Secure Electronic Healthcare System for Myanmar by using Cryptographic Process

Chan Myae Aye
University of Computer Studies (Taunggyi)
chanmyaeaye@ucstgi.edu.mm

Hsu Mon Kyi
University of Computer Studies (Taunggyi)
hsumonkyi@ucstgi.edu.mm

Yin Nyein Aye
University of Computer Studies (Taunggyi)
yinnyeinaye@ucstgi.edu.mm

Abstract

Healthcare system in the developing country like Myanmar did not come up the power of information technology yet. Electronic healthcare system can provide more effective and enhance the current healthcare system of Myanmar. Security becomes an important issue when providing electric healthcare system because patient sensitive data is collected and shared by different users and organizations. Personal identifiable information and the patient health record are needed to protect from unauthorized use, disclosure and destruction. To be more efficient and effective healthcare service, electronic healthcare system is provided to change current traditional paper based healthcare system and a secure architecture is proposed for maintaining, transmitting and retrieving patient sensitive information by using cryptographic process. Electronic Health Record is kept in encrypted format instead of plain text record. Key Management Center (KMC) provides the key sharing process between client and Electronic Health Record Server when the client requests the sensitive data.

Keywords: information security, confidentiality, electronic healthcare, cryptographic

1. Introduction

The goal of Universal Health Coverage (UHC) is defined as ensuring that everyone can use the preventive, curative, rehabilitative, and palliative health services they need. People can also use sufficient quality to be effective, while also ensuring that the employment of those services does not make the user to financial hardship. Myanmar aspire all the goals of UHC.

To strengthen the country's health system and pave the way towards UHC is National health plans between now and 2030. [5] Transforming the present healthcare system to electronic healthcare system may well be how to boost the goal of UHC. There are some private hospitals who are already transform electronic healthcare system but there is just for their local hospital and cannot interact with other hospital, especially with public hospital in Myanmar.

Hospital information is collected monthly from all public hospitals and distributed through annual hospital statistics reports. Introduction of an electronic information system was one among the measures identified to strengthen the information system. There have been many constraints to overcome. Those are namely inadequacy and stability of electricity supply, availability and speed of Internet services and, most significantly, data sensitivity in a setting where security considerations overwhelm everything. [11] Data confidentiality is an important issue for electronic healthcare system (EHS). Patient sensitive data must be store securely and share with patient permission. Medical center such as hospital, private healthcare center shared patient information through medical processes. The medical staff access collective patient information and the confidentiality and privacy of the patient sensitive information can be easily shared due to lack of strict security control in healthcare system.

The information is a valuable resource in today information technology world. This information is stored in computer systems for easy retrieval. Even as information is becoming more valuable, unwittingly, users are also making it easier for attackers to retrieve this valuable information. *Information security means as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to get integrity, confidentiality and availability.* While the above definition is based on the code of law of the United States (section 3542, Chapter 35, title 44), the definition is remarkably consistent across the industry. [3]

The information security becomes an important issue in recent years. Confidentiality, integrity and availability of the information are needed to maintain in certain ways.

Electronic healthcare system is planned to develop for improving old-fashion healthcare system and also preserving the security of electronic healthcare system in this paper. To provide the confidentiality of the patient electronic health record (EHR), they are encrypted and stored at server by individual patient's secret key. If the client can prove his or her identity, the secret key of the encrypted information is send to client. Key management center (KMC) will provide the secret key exchange between clients who request the encrypted data and also will check the identity of the client. The system can serve the confidentiality and privacy of the client's EHR by using cryptographic process.

2. Related Works

One of the foremost most responsibilities in medical database is to stay up Confidentiality. Unless an agreement is given by the patient to publicize the information, health care system database provider must retain the patient's personal health information as confidential. Generally the patients share their health issues and personal information with doctors and such information are retained as record in healthcare database. It is terribly very important to guard the confidentiality of such information, otherwise the trust of patient on physician and healthcare area unit are going to be diminished.

The various privacy problems related to clinical database and possible ways to protect the privacy of patient information offered thorough a healthcare database from malicious people are focused on [**8**]. Data collected from varied hospitals are kept in centralized system known as health database server. The attribute information both single attribute and cluster of attributes facilitate the opponent to acknowledge a person are identified. When an opponent or ordinary user submits the query, such sensitive attributes data are de-identified [4] before it is discovered to the users. The modification process can use one among the processes like modification, cryptography, generalization or partial suppression of data or column modification.

