Fine-Grained Access Control Mechanism to Enhance Data Privacy and Integrity in Cloud-Based EHR

C. Eben Exceline[1], Sivakumar N[2*]

Abstract

The confidential nature of Electronic Health Records has attracted a lot amount of research to provide data security. Cloud-based electronic health record systems adopt attribute-based encryption to provide fine-grained control of access over medical records. Designing better fine-grained control of access mechanism to electronic health records improve data privacy and integrity. Most attribute-based encryption schemes generate the secret key by using volatile attributes common to many users. The volatile attributes are prone to masquerading attacks resulting in a serious breach of data privacy and integrity. Biometrics, a physical feature of users, a non-volatile attribute combined with other volatile attributes can enhance the privacy and integrity of electronic health records. So in this paper, fingerprint biometrics a non-volatile attribute is combined with other volatile attributes of the users to improve data privacy and integrity of electronic health records. Also, the proposed system fragments the patient's electronic health records to provide flexible access. Fragmentation of health records is done according to the search keywords. The time complexity and the computational cost is evaluated by implementing the proposed system. The system is analyzed, and found that masquerading attacks are limited compared with other existing systems.

Key Words: Control, Data, Privacy, Enhance.

DOI Number: 10.14704/nq.2022.20.8.NQ44240 **NeuroQuantology 2022; 20(8):2181-2193**

Introduction

Users from all around the world can now view the information gathered and processed in a specific place during this current digital age. Likewise, an electronic health record (EHR) is a digital medical record storage system enabling sharing of patient's health data among various users such as health professionals, family, and friends. The secure storing and sharing of EHR is achieved by the cloud computing paradigm that provides users with unlimited storage and computing resources (Rani & Baburaj, 2016). By cloud computing, patients are benefited from global health providers. Cloud computing allow users to access the EHR of a patient simultaneously (Menachemi & Collum, 2011) leading to collaborative medical decisions and efficient healthcare delivery.

Although storing EHR in the cloud benefits the patients and the providers, the patients lose control over his/her personal data and medical records. Global information estimates hacking of EHR is ten times more than credit card numbers. The stored data could be lost, leaked, stolen, and modified ending in the breach of data privacy, integrity, and availability (Rodrigues, De La Torre, Fernández, & López-Coronado, 2013)(Omotosho & Emuoyibofarhe, 2014). EHR outsourced to the cloud should provide health data privacy, availability, health record integrity, and fine-grained access control (Harman, Flite, & Bond, 2012)(Lazakidou & Siassiakos, 2008)(Jardim, 2013)(Fernández-Alemán, Señor, Lozoya, & Toval, 2013)(Li, Yu, Zheng, Ren, & Lou, 2013). The afore-mentioned security requirements for EHR have to be satisfied to deliver quality healthcare to the patients.

Corresponding author: Sivakumar N
Address: [1]School of Information Technology and Engineering, VIT University, Vellore, India, [2]School of Computer Science and Engineering, VIT University, Vellore, India
E-mail: nsivakumar@vit.ac.in

Patient's health data is a valuable commodity that should be held confidential for any health organization. Leakage or disclosure of information leads the patients of the health organization face serious consequences. Maintaining confidentiality of patient's information from unauthorized users and the cloud servers is vital. HIPAA provides security regulations to develop efficient privacy-preserving EHR systems to services the patients (of Health, Services, & of the National Coordinator for Health Information Technology, n.d.).

The promising way to satisfy the security requirements for EHR is to encrypt EHR and enforce efficient access control strategies before outsourcing to the cloud. The various encryption scheme to encrypt medical records are symmetric key encryption (Ueckert & Prokosch, 2002)(Riedl et al., 2007)(W. D. Yu & Chekhanovskiy, 2007)(Jian et al., 2011), public-key encryption (PKE) (Zhang & Liu, 2010)(Sun & Fang, 2010), identity-based encryption (IBE) (Sun, Zhu, Zhang, & Fang, 2011) and fuzzy identity-based encryption or attribute-based encryption (ABE) (Li et al., 2013)(Wan, Liu, & Deng, 2012). Encrypting EHR using ABE is well suited as it provides fine-grained control of access to medical records (S. Yu, Wang, Ren, & Lou, 2010). In ABE, from the user's attributes, a secret key for the user is generated, and the medical records are encrypted using a set of attributes.

Data privacy and integrity are the vital security requirement of EHR. Although ABE allows for fine-grained data access to EHR, most of the attributes are common to several users. Since identifying the users who manipulated the EHR is challenging, data privacy is compromised. For example, the doctors from the same department have the same attribute values. Forging of attributes is easy as they are volatile. Therefore, in this paper, fingerprint biometrics, a non-volatile attribute is combined with other volatile user attributes to provide fine-grained data access to EHR. As biometrics are physical features of users and are unique, impersonation is difficult. Biometric plays a vital role in tracing the user who did access to EHR. The user cannot deny that they did not access the EHR improving data integrity. Thus, the proposed scheme is well suited for hospital managed EHR that provides data privacy and integrity. The scheme introduced in this paper is a more advanced version of the Wan et al. scheme. The following are the contributions of this paper

1) The EHR is fragmented and hierarchically defined according to the search keywords.

2) Biometrics of users are added with other volatile attributes to encrypt medical records to enhance data privacy and integrity by avoiding masquerading attacks.

3) The proximity between the biometrics submitted during the decryption phase and the biometrics submitted during the setup phase is calculated using the Mahalanobis distance metric. It is the Euclidean distance generalization. The distance value calculated should be lower than the threshold value of t.

4) Finally, the proposed system is implemented to evaluate the performance in the aspect of execution time taken by each algorithm. The system proposed in this paper shows satisfactory performance.

The following is how the paper is organised: The works relevant to the proposed scheme are described in Section 2. Section 3 delves into the detail of the proposed scheme's architecture. Section 4 outlines how the proposed system is implemented and evaluates the computational complexity of the system. The paper finally concluded in section 5.

Related Work

This section explains how ABE provides fine-grained control of access on EHR comparing with other encryption techniques. PKE and IBE experience a high cost of key management, and it is required to encrypt a medical record multiple times with different user keys to bestow access for many users. ABE allows one-to-many encryption to solve the afore-mentioned problems in PKE and IBE (Goyal et al., 2006). The medical records are encrypted only once using a collection of attributes. Users who fulfill the collection of attributes used to encrypt the medical records can decrypt it.

