Augmenting security for electronic patient health record (ePHR) monitoring system using cryptographic key management schemes

Shibin David[1], Andrew J[2], K. Martin Sagayam[3], Ahmed A. Elngar[4]*

[1,2]Department of Computer Science and Engineering,
Karunya Institute of Technology and Sciences, Coimbatore, India
[3]Department of Electronics and Communication Engineering,
Karunya Institute of Technology and Sciences, Coimbatore, India
[4]Faculty of Computers and Artificial Intelligence,
Beni-Suef University, Beni-Suef, 62511, Egypt, +201007400752

Emails: zionshibin@gmail.com; onesimu@gmail.com;martinsagayam.k@gmail.com
;elngar_7@yahoo.co.uk

Abstract

Security plays a major role in most fields including the pharmaceutical field. Authorization and Authentication are the key concepts in supporting notable areas of the cyber-health world. HIPAA's (Health Insurance Portability and Accountability Act) ultimate focus is to preserve the privacy of the health records of an individual without disclosing it and preventing the data from unauthorized access. A complaint key management solution is applied to the patient's health records to reduce the risk factor while engaging with cryptographic mechanisms. Though there are many existing cryptographic algorithms such as Elliptic curve cryptography, and Elgammal's key exchange algorithm which provides security to the access of patient's health records, the proposed key management solution will overlay the same variant of security to the Electronic Health Records (EHR). This paper provides the countermeasures for improving security and suggests a key recovery mechanism for the protection of keys used in the security mechanism.

Keywords: Health Insurance Portability and Accountability Act (HIPAA); Electronic Protected Health Information (ePHI); Key management; RFID cards

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. With the emergence of technology, manual paper-based health record maintenance has been changed to electronic record maintenance. This simplifies the paperwork such as arranging, organizing and searching for medical records on demand. Though, electronic-based health record maintenance provides huge advantages it comes with certain threats. The security and privacy of electronic health record (EHR) is vital. EHR may be targeted by hackers, viruses, and worms unexpectedly even without the knowledge of the administrator. Electronic Health

DOI: https://doi.org/10.54216/FPA.050201
Received: February 02, 2021 Accepted: August 07, 2021

Records (EHRs) are electronic versions of the paper charts available with the doctor or other health care provider's office. An EHR may include detailed information about your medical history, observations, prescriptions, 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 accessed from several websites through proper channels. These privacy and security regulations increase the availability and confidentiality of health information. A brief discussion on the problems associated with the privacy and security regulations is discussed to offer a possible solution to the current obstacles. As accuracy and confidentiality increase, there are certain potential threats to the confidentiality of information. Hence, there occurs a need to implement technical measures to guard against unauthorized access in this environment. The purpose of integrity controls is to ensure that the ePHI data is not altered during transmission. Encryption serves to be the best approach for this which is not easily readable or decrypted without proper authorization.

The main cognitive content of security [1, 2] are confidentiality, availability, and integrity where Confidentiality is the process of ensuring that information is accessible only to those authorized to have access to it, and Integrity is the process of ensuring the information is accurate and it is not modified in an unauthorized fashion and 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, and patient's present, past, and future behavior. Authorization refers to the that each healthcare institution must obtain an individual's permission while using and/or disclosing an individual's PHIs.

The cryptographic system provides the security of the PHI proposed by the HIPAA [3-7]. A compliant key management solution is used to reduce harm and risk in managing and transmitting health care records electronically while providing cryptographic mechanisms. Lee's method offers a cryptographic solution for preserving a patient's privacy. But this was found to be inefficient as patients cannot freely change their passwords.

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

There are plenty of existing schemes that use smart cards. Smart cards are found to be ineffective because of problems including highly expensive and also found to be established by malicious attacks and are not reusable. The proposed method uses Radio Frequency Identification (RFID) cards for storing encrypted data of the patient [3]. Authorization is performed by the patient's RFID cards that have patient detailed information stored in them. The key is valid only within a consistent period. The proposed method provides a key management scheme that handles keys for controlling patients' access to ePHI. Also, can revoke access if the authorization is not in between the valid period.

The entire paper is organized in the following way consisting of Section 2 which deals with the related works. The proposed methodology is elaborated in Section 3. The performance metrics of the proposed methodology are explained in Section 4, and finally, the conclusions are summed up in Section 5.