Intelligence based E-health system is presented in [2]. A comprehensive analysis is worked by selecting the present approaches and models that were planned to stay and support the security and privacy of the e-healthcare systems. A completely unique Intelligent based Security and Privacy Model (ISPM) is proposed to retain up and support the security and privacy of e-healthcare systems. The proposed model contains multiple agents; each is responsible for taking a different form of tasks. This agent based design aims at simple and efficient access control mechanism based on the patient's situation and the requester's assigned roles. The implementation of proposed model with real-time health datasets in order to calculate its efficiency and accuracy is still needed.

An integrated approach of cloud based healthcare application architecture and electronic medical record mining are presented in [10]. A three tier cloud based application "eHealth Cloud" is proposed which will include various parties to improve old-fashioned healthcare system. RIA (Rich Internet Application) based client, SimpleDB based server and a logic layer have been established to build an simply accessible network. By using the "eHealth Cloud", enormous electronic medical record (EMR) will be kept on daily basics. Data mining from the large amount of EMR has been proposed. The process of data mining, a standard for exchanging data and a mining model is presented. Data mining technology will develop the condition easier to protect us from diseases, epidemics and unusual deaths. Government along with its people and physician will enhance the overall healthcare system using Electronic Health Cloud.

A design and implementation of self-protecting electronic medical records (EMRs) using attribute-based encryption on mobile devices are proposed in [1]. This system offers healthcare organizations to export EMRs to locations outside of their trust boundaries. The availability of EMR is maintained even when provider is offline. For the needs of emergency care and patient privacy, system is implemented to support engrained encryption and is able to protect each item within an EMR, where every encrypted item have its own access control policy. A prototype system is designed by applying a new key and cipher text policy attribute based encryption library. Implementations include an iPhone application for storing and managing EMRs offline and provide flexible and automated policy generation.

A cryptographic access control mechanism to protect the health information in EHR systems is proposed in [9]. Moreover, a new encryption framework for the cryptographic access control is developed to maintain a high level of protection. Then, systematically review the traditional cryptography methods to identify the weaknesses in order to overcome those weaknesses in new method. The following two security options are illustrated the evaluation process. Data are encrypted before save into database and Data are decrypted when access required. The system is needed to extend the algorithm to differentiate lower case and upper case letters and support to other special symbols as well.

Very recently, Myanmar government formally promulgated that the nation-wide health insurance policy would be sale for the primary time underneath an annual trial as of July 1, 2015. [12] State-owned Myanmar Insurance and personal domestic companies will deal identical policies, with customers able to get between one to five units of coverage (one unit prices more or less 50 USD), with one unit providing the foremost basic level of coverage. Myanmar citizens and foreign nationals residing within the country aged inside 6 to 65 years and who are in good health can buy the insurance. Insurers can pay about 15 USD per day of hospitalization per unit. A policy holder might receive 30 days' costa of hospitalization price per year. If a policy holder expires in hospital, their designated beneficiary will receive approximately 1,000 USD per unit of insurance in compensation. So, the security control on electronic health record becomes more importance for Myanmar. [6] Privacy and security concerns are importance issues in adoption of the health insurance policy.

An electronic health record (EHR) system is designed to allow individuals and health care providers to access their key. This system is more efficient and secure than traditional paper based systems. EHR systems would be accepted by individuals if they ensure their health information is securely stored, an access control mechanism is used and any unauthorized disclosure is prevented.

3. Electronic Healthcare System

Electronic healthcare system is firstly developed for all the patient, doctors, hospitals and healthcare provider in Myanmar. The basic architecture of the healthcare system is shown in Figure 1.

There are three sections for the electronic healthcare system. For the clients, there will be the data owners called patients and data requesters called doctors (health services provider) and researchers. The clients are the users of the EHS and they can access electronic healthcare system from their end user devices such as laptop, personal computers and mobile devices.

Cloud server is stored and processed the electronic health record (EHR). Cloud server will simplify and maintain the electronic health record database. Cloud services have a very large kind of services. According to National Institute of Security Training (NIST), there are five essential characteristics of cloud computing. They are on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. It also lists three “service models” (software, platform, and infrastructure), and four “deployment models” (private, community, public, and hybrid) that together categorize ways to deliver cloud services.