2.1 Attribute-based encryption (ABE)

An ABE system is deemed for encrypting the EHR before outsourcing to the cloud to prevent key management problems found in PKE and IBE. Moreover, ABE provides fine-grained control of access on EHR. Sahai and Waters were the first to implement and incorporate ABE (Sahai & Waters, 2005). ABE generates ciphertext and hidden keys for users based on a collection of user attributes. The user's private key must match the attributes in the ciphertext for the ciphertext to be decrypted. Enforcing policy over attributes reduce expressibility problems found in ABE adopting the linear set of attributes. According to the association of the access policy with the private key or ciphertext, ABE is listed as KP-ABE (Goyal et al., 2006) or CP-ABE (Goyal et al., 2006). (Bethencourt et al., 2007). A tree access policy over attributes is connected to the user's private key while a linear set of attributes is linked to the ciphertext in KP-ABE. In CP-ABE, the ciphertext is coupled with a tree access structure over attributes, and the user's secret key is coupled with a linear list of attributes. The KP-ABE suggested by Yu et al. for encrypting EHR lacks flexibility and scalability (S. Yu et al., 2010). Because the patient who generates ciphertext can only decide the set of attributes for the EHR but not the users who could decrypt the EHR. The trust in KP-ABE is based on the key generator, so data privacy is not guaranteed. As a result, KP-ABE is not the safest choice for securing EHR in the cloud. Narayan et al. (Narayan, Gagné, & Safavi-Naini, 2010) adopted CP-ABE that encrypted EHR using a broadcast variant. Although the scheme provides data privacy, the ciphertext size is too large and grows with respect to the number of unrevoked users. Ibrami et al. (Ibraimi, Asim, & Petković, 2010) also adopted CP-ABE and divided the users of EHR into professional and personal domain.

2.2 Multi-authority ABE (MA-ABE)

The primary drawback of the afore-mentioned schemes is it adopts a single trusted authority. Managing all the attributes of the user by a single authority is burdensome. As the authority generates the user's private key, the authority can access all the encrypted files belonging to a user lacking user privacy. MA-ABE proposed by Li et al. solves the overhead problem of single authority EHR systems (Li et al., 2013). The scheme classified the users of EHR into two categories. First, the family members and friends of the patient as the personal domain. Second, users who use EHR for professional purposes as doctors, medical researchers, nurses as the professional domain. As there are limited users in the personal domain, patients themselves can manage the users. The medical records are encrypted using KP-ABE. In the public domain, a single authority cannot maintain all user's attributes, as there are many users. The Li et al. scheme adopted MA-CP-ABE to manage users in the public domain. Qian et al. also developed MA-ABE by dividing the user into two categories as Li et al. scheme for securing EHR (Qian, Li, Zhang, & Han, 2014). The scheme uses an anonymous key issuance protocol to derive the user's private key while the attribute authorities monitor the user's attributes. Despite the involvement of compromised authorities in the system, the scheme enhanced user privacy. Although the system maintains data privacy in the personal domain, the patient loses control over his/her medical records in the public domain, lacking data privacy.

2.3 Hierarchical attribute set based encryption (HASBE)

CP-ABE derives the user's secret key from a logically organized single attribute set. To satisfy the access structure coupled with the ciphertext, users can only create the most likely combinations from the single attribute set. As a result, Bobba et al. developed attribute set-based encryption (ASBE), which uses a recursive set key structure to coordinate the user's attributes (Bobba, Khurana, & Prabhakaran, 2009). To satisfy the access structure combined with the ciphertext, dynamic constraints can be used to keep different values for each attribute in the user's recursive set key structure. As with CP-ABE systems, the attributes from the same set are freely merged. However, a translating function is defined to combine the attributes from different attribute subsets. The afore-mentioned property provides greater flexibility in accessing the medical records compared to formal CP-ABE schemes. So Wan et al. (Wan et al., 2012) extended the ASBE scheme by combining Wang et al. scheme with Bobba et al. scheme to provide a hierarchy for users and multiple values for each attribute. The top-level authorities can generate secret keys for the lower-level authorities and the data consumers who want to access the EHR as in the scheme proposed by Wang et al. (Wang, Liu, Wu, & Guo, 2011). Despite the fact that the system offers flexibility and fine-grained data access, it fails to fulfil many of the security criteria for EHR. The following are the observations made from prior literature:

1. The above methods have their own disadvantages, and because non-volatile attributes are used, it is possible for an unauthorised user to impersonate an authorised user in order to access the EHR stored in the cloud.

The unauthorized access will lead to the unavailability of medical records and modification in medical records stored in the cloud leading to a lack of data integrity, which is the vital security requirement of EHR.

The patient loses control over their EHR in the public domain. It is difficult for patients to track the user who accessed the EHR as the attributes are common to many users. Therefore, there is a lack of data privacy.

In this paper, most of the reviewed systems adopted patient collecting the EHR from the hospital and upload it in the cloud. However, nowadays, hospitals maintain a private cloud to manage their patient's EHR and to upload it. The hospital gives access permission to the patients and other users to access the EHR.

Proposed system

The proposed system considers providing data privacy and data integrity for EHR outsourced to the cloud. A biometric attribute-based encryption scheme is proposed for the same and it is explained in the following subsections.

3.1 System Components

The following are the components involved in the proposed EHR scheme:

Patients: EHR owners who define the access structure.

Cloud: The storage system used to store the encrypted EHR of the patients.

Hospitals: The entities encrypt the medical records and outsource them to the cloud.

Attribute Authorities (AAs): The entity responsible for generating keys for the users and are delegated by the hospital.

Users: People who can access EHR outsourced to the cloud example: doctors, nurses, pharmacies, relatives of the patients.

Fingerprint Scanner: The equipment scans the fingerprint biometric of the users.

3.2 Overview of the proposed system

Figure 1 depicts the functioning of the proposed scheme. The steps involved in the proposed biometric hierarchical attribute set based encryption for cloud-based EHR are as follows:

The hospital owns a cloud and has full control over outsourcing EHR to the cloud.

The users/patients register themselves by submitting some personal information and biometric to the hospital.

The personal information forms the attributes of the system.

The setup algorithm defines the distance parameter M, the threshold value t, and the key structure depth d.

The parameters (M, t, and d) are fed into the setup algorithm. The public parameter PP and the master secret key msk are generated.

The hospital generates private key PK for the authorities with the key structure K, msk, and biometric vector v of the attribute authorities.

The hospital generates the biometric key, and the attribute authorities generate the attribute keys for the users.

The hospital fragments the medical records of each patient collected in the hospital according to the search keywords.

The patient determines the access policy T, which dictates which users have access to the cloud-based medical record.

