International Journal of Pharmacology

ISSN 1811-7775

science alert

ansinet
Asian Network for Scientific Information

International Journal of Pharmacology 6 (6): 954-958, 2010
ISSN 1811-7775

Secure Topology for Electronic Medical Record Transmissions

[1,5]Hamdan O. Alanazi, [1,3]M.L. Mat Kiah, [2,3]A.A. Zaidan, [2,3]B.B. Zaidan and [4]Gazi Mahabubul Alam
[1]Faculty of Computer Science and Information Technology, University Malaysia,
50603, Kuala Lumpur, Malaysia
[2]Faculty of Engineering, Multimedia University Jalan Multimedia, 63100 Cyberjaya, Selangor, Malaysia
[3]Network and Communication Security Research Group, ICT and Computational Science Research Cluster,
University of Malaya, 50603 Kuala Lumpur, Malaysia
[4]Department of Educational Management, Planning and Policy, Faculty of Education,
University of Malaya, 50606 Kuala Lumpur, Malaysia
[5]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 can not 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 organization, 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; Schridde *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

Corresponding Author: Hamdan O. Alanazi, Faculty of Computer Science and Information Technology, University Malaysia, 50603, Kuala Lumpur, Malaysia

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_S and private key Pr_S.

Scenario one: First registration at the medical center.

In this scenario, the patient registers at the medical center for the first time. The medical center admin register 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$(M)_S$
2: Server decrypt the request using the patient session key S and get the message M, Server dec$(M)_S$
3: Server generate the public and private key for patient X, Pu_X, Pr_X

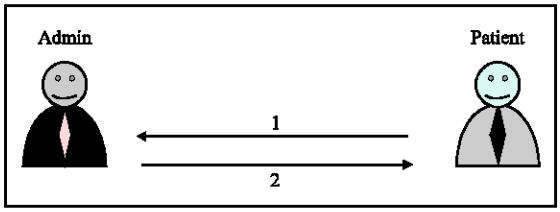

Fig. 1: Patient first registration

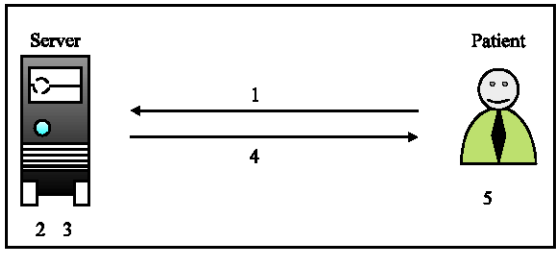

Fig. 2: Patient signup his/her account

4: Sever send Pu_X, Pr_X to the patient encrypted by session key S, Server enc(Pu_X, Pr_X)$_S$
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_S
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 X enc((R) $_{PuS}$)$_S$
4: Server decrypt the request by the patient session key and server private key Server dec((R) $_{PrS}$)$_S$
5: Server encrypt the medical record MR using the patient public key and patient session key Server enc((MR) $_{PuX}$)$_S$
6: Patient decrypt the record using his/her session key and private key X dec((MR) $_{PrX}$)$_S$

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_S
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 Dr_X enc((R) $_{PuS}$)$_{Sx}$

