Parasitic overview on different key management schemes for protection of Patients Health Records

Shibin David[1*], K. Martin Sagayam[2], Ahmed A. Elngar[3]
[1]Department of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore 641114, India.
E-mail: **zionshibin@gmail.com**
[2]Department of ECE, Karunya Institute of Technology and Sciences, Coimbatore 641114, India.
E-mail: **martinsagayam.k@gmail.com**
[3]Faculty of Computers and Artificial Intelligence, Beni-Suef University, Beni Suef City, 62511, Egypt
E-mail: **elngar_7@yahoo.co.uk**
Corresponding Author: (Shibin David[1*], zionshibin@gmail.com**)**

Abstract: The main goal of HIPAA (Health Insurance Portability and Accountability Act) is to protect health information of individuals against access without consent or authorization. Security and privacy are the main issues in HIPAA. A compliant key management solution is used to reduce harm and risk while providing cryptographic mechanisms. Using ECC (Elliptic Curve Cryptography) we ensure more security for access of patient's health records. This provides same level of security for access of patient's health records. Patient's health Information is stored in RFID cards. Finally, the proposed method ensures higher level of security than other existing cryptographic techniques. ECC provides more security even with small key sizes. Proposed scheme describes the various counter measures for improving security and a key recovery mechanism for the protection of keys.

Keywords: *Health Insurance Portability and Accountability Act (HIPAA), Electronic Protected Health Information (EPHI), Key management, RFID cards.*

Received: January 25, 2021 Revised: March 30, 20201 Accepted: April 11, 2021

DOI: 10.5281/zenodo.4898049

1. Introduction

The Health Insurance Portability and Accountability Act (HIPAA) is the most widely used regulation that protects the person's health information and prevents unauthorized access by ensuring health information security and patient privacy to the users. With the emergence of technology, paper-based health records have change to electronic based for more convenient usage and maintenance. The protection and security of personal information is very important in health sector. Security and privacy in Electronic health record (EHR) can be affected by hackers, viruses, and worms. EHRs are electronic versions of the paper charts in your doctor's or other health care provider's office. An EHR may include detailed information about your medical history, notes, and other information about your health including your symptoms, diagnoses, medications, lab results, vital signs, immunizations, and reports from diagnostic tests such as x-rays. Patients EHR can be accessible from several sites. These privacy and security regulations increase availability and confidentiality of health information. We discuss the problems associated with the privacy and security regulations and offer a possible solution to the current obstacles. As accuracy and confidentiality increases, there are certain potential threats to the confidentiality of information. Hence, we implement technical measures to guard against unauthorized access. The purpose of integrity controls is to ensure the ePHI data is not altered while transmitting. Encryption serves to be the best approach for this which is not easily readable or decrypted without proper authorization.

The main goals of security are confidentiality, availability and integrity. Confidentiality is the process of ensuring that information is accessible only to those authorized to have access to it. Integrity is the process of ensuring the information is accurate and it is not modified in an unauthorized fashion. Availability refers to the process of being accessible and useable upon demand by an authorized entity. The Protected Health Information (PHI) consists of name, address, telephone number, medical record number, patient's present, past and future behaviour. Authorization refers to each healthcare institutions must obtain individual's permission while using and/or disclosing individual's PHI's.

The cryptographic system provides the security of the PHI proposed by the HIPAA.A compliant key management solution is used to reduce harm and risk while providing cryptographic mechanisms. Lee's method offers a cryptographic solution for preserving patient's privacy. But this was found to be inefficient as patients cannot freely change their own passwords.

Patient's records are stored in the hospital after creating. Also, consent exception cases are also discussed in our method for if a patient is unable to authorize the access. This includes emergency cases like if the patient is unconscious etc. For this, key recovery mechanism is used for decryption to reveal the encrypted PHI. This fosters the trust between patients and healthcare institutes. ECC (Elliptic Curve Cryptography) is an emerging public key cryptosystem that offers high level of security with smaller key sizes.

There are certain consent exception cases discussed here. There may be situations where patient is unconscious and unable to access her medical record, at that time for the purpose of saving life of the patient, privacy regulations state that the use and disclose of PHI is possible. In those situations, an unauthorized healthcare provider can obtain the encryption key under third party supervision, such as a governmental agency, to access patients' PHIs.

Received: January 25, 2021 Revised: March 30, 20201 Accepted: April 11, 2021

DOI: 10.5281/zenodo.4898049

2. Literature Survey

Patients Health Information is stored in smart cards. So, for providing security for the details stored against unauthorized access many algorithms were proposed.