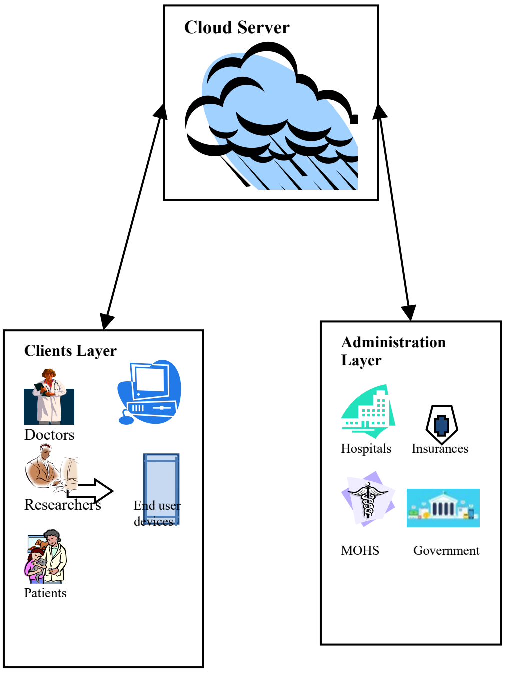

Figure 1. Electronic Healthcare system

The patients have access right to their medical record anytime. The doctor is only allowed to access the patient data if they have access right. If the doctor is not in charge of the patient they might not allow accessing the patient medical record. Moreover, researcher also request patient data for their research purpose. Patient data are shared and used for medical research without patient permission in these days. There is no privacy control over patient data on academic use in Myanmar. So the data request from the researcher also needed to review and protect the patient personal identifiable information. The security control in this paper will be focus on patient and doctor only.

The administration section will control and create security rules for the entire system. They are government and Ministry of Health and Sport (MOHS) who can control the system from top level. Healthcare policies, security policies and also health insurance policies are defined by the government and MOHS. Hospitals are also responsible to define security constraints for doctors and patients. Hospitals will determine who can access patient sensitive data and will constraint the patient’s data by authorized doctor. When all the security policy and constraints are set up for all the doctors and patients by providing role based access control for the authentication and authorization of the clients, the security mechanism proposed in this system will provide the secure storage about electronic health record. This process will be explained detail on the following sub section.

3.1 Security Control in Electronic Healthcare Sysetm

Role based access control (RBAC) is applied to control and limit access to resources by authorized user. This access control is a simple and very much effective approach for the system security. RBAC is setting access privileges for doctor, patients and healthcare providers. All the security constraints are defined, access role and actions of each user in the system are set up, and then cryptographic process will be taken place. This paper will mainly focus on the cryptographic process for EHR encryption and decryption and key distribution.

Although the privacy and confidentiality of the patient data are controlled by role based access control and specified security constraints, the sensitive data are still keeping in database as simple plain text. If the attacker can exploit the EHR server, the data can be disclosed by the attacker and patient privacy and confidentiality can compromised. To prevent this from happening, the encrypted version of the data instead of the plain text will be stored at the EHR database.

Moreover, the cloud server is also has a vulnerability. There may be concern about the privacy of the information when using cloud service. Currently, the cloud service providers take care of encryption, i.e., the cloud service providers and not the data owners have the encryption keys to the data. This allows the cloud service providers to view data on demand. Thus, the business model of advertising-for-storage is embedded in the service provider's ownership of the encryption keys. The sensitive data is needed to encrypt before upload the data to the cloud service provider. Then there would be another problem that the key owner be responsible for key management because if the owner lost their decryption keys, there would not be able to read their own data. [4]

In cryptographic process to solve this problem, the encryption processes is applied on patients’ sensitive data when storing data into the database. The patient sensitive data is encrypted by using a data key. Only the patient and the authorized user such as a doctor who treats the patient can use this key to decrypt the data. So, the Key Management Center (KMC) is proposed in this system to supervise secret key that is used to encrypt and decrypt the data. In this case, Key Management Center (KMC) is a dedicated server that can be used to manage key sharing between client and cloud server. Cryptographic processes for securing patient electronic health records are described in the following.

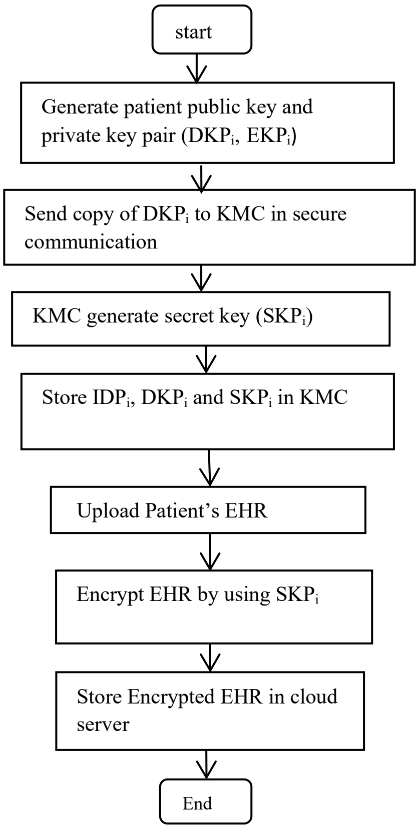
start
Generate patient public key and private key pair (DKPi, EKPi)
Send copy of DKPi to KMC in secure communication
KMC generate secret key (SKPi)
Store IDPi, DKPi and SKPi in KMC
Upload Patient's EHR
Encrypt EHR by using SKPi
Store Encrypted EHR in cloud server
End

Figure 2. Flow chart for Patient registration and EHR encryption process

3.2 Cryphtographic Processes of Secure Electronic Healthcare System

There are two types of clients called patient and doctor. Client is the data owner and the doctor is the data requester. The patient sensitive data will be stored in cloud server in encrypted form.

