ISSN 2395-1621

NFC Based Secure Centralized Healthcare System for Smart Cities

[#1]Snehal Deshmukh, [#2]Aparna Madiwale, [#3]Shubhangi Paygude, [#4]Nishigandha Yadav, [#5]Prof.Asha Pawar

[1]deshmukhsnehal77@gmail.com,
[2]aparnamadiwale95@gmail.com,
[3]shubhangipaygude1995@gmail.com,
[4]nishiyadav1995@gmail.com,
[5]asha.pawar@zealeducation.com

[#12345]Deparment of Computer Engineering, ZES's, Zeal College of Engineering & Research, Narhe,Pune-411041

ABSTRACT

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, where there is a mass population to handle in hospitals and robust healthcare procedures are required. An efficient, reliable, robust and secure health flow is important to manage patients, their health records smoothly and for the right care to reach to the patient at the right time. Hospital administration has an application for securely reading/writing with a mobile device, ADMIN, to manage smartcard based tags and patient Health cards. Patient can register by using NFC card which will provide authentication and health information will be stored on the centralized server. We proposed Secure Medical Tags for reducing medical errors and Secure Health card for storing Health Record (HR). It can also provide portability of devices and usability for health management in emergency situation, overpopulated hospitals and remote locations. And provided online payment transaction system from NFC user which is connected to the bank server. (here the term mobile means at the remote areas)

Keywords — Near Field Communication, Java Card, RFID, MIFARE Classic, Secure Element

ARTICLE INFO

Article History

Received :24th May 2016

Received in revised form :

26th May 2016

Accepted :28th May 2016

Published online :

31st May 2016

I. INTRODUCTION

In developed countries maximum systems are centralized but in India we don't have centralized health record management system. NFC i.e. Near Field Communication is used to communicate between two devices. The proposed Centralized architecture using NFC is for

i) Secure Medical Tags for reducing medical errors and
ii) Secure Health card for storing Electronic Health Record (EHR) based on Secure NFC Tags.

We have also briefly mentioned a basic security framework requirement for the applications. Since NFC NDEF format is prone to security attacks, we have utilized low level APIs on Android based mobile devices, to securely access NFC tags such as MIFARE Classic tags with NFC-A (ISO I443-3A) properties. It can also provide portability of devices and usability for health management in emergency situation, overpopulated hospitals and remote locations.
NFC cards are easy to carry, patient can use them for self help or to communicate with a professional and or to monitor the health of the patient.

II. LITERATURE SURVEY

This paper presents the A Smartphone-based System for Population-scale Anonymized Public Health Data Collection and Intervention [1]

This paper presents Anonymization of Longitudinal Electronic Medical Records**,** this study need to dissemi-nate patient-specific longitudinal data in a privacy-preserving manner. To sharing such data while providing

computational privacy guarantees. uses sequence alignment and clustering-based heuristics to anonymize longitudinal patient records [2]

This paper proposed Sharing with Care: An Information Accountability Perspective Health information sharing has become a vital part of modern healthcare delivery. E-health technologies provide efficient and effective ways to share medical information, but they also raise issues over which medical professionals and consumers have no control.[3]

This paper proposed Implementing Electronic Medical Record Systems Healthcare Management described the industry as a knowledge-based enterprise that doesn't consider knowledge part of its value proposition. EMR is for storing the medical records for particular hospitals.[4].

This paper proposed "Information Security and Privacy of Patient-Centered Health IT Services: What needs to be done?" To account for the paradigm shift from paternalism towards increased patient involvement of today's health care systems, we derived information security and privacy requirements of PHS. [5]

This paper presents the "Near Field Communication Technology based mHealth for Telemonitoring of Patients with Chronic Diseases" mHealth in general and NFC based concepts in particular thus are poised to contribute to the concepts of individualized and pervasive healthcare in the sense of anywhere, anytime, including anything for anyone.[6]

This paper proposed "NFC+ Android Application by using NFC technology for Hospital Management System" The Android Smartphone's having NFC application used in any Hospital, Clinic, Dispensary or Pathology labs .Here we tried to show how NFC enabled mobile can used for identification and be connected via the any network to exchange information across any device that is incompatible or does not have an NFC reader. Hence we can conclude that NFC technology appear to be credible for providing a efficient solution in many health care organization.[7]

This paper proposed "Empowering patients using cloud based healthcare system" a personal health record system (PHRS) that is to self-monitor and control personal health Using mobile application to collect medical data and stored in HL7 CDA format for interoperability. The cloud based repository may be shared with the clinicians when needed.[8]

This paper presents "Practical challenges for large-scale deployment of mHealth solution" There is a chronic shortage of well-trained healthcare workers in low and middle-income countries. Task shifting has resources environments, with the added ability to evolve quickly while ensuring quality care for the patients. This paper proposed "Body Sensor Networks in Fetal Monitoring with NFC Enabled Android Devices" to provide obstetricians and gynecologists with a new portable wireless fetal heart monitoring system that will improve accurate, reliable and secure data collection.