A Cryptographic Key Management Solution for HIPAA Privacy/Security Regulations

(Wei-Bin Lee and Chien –Ding Lee 2008) proposed a cryptographic key management solution to meet the challenges of privacy/security issues. This method improves healthcare quality and product patient's privacy. The patient's health information is stored in smart card. They provide a key recovery mechanism to solve the problem of consent exception which describes that use and disclose of patients details without the patient's permission for life saving purposes. To achieve these, they provide digital signatures for verification of signature. Secure hash algorithm (SHA-256) is used to provide data integrity. To provide unauthorized access of patient's health records a symmetric cryptosystem (AES) with 256-bit keys that ensure confidentiality and overhead. Patients cannot freely change their own passwords and don't support multiple access.

A Novel Key Management Solution for Reinforcing Compliance with HIPAA Privacy/Security Regulations

(Kevin I.J.Ho,et.al..,2011) A novel key management solution is proposed for ensuring privacy and security in health records. Propose a protection model for decrypting medical images from unauthorized access. Implementation of this model includes asymmetric cipher, a one-way hash function, an identification watermark generator, and a watermark embedding/extracting mechanism. Watermarking techniques are used to get high quality medical images. Prevents from illegal distribution tracking. The method used is secure and feasible.

Preserving PHI in compliance with HIPAA privacy/security regulations using cryptographic techniques

(Jing Li, et.al.,2008) A novel model was proposed by using smart card and protected health recorders. Public key infrastructure used here is DSA. To provide confidentiality of health records symmetric encryption/decryption are used. For authorization purpose a hash algorithms and DES.

Efficient key management for preserving HIPAA regulations

(Hui-feng Huang and kuo-Ching Liu 2010) Elliptic curve cryptography an efficient key management solution was proposed that guarantees security. This has an advantage of using smaller key sizes and faster computation than smart card based cryptographic solution. Patients can freely update their passwords. Consent exception cases can be solved. For encrypting data AES is used. the disadvantage of using this method is only one authorized user can access his/her medical record at a time.

A Hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations

Received: January 25, 2021 Revised: March 30, 20201 Accepted: April 11, 2021

DOI: 10.5281/zenodo.4898049

(Hsiao-Hwa Chen et.al.,2009) Hybrid public key infrastructure solution is introduced to comply with security/privacy regulations. Supports recent paper-based e-health system environment. Disadvantages of this model were there was no solution for consent exception and do not support foreign accesss.AES was used for encryption to control unauthorized access.

A certificate Authority based cryptographic solution for HIPAA privacy/security regulations

(Sangram Ray and G. P. Biswas 2013) Medical center server is located in each hospital instead of using smart card for storing patients PHI and can be accessed by using Internet. Public key certificates are maintained by certificate authority. This ensures patients privacy even through e-health system. It protects from replay attacks. Supports foreign and multiple access. Symmetric secret key is generated using Diffie Hellman. Communication and processing overhead are low compared with other techniques.

Design of RSA-CA based e-health system for supporting HIPAA privacy/security regulations

(Sangram Ray and G.P.Biswas 2012) describes patient-centric e-health system based on RSA-CA based public key certificate that ensures security while sharing patients records on internet. Data are stored in medical center server (MCS). This system is easily implementable which shows better performance and also avoid relay attacks. This also supports duality (MCS or smart card based).

3. Conclusion

A compliant key management scheme was developed with key recovery mechanism to solve the problem of consent exception. Thus, even though EHRs do increase the accuracy and accessibility of patient's records, more potential threats are there to security and privacy of information. Proposed method helps for managing the EHRs and ensuring complete security along the patient's records. The patient can add/revoke their authorization with more than designated healthcare institutes. The advantages of RFID cards have great impact on the security of our proposed method. The reusability concept of RFID brings significant efficiency to the protection of patient's health record. ECC (Elliptic curve cryptography) ensures security with smaller number of keys.

References

[1] Alese, B. K., Philemon E. D., Falaki, S. O. (2012), "Comparative Analysis of Public-Key Encryption Schemes", International Journal of Engineering and Technology Volume 2 No. 9.

[2] Andrew Clarke, Robert Steele (2012), "Secure and Reliable Distributed Health Records: Achieving Query Assurance across Repositories of Encrypted Health Data", 45th International Conference on System Sciences.

[3] C.-D. Lee,K.I.-J. Ho, W.-B. Lee (2011), "A novel key management solution for reinforcing compliance with HIPAA privacy/security regulations", IEEE Transactions on Information Technology in Biomedicine 15 (July (4)) 550–556.

[4] Dr. Najib A. kofahi (2013), "An Empirical Study to Compare the Performance of some Symmetric and Asymmetric Ciphers", International Journal of Security and Its Applications Vol.7, No.5.

[5] H.-F.Huang, K.-C. Liu (2011), "Efficient key management for preserving HIPAA regulations", Journal of Systems and Software 84 (2011) 113–119.

[6] J. Hu, H.-H. Chen, T.-W. Hou (2010), "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations", Computer Standards & Interfaces 32 (October (5/6)) (2010) 274–280.

