International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 01, January-2020

Secure Mobile App using NFC Authentication to Access the Health Records in Cloud

Sundari David
MTech, Cambridge Institute of Technology,
Bangalore,

Prof. Sandeep Kumar
Guide:
Dept of CSE, CiTech

***Abstract*:- Electronic Medical Record (EMR) frameworks have been receiving consideration where medical practitioner few of them additionally have been making use of such frameworks. The framework is easy to use and secure in administrations where numerous new ways have been put to use so as to get patient medical services data.**

For Patient's quality care, portable medical system development and implementation is the need. With the use of Near Field Communication (NFC), a unique mobile framework is developed with the use of basic architecture of m-health services. The challenge of m-health care services is to move patient sensitive data to the cloud, however, many organization are of the opinion that the cloud is not safe and secure compared to their own respective data center, hence we are using Cryptography. Cryptography is not just science of putting into use of complex mathematical concepts, algorithms and logic to plan solid techniques to shroud information called encryption, yet in addition to retrieve the actual or original information back which is known as decoding or de-cipher.

The aim and function of Cryptography is to send data between sender and receiver in a way that is secure, where an unauthorized person should not gain access to the data hence we need a strong, well defined algorithms, secure keys to encrypt and decrypt the data following a definite process.
I would like to present an idea of DNA Deep Learning Cryptography which is characterized as a method of hiding information regarding DNA grouping.

INTRODUCTION:

Mobile phones are considered to be personal and are always with the patient, consisting of features of location control and new digital media. In this way, the patient can utilize them for their further improvement and furthermore to screen the well-being of the patient with the assistance of the medical practitioner. To follow the patient's healthcare system the mobile phone play an important role where it is considered appropriate device. As we know, the quality of people's life has always been enhanced with the improvement of technology in various domains, where for few healthcare concerns and challenges, mobile phones are slowly used for their services. The World Health Organization (WHO) report "No Health with Thought researchers" must be kept up intricately. This sort of research is important and fundamental for some significant results and innovation. In the realm of healthcare industry a huge strain to be placed that caused by morality of the diseases.

OBJECTIVE

The objective of the framework is to maintain healthcare records in a proper and appropriate manner instead of storing the information manually with the aim of helping patient who are in a knocked out condition. In today's world, healthcare system is very important as it consists of patient personal and sensitive healthcare data where the records cannot be maintained in a manual format to avoid information leakage, hence, the healthcare data is digitized, encrypted, and accordingly stored in the cloud.
Since patient will not be able to go to the hospital always to get simple records where NFC technology is implemented if the patient is owning an android phone where he can install NFC application through which a respective patient healthcare reports can be downloaded from the cloud.

LITERATURE REVIEW:

S. Grünberger, [1] explain in this paper that mobile phone is in the reader/writer mode where the ticketing system is in the card emulation mode. The advantage of this system for the inverse scenario is that it can be implemented very easily by using lightweight protocols, which are compatible to existing mobile phones. In this paper author did not use any encryption methodology or frameworks to secure the user private date. Therefore, this kind of situation may lose control of their files naturally.
Vedat Coskun [2] proposed to have built a framework that integrates NFC loyal system in the cloud. He adapted NFC mobiles together with their secure element (SE) to cloud (Infrastructure as a Service – IaaS) using cloud computing methodology. In this paper the author did not use encryption process to secure the user private data. Hence, this framework will lose control of their files or data.
Zhe Lou [3] presented a brilliant postal application, where the NFC technology innovation is applied to the existing postal framework so as to make another new mailing experience. The new postal system is very much capable of addressing and facilitate the mail method, thereby improving the quality of the existing postal system. Author did not use any encryption method to secure the user private data; hence, this framework may lose control of their files or data where hackers can hack user post during transaction time with ease.
Mehdi Bahrami [4] presented a novel cloud distributed computing system consisting of a Service-Oriented cloud architecture. This proposed system can be ran on top of cloud computing systems that provides standard, dynamic

and customized services for e-Health systems. Here the proposed system allows cloud(s) provide a uniform service interface for e-Health system that helps the users to easily and freely transfer their data and application from one vendor to other vendors. In this system, Author uses encryption method to secure the user private data. However, the system did not use NFC login, compare to usual login this NFC card system works fast and secure manner.

PROBLEM STATEMENT:

The patient healthcare data management is vital and essential to patients and hospital management. In developing countries (like India) where there is no centralized repository or system for healthcare data management and the patient data are mostly maintained and retained by the patients in a manual paper format OPD (Out Patient Department) card which is very difficult to maintain along with the paper based reports where it is not reliable. It is not appropriate to have all patient information in paper documentation where it may cause trouble or mischievous.

EXISTING SYSTEM:

The Patient Healthcare Record Management (PHRM) plays a vital role where the data is essential to patients and hospital management. However, in many developing countries (like India) the data is in a manual paper format which is both unreliable to keep up with the paper based reports, besides where it may cause conflict or mislead the actual information.

