Secure Topology for Electronic Medical Record Transmissions

Hamdan O. Alanazi, M.L. Mat Kiah, A.A. Zaidan, B.B. Zaidan and Gazi Mahabubul Alam

Faculty of Computer Science and Information Technology, University Malaysia, 50603, Kuala Lumpur, Malaysia

Faculty of Engineering, Multimedia University Jalan Multimedia, 63100 Cyberjaya, Selangor, Malaysia

Network and Communication Security Research Group, ICT and Computational Science Research Cluster, University of Malaya, 50603 Kuala Lumpur, Malaysia

Department of Educational Management, Planning and Policy, Faculty of Education, University of Malaya, 50606 Kuala Lumpur, Malaysia

Faculty of Applied Medical Science, King Saud University, King Saud University, P.O. Box 2454, Riyadh 11451, Kingdom of Saudi Arabia

Abstract: In this study, handshake protocol for patient, medical center and doctor, medical center is proposed for electronic medical record transmission to improve the confidentiality of data transmission and non-repudiation of sending and receiving medical records. The proposed topology depends on symmetric and asymmetric cryptography to achieve high level of secrecy for electronic medical records. The new topology has been described on multi-users (i.e., Doctors and Patient). The new topology has been implemented using Ntru crypto-system and AES encryption method. The proposed solution has been tested to have high level of confidentiality up to the legal age of the medical records.

Key words: Electronic medical records, confidentiality, non-repudiation, PKI, AES, Ntru

INTRODUCTION

Security is defined as the degree of protection against danger, damage, loss and criminal activity (Qabajeh et al., 2009; Hameed et al., 2010). Particularly when a message must be delivered to more than one destination, authentication and confidentiality are required (Al-Frajat et al., 2010; Raad et al., 2010). Providing security for electronic documents is an important issue (Zaidan et al., 2010h; Ahmed et al., 2010). In information security confidential information or confidential data must only be used, accessed, disclosed or copied by users who have the authorization and only when there is a real need (Zaidan et al., 2010c; Alam et al., 2010). While integrity means that data can not be modified without authorization (Hmood et al., 2010c; Zaidan et al., 2010i). Non-repudiation is the receiver cannot deny having received the data nor can the other party denies having sent a data (Naji et al., 2009; Zaidan et al., 2010f). Electronic medical records or EMR is typically digitalizing the legal medical record created at the delivers care organizations, such as hospital and doctors’ surgery. Many people consider their health information to be highly sensitive data and deserving the strongest protection under the law (Alanazi et al., 2010; Hashim et al., 2010). Several electronic medical record systems have been implemented in the literature however; these systems have weaknesses in the security. Brandner et al. (2002) provided an electronic signature using PKI. Moreover, they mentioned about the signature law and how it has to be incorporated in electronic patient records. Their intended PKI is based in the German signature Law. Smith and Eloff (1999) has stated that RSA Digital Signature Technology be able to enroll the authenticity of images to at least the stage of confidence necessary for interbank electronic transfer. Epstein et al. (1998) gave an impression of new security concerns, new legislation mandating secure medical records and solutions given that security, he depicted that RSA as a digital signature algorithm to secure the medical records. Janbandhu and Siyal (2001) proposed biometric signatures to secure the medical records; the new approach has integrated the biometrics with RSA PKI based on digital signature generation. According to (Maitra and Sarkar, 2008; Schriddle et al., 2009) we can observe that RSA is no more security supplementary. Gobi and Vivekanandan (2009) proposed the digital envelope that combines MD5 and advance encryption.
standard AES with Hyper Elliptic Curve Cryptography (HECC). Suitability of this algorithm due to the limitation of the hardware is quite expensive. Moreover, there are number of attackers available on ECC.

Electronic medical records required security solution that can provide confidentiality for more than 30 year (the legal age of electronic medical records).

CRYPTOGRAPHY

Encryption is the process of transforming data (i.e., plaintext) to unreadable data (i.e., cipher) using one of the cryptography methods. Decryption is the process of retrieve the plaintext from the cipher using revised process of encryption (Zaidan et al., 2010a; Al-Bakri and Kiah, 2010).

Cryptography has two main techniques, symmetric and asymmetric. An encryption method called symmetric cryptography when sender and receiver use the same key for encryption and decryption (Abomhara et al., 2010a; Zaidan et al., 2010e). Asymmetric cryptography refers to the cryptography systems using two keys (i.e., public and private key), one for encryption and other key for decryption (Abomhara et al., 2010a, b; Zaidan et al., 2010d).

Symmetric cryptography is faster than the asymmetric; however, with symmetric cryptography we can only achieve data confidentiality (Zaidan et al., 2010j; Al-Bakri and Kiah, 2010). Unlike symmetric, asymmetric provide data integrity and non-repudiation in addition to the confidentiality.