EKP_i	Private key of patient i
DKP_i	Public key of patient i
SKP_i	Shared key of patient i
IDP_i	Identity of patient i
i	i=1..n (n is number of patients)
EK_C	Private key of KMC
DK_C	Public key of KMC

Table1. Key Terms and Definitions

3.2.1 Patient Registration and Storing Process for Electronic Health Records

When the client takes treatment from doctor, doctor first check the patient is already registered or not. If the patient is not register, the doctor makes registration for the patient. Both public key (DKP_i) and private key (EKP_i) key pair of patient is needed to generate at registration step. The copy of DKP_i is send to KMC in secure communication and this public key is stored at KMC together with patient identity (IDP_i). Then data key (SKP_i) is generated for further encryption process for patient sensitive data. This data key is a secret key and used as an encryption key for patient sensitive data. Key terms and definitions used in this scheme are shown in table 1 and the flow chart for registration and storing process for EHR is shown in figure 2.

When the doctor inserts the patients' health record, these records are encrypted by using blowfish algorithm and store the encrypted data in cloud server.

The Blowfish algorithm is suitable and efficient for hardware implementation and no license is required. The elementary operators of Blowfish algorithm contain table lookup, addition and XOR. The table includes four S-boxes and a P-array. Blowfish is a cipher based on Feistel rounds, and the design of the F-function uses amounts to a simplification of the methods used in DES to provide the same security with greater speed and efficiency in software. [7]

Blowfish contains 16 rounds. Each round contains XOR operation and a function. Each round contains key expansion and data encryption. Key expansion generally used for generating initial contents of one array and data encryption uses a 16 round feiestek network methods. Plain text and key are the inputs of this algorithm. 64 bit plain text taken is divided into two 32 bits data and at each round the given key is expanded and stored in 18 p-array and gives 32 bit key as input and XORed with previous round data.

```
Then,
for i = 1 to 14:
xL = xL XOR Pi
xR = F(xL) XOR
xR Swap xL and xR
```

After the sixteenth round, swap xL and xR again to undothe last swap.

Then, xR = xR XOR P15 and xL = xL XOR P16.

Finally, recombine xL and xR to get the cipher text. Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order. [13]

3.2.2 Retrieving Patient Electronic Healthcare Records

The KMC also provide certification authority for the client and cloud server. When the clients need to access their sensitive data, they must send request to cloud server. The cloud server is needed to get certificate from KMC. The KMC serves as a certification process for client and server is shown in figure 3. As this paper is focused on secret key sharing for data encryption and decryption, the detailed certification process will be skipped.

When the client received certification from KMC, client send data request to server and server will redirected this request to KMC.

The following steps are taken place when the client makes a data request to KMC.

1. The client uses KMC's public key (DK_C) to encrypt a message to KMC consisting of public key DKP_i, the identity of the client (IDP_i) and nonce (N1), which is used to identify this transaction uniquely.

2. KMC sends message to client encrypted with client public key (DKP_i) and containing client's nonce (N1) as well as a new nonce generated by KMC (N2). Because only KMC could have decrypted the message in step (1), the presence of N1 in message (2) assures client that the correspondence is KMC.
3. Client returns N2, encrypted using KMC's public key (DK_C) to assure KMC that it's correspond is KMC. [14]

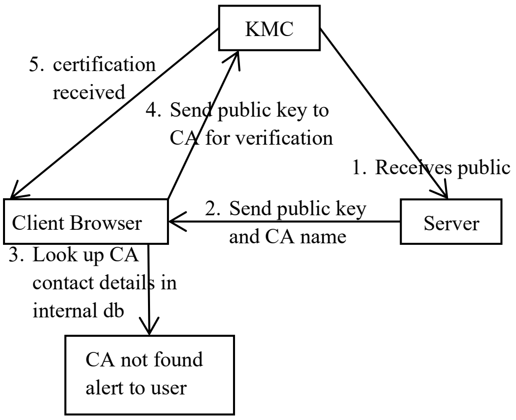
KMC
5. certification received
4. Send public key to CA for verification
1. Receives public
Client Browser
2. Send public key and CA name
Server
3. Look up CA contact details in internal db
CA not found alert to user

Figure 3. Certification process of KMC

These first three steps are taken place for exchanging the secret key between client and KMC. After the client and KMC trusted each other, KMC will send data key (shared secret key) to client. These key sharing processes are explained in the following steps.

