VOL. 10, NO. 14, AUGUST 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

SECURING THE PRIVACY OF SENSITIVE DATA ON HEALTH MANAGEMENT SYSTEM USING ELGAMAL ENCRYPTION

G. Nagapriya[1] and Jeberson Retnaraj[2]
[1]M.Tech IT, Sathyabama University, Chennai, Tamilnadu, India
[2]Department of Information Technology, Sathyabama University, Chennai, Tamilnadu, India
E-Mail: gnagappriya@gmail.com

ABSTRACT

Most healthcare systems still rely on paper medical records. To coordinate care between patients and physicians and amongst the medical community is limited. The online health analysis system will help to check the patient health condition regardless of the patient or doctors geographical location. In practical life patients such as old aged or handcrafted peoples face lot of difficulties in tracking their health status. In this paper, the proposed solution is track the patient's health records in digital format and uploads the file in to cloud space using personal computers. The patient health record file can be encrypted by using strong security algorithm and stored in the cloud space. The doctors will check their assigned patient status by checking the client module. The Doctors and Nurses who are authenticated or Government approved doctors can be registered in to the system; they can able to view the patient records. Doctors will login in to the system, get the patient's health records from cloud space, review their health condition and reply the patients by proposing the prescribed medicines. The proposed application will help the patients by reducing their traveling time to hospitals, reduce time spending in getting their appointments, reduce time spending in taking the proposed reports by doctors and the patient reports can be viewed online without any issues.

Keywords: online health analysis system, elGamal encryption, cloud space and service, mobile communication.

INTRODUCTION

In recent days mobile technology playing a vital role and more number of mobile applications emerged which are used in day to day life and help people to reduce their workload. That is, people can use the cloud service applications, for scheduling the meetings, attend online conferences, assign the work to their team members etc. With respect to healthcare there are lot of security algorithms are used to encrypt the patient health records which are maintained in a secure way. In regular life, old aged / diseased people use to face lot of difficulties in getting appointments from doctors and diagnosing the health status from their reports.

In recent days there are lots of healthcare monitoring systems are developed and introduced in the market. Many health care monitoring applications are mobile applications which will track the patient's health condition very accurate and send the remainder messages time to time. The patient health records can be kept very safe by allowing access only to the care taker of the patient and the concern doctors and nurses who are authorized by the care takers. Only certain details can be shared with the cloud service providers and rest of the patient records are kept very secure manner in the cloud space. Government and the affiliated health care organizations are also involved in protecting patient health records so that intruders are detected before being any attacks by them.

Due to this kind of online applications and cloud storage the entire medical history of the patients are available to the doctors and nurses at any point of time. This avoids the patients can carry the health records every time when consulting the existing or new specialists. This will reduce the healthcare costs and reduces the confidentiality risks. More than the cloud sharing and installing mobile applications the safety of the patients health records are kept confidential.

Intruders from outside can hack the system and access the patient health records and try to use it in a malicious way. All these attacks from outside users are kept safe in cloud space by applying effective security algorithms. With patient health records only certain portion of data are visible to the healthcare providers and rest of the details are kept very secure manner. Only the prescribed doctors and the patient or patient health taker can able to view the complete health records.

Proposed work

In this section, we are going to present relevant work similar to sharing data in cloud for health monitoring.

Cloud - Current market dynamics

Healthcare cloud computing is used to share patient health records in electronic format between healthcare providers and pharmacists. It also plays a important role in payment of patient billing and reduces capital expenditure. Also if the patient health records are available in digital format then it enhance the speed, service and flexibility of healthcare services such as electronic medical reports available at anywhere, any time,

telemedicine, electronic medical records, and decease diagnostic techniques. Many factors such as increasing demand for best healthcare facilities, getting government initiatives and better service in low cost effectiveness are driving the global market factors for healthcare cloud computing. To add on this, increased investments from healthcare IT players and increased popularity of wireless, cloud technology and cloud services are some of the major driving force for the global healthcare cloud computing market. However, there are some drawbacks such as lack of experienced professionals that is who is aware of cloud and healthcare is key resources for the global healthcare cloud computing technology. Another important area is security, lack of security and lack of privacy of patient's information are obstructs the enhancement of the global healthcare cloud computing market.

