Cloud based NFC Health Card System

Gunjan V. Ukalkar
Department of Computer Engineering,
MIT College of Engineering,
Pune, India
gunjan.ukalkar91@gmail.com

Prof. Prasad S. Halgaonkar
Department of Computer Engineering,
MIT College of Engineering,
Pune, India
prasad.halgaonkar@mitcoe.edu.in

***Abstract*— NFC in the area of health, it has been used to solve serious medical issues. It provides fast information for authentication, access to medical history and provide emergency medical information.NFC does not provide any security by itself. We have proposed novel architecture of secure NFC based e-health card for improving healthcare system by using Amazon Cloud. As many medical hospitals and clinics desire to obtain the services of cloud computing, the major concern is the security of their data in the Cloud and the NFC Card. The main contribution of this paper is To ensure the security of data in NFC health card and in Cloud environment, we propose a method by implementing Enhanced Encapsulation Security channel using RSA algorithm, so the data information on NFC channel will be secured. To Provide a strong Login Mechanism for Admin and Doctors. Due to this security technique, communication data will not be exposed to unauthorized users. It will also maintain quality of service in healthcare domain.**

Keywords—Cloud, NFC in healthcare, e-health card, RFID, Enhanced Encapsulation Security channel .

I. INTRODUCTION

Day by day people are trying to make their life more comfortable and easy with the upgrading technology. As there is increase in use of mobile devices they are personally available to user and location aware .It is soon becoming very important in improving the quality of healthcare services and management. Patient uses mobile device for self-help and to communicate with doctor.

Android based mobile devices with NFC, Bluetooth interfaces, smart card technology on tamper resistant secure element to store information in secured manner and helps it to avoid from attackers this makes mobile an appropriate device for remote healthcare than any other media.

NFC plays very big role in healthcare management. Traditionally, registration of patients to specific doctor and giving prescriptions to patients was manually entered using web browser and the storage of health record data of patients would be so huge on the server that it became difficult for the hospital to manage and give better medicine to patient. To overcome this problem Identification of objects for secure medical procedures is very essential for a secure work flow to reduce medical errors. for example, secure identifiers on the medicines can help doctor/professional healthcare to administer correct medication to a patient.

NFC enable mobile phones are tap with NFC tags which shows all the information of patient stored in NFC tags retained with e-health card . Patient's are given unique NFC tags with unique identification number in such a way the patient can be identified and his/her credential information can be transmitted to the nurse however it provides medical professionals with information about what treatments a patient should receive, and it keeps all track when the nurses and doctor check in and check out during a patient visit.NFC can work off-line with automated recordings of visits. These tags are reusable, programmable and transmit data about the location, operation. This way the execution of all planned visits can be monitored and the amount of working hours can be properly recorded.

A. Technology

NFC is a short range high frequency wireless technology it allows to exchange data between two devices at the distance of 10 cm operate speed between 106- 424 kbps. NFC is based on RFID (Radio Frequency Identification) its frequency speed is 13.56MHz [1]. It uses the magnetic field induction to enable communication between two electronic devices in close approximate.

NFC works on three Operating modes: i) Reader/Writer mode: In this mode NFC behaves as a reader for NFC tags .It detects a tag immediately in close proximity by using collision avoidance mechanism. An application on NFC device can read data from and write data to the detected tag. ii) Peer to Peer (P2P) mode : It allows two NFC enabled devices to exchange information to each other. iii) Card Emulation mode : In this mode NFC enabled device act as a contact-less smart card.

There are different types of NFC tags. NDEF (NFC data exchange format) is a standardized format use for storing data and transporting data across a peer to peer link between two NFC devices. NDEF provides no security against data manipulation, overwrite protection against data manipulation and digital signature records cannot avoid malicious modification of tag. Hence we utilize MIFARE Classic 1 K [2] tags which covers proprietary technologies based upon various levels of the ISO/IEC 14443 Type A and write raw data using

NFC-A (ISO 14443-3A). The MIFARE Classic 1K tag offers 1024 bytes of data storage, split into 16 sectors.