2. Related Works

Cryptographic key management [8] solution is proposed to meet the challenges of privacy/security issues. This method improves healthcare quality and product a patient's privacy. The patient's health information is stored in a smart card. They provide a key recovery mechanism to solve the problem of consent exception which describes the use and disclosure of a patient's details without the patient's permission for life-saving purposes. To achieve these, they provide digital signatures for verification of the signature. Secure hash algorithm (SHA-256) data integrity. To provide unauthorized access to patients' health records asymmetric cryptosystem (AES) with 256-bit keys that ensure confidentiality and overhead. Patients cannot freely change their passwords and don't support multiple access.

A novel key management solution [9-12] 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 an asymmetric cipher, a one-way hash function, and identification watermark generator, and a watermark embedding extracting mechanism. Watermarking techniques are used to get high-quality medical images. This prevents illegal distribution tracking. The method used was secure and feasible.

DOI: https://doi.org/10.54216/FPA.050201
Received: February 02, 2021 Accepted: August 07, 2021

A novel model [3-5] was proposed by using a smart card and protected health recorders. The public key infrastructure used here was DSA. To provide confidentiality of health records symmetric encryption/decryption is used. For authorization purpose, hash algorithms and DES was used.

Elliptic curve cryptography an efficient key management solution was proposed that guarantees security [6]. This has the advantage of using smaller key sizes and faster computation than a smart card-based cryptographic solution. Patients can freely update their passwords. Consent exception cases can be solved. For encrypting data, AES was used and 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 [9, 10, 13] is introduced to comply with security/privacy regulations which supports an e-health system environment. The disadvantage of this model was there was no solution for consent exception and do not support foreign access. AES was used for encryption to control unauthorized access. The medical center server [4] was located in each hospital instead of using a smart card for storing patient's PHI and can be accessed by using the Internet. Public key certificates are maintained by a certificate authority. This ensures patient's privacy even through the e-health system. It protects from replay attacks. The symmetric secret key is generated using the Diffie Hellman algorithm where the communication and processing overhead is low compared with other techniques.

3. Proposed Methodology

The proposed method describes HIPAA as an efficient key management scheme with a key recovery mechanism. This method satisfies the privacy and security concerns issued by HIPAA. The proposed method consists of a trusted server, a patient, and a hospital-associated. The trusted server is used to manage the keys used by all the users in the system. The system permits all the users to authorize and revoke the hospitals within a time period before the expiry date. The cryptographic system provides the security of the PHI proposed by the HIPAA. The key management scheme used is the Master Key Approach. Keys are stored in Radio- frequency identification (RFID) cards. In the existing system, they are solved in Smart cards. The project is all about improving the features of Taiwan's Healthcare Certificate Authority by providing users with certain privileges. Also, the system does not demand multiple encryptions of the data.

RFID cards have some advantages over smart cards [14-19].

- Manipulation of data or information is permitted
- RFID tags are more reusable
- RFID card will have a card detecting range that is more than a contactless smart card
- Cost-effective

It includes security features such as data encryption, password protection, and lay down to embrace a 'kill' facet to permanently remove the data.

This has four phases [5-7, 20, 21] including,

Authorization: A patient can authorize a set of healthcare institutes to access his/her encrypted PHIs within a specific time period by allowing these institutes to be able to obtain the encryption key within the period. Elliptic curve cryptography was used to provide more efficiency. An advantage of using this method is that it has a smaller key size and provides the same level of security as in RSA. Using the below-mentioned input and a master key provided by a trusted server in HCA the patient authorizes the hospitals with the help of n- degree Lagrange Polynomial. The signature (Cri, Cs) and a hash value (HMKi) are stored on the card.

Key Derivation: In each hospital, a patient's PHI is encrypted by an encryption key derived from the master key MKi. To perform the decryption, MKi must be retrieved to obtain the encryption key. Interpolation polynomial is reconstructed. And then using the private key of the hospital, the private key of the patient is retrieved. Using the polynomial, Master Key is retrieved. The Master Key of the patient is MKi.