III. EXISTING SYSTEM

System using bar code scanners rely on unchangeable information stored in the bar code. In case barcode got Scratched, scanner could not read the data, causing failure or erroneous identification. NFC tags data can be read or rewritten without actually seeing the tag, The NFC tags can store up to a few bits to kilobytes. Previously in the hospitals EMR systems are used to store health data electronically.

IV. PROPOSED SYSTEM

Here in this process we going to see NFC(Near Field Communication) based mobile healthcare system using NFC card reader sending the details to monitor in PC. Doctors or Nurses will use the NFC card in card reader so that it sensors will send the details to microcontroller, we can view in PC.
Centralized Electronic Medical Records (EMR) system makes the entire process of patient record keeping easier, more accurate and comprehensive, and more efficient. With an EMR system, doctors use specialized software that allows them to enter their patient records electronically. The software stores the patient information on a server and each patient's complete history is available instantly, including digitized copies of x-rays, lab results, prescriptions ordered and other necessary medical data. Physicians can use their desktop, laptop, or an electronic clipboard-type computer to navigate through their patient charts and record notes. EMR software also coordinates with their medical billing software, such as transferring diagnosis and procedural codes in order to facilitate the billing process after each patient visit and securely payment transaction system using AES algorithm and OTP Concept.

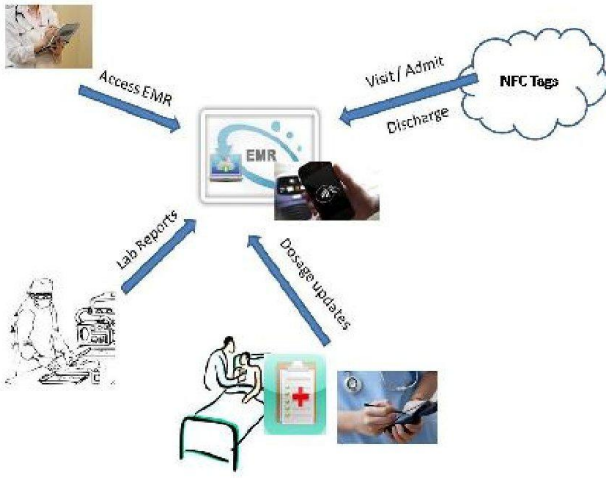


Fig1: System Architecture of e-healthcare

Actual working using EMR and NFC card :

1. While a person gets Admit/Visit to the hospital should carry their own NFC card, the health information about the person will be accessed through there NFC tags which will be synchronized and stored temporarily on that particular hospital Electronic Medical Record (EMR) Database and patient will be registered with unique ID. The doctor can easily access full information about the patient by viewing the patient EMR instead of going through bundle of paper

reports.
2.If the patient is been asked to take any particular test then those test reports will also be updated in that Centralized EMR.
3.Based on the test the updates which the doctor prescribed will be updated too in their EMR. And transactions will be done through NFC bank using AES algorithm.
4.Finally while the patient Leave/Discharge all those information which have been updated in his EMR will be synchronized and transferred back to his NFC tag which will hold the complete medical report about what happened that particular day. So it will help doctors to treat patients in very efficient way.

NEAR FIELD COMMUNICATION (NFC):
NFC is a set of standards for portable devices. It allows them to establish peer-to-peer radio communications, passing data from one device to another by touching them or putting them very close together NFC came out of RFID. RFID, or radio-frequency identification, is the technology used by shipping companies and in superstores to keep track of goods, it uses electromagnetic induction in order to transmit information NFC can also used in the cell phones. The standards are defined by a group called the NFC Forum, which includes Nokia, Sony and Philips. In essence, if your phone has NFC as a feature it can be used to transfer data to other phones or to NFC readers. NFC Cards also contains the RFID Tags for tracking and transmitting the information.

The architecture is described in the area of NFC-based Real -time Hospital Patient Management System (HPMS).