Disadvantages:

1. Bulky to keep up with paper based reports and furthermore difficult, questionable and not reliable.
2. There may be of medical errors and negligence.

PROPOSED SYSTEM:

The main aim of this paper is to propose a system application using DNA Algorithm for the Cryptography for

1. Secure Medical Tags for decreasing medicinal blunders and

2. Secure Health card (Fig-1) for taking care of Electronic Health Record (EHR) consisting of Secure NFC Tags,

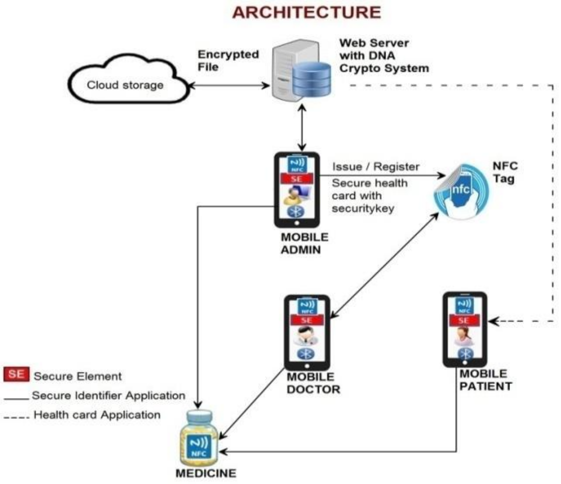

Fig-1 System model

mobile phone using NFC P2P Mode or Card Emulation Mode. Also, states the basic security framework requirement that is essential for the applications. NFC NDEF format are prone to security attacks, hence we have used low level APIs on the Android mobile phone to securely access NFC tags with NFC-A properties. In this scenario, the data is encrypted with DNA encryption algorithm and uploaded onto cloud for storage.

DNA:

Utilizing DNA grouping as data transporter to shroud data is a key test. In light of some exceptional property of DNA, it tends to be utilized hidden away from everything information since it is hard to isolate a unique DNA succession and a manufactured one". DNA acquaints an upgraded procedure with store tremendous measure of information in the little section of DNA and gives security and information respectability. A high effectiveness and enormous information stockpiling can be seen in the structure of DNA molecule. DNA Cryptography is commonly characterized as concealing information in DNA grouping. "The four sorts of DNA nitrogen bases are adenine (An) and thymine (T) or cytosine (C) and guanine (G) in DNA succession. The least complex DNA coding examples to encode the 4 nucleotide bases (A, T, C, G) is by methods for 4 digits: 0(00), 1(01), 2(10), 3(11) which is spoken to in the DNA Based Coding DNA Base Code A - 00 C - 01 G - 10 T - 11 In the proposed calculation, a DNA succession and the arbitrary key is produced and different advances are done with the goal that unique information will be changed over to encoded structure at the sender's side. The decoding strategies are applied at the collector's side so as to get back the original message.

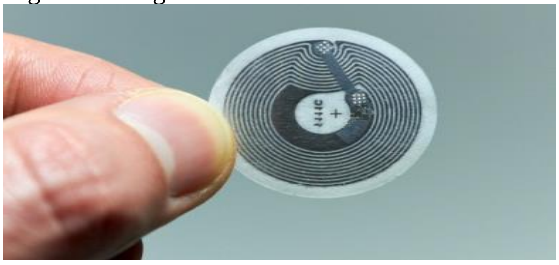

Fig 2: NFC Tag

NFC (NEAR FIELD COMMUNICATION):

At the time of interacting of electromagnetic radio fields, a type of short-range wireless RFID technology is used which is NFC. These days, there is a lot of discussion and awareness concerning security breach hence focus on security becomes very important in various process, design methodologies and architecture where we use the latest technologies. The techniques that is pursued must be strengthened to ensure end-to-end security of the applications to meet the objective of 'no security breach'.

NFC WRITING

NFC further builds and expands on Radio Frequency Identification (RFID) systems that allows two-way communication between the ends in contrast to the earlier systems such as contactless smart cards have been one-way. NFC tags are untapped electronic devices where it works without their own power supply and very much depending upon another working device to come in range to get activated or switched on. The trade-off in this scenario is that these devices cannot do any activation on their own. However, they are only used to exchange data to a functioning device.

In order to control the NFC tags, electromagnetic ratification and acknowledgement is used and essential to make a current in the remote device. We won't get very particular on this, yet the fundamental rule is that circles of wire can be used to transport electromagnetic waves, which would then have the option to be gotten and changed again into current by an another circular twist of wire. This in principle is the same as the systems that are used for remote charging headways, though noteworthy less impressive.