The encryption algorithm encrypts the fragmented patient data and sends them to the server, according to the access structure T.

To access the EHR, the user has to query the cloud with search keywords and submit the fingerprint biometric.

The decryption algorithm checks the distance between the submitted fingerprint and the fingerprint submitted during the setup phase using Mahalanobis distance M.

For the decryption algorithm to produce the original medical record, the Mahalanobis distance should be less than the threshold value t, and the user's secret key should satisfy the access control structure T.

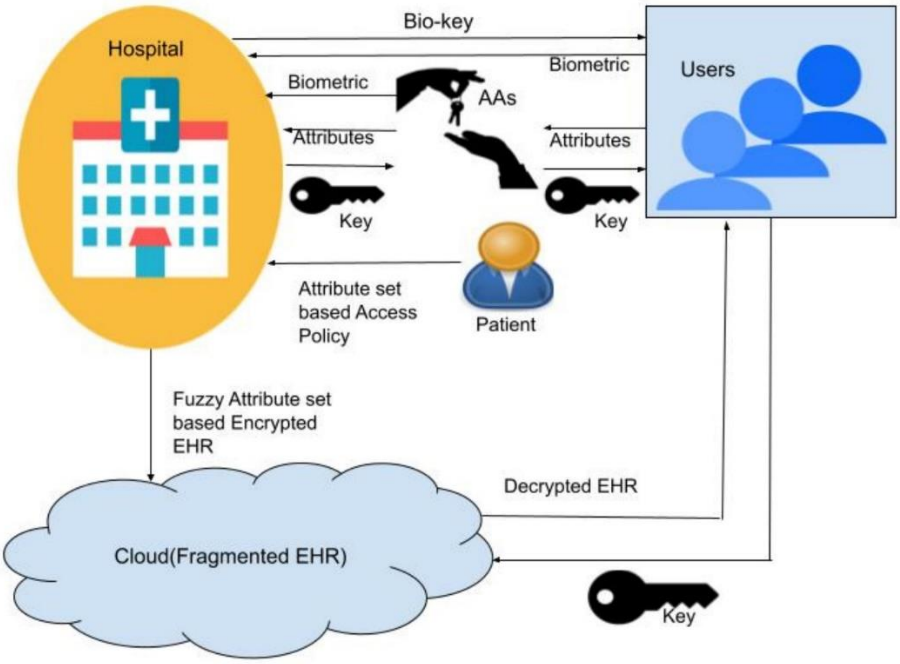

Figure 1. The Functioning of the Proposed Cloud-based EHR System

3.3 Preliminaries

This subsection defines the various techniques adopted in the proposed system.

3.3.1 Elliptic curve

The following equation defines the elliptic curve over finite field Fq.
$Y^2 mod\ q = X^3 + aX + b\ mod\ q$, where $4a^3 + 27b^2\ mod\ p \neq 0$
Elliptic curves over finite fields have been used in cryptography since 1985. The discrete logarithmic problem over groups of points on the elliptic curve, discovered by Koblitz and Miller, provides better security. Furthermore, the elliptic curve is said to produce shorter keys (Chatterjee & Sarkar, 2011).

3.3.2 Pairing-based cryptography

Pairing-based cryptography takes two points from elliptic curve $G1$ and outputs from multiplicative abelian group GT. The pairing has a special property called bi-linearity suitable for cryptography. Bilinear maps are known to be pairing since it pairs elements from $G1$ to GT.
Definition of the bilinear map:
Assume $G1$ as well as GT to be two cyclic groups of the same prime order p. A map of bilinear from $G1 \times G1$ to GT is a function $e: G1 \times G1 \rightarrow GT$.
The bilinear map must satisfy the following properties:
Bi-linearity: A map e: $G1 \times G1 \rightarrow GT$ is bilinear if $e(P^a, Q^b) = e(P,Q)^{ab}$ for all $P, Q \epsilon G1$, and $a, b \epsilon Z$.
Non–degenerate: $e(P,P)$ is the generator of GT if P is the $G1$ generator.
Computable: For every $P, Q \epsilon G1$ there is an algorithm that efficiently computes $e(P,Q)$ (Boneh & Franklin, 2001).

3.3.3 Decisional Bilinear Diffie Hellman (DBDH)

DBDH computes $e(g,g)^{abc} \in GT$ and decides whether $z = e(g,g)^{abc}$when given g, ga, gb, gc and z, where a, b and c are uniform random elements of Zp, the generator of G1 is g, e refers to the bilinear map and z refers to an element of random type in GT [30].
The following equation defines the probability of an adversary A to solve the DBDH$ADV(A) = \{\Pr[g, g^a, g^b, g^c, z) \rightarrow 1|z = e(g,g)^{abc}] - \Pr\ [A(g, g^a, g^b, g^c, z) \rightarrow 1|z\ is\ random]\}$
If the assumption of DBDH exists in the group of pairings, every polynomial-time adversary's advantage in solving the DBDH is ignored.

3.3.4 Definition of Mahalanobis distance

Assume $x = (x1, x2, x3, \dots\dots\dots, xn)$ and $y = (y1, y2, y3, \dots\dots\dots\dots.., yn)$ be a couple of n length vectors of the same distribution having the covariance matrix F (Guo, Susilo, & Mu, 2016). The equation that defines Mahalanobis distance is

$$D_m(x,y) = \sqrt{(x-y)F^{-1}(x-y)^T}$$

Let the inverse of the covariance matrix is

$$F^{-1} = \begin{pmatrix} f_{1,1} & \cdots & f_{1,n} \\ \vdots & \ddots & \vdots \\ f_{n,1} & \cdots & f_{n,n} \end{pmatrix}$$

3.4 The workflow of the proposed system

This subsection explains the detailed functioning of the proposed scheme. The following are the five algorithms present in the proposed system

3.4.1 Setup Algorithm

In the setup algorithm, the users of the proposed EHR system register their biometric and attributes. The attributes are arranged hierarchically to form the user key structure. Figure 2 depicts an example user key structure.