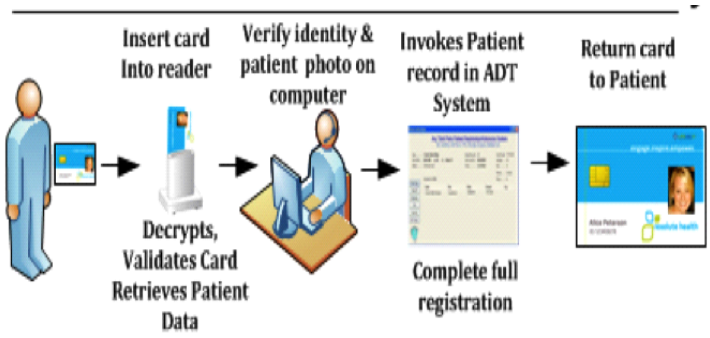


Fig2: Flow of System

Fig3: NFC chip

V. SECURITY ALGORITHM

Here we used AES algorithm at the admin side to provide security for password.

AES ALGORITHM:

1..KeyExpansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block.

2.InitialRound

1. AddRoundKey: each byte of the state is combined with a block of the round key using bitwise xor.

3.Rounds

1. SubBytes: it's substitution step where each byte is replaced with a 1subByte using s-box. S box is matrix given by rijndael.

2. ShiftRows: a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

3.MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

4.AddRoundKey

4.Final Round (no MixColumns)

1.SubBytes

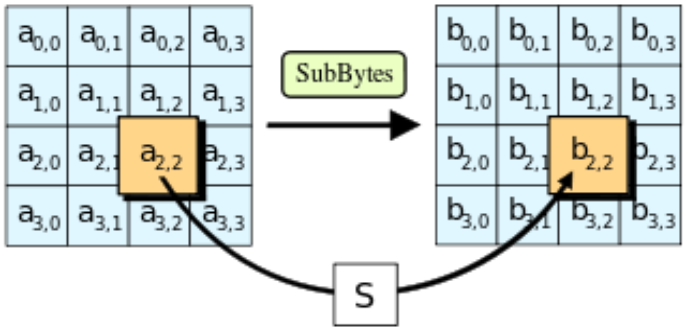
2.ShiftRows

3.AddRoundKey.

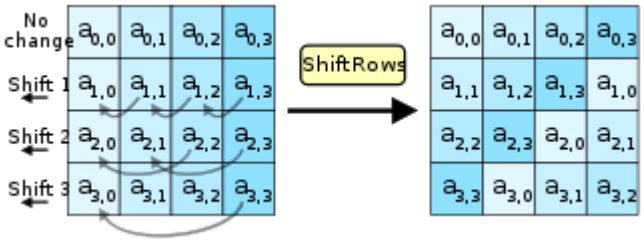
1] In the SubBytes step: each byte in the state matrix is replaced with a SubByte using an 8-bit substitution box, the Rijndael S-box.

2]Shift-row step :The first row is left unchanged. it cyclically shifts the bytes in each row.

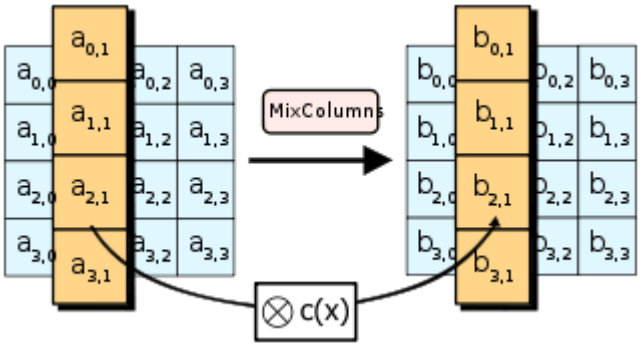
3] MixColumn step: The four bytes of each column of the state are combined using invertible linear transformation.
4] AddRoundKey step:In thethisstep, the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule;
Following diagrams will give you detail information :
SubBytes.



ShiftRows



MixColumns



We have proposed a novel architecture for improving healthcare process for secure medical object identification using NFC. The applications are simple to use with a simple NFC card swipe. NFC for secure communication. This will improve the health flow in crowded hospitals of developing countries like India as well as of developed nations. The business model will benefit the patients as well as medical professional.

VI. REFERENCES

[1] Andrew Clarke and Robert Steele, " A Smartphone -based System for Population-scale Anonymized Public Health Data Collection and Intervention,2014".

[2] Tamersoy, A. Vanderbilt Univ., Nashville" Anonymization of Longitudinal Electronic Medical Records ",2014

[3] MacKinnon, W. ; Sch. of Bus., Clarkson Univ.Potsdam, NY, USA ; Wasserman, M." Implementing Electronic Medical Record Systems" ,2014

