International Journal of Innovative Research in Science and Engineering
Vol. No.2, Issue 11, November 2016
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

# SMART HEALTH CARE USING NFC

**Mrunalinee Patole[1], Smruti Chandwani[2], Purva Taware[3]**

[1, 2, 3] *Department of Computer Engineering, RMDSSOE, Savitribai Phule Pune (India)*

## ABSTRACT

*NFC, RFID, like, such as contactless transactions, micropayments, identity management and mobile health ID, etc., NFC standard is not in itself provide built-in security features of the application domain is a contactless identification technology that has gained widespread adoption. This means that each of the developers of the need to implement security features in its own NFC applications. This developer is safe from NFC-based security vulnerability results because users choose to implement. Clearly, this is a major obstacle to widespread adoption and application environment NFC deployment. In this paper, we propose a light weight security middleware concept that can be implemented to protect the security of different applications require large array. In turn, the application can then apply security features related to their situation. Furthermore, we apply security protection to deal with malicious content NFC tag application. Our assessment is both lightweight and security middleware is working to reduce the latency.*

***Keywords: ADT system, Android phones, Near field communication (NFC), Security Middleware, Smart health car***d.

## I. INTRODUCTION

Access to electronic health records and patient data system as an important tool, such as a hospital and a medical examination is filed work to maintain the history. Mobile device users secure and offer users new ways to access to health services, and data friendly atmosphere. We have developed anywhere in the supply of health facilities that have been added to the mobile device using any wireless technology using Near Field Communication (NFC), the original architecture of the M-health services. Early detection of disease prevention is to improve the health, quality of life using different technology approach. Patient records must be kept in the right document. A daily field communication, wireless communication model is closer to one of the safe interaction between electronic devices within a small range. It means coming to a simple, touching each other or the area can communicate with each other. NFC devices can be used in arbitrary applications. NFC-enabled mobile devices to specific payment, [7] [9], the retail system [6], [12] and tickets for public transport [14] is a huge potential in the deployment of the system. NFC also [11] advertisements, consumer electronics, gaming, health and wellness,[10] not filled opportunities and social networks [8] [13].Read our proposed framework and the implementation of data manipulation functionality, act as the intermediate layer in order to verify the defective NFC, Data interchange format (NDEF). The framework is integrated Identification of such native NFC Reader NFC functionality is available in all the malicious components Mobile device applications are not rooting. when the user Smart poster will swipe his phone, data transmission will be supplied middleware. At this stage, according to the data will inspect the URL format and middleware NDEF Essentially applied three methods of white listing, Black list and find faith and credit of the malicious URL.

International Journal of Innovative Research in Science and Engineering
Vol. No.2, Issue 11, November 2016
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

## II. EXISTING METHODOLOGIES

Missing or incorrect data in the database with the name of the hospital if already exist or do not have the wrong person in the database. Is entered. This leads to incorrect information stored in the patient. Sometimes patients can sometimes get lost or missing data is in the form of paper. But this problem does not exist in the proposed system, all patient data is stored according to the NFC unique ID.

Comparison between NFC and other existing technologies is as follows:

Set up time of Bluetooth is -6 sec and whereas for NFC it is <0.1 m/s. Range of Bluetooth is up to 30 m/s whereas for NFC it up to 10cms.Usability of Bluetooth is data centric medium whereas for NFC it is human centric, intuitive and easy. Therefore NFC is a better wireless technology for the proposed system.

The comparison with other technologies is as shown in the table below:

**2.1 Comparison Table**

| | NFC | RFID | IrDa | Bluetooth |
|---|---|---|---|---|
| Set –up time | <0.1ms | <0.1ms | ~O.5s | ~6 sec |
| Range | Up to 10cm | Up to 3m | Up to 5m | Up to 30m |
| Usability | Human centric Easy, intuitive, fast | Item centric Easy | Data centric Easy | Data centric Medium |
| Selectivity | High, given, security | Partly given | Line of sight | Who are you? |
| Use cases | Pay, get access, share, initiate service, easy set up | Item tracking | Control & exchange data | Network for data exchange, headset |
| Consumer experience | Touch, wave, simply connect | Get information | Easy | Configuration needed |

## III. LITERATURE REVIEW

**3.1 Table for Literature Survey**

| Sr. no. | Title | Publication | Techniques used | Comments |
|---|---|---|---|---|
| 1 | "Electronic health record application support service enablers" | IEEE 2015 | Web based application. | -Very complex design. -not secure. |
| 2. | "Remote patient monitoring and electronic health | IEEE 2016 | Use of HW sensor to generate | -costly |

