HECC based Patient Privacy Preserving Access Control Model

Prasanalakshmi B[1†] and Ganesh Kumar Pugalendhi[2††],

King Khalid University[1†] Anna University[2††]

Summary
An Electronic patient medical record monitoring system has been actively developed and implemented in many countries with their own principles on implementation. Even though the history of implementation goes back to years, it is true that it has not yet completed its development stage. Still the system lags with some drawbacks and limitations. This paper discusses and describes the implementation of an Access control model that purely concentrates on the privacy preserving aspects of the patients with access control policies described. The Access control model proposed takes into concern the situation-based model also. This situation-based model takes into concern the authorization of the relatives or the family physician when a situation arises for the patient to authenticate the emergency doctor to retrieve his medical records. Also, a biometric authentication of the patient or the authorizing (relatives or the family physician) person is proposed to be unique and fast enough so that the data is retrieved only on the authorization of the concerned person. This system proves a highest level of privacy in concern with the medical records of a patient. Also, the Hyper Elliptic curve cryptography enhances the security level in authentication.

Key words:
Hyper Elliptic curve cryptography, Electronic health record, Access control model, Situation based access control model, Patient centric privacy.

1. Introduction

Every personal data need security and especially privacy. But all data cannot be kept under privacy at all instances and from everyone. As depicted in Fig. 1, the EHR system includes communication strategies with all its related fields like patient, Physician, Pharmacy, Association bank etc., In emergency situations when a patient arrives the hospital or the doctor reaches the spot for emergency treatment, as an initial case he would be in a need to know the patient history of disease or treatment if it is an utmost emergency case since the patient may be allergic to any sort of medicine or he may be suffering or under treatment for a most deadly disease. In the meantime, it is important to safeguard the privacy of the patient data.

In order, to make the doctor convincible with the data needed and at the same instance to safeguard the patient privacy, it is mandatory to involve the patients priority of revealing his own medical data and very important to get a concern from the patient to authenticate one or two persons who can act instead of him for authenticating his own medical data to be provided by the data provider to the requester(doctor attending the patient in emergency). Also, it is up to the patient to decide which data can be provided open on access request and which data (in case of unrevealable disease like HIV, Cancer or any other) to be secured. In order to justify the necessity for the requester to access all sort of data under emergency situations role based and situation-based access control is required with time bound and audit records for backtracking and traceability.

2. Related works

The state of art system in introducing security and private key generation from the actor of the system through their biometric data, which is considered to be the real-time authentication for a situation based access control system does not exist to a countable rate, some literature that coincides with the overall model is taken into account to grasp some ideas of implementation.

Mario et al., [1] designed a semantic access control system for fine-grained access policies in Health Information system with enhanced flexibility. The proposed model was based on the ontological approach that was able to increase the usability and feasibility in the real time information system.

Tiwari et al., [2] uses a Role based access control that helps to restrict the usage of data based on the role of the actor. Also an algorithm with a combination of selective policies of each user of the EHR database is define that is extended to the classification of role based on data mining techniques. The author considers role as class and their features as vectors.

Auditing any data is considered wise to preserve privacy. Weiran et al., [3] in his work considers the privacy concern of the patient data and introduces the role based access control system in a different perspective. The specified access policy is encapsulated and verified by the public auditor, who uses the apriori approach to find the fraudulent access. Once if a user is detected to be fraud, he is not provided access to any medical record in the future.

Jinyuanet al.,[4] proposes a Healthcare system for Patient Privacy, based on cryptographic constructions and existing wireless network infrastructures, to provide privacy protection to patients under any circumstances while enabling timely PHI retrieval for life-saving treatment in emergency situations. Furthermore, our HCPP system

Manuscript received March 5, 2019
Manuscript revised March 20, 2019

restricts PHI access to authorized (not arbitrary) physicians, who can be traced and held accountable if the accessed PHI is found improperly disclosed. Identity based authentication scheme is used for authenticating a physician to access the data of the patient.