[7] J. Li, J.-S. Lee, C.-C.Chang (2008), "Preserving PHI in compliance with HIPAA privacy/security regulations using cryptographic techniques", International Conference on Intelligent Information Hiding and Multimedia Signal Processing.

Received: January 25, 2021 Revised: March 30, 20201 Accepted: April 11, 2021

DOI: 10.5281/zenodo.4898049

[8] Jelena Mirkovic, Haakon Bryhni, Cornelia M. Ruland (2011) "Secure Solution for Mobile Access to Patient's Health Care Record", IEEE 13th conference.
[9] Jerry Krasner (2004), "Using Elliptic Curve Cryptography (ECC) for Enhanced Embedded Security", American Technology International.
[10] Jinyuan Sun, Xiaoyan Zhu, Chi Zhang, and Yuguang Fang (2011), "HCPP: Cryptography Based Secure EHR System for Patient Privacy and Emergency Healthcare", 31st International Conference on Distributed Computing Systems.
[11] Johann Grobsch adl and Dan Page (2012), "Efficient Java Implementation of Elliptic Curve".
[12] Joppe W. Bos, J. Alex Halderman, Nadia Heninger, "Elliptic curve cryptography in practice".
[13] Josh Benaloh, Melissa Chase, Eric Horvitz, and Kristin Lauter (2009), "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records", Microsoft, November 13.
[14] Kamlesh Gupta and Sanjay Silakari (2011), "ECC Over RSA for Asymmetric Encryption: A Review", IJCSI International Journal of Computer Sciences Issues, vol 18, Issue 3, no 2.

[15] Konstantinos Chalkias, George Filiadis, and George Stephanides (2007), "Implementing Authentication Protocol for Exchanging Encrypted Messages via an Authentication Server based on Elliptic Curve Cryptography with the ElGamal's Algorithm", International Journal of Computer, Information, Systems and Control Engineering Vol:1 No:7.
[16] M.A.C. Dekkera, S. Etalle (2007), "Audit-Based Access Control for Electronic Health Records", Electronic Notes in Theoretical Computer Science 168 ,221–236.
[17] Marci Meingast, Tanya Roosta, Shankar Sastry (2006), "Security and Privacy Issues with Health Care Information Technology", Proceedings of the 28th IEEE EMBS Annual International Conference New York City, USA, Aug 30-Sept 3.
[18] Mario Sicuranza Angelo Esposito (2013), "An Access Control Model for easy management of patient privacy in EHR systems", The 8th International Conference for Internet Technology and Secured Transactions (ICITST).
[19] Ms. Shubhi Gupta, Ms. Swati Vashisht (2014) "Implementation of ECC Using Socket Programming in Java" IOSR Journal of Computer Engineering 8727Volume 16, Issue 4.
[20] Pavan Roy Marupally, Vamsi Paruchuri Sriram Chellappan(2009), "Privacy Preserving Portable Health Record (P3HR)" International Conference on Network-Based Information Systems.
[21] Sangram Ray, G.P. Biswas (2013), "A Certificate Authority (CA)-based cryptographic solution for HIPAA privacy/security regulations", Journal of King Saud University – Computer and Information Sciences.
[22] Sangram Ray, G. P. Biswas (2012), "Design of RSA-CA Based E-Health System for Supporting HIPAA Privacy-Security Regulations" 2nd International Conference on Communication, Computing & Security [ICCCS].
[23] Swadeep Singh, Anupriya Garg and Anshul Sachdeva (2013), "Comparison of Cryptographic Algorithms: ECC & RSA", International Journal of Computer Science and Communication Engineering IJCSCE Special issue on "Recent Advances in Engineering & Technology" NCRAET.
[24] V. Gayoso Mart´nez and L. Herandez Encinas (2013) "Implementing ECC with Java Standard Edition 7" International Journal of Computer Science and Artificial Intelligence Dec. 2013, Vol. 3 Issue . 4, PP. 134-142.
[25] V.Gayoso Martinez and Hernandoz (2010), "A Survey of the Elliptic Curve Integrated Encryption Scheme", Journal of Computer Science And Engineering, Volume 2, Issue 2.
[26] Wei-Bin Lee, Chien-Ding Lee (2008), "A Cryptographic Key Management Solution for HIPAA Privacy/Security Regulations", IEEE Transactions on Information technology in Biomedicine 12(January (1)) .
[27] Yanjiang Yang, Xiaoxi Han, Feng Bao, and Robert H. Deng (2004), "A Smart-Card-Enabled Privacy Preserving E-Prescription System", IEEE transactions on information technology in biomedicine, vol 8, no. 1, March.

Received: January 25, 2021 Revised: March 30, 20201 Accepted: April 11, 2021

DOI: 10.5281/zenodo.4898049