ISSN (O) 2454-9665
ISSN (P) 2454-0663

| | | | | |
|---|---|---|---|---|
| | record system based on web services" | | records. | |
| 3. | "Predictive analytics on Electronics Health Records (EHRs)" | IEEE 2015 | Use of parallel processing to analyse the data. | -it doesn't talk about how to store/ access the data. |
| 4. | "Digital imaging and electronic health record systems: Implementation and regulatory challenges faced by health care providers." | IEEE 2015 | It talks about collaboration and communication between providers and entities involved in patient care. | -it does image processing to retrieve the data |
| 5. | "Utilization of EPIC Electronic Health Record System for Clinical Trials Management at Duke University" | IEEE 2015 | Hospital level EHR system | -hospital level EHR system. |

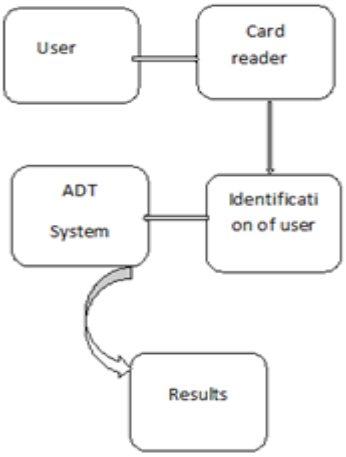
## IV. PROPOSED SYSTEM

We can have access to the patient and the doctor want to develop secure EHR server through the NFC tag. This is a client-server-client application

- Client application to see the doctor and the medical record.
- The central storage server information application
- Client application to see the patient and his / her record

The diagrammatic representation of the proposed system is given below:

International Journal of Innovative Research in Science and Engineering
Vol. No.2, Issue 11, November 2016
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663




### 4.1 Algorithms

we use 3 algorithms in this system, namely:

1. MD5 Hashing Algorithm
2. Linear Congruential Generator
3. Advanced Encryption Standard

These algorithms are described below:

### 4.2 MD5 Hashing Algorithm

Expressed 128-bit (16-byte) hash value production, especially in the form of a 32-digit hexadecimal number text.

- We encrypt users on the server using the MD5 pin sending pin

- MD5 is a one-way function; it is no encryption or encoding. It can not be reversed in addition to brute force attacks.

- 512-bit input message block is broken up into chunks (sixteen 32-bit words)

The message is padded so that its length is equal to 512

### 4.3 Linear Congruential Generator Algorithm

- To create a unique passcode random value.
- Linear congruential generator (LCG) is a piecewise linear equation algorithm to calculate a break of a pseudo-randomized order production.
- It is relatively easy to understand the theory behind them, and they are fast and easy to implement and can provide computer hardware arithmetic denominator by truncation especially storage - bit.

The generator is defined by recurrence relation:

$$X_{n+1} = (aX_n + c) \mod m$$

Where X is the sequence of pseudorandom values, and

ISSN (O) 2454-9665
ISSN (P) 2454-0663

$m$, $0 < m$ – the "modulus"
$a$, $0 < a < m$ – the "multiplier"
$c$, $0 \leq c < m$ – the "increment"
$X_0$, $0 \leq X_0 < m$ – the "seed" or "start value"

Are integer constants that specify the generator.

### 4.4 Advanced Encryption Standard (AES)

AES, 128 bits block cipher with a block length:

- 256-bit encryption keys, including 128-bit keys to process 192-bit keys, 10 rounds, 12 rounds, 14 rounds Before the start of the lap-based process can for encryption, the input field is XORed first four words of the state plan. The same thing happens during the decryption - except for a term of four key project areas in the state and now we XOR cipher text.

$$\begin{bmatrix} byte_0 & byte_4 & byte_8 & byte_{12} \\ byte_1 & byte_5 & byte_9 & byte_{13} \\ byte_2 & byte_6 & byte_{10} & byte_{14} \\ byte_3 & byte_7 & byte_{11} & byte_{15} \end{bmatrix}$$

- Encryption, each round consists of the following four steps Item: rows 1) Replacement flat, 2) shifting 3) Add to the mix the column and 4) body. In the last three stages of the final stage, the plan is four words XORing production.
- cryptanalysis, each round consists of the following four steps factors: 1) the inverse shift lines, 2) engage the housing options, 3) and 4 of the body) Add to busy mixing column. The third step involves XORing plan with production from four words, the last two steps.