Omotosho et al., [5] proposed the development of privacy and security system for cryptography-based-EHR by considering two biometric entities Fingerprint and Iris to secure cryptographic keys in a bio-cryptography framework. Fuzzy vault system is used for cryptographic process, Key generation is made possible using GLCM of the input image.

3. Proposed Scheme

The proposed Patient HECC based Patient Privacy Preserving Access Control Model (HP3ACM) concentrates on the collaborative approach to combine Situation based and Time bound access control also concentrating on preserving privacy of patient data.

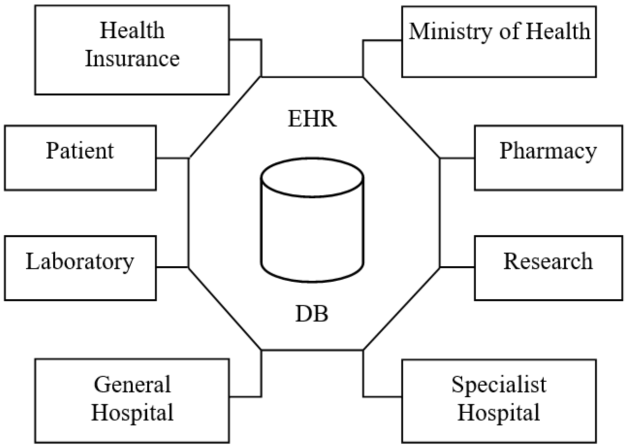

Fig. 1 Component Structure of EHR

The authentication is purely based on PKI, designed and proposed as a Hyper elliptic curve cryptography model. This system also stays as an alert system which indicates the admission of the patient to the hospital in emergency situation.

3.1 System Design

The proposed system design is adopted based on the e-payment scheme as proposed by Yang et al.,[6]. Fig. 2 shows the communication strategy followed in integrating the data of the patient and physician with the association bank. The protocol includes five phases (a) Setup phase : to determine the HECC curve and security parameters based on the input parameters from the emergency physician (b) Authentication initiation phase : to initiate the authentication phase with requirements from the Data exchange association as per the request made by the emergency physician's side (c) Authentication Phase: to authenticate the request and instruct association to issue required medical data (d) Exchange phase: Response prepared to be provided by the association bank to the Emergency physician (e) Transfer phase: Transfer of data and tracking of Audit logs.

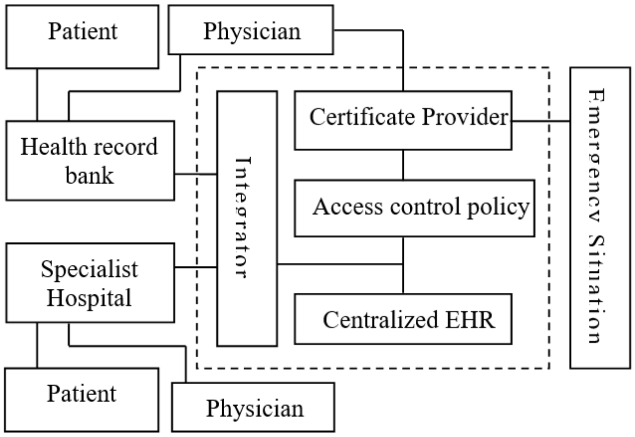

Fig. 2 EHR- Information Exchange Mechanism

3.1.1 Set – up phase

The overall means of data request- response module is presented as a handshake flow diagram in figure 3. The setup phase of the proposed system includes deciding over the curve parameters and security parameters . A hash function is defined as$\{0,1\}^* \rightarrow \{\{0,1\}^{l_{c1}}, \{0,1\}^{l_{c2}}$, where l_{c1} and l_{c2} denotes the length of cryptographic and Hash function keys. The communicating entities or in general include the Emergency Assist Physician, Data Exchange Association , Authenticator(Family physician and or caretaker) . Each entity prepares their own public and private parameters $P_U = P_R * R_D$, PR_i is the key generated from the biometric entity(Palm vein) . The order of Divisor of HECC , D is given as the smallest possible integer *i*, such that *i=div(1,0).*

Let C represent the hyperelliptic curve defined over a finite field F_p, J representing the Jacobian of the curve C and R_D represents the reduced divisor of order *i* . PR is the private key generated from the biometric entity which is an hexadecimal integer and the corresponding public key is defined as $PU= PR *R_D$.

