Experimental Evaluation to Enhance Security for Health Care System Using Cloud Computing and Near Field Communication

Sanjeev Sharma

Electronics & Telecommunication Engineering Department, Sandip Institute of Technology & Research Center, Nashik, Maharashtra, India,

E-mail: sanjeev.sharma@sitrc.org

Abstract—Developed countries and increasingly mature society of the need to develop smart call in many health care facilities to deliver best medical facilities. Data sharing structure based systems such as online networks of Healthcare Application System has huge demands for distributed data security and efficiency. Use of NFC (Near Field Communication Technology) and proposed Cipher text policy attribute based encryption (CP-ABE standard scheme) in HAS (Healthcare Application System) provides these aspects very well and removes drawback of existing key escrow problems. NFC is a wireless technology operates very close distance of each other less than 3.9 inches or less and stores a unique identification number in it. Application of CP-ABE encryption standard cryptographic standard for data storage and retrieve from server.

Keywords- NFC, CP-ABE, HAS, Cloud Computing

I. INTRODUCTION

Today’s era security is a big challenges over online networks/cloud. Many developed countries and increasingly mature society of the need to develop smart call in many health care facilities, to deliver best Medical facilities. This study suggests a practical idea based on NFC technology for an application that can offer different medicines services to patients. NFC is a high frequency secure wireless communication technology [7].

In the proposed system try to shootout all those issues which are affected on health care system tends to improve security and efficiency over the cloud network for healthcare system. Monitoring the patients in hospitals, doctor need to operate on every patient differently because every patient has a different illness and different symptoms and chances of getting confusion between patient’s disease and treatment are more.

Along with this issue patients, health records [1] which depict patient treatment history and reports are retained on paper which is difficult to maintain and unreliable for a longer period. Building healthcare system [2], [3], [4], [5], [6] using NFC Technology it may protect patients and helps the doctor to side out such fatal mistakes while doing treatment and CP-ABE provides a cryptographic solution for data security on the cloud network. Also, use of NFC technology makes the insurance claim nation faster with complete transparency and credibility by connecting it with unique ID of NFC tag and with the use of CP-ABE encryption standard for security purpose.

NFC-enabled handsets are ongoing and finalized with a simple wave or close track of two devices to each other. NFC enables communication between the tags and electronic equipment, which means that readers and writers [8]. NFC is already used for applications related to financial payments [9] and ticketing. We are proposing a new use of NFC mobile devices to access medical external tags to identify patient health cards. Health cards could be on an external label or retained on patient identification.

NFC allowing users to do safely contact less transactions, the spontaneous digital content, access and connect electronic devices simply by touching or in close taking devices proximity [8]. NFC technology allows three modes: read / write mode connection, peer-to-peer mode connection, and card emulation mode connection [10]. Radio Frequency Identification Technology has been used in different service sector [11]. NFC device can perform as an NFC tag emulator or a tag reader. In reader / writer mode NFC device looks information in the NFC tag or write the information to the tag. These labels can be stuck on chip displays, allowing the user to retrieve additional information by understanding the label with the NFC device.

It detects a label near immediate impact using the escape mechanism. An application on an NFC device can read data from and write data to the tag detected using read-write mode operations [8]. This tag also has to run different applications with the support of NFC device. The supported data rate in this mode is 106 Kbit / s. The second mode is peer to peer mode. In this mode, data is exchanged between the two devices.

NFC has two types of communication. One is the active communication mode and the passive communication. In the active mode of communication throughout the data transmission procedure and the parties themselves generate a carrier.

In the passive communication mode, mobile phone initiating provides support and independent field device responds by modulating the current field. In this mode, the camera can draw its independent operating energy of the electromagnetic field provided Initiator and the creation of a target device transponder. Communication can be active mode / passive mode. Attribute-based encryption (ABE) is a promising approach that achieves a
cryptographic access control to fine-grained data [12], [13], [14]. It provides a way to set access policies [15], [16] based on different attributes of the requester, the environment, or the data object. In CP-ABE Standard encryption defines their own attribute set over a group of attributes that must be possessed with decryption in order to decrypt the cipher text [17], [18], [19] and enforce it on the contents [20], [21]. Thus, each user with a different set of attributes is authorized to decrypt the individual data items by the security policy. Also, it removes existing disadvantage of key escrow problems [22].

II. REVIEW OF LITERATURE

Nowadays, most research in the health care system is to improve medical facilities to provide the better healthy environment for the patient. In many hospitals, they are very difficult to manage patient records and to provide a better medicine.

Because huge data to be stored on the server and nurses are manually entered using a web browser or client software. In the previous health surveillance system, the doctor needs to attend patients when they take medication at home. Different medical devices that measure, for e.g., blood pressure, weight or heart rate are integrated into the system. They send the measurements to a radio receiver connected to a PC. Users identify themselves using an NFC tag they must put near an NFC enabled-reader PC-drive to store the measurements in the background organization [23]. NFC medium formed the NFC Data Exchange Format (NDEF) and NFC tag operations. NFC tags are contactless cards based on RFID architecture [24].

