- i) Secure Health card for storing patient id and ii) Server which stores Electronic Health Record. This system can benefit both the patient and the doctors by providing a robust and secure health flow. It can also provide portability to devices and provide usability for health management in emergency situation, to overpopulated hospitals and remote locations.

1. WHAT IS NFC?

NFC (Near Field Communication) is a short range wireless RFID technology. NFC makes use of interacting electromagnetic radio fields in mobile phones. Near Field Communication (NFC) is a set of standards for portable devices. It allows establishing the peer-to-peer radio communications [14]. If your phone has NFC then it could be used to transfer data to other phones or to NFC readers [2].

2. Difference between RFID and NFC:

RFID	NFC
Frequency range 13.56 MHz (High freq) and 902-928 MHz ultra-high frequency.	Operates at frequency 13.56 MHz.
One way communication.	Two way communication.
Can be used for communication between devices at a distance upto 1m.	Limited to close proximity communication (10 cm).
Tags can be scanned simultaneously	Tags cannot be scanned simultaneously.
Are not available in mobile phones	These are available in mobile phones.

3. APPLICATIONS OF NFC:

NFC is a simple and mobile feature which can transfer small amount of data between two devices [12]. It can be used for simple operations, such as making payments or sharing information. Following are the areas where it is being used [1]:

ISSN 2348 – 7968

1. It can help with the problem of split bills
NFC enables you to pay for anything like a cab, dinner or almost anything else with a tap. Which means even if you forget your wallet, you can easily do the payment by transferring funds between devices with a quick tap.

2. It could be used as your bus or train ticket
NFC can make your phone become your ticket for train, bus or ferry. For this to happen all you can do is swipe your NFC device when you're boarding and again when you hop off. Using this you can get rid of cards or passes. Your mobile holds your ticket details and allows you to go on and off the train.

3. It can remember passwords for you

Passwords are usually long, complicated and difficult to remember. Therefore instead of remembering which letters are capital and where the numbers are, NFC technology can be used for scanning and logging a device onto a network. Users can use this technique to connect to Wi-Fi without typing password by tapping the devices against each other so as to connect to internet.

4. It can be used connect phone to car

A car radio which is Bluetooth-compatible can be used with an NFC tag. You can modify it to connect to your phone, play your favorite song playlist or for turning on Google Maps. This means you don't have to touch your phone while you are driving it is synced up and plays your favorite songs or tells you when to take a turn.

5. Improve your tourism experience

NFC can provide guidance to tourists around a city. They can tap their devices to tags which will give them information about important landmarks, download maps. This technique doesn't require Wi-Fi and it can easily transfer small bits of data to keep tourists informed.

4. Threats to NFC data and their respective solution [3]:

Existing systems for NFC based healthcare are vulnerable to attacks such as spoofing, identity theft or man-in-the-middle attack [7] but some systems had benefit of tale monitoring and tracking of patients. These systems are hence useful for technically unskilled patients also. Hence our problem is to find secure and automotive solution by developing a system which will reduce the difficulty in the maintenance of healthcare records of patients for any hospitals, providing facility for medical owners to view patient's prescription. This system will be beneficial for technically unskilled patients also as everything is accessible by a NFC card also it is secured. Various actors of this system such as patient, doctor, admin can easily access the data for reading, changing or adding data.

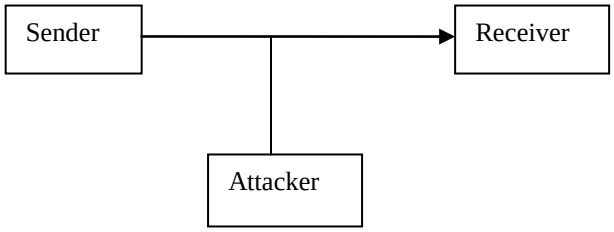
4.1 Eavesdropping:

As NFC is a wireless communication media eavesdropping is an important issue. For communication between two devices via NFC, RF waves are used. An attacker can use an antenna to receive the signals being transmitted. Either by experimenting or by traffic analysis the attacker can leak the required data. The devices required to receive the RF signal as well as the devices required to decode the RF signal must be assumed to be available with an attacker.