Authorization revocation/addition: When patient Pi intends to revoke a set RH of nRH hospitals from the authorized list, two procedures are performed on Pi's enabled Pcard. The newly created random number is K_1. N'th LaGrange equation is constructed in which N should not represent any hospitals. And newly computed information is replaced with the old information for revocation. N'th Lagrange equation is constructed with the help of the private key of the hospital. A new hospital is added or an authorized hospital is removed.

Key Revocation: Key is recovered when consent exception takes place that is the PHI is accessed by an unauthorized hospital without the authorization of the patient. Here the trusted server recovers the Master Key for the unauthorized hospitals.

DOI: https://doi.org/10.54216/FPA.050201
Received: February 02, 2021 Accepted: August 07, 2021

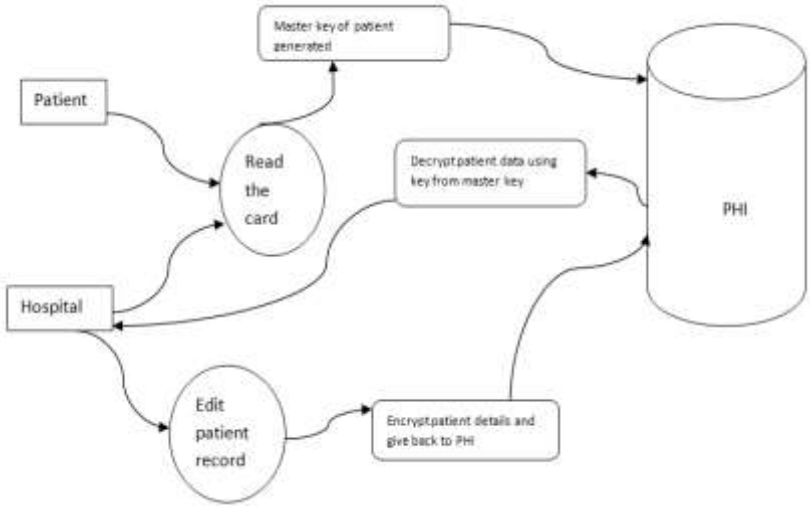

Figure 1: When patients appear in the hospital during this period, no patients involvement is needed to decrypt PHIs

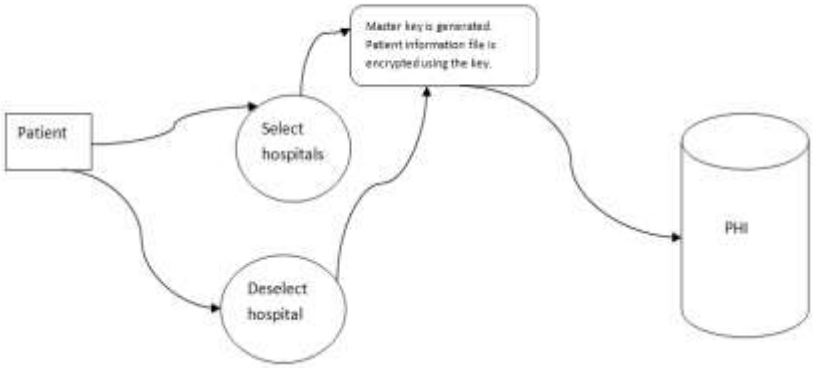

Figure 2: Authorization and revocation

Consent exception cases

There may be situations where a patient is unconscious and unable to access her medical record, at that time for the purpose of saving the life of the patient; privacy regulations state that the use and disclosure of PHI are 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 [22].

ECC (Elliptic Curve Cryptography) [23, 24-26] is a public key cryptographic technique that was found by Neal Kobliz and Victor Miller in the year 1985. It is a promising alternative for public-key cryptography especially in resource-constrained systems, pagers, PDAs, cellular phones, and smart cards. It provides a high level of security with smaller keys. It ensures greater security and more efficient performance than the first-generation public key technique (RSA and Diffie Hellman). It is used for key exchange and digital signature.160 –bit [27, 28] Elliptic Curve Digital Signature Algorithm is equivalent to 1024 – bit DSA. Due to its smaller key size, it provides faster computations, lower power consumption as well as memory and bandwidth savings. ECC is implemented by the

DOI: https://doi.org/10.54216/FPA.050201
Received: February 02, 2021 Accepted: August 07, 2021

Sun EC provider. The major aspect when implementing ECC is to find an appropriate trade-off between performance and security.