## V. MATHEMATICAL MODEL

X = {P,D,S,C,f1,f2,S,F}

P =Patient

D = Doctor

S = Server

C = Client

f1= readNfc()

f2 = writeNfc()

S = success

f = Failure

Let X be the probability of reading NFC data successfully and Y the

condition that NFC reader is faulty

Now According to 'Bayes Theorem'

ISSN (O) 2454-9665
ISSN (P) 2454-0663

$$P(X)(Y) = \frac{P(Y)(X) * P(X)}{P(Y)}$$

where A and B are events and $P(B) \neq 0$.

P(X) and P(Y) are the probabilities of observing X and Y without regard to each other.

P(X | Y), a conditional probability, is the probability of observing event X given that Y is true.

P(X | Y) is the probability of observing event Y given that X is true.

## V. CONCLUSION & FUTURE WORK

Early detection of disease prevention is to improve the health, quality of life using different technology approach. Patient records must be kept in the right document.

The paper, "Smart Health Card" idea is proposed, it will help change the way of communication between a doctor and patient. It also noted that to maintain a medical and so will help to prevent any loss of important data. Or "HCI" domain is a very good example.

Future work, we can use this concept to maintain medical records and provide to future health problems predicting the insurance companies

## VI. ACKNOWLEDGEMENTS

We would like to express our appreciation to my HOD, prof. Vina M. Lomte and we would also like to express my gratitude to our guide, prof. Mrunalinee Patole for her encouragement and guidance for this review paper.

## REFERNCES

### JOURNAL PAPERS:

[1] Quincozes, Silvio E., and Juliano F. Kazienko. "A secure architecture based on ubiquitous computing for medical records retrieval." 2016 8th Euro American Conference on Telematics and Information Systems (EATIS). IEEE, 2016.

[2] Doğan, RamazanÖzgür, and TemelKayıkçıoğlu. "Remote patient monitoring and Electronic Health Record system based on web services." 2016 24th Signal Processing and Communication Application Conference (SIU). IEEE, 2016.

[3] Chennamsetty, Haritha, Suresh Chalasani, and Derek Riley. "Predictive analytics on Electronic Health Records (EHRs) using Hadoop and Hive."Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on. IEEE, 2015.

[4] Piliouras, Teresa C., Robert J. Suss, and Pui Lam Yu. "Digital imaging & electronic health record systems: Implementation and regulatory challenges faced by healthcare providers." Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island. IEEE, 2015.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

[5] Piliouras, Teresa C., Robert J. Suss, and Pui Lam Yu. "Digital imaging & electronic health record systems: Implementation and regulatory challenges faced by healthcare providers." Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island. IEEE, 2015.

[6] G. Broll, H. Palleis, H. Richter, and A. Wiethoff. Exploring multimodal feedback for an nfc-based mobile shopping assistant. In 5th International Workshop on NFC, Feb 2013.

[7] U.B. Ceipidor, C.M. Medaglia, A. Opromolla, V. Volpi, A. Moroni, and S. Sposato. A survey about user experience improvement in mobile proximity payment. In 4th International Workshop on NFC, March 2012.

[8] A. Fressancourt, C. Herault, and E. Ptak. Nfcsocial: Social networking in mobility through ims and nfc. In Near Field Communication, 2009.NFC '09. First International Workshop on, pages 24–29, Feb 2009.

[9] OmkarGhag and SaketHegde. Article: A comprehensive study of google wallet as an nfc application. International Journal ofComputer Applications, 58(16):37–42, November 2012. Published by Foundation of Computer Science, New York, USA.

[10] A. Marcus, G. Davidzon, D. Law, N. Verma, R. Fletcher, A. Khan, and L. Sarmenta. Using nfc-enabled mobile phones for public health in developing countries. In Near Field Communication, 2009. NFC'09. First International Workshop on, pages 30–35, Feb 2009.

[11] J. Morak, D. Hayn, P. Kastner, M. Drobics, and G. Schreier. Near field communication technology as the key for data acquisition in clinical research. In Near Field Communication, 2009. NFC '09.First International Workshop on, pages 15–19, Feb 2009.

[12] Denise Paradowski and Antonio Kruger. Modularization of mobile shopping assistance systems. In Near Field Communication(NFC), 2013 5th International Workshop on, pages 1–6, Feb 2013.

[13] E. Siira and V. Tormanen. The impact of nfc on multimodal social media application. In Second International Workshop on NFC, April 2010.

[14] R. Widmann, S. Grunberger, B. Stadlmann, and J. Langer. System inte-gration of nfc ticketing into an existing public transport infrastructure. In 4th International Workshop on NFC, March 2012