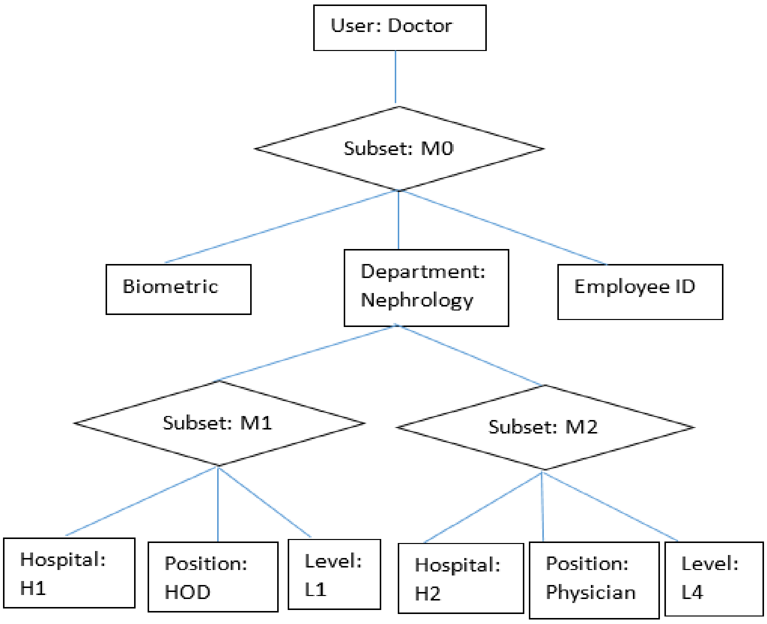

Figure 2. Example key structure of the user

With security parameter λ, attribute universe U, key structure depth d, threshold t as input, the algorithm generates master secret key msk and public parameters PP. Select bilinear group G and GT of the same prime order p. Wan et al. (Wan et al., 2012) assume $d = 2$, but for the proposed system, $d = 3$. Because the proposed system adds fingerprint biometric as the primary attribute. Choose random elements α, β_i where i ranges from 1 *to* d. Calculate $h_1 = g^{\beta_1}, h_2 = g^{\beta_2}, h_3 = g^{\beta_3}, f_1 = g^{1/\beta_1}, f_2 = g^{1/\beta_2}, f_3 = g^{1/\beta_3}$. The biometrics attribute is a vector, so for each vector element, choose y_j, where j ranges from 1 *to* n. n is the length of the biometric vector.

$$PP = G, G_T, g^{y_j}, h_1, h_2, h_3, f_1, f_2, f_3, t, e(g,g)^{\alpha}$$
$$msk = \beta_i, y_j, g^{\alpha}$$

3.4.2 Key generation algorithm for AAs

The hospital delegates attribute authorities such as the department head to generate the user secret keys. The hospital generates private keys for the attribute authority with msk, threshold t, attribute authority biometric vector v, and authority key structure K. The key generation algorithm for AAs selects $t-1$ degree polynomial randomly from Z_p for the biometric vector, where $q(0) = \alpha$. For $v = 1$ *to* j, calculate $D_j = \frac{q(j)}{y_j}. g^{\frac{1}{\beta_1}}$, where j is the length of the biometric vector v. Select r randomly for each authority from Z_p and calculate $g^{(\alpha+r)/\,\beta_2}$. Choose k random numbers $r_k \in Z_p$ for each attribute subsets in the authority key structure, where k is the number of attribute subsets in the authority key structure. Choose l random numbers $r_{k,l}$ for each attributes $a_{k,l}$ in the attribute subsets and calculate $D_{k,l} = g^{(r_k)}.H(a_{k,l})^{r_{k,l}}$, $D'_{k,l} = g^{r_{k,l}}$, $E_k = g^{(r+r_k)/\beta_3}$, where l is the count of the attributes in the subset.

$$PK_{AA} = (K, D_j, D, D_{k,l}, D'_{k,l}, E_k)$$

3.4.3 Key generation algorithm for Users

The hospital and the AAs delegated by the hospital generates decryption keys for the users. The hospital derives user keys from their fingerprint, whereas the AAs derive keys from other volatile attributes in the user key structures.

Biometric key generation by the hospital

The hospital generates part of the secret key for the users from the biometrics. The algorithm takes the input biometric vector v and threshold t as input and output biometric part of the private key. For the biometric vector v, randomly select $t-1$ degree polynomial from $Z_p[X]$, and calculate $\bar{D_J} = \frac{q(j)}{y_j}.f_1$, where $q(0) = \alpha$.

Attribute key generation by AAs

The AAs derive private keys for the users using the attributes in the user key structures. Let $\bar{K}$ denotes the user key structure. The algorithm selects $\bar{r}$ for each user from Z_p and calculates $\bar{D} = D.{f_2}^{\bar{r}}$. Select k numbers randomly $\bar{r}_k \in Z_p$ for each attribute subset in the key structure. Select l numbers randomly $r_{k,l}$ for each attribute in the attribute subset. Calculate $\bar{D}_{k,l} = D_{k,l}.g^{(\bar{r}_{k,l})}.H(a_{k,l})^{\bar{r}_{k,l}}$, $\bar{D}'_{k,l} = D'_{k,l}.g^{\bar{r}_{k,l}}$, $\bar{E}_k = E_k.{f_3}^{\bar{r}+\bar{r}_k}$.

$$Pk_u = (\bar{K}, \bar{D_J}, \bar{D}_{k,l}, \bar{D}'_{k,l}, \bar{E}_k)$$

.

3.4.5 Encryption Algorithm

The hospital generates medical records of the patients, fragments according to the search keyword, and encrypts them before outsourcing them to the cloud. A symmetric data encryption key (SDEK) is used to encrypt each fragmented medical record. After that, the SDEK is encrypted using the access control structure. For each search keyword, patients describe the access control structure. The proposed scheme adopts the same tree access structure as in (Wan et al., 2012) but added a NOT gate. Each node in the access structure is either threshold gates AND and OR or the attributes. The children of the node and its threshold value define each node. Assume node x has num_x children nodes, then the threshold value of x ranges from 0 to num_x. The various functions that deal with access structure are the $parent(x)$ denotes the parent node of x, $att(x)$ denotes the attribute in the leaf node x, and $index(x)$ denotes the number which defines node x. The following is the description of each node's threshold value.

The threshold value for each attribute in the access structure is1, and each leaf node in the access structure signifies that it is an attribute.

The AND gate node's threshold value is $num_x + 1$.

The OR gate node’s threshold value is num_x.

The NOT gate node’s threshold value is 1.

Figure 3 shows an example access structure. The example access structure states the doctor who may be a physician or department head from the endocrinology department can access the medical records. Figure 4 shows an example hierarchically fragmented medical record according to the search keywords. The search keywords in figure 4 are medical history, ECG report, Neurology, Cardiology. For each search keyword, the patient has to define the access structure. Figure 4 states the doctors of department cardiology can access the complete medical records under the keyword cardiology.