Symmetric cryptography has many algorithms such as blowfish, DES and AES. AES- Rijndael considered as the strongest symmetric cryptography algorithms (Hmood et al., 2010b; Zaidan et al., 2010g). AES- Rijndael has been chosen from US government to secure the high sensitive data.

Asymmetric cryptography has number of algorithms such as RSA, ECC and Ntru (Al-Bakri and Kiah, 2010, Zaidan et al., 2010b). In the literature, Ntru has been approved to be the fastest PKI among the RSA and ECC, moreover, Ntru is providing high security comparing with RSA and ECC. Unlike RSA and ECC, there is no real attacker available for Ntru (Yee and Kiah, 2010; Hmood et al., 2010a; Al-Bakri and Kiah, 2010).

In this research, we proposed AES- Rijndael and Ntru PKI to implement high secure electronic medical records transmission over unsecure channels.

SECURE TOPOLOGIES FOR ELECTRONIC MEDICAL RECORDS

Electronic medical records considered as sensitive data, many users have the access to this data such as internal doctors, administrator, insurance companies and patients. With this number of users, maintain the security become a difficult task. In this study, we proposed a secure topology to ensure the confidentiality, integrity and non-repudiation using symmetric and asymmetric cryptography. The new topology overcomes the weaknesses of the previous systems.

Then we will describe the system in four scenarios; these scenarios assumed the server has public key Pu, and private key Pr.

Scenario one: First registration at the medical center.

In this scenario, the patient registers at the medical center. The medical center administer the information of the patient and generate his/her session key (Fig. 1) as follow:

1. Patient register in the medical center XYZ
2. Admin full his/her information and generate session key S

Scenario two: Signup for new account

In this scenario, the patient registers as a client in the system, consider the patient X has session key S send request message M to the server (Fig. 2):

1. Send request to the server using the patient session key S, X enc(M)
2. Server decrypt the request using the patient session key S and get the message M, Server denc(M)
3. Server generate the public and private key for patient X, PuX, PrX

Fig. 1: Patient first registration

Fig. 2: Patient signup his/her account
4: Sever send \( Pu_x \), \( Pr_x \) to the patient encrypted by session key \( S \), Server \( \text{enc}(Pu_x, Pr_x) \)
5: Patient decrypts the message using his/her session key. Patient has session key \( S \), public key \( Pu_x \) and private key \( Pr_x \)

Scenario three: Patient request for his/her medical record.

In this scenario, the patient requests for his/her records are as follows (Fig. 3):

1: Patient send request for the server public key \( Pu_x \)
2: Server send the public key to the patient
3: Patient send other request \( R \) encrypted by the server public key and encrypted again by his/her session key \( \text{enc}(R) \) \( \text{enc}(R) \) \( \text{enc}(R) \)
4: Server decrypt the request by the patient session key and server private key Server \( \text{dec}(R) \) \( \text{dec}(R) \) \( \text{dec}(R) \)
5: Server encrypt the medical record \( MR \) using the patient public key and patient session key Server \( \text{enc}(MR) \) \( \text{enc}(MR) \) \( \text{enc}(MR) \)
6: Patient decrypt the record using his/her session key and private key \( X \) \( \text{dec}(MR) \) \( \text{dec}(MR) \) \( \text{dec}(MR) \)

Scenario four: Doctor request for patient records.

In this scenario the doctor request for patient records are as follows: (Fig. 4):

1: Doctor send request for the server public key \( Pu_x \)
2: Server send the public key to the doctor
3: Doctor send other request \( R \) encrypted by the server public key and encrypted again by the doctor session key \( \text{enc}(R) \) \( \text{enc}(R) \) \( \text{enc}(R) \)
4: Server decrypt the request by the doctor session key and server private key Server \( \text{dec}(R) \) \( \text{dec}(R) \) \( \text{dec}(R) \)
5: Server encrypt the medical record \( MR \) using the doctor public key and patient session key Server \( \text{enc}(MR) \) \( \text{enc}(MR) \) \( \text{enc}(MR) \)
6: Doctor decrypt the record using his/her session key and private key \( Dr \) \( \text{dec}(MR) \) \( \text{dec}(MR) \) \( \text{dec}(MR) \)

CONCLUSION

In this study we present secure topology for electronic medical records using hybrid approach consist of symmetric and asymmetric cryptography. Since available attackers for both AES-Rijndael and Ntru PKI do not exist. Ntru cryptosystem and AES-Rijndael have been proposed in our topology. The proposed topology used the share keys and PKI to achieve high confidentiality on data transmission and prevent the receivers (i.e. the patients themselves or doctor) from deny having received the data. Moreover, our system can provide evidence about the person who has the access to patient records in case of legal and illegal accesses.

ACKNOWLEDGMENTS

This research has been funded in part from University of Malaya under No. UM.C/625/1. The Authors would like to acknowledge Multimedia University as the Co-funder for this research.

REFERENCES