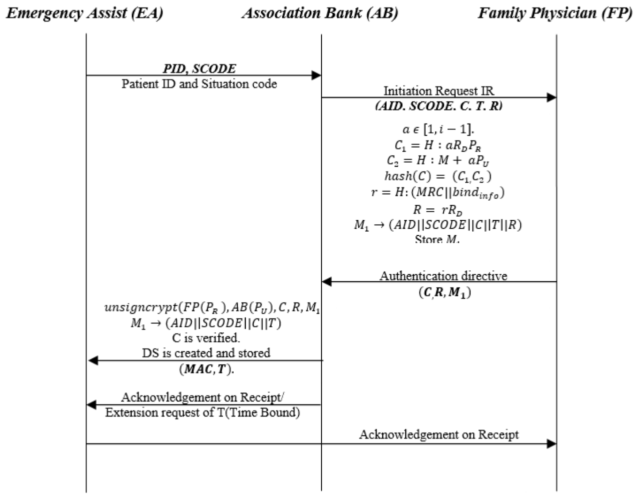

Fig. 3 Request- Response scenario of proposed system

3.1.2 Authentication Initiation Phase

The authentication phase is initiated by the emergency assist physician. EAP enters the PID (patient ID) ans Situation code(SCODE)in the website for Association bank for authentication from the Family physician/ care taker. The FP receives an initiation request (IR) through the association bank containing the EID, SCODE, which is predefined in the database of the association bank. SCODE defines the position of the patient clearly so that the FP will be able to authenticate the selected medical records of the patient. At the same time when the IR is placed to the FP a message is sent to the relative or the caretaker if the patient has opted for such a necessity while registering his basic information in the EHR.

3.1.3 Authentication Phase

The AB generates the directive of IR to the FP using the signcryption steps of HECC.

1. Select a random integer $a \epsilon [1, i-1]$.
2. Compute $C_1 = H : aR_DP_R$ and $C_2 = H : M + aP_U$
3. Return $hash(C) = (C_{1,}C_2)$
4. Compute $r = H: (MRC||bind_{info})$
5. Compute $R = rR_D$
6. $M_1 \rightarrow (AID||SCODE||C||T||R)$
7. Signcryption tuple $(C_{,}R, M_1)$ is sent to the association bank.

This signcryption tuple is referred to as the authentication directive which specifies the MRC(Medical Record Code) to be given access to the Emergency Assist along with the timestamp.

3.1.4 Exchange Phase

On receiving the Signcryption tuple the association bank unsigncrypts the directive as follows:

1. $unsigncrypt(FP(P_R), AB(P_U), C, R, M_1) \rightarrow M_1$
2. $M_1 \rightarrow (AID||SCODE||C||T)$, the bank proceeds to provide access only if C is verified.
   The Bank creates the Digital signature(DS) for the Emergency assist with the tuples (MAC, T).

3.1.5 Transfer Phase

On receiving proper authentication from the Family physician the Association bank decides on the Medical record fields to be given access to the Emergency Assist Physician. This access is provided with a time bound control from the time of sanction to the time specified in the message M_1 as T. The message M_1 consists of AID→ emergency assist ID, SCODE→situation code the assist specified in his request, C→hash function of the key, which is used to retrieve the authenticity of the public key holder using his private key and T represents the time bound for accessing the database.

The DS with (MAC,T) could be utilized by the emergency assist physician to proceed with treatment and update the details within the specified time bound. If the treatment or updation exceeds the time bound he may extend pertaining the reason for extension with the same procedure from setup phase.