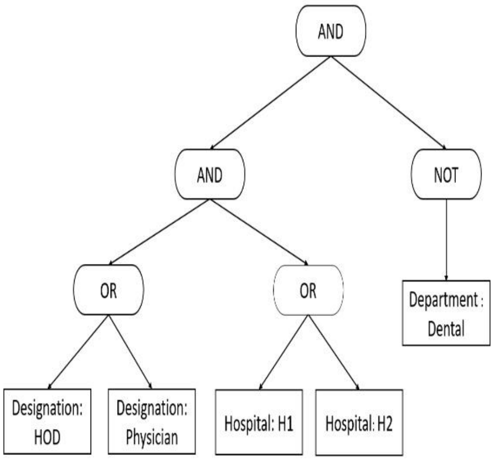

Figure 3. Example Access Structure

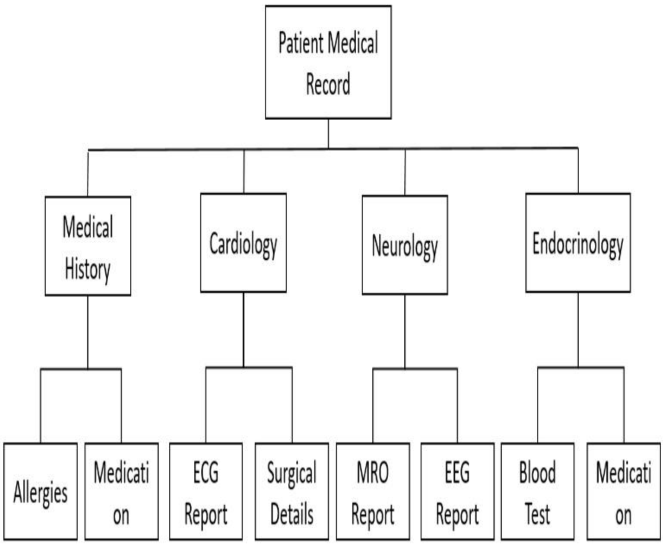

Figure 4. Hierarchically Fragmented Medical Record

The encryption algorithm takes the tree access structure T and M the medical record file being outsourced to the cloud as input and output the ciphertext CT. Randomly choose s and calculate $C_m = M.e(g,g)^s, C = g^{y_j}.h_1{}^s$, where j is the length of the biometric vector. Calculate $C_1 = h_2{}^s, C_2 = h_3{}^s$. Input n_x the number of nodes in the access structure. For $i = 1\ to\ n_x$, input threshold value t_x of the node. Choose a polynomial q_x randomly. Let the degree of the polynomial be $t_x - 1$. If x is a root node, then q=0. And other points of the q are chosen randomly. If x is a non-leaf node, then $q_x(0) = s$. And all coefficients of q_x are chosen randomly. For all leaf nodes y, calculate $c_y = g^{q_y(0)}$ and $c'_y = H(att(y))^{q_y(0)}$. For all other non-leaf nodes x, calculate $c_x = h_3{}^{q_x(0)}$. The ciphertext is

$$CT = (T, C_m, C, C_1, C_2, c_y, c'_y, c_x)$$

3.4.6 Decryption Algorithm

The user who wants to access the EHR makes a query with search keywords and submits the secret key PK. The decryption algorithm contains two conditions. The algorithm starts by measuring the Mahalanobis distance between the biometric used to generate the key and the biometric used to encrypt the health record in query. Second, the algorithm verifies that the attributes in the user key structure match the control structure for the health record in query. If the afore-mentioned two conditions are fulfilled, the algorithm decrypts the ciphertext otherwise returns a null value.

Implementation and Performance Analysis

This section outlines how the proposed system is implemented in order to assess the proposed scheme's time complexity. A comparison is made between related literature and the proposed system concerning computational complexity and security. The proposed system shows better data integrity and privacy when compares to the systems described in related literature. The proposed system shows slightly higher computational complexity and execution time than the Wan et al. scheme because of the biometrics attribute addition.

4.1 Implementation:

A system environment is a setup using Intel i3 CPU 2.30 GHz, 4GB RAM, 64-bit Windows operating system, and 1TB hard drive to implement the proposed system that provides data integrity, data privacy, and fine-grained access control. The proposed scheme is implemented using Java programming language and has adopted the external java pairing-based cryptography (JPBC) library. First, HASBE (Wan et al., 2012) is implemented and then integrated the proposed biometric attribute set-based encryption system into the prototype PHR system (Zheng, 2011). In the setup process, the security parameter is set to 80 bits, and the pairing is done with a 160-bit elliptic curve group. The fingerprint is used as a biometric in the proposed scheme to generate a private key for attribute authorities and users.

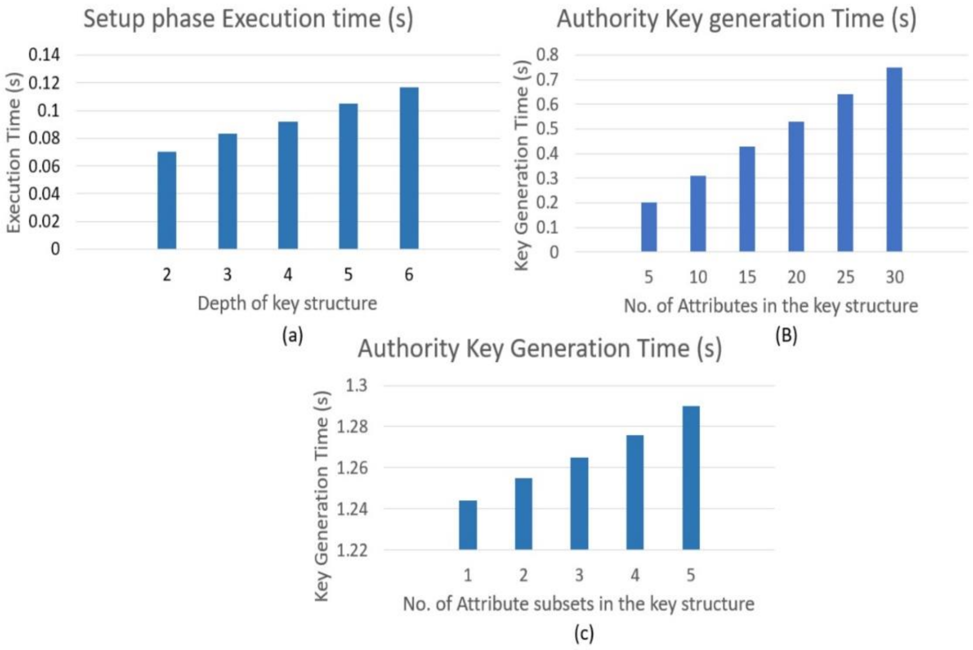

Figure 5. Execution time of Setup Algorithm and Authority key generation Algorithm