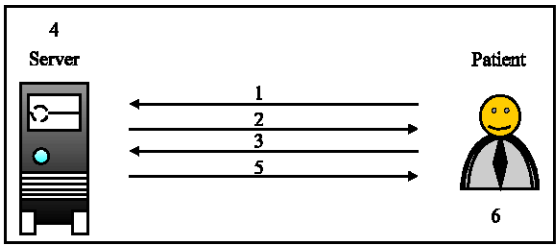

Fig. 3: Patient requests his/her records

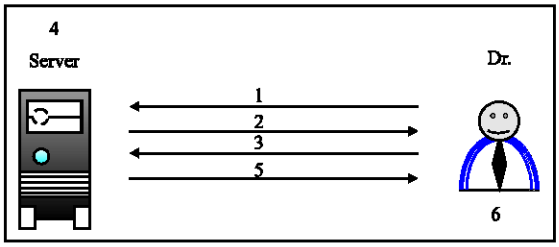

Fig. 4: Doctor requests for patient records

4: Server decrypt the request by the doctor session key and server private key Server dec((R) $_{PrS}$)$_{Sx}$
5: Server encrypt the medical record MR using the doctor public key and patient session key Server enc((MR) $_{PuX}$)$_{Sx}$
6: Doctor decrypt the record using his/her session key and private key Dr_X dec((MR) $_{PrDrX}$)$_{Sx}$

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

Abomhara, M., O. Zakaria, O.O. Khalifa, A.A. Zaidan, B.B. Zaidan and O.A. Hamdan, 2010a. Overview: Suitability of using symmetric key to secure multimedia data. J. Applied Sci., 10: 1656-1661.

Abomhara, M., O.O. Khalifa, O. Zakaria, A.A. Zaidan, B.B. Zaidan and A. Rame, 2010b. Video compression techniques: An overview. J. Applied Sci., 10: 1834-1840.

Ahmed, M.A., M.L.M. Kiah, B.B. Zaidan and A.A. Zaidan, 2010. A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm. J. Applied Sci., 10: 59-64.

Al-Bakri, S.H. and M.L.M. Kiah, 2010. A novel peer-to-peer SMS security solution using a hybrid technique of NTRU and AES-Rijndael. Sci. Res. Essays,

Al-Frajat, A.K., H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan, 2010. Hiding data in video file: An overview. J. Applied Sci., 10: 1644-1649.

Alam, G.M., M.L.M. Kiah, B.B. Zaidan, A.A. Zaidan and H.O. Alanazi, 2010. Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study. Sci. Res. Essays, 5: 3254-3260.

Alanazi, H.O., H.A. Jalab, G.M. Alam, B.B. Zaidan and A.A. Zaidan, 2010. Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance. J. Med. Plants Res., 4: 2059-2074.

Brandner, R., M. van der Haak, M. Hartmann, R. Haux and P. Schmucker, 2002. Electronic signature for medical documents-integration and evaluation of a public key infrastructure in hospitals. Methods Inform. Med., 41: 321-330.

Epstein, M.A., M.S. Pasieka, W.P. Lord, S.T.C. Wong and N.J. Mankovich, 1998. Security for the digital information age of medicine: Issues, applications and implementation. J. Digit. Imag., 11: 33-44.

Gobi, M. and K. Vivekanandan, 2009. A new digital envelope approach for secure electronic medical records. Int. J. Comput. Sci. Network Security, 9: 1-6.

Hameed, S.A., B.B. Zaidan, A.A. Zaidan, A.W. Naji and O.F. Tawfiq, 2010. An accurate method to obtain bio-metric measurements for three dimensional skull. J. Applied Sci., 10: 145-150.

Hashim, F., G.M. Alam and S. Siraj, 2010. Information and communication technology for participatory based decision-making-E-management for administrative efficiency in higher education. Int. J. Phys. Sci., 5: 383-392.

Hmood, A.K., H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan, 2010a. On the Capacity and security of steganography approaches: An overview. J. Applied Sci., 10: 1825-1833.

Hmood, A.K., Z.M. Kasirun, H.A. Jalab, G.M. Alam, A.A. Zaidan and B.B. Zaidan, 2010b. On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates. Int. J. Phys. Sci., 5: 1054-1062.

Hmood, A.K., B.B. Zaidan, A.A. Zaidan and H.A. Jalab, 2010c. An overview on hiding information technique in images. J. Applied Sci., 10: 2094-2100.

Janbandhu, P.K. and M.Y. Siyal, 2001. Novel biometric digital signatures for Internet based applications. Inform. Manage. Comput. Security, 9: 205-212.