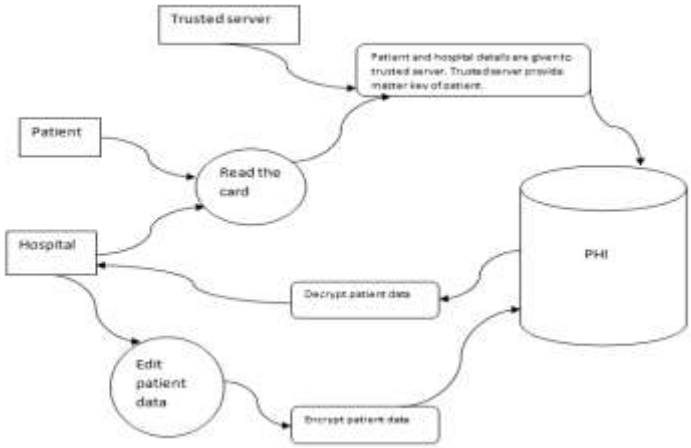

Figure 3: Key revocation

The mathematical background [27, 28, 29] of ECC is more complex than other cryptographic systems. First, the plain text has to be mapped to a numerical value upon which mathematical operation can be performed which means the message must be mapped to a point on an elliptic curve. To get the required cipher text it is necessary to perform Elliptic curve operations' which make use of addition operations of elliptic curves and ECC's multiple additions are the equivalent of RSA's modular exponentiation. An elliptic curve is generally given by $y^2 = x^3 + ax^2 + bx + c$.

Considering an elliptic curve over real numbers, which is a set of points (x, y) that can satisfy an elliptic curve equation $y^2 = x^3 + ax + b$; where a, b, x, and y are real numbers. The elliptic curve changes with different choices of the values of a and b. There are two types of fields namely prime fields and finite fields.
Let the message be encoded on the curve. As we cannot simply encode the message as x or y coordinate of the point since not all such coordinates are in Ep (a, b) where Ep (a, b) denotes elliptic group mod p. The condition to be satisfied is $y^2 = x^3 + ax + b \pmod p$. The encryption/Decryption system requires a point p and an elliptic group as parameters. Each user selects private key d and f generates a public key Q=d*p. d is said to be a random number. Q is the public key. For encrypting message m to B, A chooses a random positive integer 'k' from 1 to (n-1) and produces cipher text as a pair of point

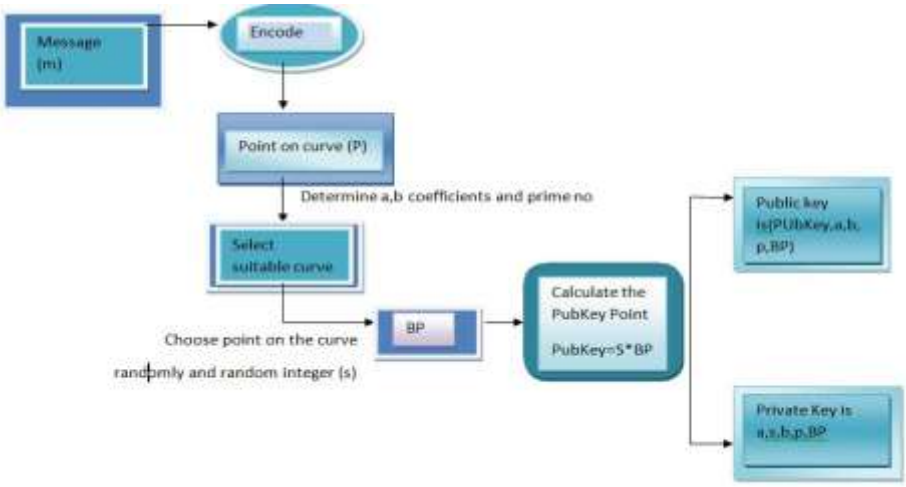

Figure 4: Key Generation

DOI: https://doi.org/10.54216/FPA.050201
Received: February 02, 2021 Accepted: August 07, 2021