Figure 5 shows the execution time of the setup algorithm and key generation algorithm. During the implementation, the key structure depth is set to 2 and above. The setup algorithm's execution time is represented in Figure 5(a). The time taken for the algorithm to generate PP and msk increases in direct proportion to the depth of the key structure. For every increase in key structure depth, the setup algorithm's execution time increases by around 0.011s. Figure 5(b) and 5(c) show that the attribute subsets count and the attributes count in the key structure determine the authority key generation time. While evaluating the authority key generation time concerning the attributes count, set the attribute subsets count to 1. In the authority key generation algorithm, the execution time increases by approximately 0.02s for each attribute addition in the authority key structure. The user key generation time is determined by the number of user attributes that match the number of authority attributes and the number of user attribute subsets that match the attribute subsets of the authority key structure. The user key generation time increases proportionally to the number of matching attributes and the number of matched attribute subsets in the user and authority key structure, as seen in Figure 6. The user key generation algorithm execution time increases approximately 0.029s for each attribute addition in the user key structure.

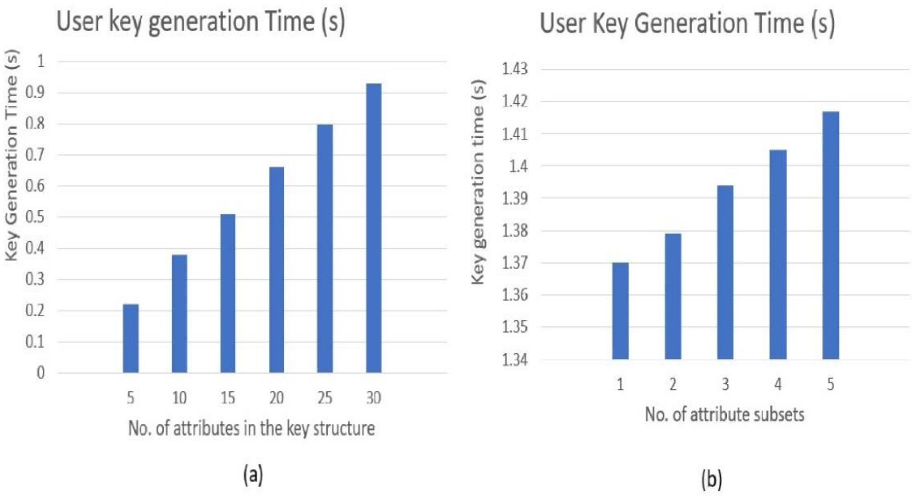

Figure 6. Execution Time of User Key Generation Algorithm

The encryption algorithm execution time to generate ciphertext depends on the the leaf nodes count in the access structure shown in figure 7(a). The execution time of the encryption algorithm increases approximately 0.02s with every attribute addition in the access structure. The decryption algorithm's execution time is determined by the attribute's count in the access structure. The amount of time it takes to decrypt the data is often determined by how closely the user key structure fits the access control structure associated with the ciphertext being queried. If the attributes in an attribute subset of the user key structure fulfill the access structure coupled to the ciphertext, then the decryption time grows linearly concerning the attributes count in the access structure shown in figure 7(b). The decryption time increases by 0.013s for each attribute insertion in the access structure when an attribute subset of the user key structure satisfies the access structure. If the attributes from different subsets of the user key structure satisfy the access structure coupled to the ciphertext, then the decryption time depends on the attributes count in the user key structure match the translating nodes count involved in the access structure. Therefore, the execution time of the decryption algorithm varies and takes more execution time. The user biometric must be checked with the biometric submitted during the setup process during decryption. As a result, the decryption algorithm's execution time grows linearly as the biometric vector length grows.

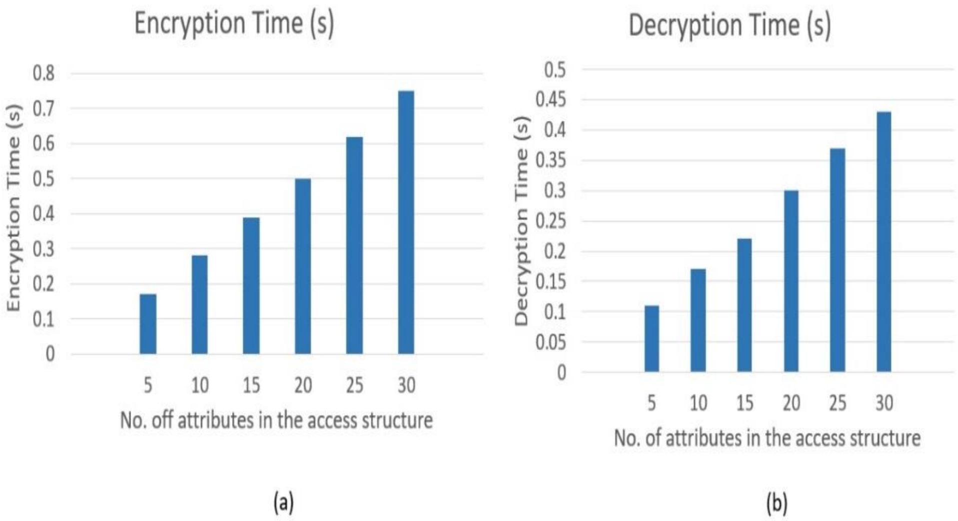

Figure 7. Execution Time of Encryption and Decryption Algorithm

4.2 Computational complexity Analysis

The setup algorithm, attribute authority key generation algorithm, user key generation algorithm, encryption algorithm, and decryption algorithm are among the five algorithms used in the proposed biometric attribute set-based encryption for a cloud-based EHR system that increases data security and privacy. The above-mentioned algorithms' computational complexity is examined in this subsection.

Setup Algorithm: The algorithm calculates public parameters and the master secret key, as discussed in subsection 3.4. The algorithm generates the group elements by picking random numbers. The operation to generate group elements is two exponentiation for each key structure depth. As a consequence, the setup algorithm's computational complexity is O(2d).

Authority Key generation Algorithm: The computational complexity of attribute authority key generation depends on the attributes count in the authority key structure, attribute subsets count in the authority key structure, and the biometric vector length of the authority. For each attribute, the algorithm performs two exponentiation operations, one for each attribute subset, and one for each element in the biometric vector. As a result, the attribute key generation computational cost is O(2N+M+j).