NFC enabled mobile devices have a secure element (SE) as a tamper-resistant platform capable of securely hosting applications and it includes a cryptographic processor to facilitate to provide secure storage and execution environment. The supported secure element factors can be, for example, UICC, Embedded secure elements. NFC enables such as Micro SD with integrated antenna and SIM-Wrapper.

Java Card technology provides a secure platform for applications [3] that run on smart cards and other trusted devices with very limited memory and processing capabilities and provides data encapsulation ,firewall and Cryptography. The smart card specification standard ISO/IEC 7816 is related to electronic identification cards with contacts and ISO/IEC 14443 for contact-less integrated circuit cards specify the host application and smart card is done through application protocol data units.

In this paper, Section II gives brief idea about the literature review. Section III describes overview of proposed sys-tem, Mathematical Model and the algorithm. Section IV gives the system analysis and results. And Section V provides Conclusion.

II. REVIEW OF LITERATURE

The work by Prabhakar et al, conducts an extensive study related to NFC for Pervasive Healthcare Monitoring [4]. Designed two products first is NFC based battery charger circuit to charge a thermometer equipped with wireless communication and second is NFC based battery-less medical grade thermometer. They show that both products has potential for critical care continuous monitoring and regimentation based parameter monitoring. But the work raises privacy issues since it can lead to the situation where patients are not aware that their private information is being shared and becomes vulnerable for threat.

The work by Divyashikha et al, proposed NFC based secure mobile healthcare system[5].Introduced two applications in system that is i) Secure medical tags for reducing medical errors and ii) Secure health card for storing Electronic health record based on secure NFC tags, mobile device using P2P Mode and Card Emulation mode. It improves healthcare process for secure medical object identification and patient health card on an external tag or mobile device itself. But the system faces security issues while accessing health card. In our work we have designed health secure service on a hybrid cloud and also solved problem of security issues.

The work by Danco et al, proposed Ergonomics design of healthcare NFC-based system [6] based on QoE metrics. It improves access to patients medical history and improved medical checkups by automatically updating information access to entire patients medical records. It added knowledge to our record.

The work by Vasquez et al, Using NFC technology for monitoring patients and identification health services [7] ,it presents the design of an intelligent system which will allow for the identification and monitoring of patients in health centers it keeps track of patients which increase security and minimize medical errors which improves the quality in healthcare.

In paper [8] authors have developed technique for improving authentication mechanism of RFID security by using One time password (OTP) authentication method which refers to use only once. It is also called as dynamic password. Its operation is created by combining set of passwords through three main token i.e. algorithm identifier, sequence integer and seed. Authors have used OTP based algorithm which is based on HMAC-SHA1 algorithm to upgrade the authentication mechanism of RFID security. Authors have provided advantage of NFC tag security for user but disadvantage of this paper is that attacks like relay attack and data modification can occur.

In paper [9] authors have developed security solution that can be used to securely establish mobile payment transactions over the Near Field Communication (NFC) radio interface. security issues are mostly related to fact that NFC specifications which specify no communication security. authors have proposed solution it uses symmetric cryptographic primitives on devices having memory and CPU resources limitations. Authors have also maintained the security of NFC communications and demonstrated that solution is simple, scalable, cost-effective, and includes minimal computational processing overheads.

In paper [10] authors developed a solution that uses NFC technology to prevent five types of medication errors i.e. wrong patient, wrong medication, wrong time, wrong dose, and wrong route. Medication errors that occur during the medication administration stage are a serious issue in healthcare these errors might happen, the smart phone application alerts the nurse prior to administering the medication to the patient. This application also provides the nurse with an option that allows him or her to alert the physician who prescribed the medication and the pharmacist who dispensed it.