Algorithm to encrypt/decrypt the patients' records

a. *Take a large prime number of p and values for the coefficients a and b such that, $4a^3 + 27b^2 \bmod p$ is not equal to 0.*
b. *Now let's consider an equation $y^2 = (x^3 + ax + b) \bmod p$.*
c. *Take all values of y between 0 to p-1 and calculate y2 mod p.*
d. *Take all values of x between 0 to p-1 and calculate $(x^3 + ax + b) \bmod p$.*
e. *Collect values of y from step 3 corresponding to values computed in step4.*
f. *Collect all points (x, y) from step 5.*
g. *Input a supposed value of g known here as the base point which belongs to points from step 6.*
h. *Calculate 2G, 3G……such that 2G=G+G, 3G=2G+G, and so on…*
i. *Computation of sender's (say, A) public key: Choose a large integer nA, so that it lies between 1 and n. Compute PA = nAG*
j. *Computation of receiver's (say, B) public key: Choose a large integer nB, so that it lies between 1 and n. Compute PB = nBG*
k. *Encryption: A will encrypt the message with B's public key – Let plain text Pm belongs to the point set in computed in step 6. Let k be the random integer that lies between 1 and n. Compute – (k_G, Pm+ k_{PB})*
l. *Decryption: Compute kGnB. Compute Pm + k PB- kGnB to get Pm.*

$C_m = \{C_a, C_b\}$, where $C_a = k*P$ and $C_b = M+K*Q$

The encoded message Cm will be sent. This encoded message is decrypted by using B multiplies the first point in the pair by b's secret key and subtracts the result from the second point.

$$M = C_b - d*Ca$$

In the above-described procedures, the initial stage begins with providing the RFID card bounded with the patient information followed by which the card can be read by the doctors for a prescription, providing medication, report writing, etc. Then the same can be given to the patient for futuristic use. The information stored in the RFID card will have to go through all the above-said stages of operation and becomes secure.

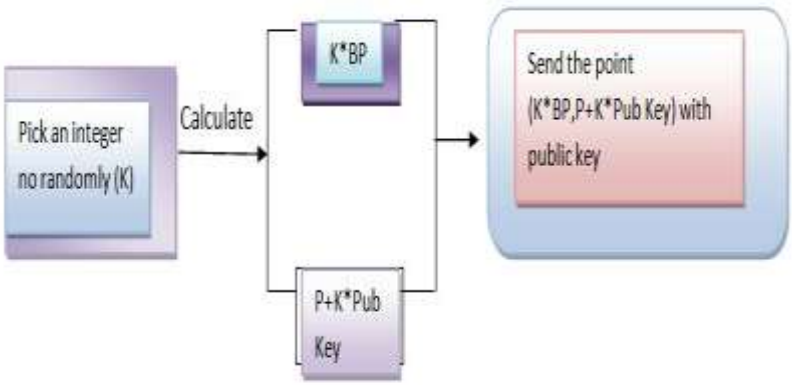

Figure 5: Encryption of the patient's record

4. Performance Analysis

In symmetric cryptosystems, any two parties interested have to share the same secret key. In asymmetric cryptosystems, key exchange is easier as compared to symmetric cryptography systems. But the drawback of asymmetric systems is speed and strength. In addition, asymmetric systems are slower than symmetric cryptosystems. ECC (Elliptic curve cryptography) is the next-generation algorithm that provides stronger security and better server utilization than current standard encryption methods. The cost of ECC can be compared with the

DOI: https://doi.org/10.54216/FPA.050201
Received: February 02, 2021 Accepted: August 07, 2021

existing RSA and it is observed that the cost of ECC is comparatively very less compared to RSA. The cost can be found by adding the difference in the times and also the memories presented at starting the execution and after the execution.

Performance metrics should be constructed to encourage performance improvement, effectiveness, efficiency, and appropriate levels of internal controls. In symmetric cryptosystems, any two parties interested have to share the same secret key. In asymmetric cryptosystems, key exchange is easier as compared to symmetric cryptography systems. But the drawback of asymmetric systems is speed and strength. Also, asymmetric systems are slower than symmetric cryptosystems. ECC (Elliptic curve cryptography) is the next-generation algorithm that provides stronger security and better server utilization than current standard encryption methods.