Solutions:

1. Note down the RF filed characteristic of the given sender device

2. Setup of the area where the attack is performed.



4.2 Data Corruption:

* Data modification

* Data insertion

In this attack rather than just listening, an attacker can also try to modify the data which is transmitted via the NFC interface. Hence the receiver will not able to understand the data sent by the sender.

Solution*:* Securing the data using data encryption.

4.3 Important solution- key agreement:

This solution is a method whereby two or more participants can agree on a key. If properly done, this removes undesired third party attacks. This does not reveal

ISSN 2348 – 7968

to any eavesdropping third party which key has been agreed upon. Two keys public and private are used. The Public Key is made available to everyone through a publicly accessible data repository or directory. On the other hand, for the Private Key it must to remain confidential to its respective owner.

5. Securing NFC data from attacks:

Existing systems for NFC based healthcare are vulnerable to attacks such as spoofing or identity theft. Hence our problem is to find secure and automotive solution by developing a system which will reduce the difficulty in the maintenance of healthcare records of patients for any hospitals, providing facility for medical owners to view patient's prescription. This system will be beneficial for technically unskilled patients also as everything is accessible by a NFC card and also data will be secured.

We are proposing an application which will make use of SHA (Secure Hash Algorithm) algorithm, for creating Secure Medical Tags for reducing medical errors and providing Secure Health card for storing Health Records (HR) [15]. It can also provide portability to devices and usability for health management operations in emergency situation, which is beneficial for overpopulated hospitals and remote locations.

2. Related Work

Mobile devices are personal; they always remain with the patient and they are location aware. The patient can use mobile devices for self-help or communicate with a professional or to monitor the health of the patient [8]. This makes the cell phone a much more appropriate device for handle healthcare than any other media.
When the number of patients is large, difficulty is to reliably maintain the patient records and also have simple automated mobile phone applications for healthcare helpers to use. Therefore an automated healthcare architecture can be used in NFC-enabled mobile phones [13] and patients having their patient ID .NFC-enabled mobile phones can read the patient's ID, followed by automated gathering of healthcare important health parameters, analysis of the information and transmission of it for expert feedback. This automation in health records processing can provide time efficient and reliable health consultation anytime anywhere [9].
Patient identification is the most basic and important requirement in clinical workflows regardless of whether the documentation is done using a computer or pen - paper or a combination of both. Today many computer based systems exists for the medical documentation and patient identification. These health systems are usually based on bar-codes, RFID or NFC tags. The objective of our project is to develop a system which will bring automation and efficiency in managing medical records in an electronic format by ensuring security. Since the health card could be accessed by various persons: patient, medical professional and emergency person, the system could make use of the concept of shared key based on Attribute Based Encryption [8], or Hash algorithm such as SHA.
This an architecture for improving healthcare system with the help of Android based mobile devices with NFC, smartcard technology can be used for storing health credentials and secure data, and a Healthcare service on a hybrid cloud for security and health record management. This method is useful for secure health card for storing Electronic Health Record (EHR) is based on the concept of Secure NFC Tags, mobile device using NFC P2P Mode or Card Emulation Mode.
Reliable medical E-health systems are important and useful for reducing errors in the hospital workflow, like giving correct medicine to a patient [4].
Healthcare recode maintenance is very difficult for any hospital, hence we are going to develop E-healthcare system for maintaining all patients' records and we are providing security for patient records [17]. EMRs system makes the entire process of patient medical records keeping easier, accurate and comprehensive, and more efficient. With the use of an EMR system, doctors use specialized software that allows them to enter their patient's records electronically.
This Healthcare medical card 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 [5].
This software will store the patient's medical information on a server and also each patient's complete history will be available instantly, including digitized copies of lab results, prescriptions created and other necessary medical information. Physicians can use their mobile phone, desktop, laptop, to take a look through their patient charts and record notes.
Doctors or Nurses will use the mobile phone with NFC so that its sensors will send the details to microcontroller, and we can see the details of patient record through PC.