In paper [11] authors have developed secure smart phone unlocking using NFC. Nowadays phone contains every confidential and often intimate detail about their owners, from personal chats, to passwords or bank account details. this smart phone has various temporal and convenience benefits. Apart from being extremely secure, it solves almost all of the problems associated with conventional unlocking systems. The major drawbacks however, are the lack of availability of

NFC in current smart phones, and the tattoo life is too short to be implemented extensively in daily life.

Features	1) Cloud based NFC health card system	2) NFC based secure mobile healthcare system	3) Ergonomics design of healthcare NFC based system
1) Availability of data is high in crash recovery system or loss of card.	Present	Absent	Absent
2) System is highly secure because Amazon Cloud ensures security of application and data.	Present	Absent	Absent
3) RSA key are encapsulated in secure packets. Less chances of tampering keys.	Present	Absent	Absent

Fig.1: Comparison with other systems

III. PROPOSED APPROACH

A. Problem Statement

Implementation of Cloud based NFC health card system. The proposed system will authenticate patient and doctor, which will help to give correct medicine to patient. The proposed sys-tem will also be secured from illegitimate users by overcoming the security threats for providing better service to people.

B. Workflow of the system(Fig.2):

1) The Admin of the System registers the Doctors and Patient. Every registered Patient gets a Unique NFC Tag (MIFARE). The Doctor holds a Mobile Application know as Secure Element (SE) which is registered with the Cloud Server and holds a Unique Identification Number (SEID).
2) When the Admin registers a Patient on the Cloud Server, the Server creates a Unique pair of Key PATPRIKEY and PATPUBKEY. These keys are used for securing the patient Health record to avoid man in the middle attack.
3) These Key are stored on the Cloud Server
4) The Admin thereafter links the Patient ID with the Doctor ID i.e. allots the doctor for the patient. Here the Cloud server creates a LINK ID that links the Patient with the Doctor.
5) The Patient Health Checkup data is taken and stored on the Cloud Server.
6) When the Patient visit the doctor, the Patient gives his/her NFC TAG to the Doctor.
7) The Doctor scans the Patient NFC Tag with the SE(1).
8) The SE sends the TAGID and SEID to the Server to check and authorized/registered patient has arrived.
9) The Server then checks the LINK ID and verifies the correct patient has arrived.
10) The Server then ACK to the Doctor SE and downloads the PATPRIKEY and PATPUBKEY on the Doctor SE.
11) The Doctor carries the Patient OPD.
12) Then the Doctor gives diagnosis and Prescription which are encrypted using RSA and securely transmitted on the Patient NFCTAG. Here the Security Framework uses PATPRIKEY and PATPUBKEY for data encryption.
13) Next time when the Patient comes Step (6),(7),(8),(9) are carried out for authentication and verification.
14) The Doctor SE now reads the previous Encrypted Health record, uses RSA Framework and displays it to the doctor (PATPRIKEY).
15) Step (11),(12) are carried out.

C. Mathematical Model

Mathematical Model is the mathematical representation of the system. Let S be a system which provides authentication of the patient and the data transfer between the tag and the smart phone and the sequential flow till the prescription approved by the doctor.

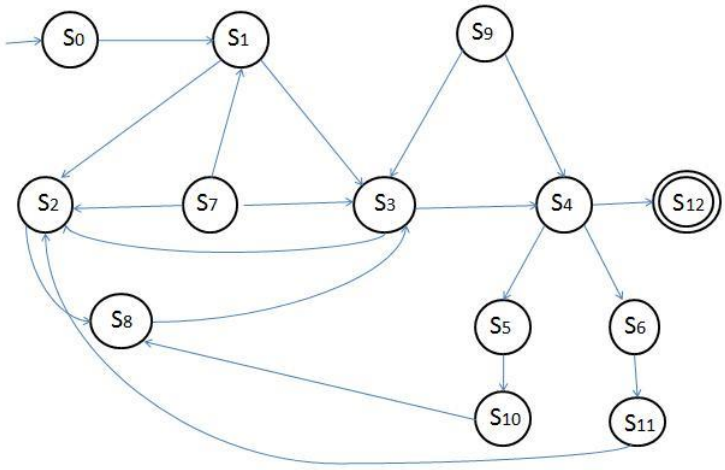

Fig.2: State transition diagram of system

States:

- S0:initial state
- S1:Admin of the system
- S2:Doctor registration
- S3:Patient registration
- S4:Cloud Server
- S5:Patient Public key
- S6:Patient Private key
- S7:Cloud Server link between doctor and patient
- S8: NFC tag
- S9:Patient verification
- S10:Encryption on tags
- S11:Decryption on Doctor mobile
- S12:Final state

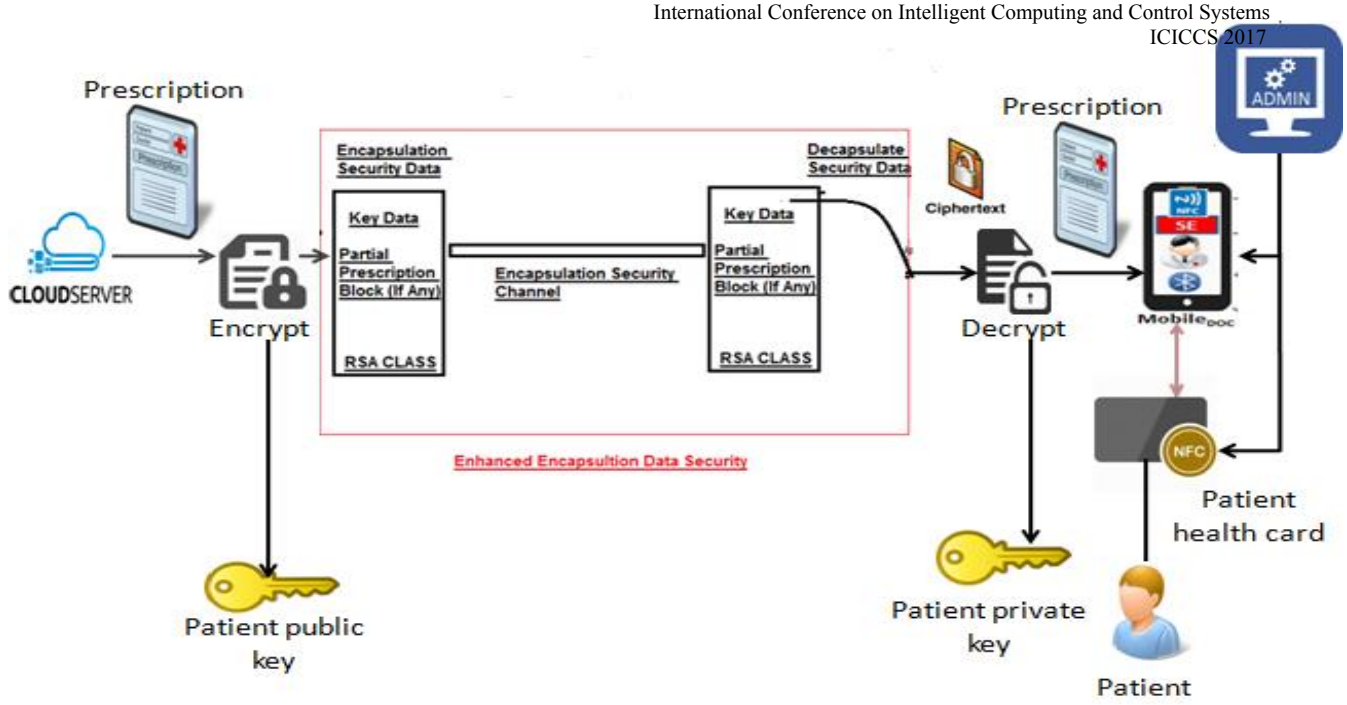

Fig.3:Cloud based NFC Health Card System Architecture

Input Files:
P=P1,P2,P3,P4,P5,Pn
I=P(D)1,P(D)2,P(D)3,P(D)4,P(D)5,...P(D)n
Where,
P is the set of patient
P(D)=Patient Data
I=Information of
Patient
Output Files:
Pr=Pr(P1),Pr(P2),Pr(P3),Pr(P4),Pr(P5)....Pr(Pn)
E=E(Pr1),E(Pr2),E(Pr3),E(Pr4),E(Pr5).....E(Prn)
Where,
Pr is prescription for treatment
Pr(P)= Prescription of each
patient E= Encryption
E(Pr)= Encryption each Prescription

D. Algorithm

In proposed work, we have to implement Encapsulation Security Channel deployed in RSA algorithm. The implementation of RSA algorithm involves following steps: Key Generation , Encryption , Decryption [12].

RSA is a block cipher, in which every message is mapped to an integer. It is widely use for securing confidential data. It protects from attacks like Data Modification and Key Tampering.RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key and Private-Key is stored on Secure Cloud. When the Doctors read the Patient NFC Health Card, the cloud validates the Doctor and Patient and on successfully validation securely downloads the Keys on DOCTOR SE. Using RSA module the SE can encrypt and decrypt the data on the patient health card.

Encapsulation Security Channel