Following are the key technology requirements for healthcare industry in terms of cloud computing:

- On-demand access to computing
- large storage facilities
- Requires big data sets for electronic health records (EHR) and for radiology image
- sharing of Electronic health records among authorized physicians and hospitals in various geographic areas, providing more timely access to life-saving information and reducing the need for duplicate testing.

Cloud - privacy and security challenges

Data maintained in the cloud servers may contain personal data, private or confidential information such as health related information which requires the correct safeguards to prevent unauthorized used to access. Globally, concerns related to data jurisdiction, security, privacy and compliance are impacting adoption by healthcare organizations.

Now a days all the organizations sharing their health records in cloud space for proper time management and for better productivity. In the large organization, for huge group of peoples, database has protected access in very less cost effective way. Simple encryption techniques are not feasible enough to handle the patient health records. It required highly protected algorithms for securing individual patient health records. Each authenticated user can be provided with a encryption key or a private key, this allows the user can enter and view their personal health records. There may many security flaws can occur as they are having direct access to the stored data and some of them sell the data to third party for gaining profit for themselves. Few examples include, administrator error, leaking patient health records and many illegal activities. Current solution is strong encryption is used for privacy and security issues.

Preliminaries

ElGamal encryption

The ElGamal encryption algorithm is an asymmetric key encryption algorithm technique for public-key cryptography. It was described by Taher Elgamal in 1985.This algorithm is very simple and efficient.

In elGamal encryption technique, to send a message to another party whose public key is G y mod P, you create a temporary public key, G^x mod P, encrypt the message by multiplying it by G^{xy} mod P, the multiplication also being modulo P, and send the temporary public key and the enciphered message as a single block.

ElGamal encryption has 3 components:

- The key generator

- chooses a large prime number p and a as primitive root g
- choose a private key a, $1 \leq a \leq p-1$
- compute and publish $A = g\,a \pmod p$

- The encryption algorithm

Randomly generate value r and encrypt data m as follows:

Encryption(m) = $m \,.b^r \bmod p$
= $m \,.c^{rx} \bmod p$

- The decryption algorithm

Decryption(E(m)) = $g^{-x} .E(m) \bmod p$
= $(c^r)^{-x} . m .c^{rx} \bmod p$
= $c^{-rx} .m .crx \bmod p$
= $m \bmod p$

Although it works, it has the following limitations.

- It does have the effect of making the cipher text twice the size of the key.
- Encryption of data depends on the keys of sender.

Limitations with elGamal encryption

Encryption with elGamal encryption depends on the keys of the sender hence not suitable for anonymous communication [10]; attacker can easily track the real key. It requires a stronger cryptographic hashing technique for stronger encryption.

Ciphertext attack

The attacker tries to encrypt and calculate the cipher as

c=(i,c*)
and sends to the receiver
c1=(i,c1*) with an arbitrary cipher text.
Then the recipient decrypts as below:
m=c1*/i

Now the attacker can able to calculate the real key which in turn identify the input data.

The issue can be resolved by hash function. Hash operation can implement by following way:

- f(0) = Initial;
- f(i) = E(f(i – 1), Mi), with M = M1, ..., Mn
- Hash(M) = f(n)

Where E(f(i),M) in the encrypted data.
Hash (M) is the hashed encrypted data.

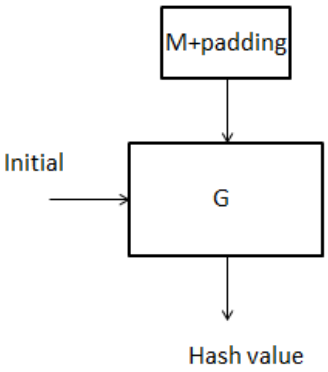

Figure-1. Hashing.

Proxy re-encryption

Proxy re-encryption technique is applied for additional security. A proxy re-encryption technique is generally used when one party wants to reveal the contents of messages sent to him and encrypted with his public key to a third party without revealing his private key. The contents are placed in different location of servers, so when decrypting the location of the servers are referenced to get the original data.