4. A selected secret key (SKP_i) is encrypted with EK_C and then encrypted again with client public key i.e. M = E (DKP_i, E (EK_C , SKP_i) to client. Encryption of this message with client's public key ensures that only client can read it; encryption with KMC's private key ensures that only KMC sent it.
5. Client computes D (DK_C, D (EKP_i,M)), decrypt M by using EKP_i and decrypt the message again by using DK_C to recover secret key. [14]

Finally the client receives secret key for the sensitive data and can now access the data.

4. Conclusion

Electronic healthcare system can provide more effective system than current healthcare in Myanmar. Framework for Secure Electronic Healthcare System is presented and the secure key distribution for encryption process of the electronic health record is proposed in this paper. The confidentiality of the electronic health record is maintained and patient's privacy can be assured by using this system. This system only focuses on key exchange between clients for data encryption and there is no detail about the security constraints and role based access control for the user of the system. There will be the opportunity for future extension on implementation of the secure electronic healthcare system and role based access control for each user.

References

[1] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U Lehmann, Z. N. J. Peterson, A. D. Rubin, "*Securing Electronic Medical Records Using Attribute-Based Encryption On Mobile Devices*", SPSM '11: Proceedings of the 1st ACM workshop on Security and privacy in smart phones and mobile devices, October 2011, pp 75–86

[2] M. A. Alanezi , Z. F. Khan, "*Intelligent based E-healthcare Systems: Towards Security and Privacy*", IJCSNS International Journal of Computer Science and Network Security, VOL.19 No.3, March 2019, pp 16 -23.

[3] M. Agrawal, A. Campoe, E. Pierce, "Information Security and IT Risk Management", Wiley, April 2014.

[4] McGraw D. , "*Building, Public Trust in Uses of Health Insurance Portability and Accountability Act De-identified Data"*, JAMIA (Journal of the American Medical Informatics Association) 2013;20(1), pp 29-34.

[5] Ministry of Health and Sports, National Health Plan, second year's annual operational plan (2018-2019), October 2018.

[6] N. N. Latt, S. M. Cho, N. M. M. Htun, Y. M. Saw, M. Noe, H. A. Myint, F. Aoki, J. A. Reyer, E. Yamamoto, Y. Yoshida and N. Hamajima, "Healthcare in Myanmar", Review Article, Nagoya J. Med. Sci. 78, 2016, pp 123-134.

[7] Pia, S. and Karamjeet, S. "Image Encryption and Decryption using Blowfish Algorithm in Matlab." International Journal of Scientific & Engineering Research, 4(7), pp 150-154 (2013).

[8] P.Kamakshi, "Privacy and Confidentiality issues in healthcare databases", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 4, Issue 4, April 2016, pp 7546-7551.

[9] P. Vimalachandran, H. Wang, Y. Zhang, G. Zhuo and H. Kuang, "*Cryptographic Access Control in Electronic Health Record Systems: A Security Implication*", Web Information Systems Engineering – WISE 2017: 18th International Conference, Puschino, Russia, October 7-11, 2017, Proceedings, Part II, pp 540-549.

[10] S. Biswas, Anisuzzaman, T. Akhter, M. S. Kaiser and S. A. Mamun, "*Cloud Based Healthcare Application Architecture and Electronic Medical Record Mining: An Integrated Approach to Improve Healthcare System*" 2014 17th International Conference on Computer and Information Technology (ICCIT), December 2014, pp 286- 291.

[11] T. T. Sein, P. Myint, N. Tin, H. Win, T. Sein, *Republic of the Union of Myanmar Health System Review (Health Systems in Transition, Vol.4 No. 3 2014*, World Health Organization,

[12] The Global New Light of Myanmar Newspaper, Vol. II, Number 56, 16, Tuesday, June 2015.

[13] Ugba T. Pius1, Eze C. Onyebuchi2, Ogidi P. Chinasa3, Ekle F. Adoba, "*A Cloud-Based Data Security System using Advanced Encryption (AES) and Blowfish algorithms*", Journal of Scientific and Engineering Research, 2018, 5(6):59-66

[14] William Stalling, "Cryptography and Network Security, Principal and Practice", Fourth Edition, Prentice Hall, November 16, 2005.