This is a enhanced security that provides ore security for transmission channel. The system when encrypt the data (partial prescription if any) and the patients keys are encapsulated into a class object. This class object is further serialized so that the values of the class object parameters are not visible during transmission. The Object is signed and send over the network. The receiving Doctor SE element decapsulate the class with the same signature and read the parameters values. These values are further converted to the Patient Original KEY Values. This Key now can be used to provide encryption and decryption at Doctor SE Module.

Due to this mechanism we are securing the transmission channel with providing Enhanced Mechanism over the data security and thus named as Enhanced Encapsulation Security Channel (EESC).

IV. SYSTEM ANALYSIS

We analyse our system performance based on different parameters of algorithm such as Time complexity and Space complexity.

A. Time Space Complexity

We have computed the time complexity by varying the Private key length of the RSA algorithm and finding the required execution time for each Private key length. The time complexity of RSA is analysed by varying the private key length in bits and noting the execution time for each key length.

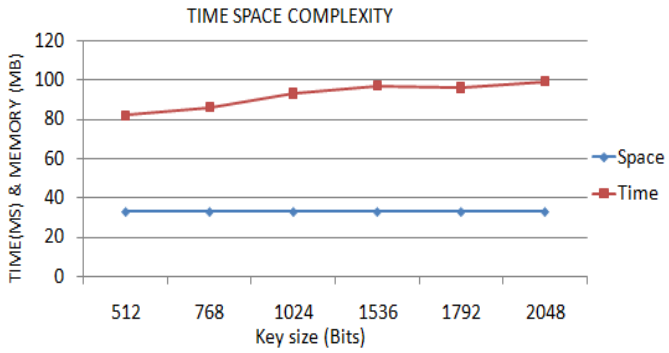

Fig.4: Time Space Complexity

B. Expected Result

The patient mainly manages the NFC card contents by securing the data using RSA public and private key. The keys are securely stored on Amazon Cloud that manages the application in secured way. The outcome is that the card contents are not easily readable due to strong encryption and is only accessible to the authorized secure element device this further improves authenticate the right patient and the associated doctors.

Fig.5:Snapshot of the app displaying Admin menu

In fig.5 Snapshot of app displaying Admin menu in which Patient, Doctor registers. Admin links doctor and patient.