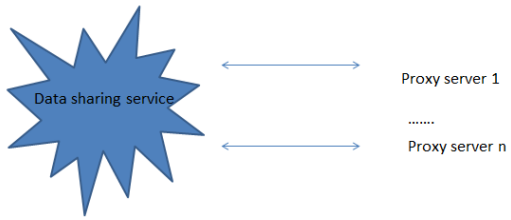

Figure-2. Proxy encryption technique.

Health analysis system

A scenario

Take a scenario where elderly patient who suffers from cardiac problems and requires immediate attention and the cardiac hospitals are located in long distance from the patient. The patients or the take career connect the ECG monitoring device such as cardio [5] and track the pulse rate of patients. Then the data can be transferred android mobile or personal computer via Bluetooth or any other communication media. Once the patient record is available the doctors can easily the analyze the patients health condition from the doctors venue from cloud storage.

System requirements

Following are the requirements for the patient and doctors:

a) At any point of time patient can able to monitor their health condition

b) The system should not depend on patient or doctor geographical location

c) The system should be used by multiple users such as many doctors or nurses

d) The system should be able to analyze different health services such pulse monitoring, to check sugar rate, to check blood pressure etc.,

System functionality

The system functionality of the proposed system is described as follows. Admin has the super user rights, he has the rights to add new user, revoke a user, transaction details, change password etc.

The patient or care taker collect the patient health report and upload the file to the doctor. The doctors can login to client module and get the patient health records. Based on the monitored data diagnose the patient decease and prescribe the solution. Figure-1 shows the flow diagram for the health analysis system.

Data model

The data model used in the health analysis system is described in the Figure-3.

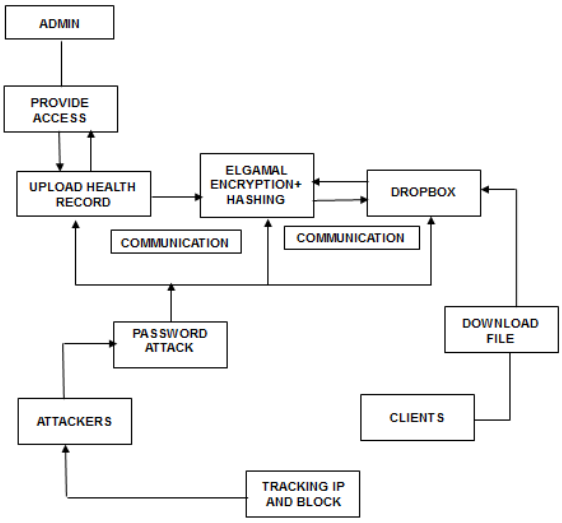

Figure-3. Data flow model.

In the proposed model, the password's digest is stored in the database; an attacker should be unable to recover the password. Then the attacker will be blocked from the accessing the application. This will eliminates the further pollution by the attacker.

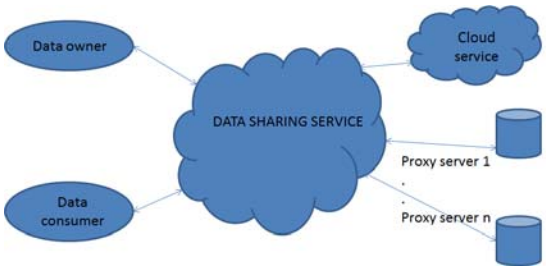

Figure-4. Flow diagram for health analysis system.

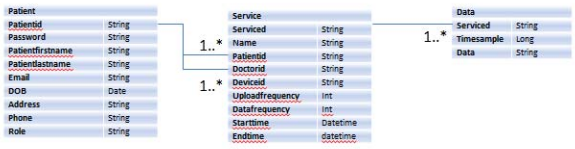

Figure-5. Data model used in health analysis system.

Implementation

The proposed system has been implemented using Java and Java Server pages and deployed the application using Tomcat server. Oracle database was used to store the user details and the patient health record file name in the cloud storage.

Evaluation

In this paper, ElGamal encryption algorithm has been evaluated.