The patient records are encrypted using the proposed encryption scheme and the series of stages to protect the information bounded within the RFID card will have the below mentioned pseudo code.

```
// To encrypt the string using the public key
inputStream = new ObjectInputStream (new FileInputStream (PUBLIC_KEY_FILE));
final PublicKey publicKey = (PublicKey) inputStream.readObject();
System.out.println("publicKey "+publicKey);
final byte [] cipher Text = encrypt (r1, public Key);
HCA.tarea. append (cipher Text+"\n");
cns.add (r1. trim ());
```

The mechanism of key derivation and key recovery during and after the transmission of information can be done by using the following pseudo-code.

```
if (r1. equals("Hospitals"))
{
r1=(String)in. read Object ();
System.out.println("Hospitals   "+r1);
getKeyderivation(r1);
getKeyrecovery(r1);
time2= ((System.currentTimeMillis())); //whereas time1 is computed using patient details
mem2= (runtime. total Memory () -runtime. free Memory ()); //memory space for patient will be calculated separately
diff1=Math.abs(time2-time1);
diff2=Math.abs(mem2-mem1);
bws1.write(diff1+"-"+diff2+"-"+(diff1+diff2));      }
```

The public and private keys to encrypt the message and to acquire privacy are done with the help of the following code.

```
public void generatePublicPrivateKeys ()
{
privatekey1=(int) ((Math. Random () *(20-2)) +2);
publickey1=(int) (Math. Pow((int)p, privatekey1));
}
```

With the help of the input keys and message, a message digest is created to enhance the integrity of the original patients' records.

```
for (int m=0; m<semilength's++)
{
Integer hi=new Integer(""+m);
double fx=(((masterkey)*((X-hi)/ (1))) +(hh*((X-hi)/ (1))));
}
String password =tsp;
MessageDigest md = MessageDigest.getInstance("SHA-256");
md.update (password. getBytes ());
byte byteData [] = md.digest();
StringBuffer sb = new StringBuffer ();
```


DOI: https://doi.org/10.54216/FPA.050201
Received: February 02, 2021 Accepted: August 07, 2021

```
for (int i = 0; i < byteData.length; i++)
{
sb. append (Integer.toString((byteData[i] & 0xff) + 0x100, 16). substring (1));
}
```

Similarly, key derivation and recovery have also been done for the valid records bounded within the RFID card and securely maintaining the privacy of the records.

The graph gives a small description of the key sizes as compared to RSA. When key sizes for the current encryption techniques like RSA increase exponentially as security level increase ECC key length increase linearly. For example, 128-bit security requires a 3,072-bit RSA key. For ECC it is 256 –a bit ECC key. Security is not the only attractive feature of elliptic curve cryptography.

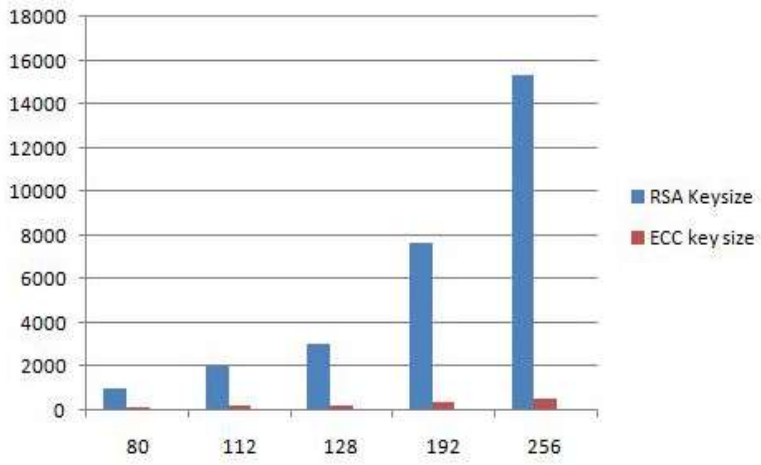

Figure 6: Key size comparisons with RSA algorithm

Elliptic curve cryptosystems also are more computationally efficient than the first-generation public-key systems, RSA and Diffie-Hellman. Although elliptic curve arithmetic is slightly more complex per bit than either RSA or DH arithmetic, the added strength per bit more than makes up for any extra compute time. Time can be calculated by finding the difference between the starting time when the process starts and then the execution time after the process is completed.