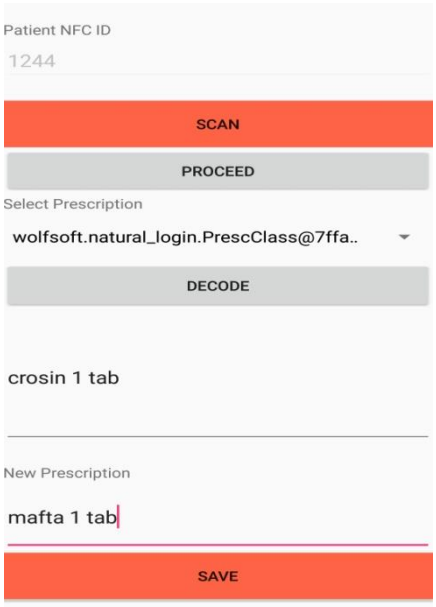

Fig.6: Snapshot of the app displaying Prescription menu

In fig.6 Doctor logins he scans the Patient NFC tag .The cloud server sends Tag ID and SE ID to the server. Server then checks link ID and verifies the correct patient has arrived. All the prescriptions are in encrypted form which are partially saved on cloud and in NFC tag.

If the Patient has arrived earlier then his previous prescription will be displayed with date time and day. In the displayed snapshot the patient has arrived earlier so his previous prescription is seen that is crosin 1 tab.

Fig.7: Snapshot of the app displaying saved prescription in encrypted form

In fig.7 when we tap NFC tag. Data is parsed. It is ready to write new prescription in encrypted form on NFC tag.

V. CONCLUSION

In this work, we have proposed Cloud based NFC Health Card system. It helps to modify quality of healthcare services. This will improve the health flow in crowded hospitals of developing countries like India as well as of developed nations. Healthcare -related data is constantly explosive and it becomes difficult to handle, manage and process. So we have introduced Amazon cloud in our system which can store huge medical data in secured manner. It protects the data from unauthorized users and also improves security by using encryption algorithm.

ACKNOWLEDGEMENT

I would like to thank Prof. Prasad S. Halgaonkar , MIT College of Engineering, Pune, India for supporting this work.

REFRENCES

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

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

[4] D. Sethia, D. Gupta, T. Mittal, U. Arora and H. Saran, ”NFC based secure mobile healthcare system,” 2014 Sixth International Conference on Communication Systems and Networks, Bangalore, 2014, pp. 1-6.

[5] T.V. Prabhakar, U. Mysore, U. Saini, K. J. Vinoy and B. Amruthur, ”NFC for Pervasive Healthcare Monitoring,” 2015 28th International Conference on VLSI Design, Bangalore, 2015, pp. 75-80.

[6] Danco Davcev, Goran Jakimovski, ”Ergonomics Design of Healthcare NFC-based System, Procedia Manufacturing”, Volume 3, 2015, Pages 5631-5638, ISSN 2351-9789.

[7] A. Vasquez , M. Huerta , R. Clotet ,R. Gonzlez , D. Rivas and V. Bautista,”Using NFC Technology for Monitoring Patients and Identifica-tion Health Services”, Conference Paper in IFMBE proceedings ,October 2014.

[8] C. H. Huang and S. C. Huang, ”RFID systems integrated OTP security authentication design,” 2013 Asia-Pacific Signal and Information Process-ing Association Annual Summit and Conference, Kaohsiung, 2013, pp. 1-8.

[9] Mohamad Badra, Rouba Borghol Badra,”A Lightweight security protocol for NFC based mobile payments,” Procedia Computer Science, Volume 83, 2016, Pages 705-711.

[10] Maali Alabdulhafith, Srinivas Sampalli,”NFC based framework for check-ing the five rights of medication administeration,”Procedia Computer Science, Volume 37, 2014, Pages 434-438.

[11] Utsav Jambusaria, Neerja Katwala, Dharmeshkumar Mistry,”Secure smartphone unlocking using NFC”,Procedia Computer Science, Volume 45, 2015, Pages 465-469.

[12] B. Asma Khatoon and Dr. Ataul Aziz Ikram,”Performance Evaluation of RSA Algorithm in Cloud Computing Security”, International Journal of Innovation and Scientific Research ISSN 2351-8014 Vol. 12 No. 1 Nov. 2014, pp. 336-345.