User Key Generation Algorithm: The user key generation algorithm is divided into two the biometric key generation part and the attribute key generation part. The hospital generates the biometric key, and the authorities delegated by the hospital generate the attribute keys. The computational cost of deriving the biometric key depends on the length of the biometric vector. Therefore, the computational cost is O (j). The user attribute key generation depends on the attributes count and the attribute subsets count in the user key structure. The computational cost of attribute key generation is O(2N+M) because it does two exponentiation operations for each attribute and one exponentiation operation for each attribute subset.

Encryption Algorithm

Encryption algorithm computational cost depends on the nodes count in the access structure. Since it performs two exponential operations for each attribute-holding leaf node and one exponentiation operation for each threshold gate node, the encryption algorithm has a computational cost of O(2Y+X).

Decryption Algorithm

The computational cost of the decryption algorithm is determined by the node's count in the access structure and the extent to which the user key structure attributes satisfy the access structure attributes. When the attributes from a subset of the user key structure match the ciphertext associated access structure, the computational cost is determined by the leaf node's count in the access structure. When the attributes from different subsets fulfill the access structure, the computational cost of decrypting the ciphertext depends on the leaf nodes count, translating nodes count in the access control structure, and the attribute subsets count in the user key structure involved in fulfilling the access control structure. As a result, the cost of running the decryption algorithm varies. The decryption algorithm evaluates one pairing operation for each element in the biometric vector, two pairing operations for each leaf node, one pairing operation, and one exponentiation operation for every translating node in the access control structure.

Table 1 shows the proposed scheme, Yu scheme (S. Yu et al., 2010), and Wan scheme (Wan et al., 2012) computational cost. The proposed system computational cost is slightly high because of biometrics attribute addition.

Table 1. The computational cost analysis of the proposed system

Operation	(Yu, Wang, Ren, & Lou, 2010)	(Wan, Liu, & Deng, 2012)	Proposed scheme
System set up	O(Y)	O(1)	O(2d)
Authority Key Generation	_	O(2N+M)	O(2N+M+j)
User biometric key generation	_	_	O(j)
User attribute key generation	O(Y)	O(2N+M)	O(2N+M)
Encryption	O(I)	O(2Y+X)	O(2Y+X)
Decryption	O(1)	_	(O(|j|+2|Y|+|X|+X), where '|' denotes pairing operation

Where Y denotes the leaf nodes count in the access structure and, X refers to the translating nodes count in the access structure, N denotes the attributes count in the user key structure, M denotes the attribute subsets count that form the user key structure, I denotes the attributes count used for encryption, j refers to the elements of the biometric vector and d refers to the user key structure depth.

4.3 Security Analysis

The proposed system is contrasted to current equivalent methods in this subsection, which are focused on the security requirements of EHR. In the proposed scheme, the user who accessed the EHR cannot deny their actions on EHR. User biometrics added as one of the attributes made it easy to trace the user who accessed the EHR and thus improves data integrity. In the other two existing systems, the professional domain consist of user attributes mostly common to many users. So, it is difficult to trace the users who accessed the EHR. The patients design the access control structure according to the search keywords. The medical record encrypted under specific keywords can be accessed by the users who satisfy the access control coupled to the encrypted medical records. Thus, providing access to the medical records for a particular person and data privacy to the patients. Storing EHR in the cloud gives interoperability and availability of data. An authorized user can access medical records from anywhere in the world. An authorized user cannot access the EHR only when the cloud server crashes or during network issues.

As the proposed system adopts fingerprint biometrics as a primary attribute it develops a secure sharing of medical records between the user and the cloud by resisting masquerading attacks. Since the access structure coupled to the ciphertext is obtained as plaintext in most ABE systems, a legitimate user or an adversary can figure out who can decrypt the ciphertext. Therefore, an adversary can know the user attributes from the access structure. The adversary can then submits the known attributes to get the private key as a legitimate user. If the adversary receives the private key, he can decrypt all the medical records related to the access structure. Besides, forging user attribute values is easy as they are common for many users in the professional domain. Masquerading the specific attributes of users is hard. In the HASBE system, the probability of guessing an attribute value depends on the number of attribute values an attribute can hold. If an attribute can retain two values, then the probability of guessing the attribute value is ½. If there are 50 attributes, then at least 30 attributes are easily forged. So, any user can easily masquerade as a legitimate user to access the ciphertext. In the proposed scheme, although the possibility of masquerading user volatile attributes is high, masquerading a user fingerprint is difficult. Thus, masquerading attacks are limited. Table 2 compares the proposed scheme's security to that of other systems currently in use.

Table 2. Comparison of security analysis with similar approaches

Security	(Yu et al., 2010)	(Li, Yu, Zheng, Ren, & Lou, 2013)	(Wan et al., 2012)	Proposed system
Data Integrity	-	-	-	Yes
Data Privacy	Yes	No	Yes	Yes
User Privacy	No	No	No	Yes
Scalability	Less (single-authority)	Greater	Greater	Greater
Fine-grained access control	Yes	Yes	Yes	Yes
Interoperabilit y	Yes	Yes	Yes	Yes
Availability	Yes	Yes	Yes	Yes
Flexibility	Less (For a single attribute, compound attributes and multiple value assignment are not supported.)	Less (For a single attribute, compound attributes and multiple value assignment are not supported.)	Greater	Greater
User revocation	Yes	Yes	Yes	Yes
Masquerading	Yes	Yes	Yes	Limited

Conclusion

Cloud-based EHR maintained by the hospital should be protected from stealing, leaking, unauthorized accessing, and hacking because it contains sensitive data. Unauthorized access to EHR stored in the cloud results in poor health care delivery and financial loss. It's important to preserve data integrity, data privacy, and fine-grained control of EHR access. The biometric attribute set-based encryption scheme mentioned in this paper guarantees data integrity and privacy while allowing for fine-grained control of EHR access. Since multiple users in the professional domain have common user attributes, monitoring the users who used the EHR is complicated, according to the current literature. The proposed system added fingerprint biometric as one of the user attributes, making it easy to trace the user who accessed the EHR. The fingerprint biometric avoids masquerading attacks as it is a non-volatile attribute and the user's unique physical features. Furthermore, the proposed system segmented medical records based on search keywords, allowing for fine-grained access control. Finally, a comparison of EHR with other current systems is made based on computational complexity and security requirements. The proposed system shows greater security and similar computational costs.