1. Proposed System Architecture-

ISSN 2348 – 7968

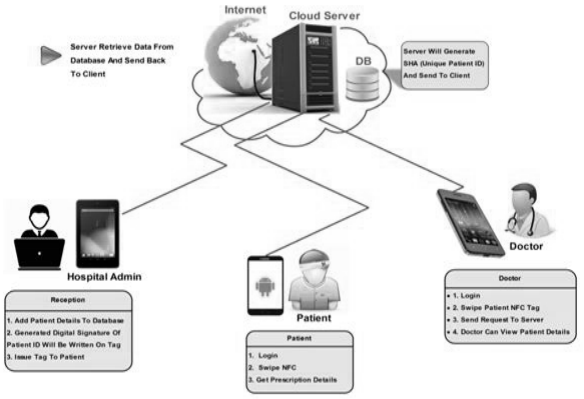


Fig.1 Proposed system architecture

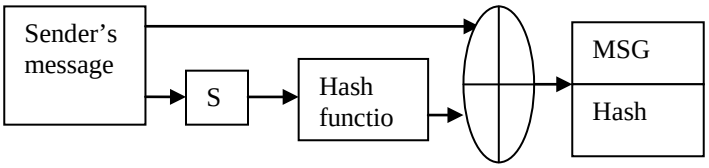
2. Work flow of diagram:

1) When patient wants to register himself for NFC healthcare service, admin will note down all his details, and then patient id will be generated by SHA algorithm.
2) While a person gets Admit or Visits the hospital, the health records of that person will be accessed through their NFC tags which will be synchronized as well as stored temporarily on that particular hospital Electronic Medical Record (EMR) Database. Because of this the doctors can easily access full information about the patient by viewing the patient EMR instead of going through bundle of paper reports.
3) If the patient is been asked to take any tests then those test reports will also be updated in that EMR.
4) Based on the test the updates which the doctor prescribed will be updated too in their EMR.
5) While the patient Leave/Discharge all those information which have been updated in his EMR will be synchronized and the data is transferred back to his NFC tag which will hold the complete medical report about what happened that particular day.

3. Need of SHA-1

Masquerade – Insertion of message from unauthorized source
Content Modification – attacker changes contents of message
Sequence Modification – Insertion, deletion and reordering of sequence
Replay – sending same message multiple times with bad intension

Basic hash function diagram-



Where s- secure key

1. SHA-1 steps [10]:

Step 1: Appending padding bits
Message is "padded or appended" with a 1 and as many 0's as necessary to make the message length of 64 bits less than an even multiple of 512.

Step 2: Append Length
Padded message is appended with 64 bits the end of the. These bits have the binary format of 64 bits indicating the length of the original message.

Step 3: Divide the inputs into 512 bit blocks
A ⟶ 01 23 45 67

B ⟶ 89 AB CD EF

C ⟶ FE DC BA 98

D ⟶ 76 54 32 10

Step 4: Prepare Processing blocks
Round 1: (B AND C) OR ((NOT B) AND D)

Round 2: B XOR C XOR D

Round 3: (B AND D) OR ((C) AND (NOT D))

Round 4: C XOR (B OR (NOT D))

2. Important properties of SHA:

- Every hash value is unique but always repeatable. It means that the word 'cat' will hash to something that no other word hashes to, but it will always hash to the same thing.
- The hash function is 'one way', which means that you can create hash of any word but cannot create original word using hash; hence it is more secure than any other security algorithm.
- Difficult to modify a message without changing its hash value.

ISSN 2348 – 7968

- No two different messages can have the same hash value.

3. Reasons for using a hash or message digest:

- For increased efficiency: The signature is much shorter and thus saves time since hashing is generally much faster than in practice.
- For compatibility of various forms of documents: Messages are typically bit strings, but some signature detection schemes operate on other domains such as arbitrary input.
- For integrity: for any other algorithm except the hash function, the data to be signed may have to be divided (separated) in blocks which are small enough for the signature algorithm scheme to act on them directly. But, the receiver is not able to recognize if all the blocks sent by the sender are present and they are in the appropriate order.