Maitra, S. and S. Sarkar, 2008. Revisiting Wiener's Attack-New Weak Keys in RSA. In: Information Security, Wu, T.C., C.L. Lei, V. Rijmen and D.T. Lee (Eds.). LNCS. 5222, Springer-Verlag, Berlin, pp: 228-233.

Naji, A.W., A.A. Zaidan and B.B. Zaidan, 2009. Challenges of hidden data in the unused area two within executable files. J. Comput. Sci., 5: 890-897.

Qabajeh, L.K., M.L.M. Kiah and M.M. Qabajeh, 2009. A scalable and secure position-based routing protocol for ad-hoc networks. Malaysian J. Comput. Sci., 22: 99-120.

Raad, M., N.M. Yeasin, G.M. Alam, B.B. Zaidan and A.A. Zaidan, 2010. Impact of spam advertisement through email: A study to assess the influence of the anti-spam on the email marketing. Afr. J. Bus. Manage., 4: 2362-2367.

Schridde, C., M. Smith and B. Freisleben, 2009. TrueIP: Prevention of IP spoofing attacks using identity-based cryptography. Proceedings of the 2nd International Conference of Security of Information and Networks, Oct. 06-10, Famagusta, Cyprus, pp: 128-137.

Smith, E. and J.H.P. Eloff, 1999. Security in health-care information systems-current trends. Int. J. Med. Inform., 54: 39-54.

Yee, P.L. and M.L.M. Kiah, 2010. Shoulder surfing resistance using penup event and neighbouring connectivity manipulation. Malaysian J. Comput. Sci., 23: 121-140.

Zaidan, A.A., B.B. Zaidan, A.K. Al-Fraja and H.A. Jalab, 2010a. Investigate the capability of applying hidden data in text file: An overview. J. Applied Sci., 10: 1916-1922.

Zaidan, A.A., B.B. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010b. An overview: Theoretical and mathematical perspectives for advance encryption standard/rijndael. J. Applied Sci., 10: 2161-2167.

Zaidan, A.A., B.B. Zaidan, H.O. Alanazi, A. Gani, O. Zakaria and G.M. Alam, 2010c. Novel approach for high (secure and rate) data hidden within triplex space for non multimedia file. Sci. Res. Essays, 5: 1965-1977.

Zaidan, A.A., B.B. Zaidan, A.Y. Taqa, K.M.S. Mustafa, G.M. Alam and H.A. Jalab, 2010d. Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem. Int. J. Phys. Sci., 5: 1992-2000.

Zaidan, B.B., A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010e. On the differences between hiding information and cryptography techniques: An overview. J. Applied Sci., 10: 1650-1655.

Zaidan, B.B., A.A. Zaidan, A. Taqa, G.M. Alam, M.L.M. Kiah and H.A. Jalab, 2010f. StegoMos: A secure novel approach of high rate data hidden using mosaic image and ANN-BMP cryptosystem. Int. J. Phys. Sci., 5: 1796-1806.

Zaidan, A.A., H.A. Karim, N.N. Ahmed, G.M. Alam and B.B. Zaidan, 2010g. A new hybrid module for skin detector using fuzzy inference system structure and explicit rules. Int. J. Phys. Sci., (In Press).

Zaidan, A.A., N.N. Ahmed, H.A. Karim, G.M. Alam and B.B. Zaidan, 2010h. Increase reliability for skin detector using backprobgation neural network and heuristic rules based on YcbCr. Sci. Res. Essays, 5: 2931-2946.

Zaidan, A.A., H.A. Karim, N.N. Ahmed, G.M. Alam and B.B. Zaidan, 2010i. A novel hybrid module of skin detector using grouping histogram technique for bayesian method and segment skin adjacent-nested technique for neural network. Int. J. Phys. Sci., (In Press).

Zaidan, A.A., N.N. Ahmed, H.A. Karim, G.M. Alam and B.B. Zaidan, 2010j. Spam influence on the business and economy: theoretical and experimental study for textual anti-spam filtering using mature document processing and naïve bayesian classifier. Afr. J. Bus. Manage.,