Encrypted text using elGamal encryption:

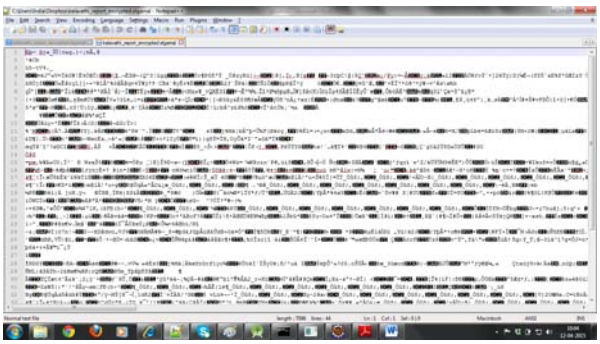

Figure-6. ElGamal encryption sample.

The system has been evaluated with uploading and downloading different size file and observed the time delay.

CONCLUSIONS

Maintaining a personal health record can be a lifesaver, literally. In emergency situations one can quickly give emergency personnel information about the patient, such as a disease that are going to be treated for, and medicines you take, any kind of allergies, and how to contact the family doctor. This allows a personal health record not only allows you to share information with your care providers but also empowers you to manage your health between visits.

There is lot of challenges with using healthcare data in shared environment for monitoring health indicates the field is still in the early stages of development growth. With well-defined dataset design and with proper data elements are generally not available today for tracking remote patient health status. Our proposed work suggests that much improvement in this area is already underway. Cloud computing is one of the way of delivering computing resources and services. Many organizations believe that the cloud and its products can improve health care services, increase health care research, and modify the face of health information technology.

This report offers an initial point for the discussion of transporting PHR in secured way, and further identification required for producing highly coordinated patient-centered care. There are lots of challenges involved in setting up such operational mechanism, identifying exactly what are the requirements which can be measured locally and compared in regionally or nationally will motivate improvements in performance is an ongoing process.

REFERENCES

[1] M. Vijayapriya. 2013. International Journal of Advanced Research in Computer Science and Software Engineering. 3(9): 2277 128X.

[2] K.S.Sureh, Mrs. Sarita Chowdary, T. Balachary. 2013. International Journal of Advanced Research in Computer Science and Software Engineering. 3(11): ISSN: 2277 128X.

[3] Jashanpreet Pal Kaur. 2014. International Journal of Advanced Research in Computer Science and Software Engineering. 4(7). ISSN: 2277 128X.

[4] Chen Deyan, Zhao Hong. 2012. Data security and privacy protection issues in Cloud computing. In: International Conference on Computer Science and Electronics Engineering (ICCSEE). 1: 647-651. http://dx.doi.org/10.1109/ICCSEE.2012.193.

[5] Zhou Minqi, Zhang Rong, Xie Wei, Qian Weining, Zhou Aoying. 2010. Sixth International Conference on "Security and Privacy in Cloud Computing: A Survey. Semantics Knowledge and Grid (SKG). pp. 105-112.

[6] Huang RuWei, Gui XiaoLin, Yu Si, Zhuang Wei. 2011. Research on privacy-preserving cloud storage framework supporting ciphertext retrieval, in: International Conference on Network Computing and Information Security. pp. 93-97.

[7] D. Subbiah, S. Muthukumaran, T. Ramkumar. 2013. The enhanced survey and proposal to secure the data in cloud computing environments. IJEST. 5(01).

[8] http://www.iusmentis.com/technology/encryption/elgamal/ elGamal encryption.

[9] http://www.arpapress.com/Volumes/Vol10Issue2/IJRRAS_10_2_16.pdf Authenticated and Secure El-Gamal Cryptosystem over Elliptic Curves, Malek Jakob Kakish, IJRRAS 10 (2), February 2012.

[10] ElGamal Encryption and Diffie-Hellman Key Exchange http://www.lkn.fe.uni-lj.si/gradiva/kk/IEEE%20%C4%8Dlanki/ElGamal%20and%20DH.pdf.

[11] ElGamal Cryptosystem http://x5.net/faqs/crypto/q29.html.