4. Digital signature:

We can create digital signature of patient id for adding more security. A digital signature is a mathematical scheme for maintaining the authenticity of a digital message or a document. A valid digital signature ensures recipient to believe that the message was created and sent by a known or authorized sender, and that it was not altered while transmission. Digital signatures are commonly being used for financial transactions, and in other places where it is important to detect forgery or eavesdropping.
Using digital signatures private key remains secret. Also, some schemes offer digital signatures a time duration (stamp), so that even if the private key is exposed, the signature is valid.

A digital signature method typically consists of three algorithms:

- In key generation private key is selected by algorithm uniformly in random order from a set of combination of possible private keys. The algorithm gives the private key and its respective corresponding public key.
- A signing algorithm which produces a digital signature when given a message and a sender's private key.
- A signature verifying algorithm that accepts or rejects the messages which claims to be authentic, given a message, public key and a signature.

4. Conclusions

Hence we can conclude that in this system the patient identification will be done using NFC card. Whole data will be stored in the server. The server will store the data of multiple patients. Using this system the user will be able to read his own medical records and/or test reports. The doctors can use this system for reading, adding and updating patient's records. Also it can be used by the medical persons for reading prescription and providing medicines as per it. In this way this system will bring automation in healthcare systems using electronic record maintenance.

.

5. References

[1] V.cooskum; Istanbul, turkey; m. n. aydin; b. ozdenizci "Benefits and future direction of nfc services" ieee 2-4

[2] Nov 2010. *a* devendran , dr t bhuvaneswari and arum Kumar Krishnan, "mobile health care system using nfc technology",ijcsi international journal of computer science issues, vol. 9, issue 3, no 3, may 2012.

[3] Klemens breitfu and ernst haselsteiner "security in near field communication (nfc)".

[4] Lahtela, a., bassinet, "rfid and nfc in health-care: safety of hospitals medication care", ieee proceedings on pervasive computing technologies for health-care, 2008.

[5] Stefan krone, bjoern almeroth, Falco guderian and Gerhard fettweis, "towards a wireless medical smart card", ieee design, automation & test in Europe conference & exhibition, pp. 1483 - 1488,2012.

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

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

[8] Adam Marcus, Guido Davidzony, Denise Law, Narmada Venna, Rich Fletcher, Aamir Khans and Luis Sannenta, "Use of NFC-enabled Mobile Phones for Public Health in Developing Countries", IEEE Proceedings on First International Workshop on Near Field Communication, pp. 30-35. 2009.

[9] Divyashikha Sethia, Shantanu Jain and Himadri Kakkar, "Automated NFC enabled Rural Healthcare for

ISSN 2348 – 7968

reliable patient record maintenance", Proceedings of Global Tele health Conference, vol. 182,2012.

[10] P. Dewi Purnamasari , M. Salman, A. A. Putri Ratna , A. Shaugi , "Analysis and comparison of MD5 and SHA-1 algorithm implementation in Simple-O authentication based security system", Quality in Research, 2013 International Conference,25-28 June 2013

[11] K. Preethi, S. Anjali," Contactless Communication through NFC" Volume 2, Issue 4, April 2012.

[12] Hussein ahmad, Mohammad rababah, "near field communication (nfc)" ijcsns International Journal of Computer Science, VOL.12 No.2, February 2012.

[13] Rohde, Schwarz NFC technology and measurements, "NFC Technology and Measurements White Paper" .

[14] N.Rajalakshmi, C. Krishna Kant, N. Venkata, Ramarathnam," Dhwani: A Secure Peer-to-Peer Acoustic Near Field Communication" August 12–16, 2013, Hong Kong, China.

[15] Anusha Rahul, Gokul Krishnan, Unni Krishnan," NFC Technology: a survey" International Journal on Cybernetics & Informatics (IJCI) Vol. 4, No. 2, April 2015.

[16] Adam Marcus, Guido Davidzony, Denise Law," Using near field communication enabled Mobile Phones for Public Health in Developing Countries".

[17] Tobias Engel, Nadiem Heydebrand, Suparna Go swami," A NFC-based Concept for Medication Related Patient Services" Conference Paper · June 2013.