NFC competence is appropriate to maintain the user-defined hi-tech experience mobile devices, nurses can perform various tasks related to patient follow up from beginning to end easy communication. NFC mobile phone may interact with RFID tags (known NFC tags) distributed by [25] environment. In the health care sector, operation and procedure of RFID technology have been researched, while its NFC subclass has been tested and found. The latest technological expansions inspired and get accessibility of NFC technology and its applications on smart devices, making good pit selection as far as much custom equipment. In addition, smart appliances have become an important part of our lives and ease of use has been definitively evaluated in general and also for elderly people and reduced. Therefore, the possibilities for the commercial potential of NFC technology are great, although the NFC applications have yet to prove their contribution and relevance to the medical field. Little research has focused on improving the value of patients’ treatment.

For example, storage of the separate drug dosing information and the avoidance of unnecessary trips to a pharmacy out of stock in the Voter circumstances [26]. In a clinical context, NFC is used by many researchers. It has implemented a solution based on NFC technology to avoid defects of drugs in hospitals. As an additional way to the success of medical data, define different responses based NFC that allow doctors or nurses to collect data by touching medical devices with a mobile phone.

Smart poster applications are one of the biggest important applications of this mode. In this application, users are able to read data from NFC posters and spend their

NFC mobile strategies. Review of Literature Survey [27], depicts NFC has been used in different sectors like smart posters, payment services, electronic wallet, loyalty management etc.

NFC has been used in different sectors like smart posters, payment services, electronic wallet, loyalty management etc. But still not much work has done in Healthcare sectors. Traditionally, NFC based Healthcare system working on the client server approach.

Nowadays many countries are using NFC in public transport systems. Tapping your phone with kiosk gives you up-to-date information about schedule and delays. Contact less cards which used for ticketing options. Many transport agencies from worldwide countries have been using NFC-enabled mobile phones. NFC device provides more information on the spot about different places and makes all things easier for tourists. NFC tags placed on monuments for checking can give more information about its monument.

NFC smart posters are the objects in or on which readable NFC tags have been placed. Various smart posters are developed using secure NFC tags. It can be done by using web server for securely retain the details of the poster. The survey is presented on several kind of areas where NFC technology has been used. Existing system like BSW CP-ABE and YWRL-CP-ABE have used CP-ABE standard scheme for security purpose.

III. SYSTEM DESIGN

NFC health care system is based on the mode of read / write. In reader-writer mode device can access NFC tag. The system architecture consists of following main elements: Doctors’ NFC Enable Smart phone, NFC tag or NFC Device, cloud server. The server centralizes the conversation between the nurse and the doctor. It also includes patients, nurses, and physician database. The server also allows the system administration to manage all this data.
Consider Following SET.

[Set S1]
STORE (F, ID, D, Encry, C): Here Receptionist enters patient’s information F into
the database D on Cloud Network C in an encrypted form with unique NFC ID.
So we can further assume to have a set 'S1' to have values 'n' number of detected
values at a particular instance.
Let us depict the current situation in the following manner
S1 = fX1 j X1D1DIDf or Tagg
where S1 is the set of all X1 such that for all X1 there exists Dataset D1 which
is uniquely identified by Unique ID of NFC tag’s.

[Set S2]
GET (F, D, Key, C): Here Doctor gets all information F about patient’s previous
Check Up History (if exists) from dataset D, Cloud Network C
by providing unique
ID of NFC Tag.
Let us depict the current situation in the following manner
S2 = fX2 j X2D2DIDf or Tagg
where S2 is the set of all X2 such that for all X2 there exists all patients Check
Up History details which can be identified by unique ID of NFC Tag.

PUT(X3, SYM, P, Key, C): Here Doctor will upload patient’s symptoms SYM on
Cloud Network C also with prescription P with X3 instances on dataset which can
be identified by unique ID of NFC Tag.

[Set S3]
GET (F, D, Key, C): Here Medical Manager gets all information F about patient’s
Medicines/Prescriptions from dataset D Cloud Network C by
providing unique ID of NFC Tag.
Let us depict the current situation in the following manner
S3 = fX4 j X4D3DIDf or Tagg
where S3 is the set of all X4 such that for all X4 there exists all patients’ medicine/prescriptions
history details which can be identified by unique ID of NFC Tag.

IV. PROBLEM FORMULATION
The view of analysis modeling, called structural analysis, considers data and the processes that transform the data as separate entities. Data objects are modeled in a way that defines attributes and relationships.

A. Mathematical Model
Let us consider that we have a Database 'D' with 'n' number of attributes of patient
information such as patient name, id, address etc.
D = fA=A Information of patient g
where D is the set of all A such that A is information of patient which to be
stored on Cloud Network. Here we can say,
A = fS1;S2;S3;S4g
Here, A consist of different sets like S1, S2, S3, S4 in that there exists different
datasets D1, D2, D3, D4 which is built as following.