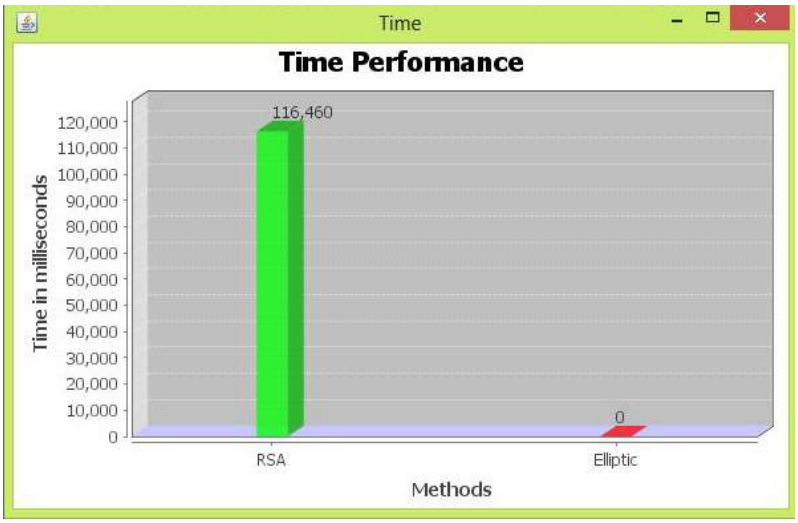

Figure 7: Comparison of time with different algorithms

DOI: https://doi.org/10.54216/FPA.050201
Received: February 02, 2021 Accepted: August 07, 2021

The cost compared to the other cryptographic techniques is low in ECC. As key size increases the cost increases. But in ECC even small key size is secured enough so the cost is less compared to the other cryptographic techniques.
The cost can be found by adding the difference of the times (t2-t1) and also the memories presented at starting execution and after the execution (m2-m1).

$$Cost = (t2-t1) + (m2-m1)$$

Figure 8: Comparison of cost w.r.t to various algorithms

Conclusion

A compliant key management scheme was developed with a 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 the security and privacy of information. The proposed method helps in 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 a great impact on the security of our proposed method. The reusability concept of RFID brings significant efficiency to the protection of the patient's health record. ECC (Elliptic curve cryptography) ensures security with a smaller number of keys.

References

[1] Alese, B. K., Philemon, E. D., &Falaki, S. O. Comparative analysis of public-key encryption schemes. International Journal of Engineering and Technology, 2(9), 1552-1568. (2012).

[2] Clarke, A., & Steele, R. Secure and reliable distributed health records: Achieving query assurance across repositories of encrypted health data. In 2012 45th Hawaii International Conference on System Sciences (pp. 3021-3029).IEEE. (2012).

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

[4] Dr. Najib A. kofahi.An empirical study to compare the performance of some symmetric and asymmetric ciphers. International Journal of Security and Its Applications, 7(5), 1-16.(2013).

[5] Huang, H. F., & Liu, K. C. Efficient key management for preserving HIPAA regulations. Journal of Systems and Software, 84(1), 113-119. (2011).

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

[7] Li, J., Lee, J. S., & Chang, C. C. Preserving PHI in compliance with HIPAA privacy/security regulations using cryptographic techniques. In 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (pp. 1545-1548). IEEE. (2008).

DOI: https://doi.org/10.54216/FPA.050201
Received: February 02, 2021 Accepted: August 07, 2021

[8] David, S., Xavier, B., & Kathrine, J. W. A panoramic overview on fast encryption techniques for outsourced data in mobile cloud computing environment.In 2017 International Conference on Inventive Computing and Informatics (ICICI) (pp. 476-480).IEEE. (2018).

[9] Dunlop, L. Electronic health records: Interoperability challenges Patients' right to privacy. Shidler JL Com. & Tech., 3, 1. (2006).

[10] Hripcsak, G., & Albers, D. J. Next-generation phenotyping of electronic health records. Journal of the American Medical Informatics Association, 20(1), 117-121. (2013).

[11] Benaloh, J., Chase, M., Horvitz, E., &Lauter, K. Patient controlled encryption: ensuring privacy of electronic medical records. In Proceedings of the 2009 ACM workshop on Cloud computing security (pp. 103-114). (2009).