4. Security Against Common Attacks

This section brings about a proof of resistance to security attacks of the proposed implementation of cryptographic security system in EHR. Some of the attacks taken into consideration includes replay attacks, man-in-the-middle attacks, impersonation attacks, double spending and server spoofing. Taking into assumption that the adversary , to attack the proposed system has access over communication channels and can interpret , modify or use the patient data for any reasons which acts as a major drawback for the proposed system in securing privacy of the patient.

4.1 Replay Attack

The authentication directive $(\boldsymbol{C_{,}R, M_1})$ is transferred from the Family physician to the Association bank for revealing the patient data under emergency to the Physician or the assist who treats the patient in the emergency situation. If the tuple is recovered and if the adversary tries to use the tuple for further retrieval of data, it becomes impossible since the message $M_1 \rightarrow (AID||SCODE||C||T)$ is bound by a time frame in which the tuple is validated. Hence the replay attack try of the adversary results in vain.

4.2 Man-in-the-middle Attack

Assuming the interception of the authentication directive $(\boldsymbol{C},\boldsymbol{R},\boldsymbol{M_1})$, is impossible since the association banks checks the time bound including the initiation of the authentication directive till the expiry time of the Time bound T.

4.3 Impersonation Attacks

The Adversary cannot imitate to be the Family physician to create a valid authentication directive tuple $(\boldsymbol{C},\boldsymbol{R},\boldsymbol{M_1})$, since the private key of the adversary will never match that of the family physician . The private key of the FP is an biometric entity from which the view of the data is to be generated and the specified biometric entity from which the private key of the Family physician is generated is already enrolled to the database of the Association bank as an authenticator ID at the time of enrolling patient data.

4.4 Double Spending

The Association bank stores the tuple (MAC,T), the Digital signature either till the transaction is completed or the time bound exceeds, whichever is earlier. After the prior mentioned situation of termination , the AB deletes the tuple so that the digital signature can never be used to retrieve same set of data.

4.5 Server Spoofing

The adversary would never be able to spoof the server data since the session key generated between the Family physician and the Association bank or The Association bank and the emergency Assist is maintained throughout the transaction , in which the session keys are generated using the private keys of the actors of situation. Unless or otherwise the adversary would be able to invoke the private key, he could not create the session key, hence server spoofing is impossible.

5. Conclusion

This paper proposes a novel Hyper elliptic curve cryptosystem based authentication for accessing the patient data by an Emergency Assist , in which the authentication to reveal data is provided by the family physician. The proposed system includes HECC based cryptography that includes the biometric key generated from the biometric entity of the actor as the private key for the concerned, Situation based access control that considers the situation by the family physician to authenticate certain fields which would be necessary for the physician to proceed with treating the patient in emergency situation. Also the proposed system is resistant to the security attacks which are proved.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

References

[1] Mario Sicuranza, Mario Ciampi , " A Semantic Access Control for easy management of the privacy for EHR Systems(2014)" .

[2] Tiwari B, Kumar A, "Role-based access control through on-demand classification of electronic health record." , Int J Electron Healthc. 2015;8(1):9-24. Available online :https://www.ncbi.nlm.nih.gov/pubmed/26559071

[3] Weiran Liu Xiao Liu Jianwei Liu Qianhong Wu, "Auditing Revocable Privacy-Preserving Access Control for EHRs in Clouds" ,*The Computer Journal*, Volume 60, Issue 12, 1 December 2017, Pages 1871–1888, Available online : https://doi.org/10.1093/comjnl/bxx071

[4] Jinyuan Sun, Xiaoyan Zhu, Chi Zhang, and Yuguang Fang, "HCPP: Cryptography Based Secure EHR System forPatient Privacy and Emergency Healthcare", (2011)

[5] Adebayo Omotosho, Justice Emuoyibofarhe, Christoph Meinel, "Ensuring patients' privacy in a cryptographic-based electronic health records using bio-cryptography".

[6] Yang, J., Chang, Y., Chen, Y., , "An Efficient Authenticated Encryption Scheme Based on ECC and its Application for Electronic Payment", 42, 315–324.