PUT(X4, PAY, P, key, C): Here Medical Manager will update the patient’s payment details PAY (Smart Card) on Cloud Network C also with prescription P with X4 instances on dataset identified by unique ID of NFC Tag.

[Set S4]

GET (F, D, Key, C): Here Pathology Manager will conduct the Test and access the Test Report from Cloud Network C, dataset D by providing unique ID of NFC Tag.

Let us depict the current situation in the following manner

\[ S_4 = \{ X_5 \mid X_5 \in D \} \]

Where, \( S_4 \) is the set of all \( X_5 \) such that for all \( X_5 \) there exists all Patients Test Conduction Reports History details which can be identified by unique ID of NFC Tags.

Conduction Reports History details which can be identified by unique ID of NFC Tags.

PUT(X5, PAY, P, Key, C): Here Pathology Manager will update the patient’s payment details PAY (Smart Card) on Cloud Network C also with Test Report R with X5 instances on dataset identified by unique ID of NFC Tag.

PUTP(X4, REPORTS, C): Here pathologist will upload patient’s reports on Cloud Network C.

So, Lastly

We can Say,

\[ D = \{ A = A_1 \cup A_2 \cup A_3 \cup A_4 \} \]

V. PERFORMANCE EVALUATION

Results are depicted in terms of parameters i.e. generation time and no of attributes with the help of graphs and tables. System security becomes stronger as the size of no of attributes increases in the Key-Gen. The further section describes different data sets used in data extraction from multiple data sources. Specially, BSW CP-ABE analytical data set have been considered here and on the basis of all records, analysis gives the brief idea about which input data is used to get the result and analyze the data extraction with similar system.

Here when patient needs to be admitted in hospital receptionist will allocate NFC tag and MIFARE card to patient and its all information.

A. Evaluation of Key-Gen Operation in Proposed CP-ABE Toolkit

The running time of cpabe-keygen, cpabe-enc and cpabe-dec are linear with different attributes lattice. Evaluation of CP-ABE-keygen on a range of problem sizes for proposed CP-ABE scheme with attribute lattice are shown below. Cpabe-keygen runs in time precisely linear in the number of attributes lattice associated with the key it is issuing.

In BSW-CP ABE [13] scheme takes 0.015 - 0.0340 sec. for Single attribute in Key Gen operation. In proposed CP-ABE scheme SE inputs key takes 0.0320 sec. at high end. For 12 bit key size, SE Tag requires 0.0320 sec. to read complete key. It is differentiating by 0.0340 - 0.0320 = 0.0020 sec. Proposed scheme reduces running time with SE input key and varies from 0.010 - 0.0320 sec. for Single SE attribute.

Below three dimensional graph is showing the surface that connect set of points with respect to the Type of Scheme, Time in sec and No. of Attributes for CP-ABE Toolkit Key-Gen Time for Single SE input Attr.

Figure: CP-ABE Toolkit Key-Gen Time for Single SE input Attr.

It is showing the value for BSW CP-ABE Low, BSW CP-ABE High, Proposed CPABE Low, Proposed CP-ABE High. At right side of graph (BSW CP-ABE Low) from lower end to top corner is showing the value for 0 to 1 Attribute. Here, Low end value is 0 and High end value is 0.015 sec. (For BSW CP-ABE Low Single SE input).
The proposed CP-ABE standard scheme provides an improved performance and efficiency with the use of secure element in the key-gen, CP-ABE-enc and CP-ABE-dec operation. This helps to improve running time of CP-ABE standard scheme operation for no of attributes. It has been observe that single SE input attribute average time require 0.0320 sec and multiple time varies from 0.010 - 0.0320 sec.

The use of NFC technology as a Secure Element and Unique identifications is also making the great impact to automate the Healthcare sector.

In proposed system many new additional features can be added. Further include dynamic data of patient. Patient has to wear wearable ECG sensors that will monitor and control patient's health parameters at run time.

VI. CONCLUSION

The proposed CP-ABE standard scheme provides an improved performance and efficiency with the use of secure element in the Key-Gen, CP-ABE-enc and CP-ABE-dec operation. This helps to improve running time of CP-ABE standard scheme operation for no of attributes. It has been observe that single SE input attribute average time require 0.0320 sec and multiple time varies from 0.010 - 0.0320 sec.

The use of NFC technology as a Secure Element and Unique identifications is also making the great impact to automate the Healthcare sector.

In proposed system many new additional features can be added. Further include dynamic data of patient. Patient has to wear wearable ECG sensors that will monitor and control patient's health parameters at run time.

REFERENCES


Authors Profile

Prof. Sanjeev Sharma is a Asst. Professor of the Department of electronics Engineering, Sandip Foundation's, Sandip Institute of Technology and Research Centre, Nashik, Maharashtra, India.