References

Bethencourt, J., Sahai, A., & Waters, B. Ciphertext-policy attribute-based encryption. Proceedings - IEEE Symposium on Security and Privacy, 2007, 321–334. https://doi.org/10.1109/SP.2007.11

Bobba, R., Khurana, H., & Prabhakaran, M. Attribute-sets: A practically motivated enhancement to attribute-based encryption. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 5789 LNCS, 2009, 587–604. https://doi.org/10.1007/978-3-642-04444-1_36

Boneh, D., & Franklin, M. . Identity-Based Encryption from the Weil Pairing, 2001,213–229.

Chatterjee, S., & Sarkar, P. Identity based encryption. Springer Science & Business Media 2011.

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. ángel O., & Toval, A. Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, 46(3), 2013, 541–562. https://doi.org/10.1016/j.jbi.2012.12.003

Goyal, V., Pandey, O., Sahai, A., & Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the ACM Conference on Computer and Communications Security, 2006, 89–98. https://doi.org/10.1145/1180405.1180418

Guo, F., Susilo, W., & Mu, Y. Distance-based encryption: How to embed fuzziness in biometric-based encryption. IEEE

Transactions on Information Forensics and Security, 11(2), 2016, 247–257. https://doi.org/10.1109/TIFS.2015.2489179

Harman, L. B., Flite, C. A., & Bond, K. State of the Art and Science. Electronic Health Records: Privacy, Confidentiality, and Security. American Medical Association Journal of Ethics, 14(9), 2012, 712–719.

Ibraimi, L., Asim, M., & Petković, M. Secure management of personal health records by applying attribute-based encryption. Proceedings of the 6th International Workshop on Wearable, Micro, and Nano Technologies for Personalized Health: "Facing Future Healthcare Needs",PHealth, 2009,71–74. https://doi.org/10.1109/PHEALTH.2009.5754828.

Jardim, S. V. B. The Electronic Health Record and its Contribution to Healthcare Information Systems Interoperability. Procedia Technology, 9, 2013, 940–948. https://doi.org/10.1016/j.protcy.2013.12.105

Jian, W. S., Wen, H. C., Scholl, J., Shabbir, S. A., Lee, P., Hsu, C. Y., & Li, Y. C. The Taiwanese method for providing patients data from multiple hospital EHR systems. Journal of Biomedical Informatics, 44(2), 2011, 326–332. https://doi.org/10.1016/j.jbi.2010.11.004

Lazakidou, A. A., & Siassiakos, K. M. Handbook of research on distributed medical informatics and e-health. In Handbook of Research on Distributed Medical Informatics and E-Health, 2008, https://doi.org/10.4018/978-1-60566-002-8

Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Transactions on Parallel and Distributed Systems, 24(1), 2013, 131–143. https://doi.org/10.1109/TPDS.2012.97

Menachemi, N., & Collum, T. H. Benefits and drawbacks of electronic health record systems. Risk Management and Healthcare Policy, 4, 2011, 47–55. https://doi.org/10.2147/RMHP.S12985

Narayan, S., Gagné, M., & Safavi-Naini, R. Privacy preserving ehr system using attribute-based infrastructure. Proceedings of the ACM Conference on Computer and Communications Security, 2010, 47–52. https://doi.org/10.1145/1866835.1866845

of Health, D., Services, H., & of the National Coordinator for Health Information Technology, O. (n.d.). Chapter 4 Understanding Electronic Health Records, the HIPAA Security Rule, and Cybersecurity, Guide to Privacy and Security of Electronic Health Information. 26–31. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

Omotosho, A., & Emuoyibofarhe, J. A Criticism of the Current Security, Privacy and Accountability Issues in Electronic Health Records. International Journal of Applied Information Systems, 7(8), 2014, 11–18. https://doi.org/10.5120/ijais14-451225

Qian, H., Li, J., Zhang, Y., & Han, J. Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation. International Journal of Information Security, 14(6), 2014, 487–497. https://doi.org/10.1007/s10207-014-0270-9

Rani, A. A. V., & Baburaj, E. An efficient secure authentication on cloud based e-health care system in WBAN. Biomedical Research (India), 2016, S53–S59.

Riedl, B., Neubauer, T., Goluch, G., Boehm, O., Reinauer, G., & Krumboeck, A. A secure architecture for the pseudonymization of medical data. Proceedings - Second International Conference on Availability, Reliability and Security, ARES 2007, 318–324. https://doi.org/10.1109/ARES.2007.22

Rodrigues, J. J. P. C., De La Torre, I., Fernández, G., & López-Coronado, M. Analysis of the security and privacy requirements of cloud-based electronic health records systems. Journal of Medical Internet Research, 15(8), 2013, 1–9. https://doi.org/10.2196/jmir.2494

Sahai, A., & Waters, B. Fuzzy Identity-Based Encryption, 2005, 457–473.

Sun, J., & Fang, Y. Cross-domain data sharing in distributed electronic health record systems. IEEE Transactions on Parallel and Distributed Systems, 21(6), 2010, 754–764. https://doi.org/10.1109/TPDS.2009.124

Sun, J., Zhu, X., Zhang, C., & Fang, Y. HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare. Proceedings - International Conference on Distributed Computing Systems, 2011, 373–382. https://doi.org/10.1109/ICDCS.2011.83

Ueckert, F. K., & Prokosch, H. U. Implementing security and access control mechanisms for an electronic healthcare record. Proceedings / AMIA ... Annual Symposium. AMIA Symposium, 2002, 825–829.

Wan, Z., Liu, J., & Deng, R. H. HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. IEEE Transactions on Information Forensics and Security, 7(2), 2012, 743–754. https://doi.org/10.1109/TIFS.2011.2172209

Wang, G., Liu, Q., Wu, J., & Guo, M. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers. Computers & Security, 30(5), 2011, 320–331. https://doi.org/10.1016/j.cose.2011.05.006

Yu, S., Wang, C., Ren, K., & Lou, W. Achieving secure, scalable, and fine-grained data access control in cloud computing. Proceedings - IEEE INFOCOM, 2010, 1–9. https://doi.org/10.1109/INFCOM.2010.5462174

Yu, W. D., & Chekhanovskiy, M. A. An electronic health record content protection system using SmartCard and PMRTM. HEALTHCOM 2007: Ubiquitous Health in Aging Societies - 2007 9th International Conference on e-Health Networking, Application and Services, 2007, 11–18. https://doi.org/10.1109/HEALTH.2007.381595

Zhang, R., & Liu, L. Security models and requirements for healthcare application clouds. Proceedings - 2010 IEEE 3rd International Conference on Cloud Computing, CLOUD 2010, 268–275. https://doi.org/10.1109/CLOUD.2010.62.

Zheng, Y. A. O. Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption, 2011.