The dynamic devices, for instance, advanced cell, are responsible for creating the magnetic field. This is done, with a clear circle of wire, which produces attractive fields inverse to the stream of the exchanging current in the wire. The quality of the attractive field is adjusted by fluctuating the quantity of turns in the wire lopping or extending the present coursing through the wire, increasingly current may for certain require more energy, and unusually high power necessities would not be alluring for use in battery fueled portable advances.

Fig-3: NFC Reading / Writing Process

Along these lines is why NFC works over just two to three inches, instead of numerous meters that we're used to with various sorts of remote communications.

Since unpowered Fig-2 shows NFC "tags" can likewise be read by NFC devices, it is also equipped of replace the previous one-way applications.

Fig-3: In this module the classified data like patient user ID and decryption key of patient records is dumped into the tag, before dumping into the card first the data is Declare an Intent Filter to state or signal to the system that it is activated to work on NFC. Have a methodology where Android will call when NFC is spotted or detected. Create a methodology to build a NDEF message. Create a methodology to write the NDEF (NFC Data Exchange Format) message.

NFC READING

At the time of use, when the patient taps the card to his application, first encrypted data is transformed into original data with the use of decryption key and reading NDEF data from an NFC tag with language convention English. Patient ID and decryption key of patient documents is dumped into the tag, before into the card first data is Declare an Intent Filter to announce to the system that it is activated to work on NFC. Have a methodology where Android will call when NFC is spotted or detected. Create a methodology to build a NDEF message. Create a methodology to write the NDEF (NFC Data Exchange Format) message.

Advantages:

1. It reduces medical error
2. Helps to save the patient's life when they are unconscious.
3. Secure data

CRYPTOGRAPHY:

Cryptography is related with the process of transforming ordinary plain text into cipher text and vise-versa. It is a methodology of encrypting and decrypting data in a specific secure way so that the intended user can access and retrieve the data. Cryptography also protects from the hackers and helps in user authentication and integrity.

Cloud storage

Cloud storage is a way for businesses and consumers to store data securely online (via internet), where it can be accessed anytime from any locations and easily shared with those who are having authorized user credentials.

CONCLUSION:

This implementation (DNA Algorithm) helps health records to be stored and retrieved from cloud system for easy access to an authorized user (patient, doctor, admin) from anytime, anywhere. For security access, we are encrypting data storing into the cloud space. And when we are providing more security it becomes difficult for user to access the file hence we need system where it should have the high level of security as well as user friendly access and for this purpose the NFC health care system is developed using DNA based encryption technology to encrypt the file and store it in cloud storage and for the additional security authentication purpose we are using NFC tags where all the patients and doctors have the NFC tag. And with help of the NFC tag only they can login into their mobile phones. Based on that authentication only they can retrieve the relevant file in a user-friendly manner, so I conclude this project will be very useful to the medical field.

REFERENCES

[1] C. Saminger, S. Grünberger, J. Langer "NFC ticketing system with a new approach of an inverse reader mode"5th International Workshop on Near Field Communication (NFC) 2013.

[2] Vedat Coskun ; Busra Ozdenizci ; Kerem Ok ; Mohammed Alsadi “NFC loyal system on the cloud” 7th International Conference,2013.

[3] Zhe Lou “NFC Enabled Smart Postal System”,Second International Workshop on Near Field Communication,2010.

[4] Mehdi Bahrami, Mukesh Singhal “A dynamic cloud computing platform for eHealth systems” 2015 17th International Conference on E-health Networking,2015.

[5] T. Agarwal, Biometric Sensors Types and Its Working, 2014. [Online]. Available: https://www.elprocus.com/differenttypes-biometric-sensors

[6] M. Roland and .I. Langer, "Digital Signature Records for the NFC Data Exchange Fonnat", IEEE Proceedings of the Second International Workshop on Near Field Communication (NFC), pp, 71-76, 2010.

[7] Rashtriya Bima Yojana, http://en.wikipedia.org/wikilRashtriya_Swasthya_Bima_ Y ojan

[8] Smart Card Technology in U.S. Healthcare: Frequently Asked Questions, http://www.smartcardalliance.org/resources/pdf/Smart_ Card Technolog yjn_HealthcareJA□FlNAL_096012.pdf, 2012

[9] Sasikanth Avancha, Amit Baxi, and David Kotz, "Privacy in mobile technology for personal healthcare", ACM Computing Surveys (CSUR), vol. 45 Issue I, article 3, 2012.

[10] NFC Forum Tedchnical Specifications, http://www. nfc-forum.org/specs/spec -' istlndefts

[11] M1F ARE Classic IK specification document, http://www.nxp.com/documents/data sheetIMF 1 S50YYX. pdf

[12] NFCA on Android, http://developerandroid.comlreference/androidlnfc/techlNfcA.html

[13] MobilelNFC Security Fundamentals Secure Elements 101, http://www.smartcardalliance. org/resources/webi nars/Secure _Elements_10IJINAL3_032813.pdf,2013

[14] GO-Trust® Secure microSD .lava, http://www.go-trus1. com/products/microsd-java