[12] Krasner, J. Using Elliptic Curve Cryptography (ECC) for Enhanced Embedded Security-Financial Advantages of ECC over RSA or Diffie-Hellman (DH). Embedded Market Forecasters, American Technology. (2004).

[13] Sun, J., Zhu, X., Zhang, C., & Fang, Y. HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare. In 2011 31st International Conference on Distributed Computing Systems (pp. 373-382).IEEE. (2011).

[14] Großschädl, J., Page, D., & Tillich, S. Efficient java implementation of elliptic curve cryptography for J2ME-Enabled mobile devices. In IFIP international workshop on information security theory and practice (pp. 189-207).Springer, Berlin, Heidelberg.(2012).

[15] Bos, J. W., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., &Wustrow, E. Elliptic curve cryptography in practice. In International Conference on Financial Cryptography and Data Security (pp. 157-175).Springer, Berlin, Heidelberg. (2014).

[16] Meystre, S. M., Savova, G. K., Kipper-Schuler, K. C., & Hurdle, J. F. Extracting information from textual documents in the electronic health record: a review of recent research. Yearbook of medical informatics, 17(01), 128-144. (2008).

[17] Palojoki, S., Mäkelä, M., Lehtonen, L., &Saranto, K. An analysis of electronic health record–related patient safety incidents.Health informatics journal, 23(2), 134-145. (2017).

[18] Vijayakumar, P., Anand, K., Bose, S., Maheswari, V., Kowsalya, R., &Kannan, A. Hierarchical key management scheme for securing mobile agents with optimal computation time. Procedia engineering, 38, 1432-1443. (2012).

[19] McDonald, Clement. J., Tang, P. C., &Hripcsak, G. Electronic health record systems.In Biomedical Informatics (pp. 391-421).Springer, London. (2014).

[20] Mirkovic, J., Bryhni, H., &Ruland, C. M. Secure solution for mobile access to patient's health care record. In 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services (pp. 296-303).IEEE. (2011).

[21] Hripcsak, G., Albers, D. J., &Perotte, A. Parameterizing time in electronic health record studies. Journal of the American Medical Informatics Association, 22(4), 794-804. (2015).

[22] Ratwani, R. M., Fairbanks, R. J., Hettinger, A. Z., & Benda, N. C. Electronic health record usability: analysis of the user-centered design processes of eleven electronic health record vendors. Journal of the American Medical Informatics Association, 22(6), 1179-1182. (2015).

[23] Sciancalepore, S., Piro, G., Boggia, G., & Bianchi, G. Public key authentication and key agreement in IoT devices with minimal airtime consumption. IEEE Embedded Systems Letters, 9(1), 1-4. (2016).

[24] Gupta, K., &Silakari, S. Ecc over rsa for asymmetric encryption: A review. International Journal of Computer Science Issues (IJCSI), 8(3), 370.(2011).

[25] Fraser, H., Biondich, P., Moodley, D., Choi, S., Mamlin, B., &Szolovits, P. Implementing electronic medical record systems in developing countries. Journal of Innovation in Health Informatics, 13(2), 83-95. (2005).

[26] Krawczyk, H. Cryptographic extraction and key derivation: The HKDF scheme. In Annual Cryptology Conference (pp. 631-648).Springer, Berlin, Heidelberg. (2010).

[27] Yang, Y., Han, X., Bao, F., & Deng, R. H. A smart-card-enabled privacy preserving E-prescription system. IEEE Transactions on Information Technology in Biomedicine, 8(1), 47-58. (2004).

[28] Ray, S., &Biswas, G. P. A Certificate Authority (CA)-based cryptographic solution for HIPAA privacy/security regulations. Journal of King Saud University-Computer and Information Sciences, 26(2), 170-180. (2014).

DOI: https://doi.org/10.54216/FPA.050201
Received: February 02, 2021 Accepted: August 07, 2021

[29] Sicuranza, M., & Esposito, A. An access control model for easy management of patient privacy in EHR systems.In 8th International Conference for Internet Technology and Secured Transactions (ICITST

DOI: https://doi.org/10.54216/FPA.050201
Received: February 02, 2021 Accepted: August 07, 2021