EAI Endorsed Transactions
on Pervasive Health and Technology

Research Article EAI.EU

Biometric based Multi-Authority Inner Product Encryption for Electronic Health Record

C. Eben Exceline[1,*] and Jasmine Norman[2]

[1] Research scholar, School of Information Technology and Engineering, Vellore Institute of Technology, India
[2]Associate professor, School of Information Technology and Engineering, Vellore Institute of Technology, India

Abstract

Introduction: Attribute-based encryption enhances the security of electronic health records outsourced to the cloud. At the same time, single authority attribute based encryption leads to user privacy breech and attribute management complexity. Multi authority attribute-based encryption enhances user privacy and attribute management, but lacks privacy and integrity of data. Therefore, biometric-based multi-authority inner product encryption is proposed to improve data integrity, data privacy, and user privacy.
Objectives: The proposed scheme aims to enhance data integrity, data privacy, and user privacy in cloud-based Electronic Health Record.
Methods: An exhaustive literature review has been made related to securing electronic health record outsourced to the cloud and found that data integrity is lacking in existing schemes. So an efficient encryption scheme has been proposed which adopts elliptic curve cryptography to enhance data integrity. The security analysis and computational complexity of the proposed scheme is done and compared with existing schemes.
Results: The proposed scheme guarantees data integrity and privacy of the sensitive information stored in the electronic health records. The scheme also satisfied the security requirements user privacy, fine-grained access control, and scalability needed for electronic health record outsourced to the cloud. The computational complexity of the proposed scheme is compared with the existing schemes. The result shows that user access rejection complexity and key generation complexity are comparatively low.
Conclusion: Biometric, as a global identifier of the user, could improve data integrity for the electronic health records outsourced to the cloud. Multi-authority Inner Product Encryption hides the access structure, along with the data, could improve data privacy and user privacy. Employing NOT gate in the access structure reduces user access rejection complexity.

Keywords: Electronic Health Record, Multi-Authority Attribute-based Encryption, Elliptic Curve Cryptography, Biometric, Inner Product Encryption.

Received on 29 September 2019, accepted on 14 October 2019, published on 13 November 2019

doi: 10.4108/eai.13-7-2018.163135

1. Introduction

Electronic Health Record (EHR) is a database of an electronically recorded medical file for patients that can be shared and accessed through the cloud computing framework by several authorized users. EHR users are providers of health care, medical examiners, patient family members, and providers of insurance. Securing EHR from unauthorized users face many problems as it is outsourced to the third-party cloud and to wide variety of users. Sensitive information can be leaked from EHR at an unprecedented rate. The first significant security requirement is to keep data private, for outsiders including cloud servers. Maintaining data integrity is the second security requirement that EHR needs. For adequate healthcare delivery, the data in EHR should maintain correctness. Adversaries or authorized users

[*] Corresponding author. Email:ebencse@gmail.com

may intentionally change the information in EHR, resulting in lack of quality delivery of healthcare. The third requirement is to retain the privacy of the user to prevent key escrow. In order to provide this, the secret key of an authorized user should be confidential to the issuing authority. In addition to these security requirements, EHR outsourced to the cloud should provide flexibility to authorized users in accessing the EHR.

Researchers have developed many theories in providing security to EHR [1]. Researchers found that EHR's security issues can be limited by encrypting the information before being outsourced to the cloud [2]. And they found that attribute-based encryption (ABE) can achieve flexibility in accessing the encrypted EHR. The benefit of ABE is that it allows access to the same message by multiple users. Sahai and Waters [3] implemented the first ABE scheme for the encryption of EHR. ABE scheme enables users with attributes that fulfill the access structure to decrypt the data stored in EHR. ABE is of two forms, (KP-ABE) key policy ABE [4] and ciphertext policy ABE (CP-ABE) [5]. KP-ABE associates user decryption key with the structure of the access tree and associates ciphertext with the attribute set. In CP-ABE, the ciphertext is associated with the structure of the access tree, and the key is associated with the attribute set. The data owner is the authority in the single authority ABE to issue secret keys to users. Users holding the corresponding decryption key can decrypt EHR, keeping it confidential for others. The data owner should have full control over the EHR to provide data privacy. Thus, the data owner has to decide the authorized users to access the EHR before the encryption process. Since the data owner has to maintain all the attributes in single authority ABE which are cumbersome. Moreover, there may be a situation that data owners cannot maintain all attributes of the users.

Researchers found that multi-authority ABE will, therefore, be more efficient in providing security to EHR than previous single-authority ABE schemes. The main challenge for researchers in the design of multi-authority ABE is to inherit the collision-resistant property. Chase [6] originally developed a collision-resistant multi-authority ABE scheme using the Global Identifier (GID) to classify users and have a central authority. Instead, by excluding central authority, Chase and Chow [7] advanced the former multi-authority ABE scheme. This scheme offers user privacy by preventing key escrow, but lacks in data privacy. The data owner loses power over the EHR as other authorities regulate the EHR. Consequently, multi-authority ABE is not an ideal solution for securing EHR without the central authority. In fact, corrupt authorities collide in multi-authority ABE schemes to trace the GID of users to get their attributes. Anonymous key issuing protocol was a solution to prevent public exposure of user attributes, but it resulted in key complexity overhead.

This paper tends to propose a unique multi-authority inner product encryption (IPE) for confidential sharing of EHR in a cloud computing platform. The paper [8] projected the primary IPE scheme that hides the attributes related to the ciphertext, from authorized users and malicious users. Thus IPE limits the adversaries from guessing the attributes needed to decrypt the ciphertext. IPE schemes developed so far are not multi-authority to provide user privacy, data integrity, and efficient key management. Our multi-authority IPE scheme addresses the lack of data integrity by adopting biometric as the GID for users and attribute authorities. Since biometric is a unique physical trait for each user, adversaries cannot masquerade to access the information stored in EHR. And our scheme maintains data privacy by having a central authority, which is the data owner. The trusted authority issues the private keys to attribute authorities. In a multi-authority ABE scheme, user privacy is maintained through pseudorandom functions initiated by attribute authorities. In addition to this, our system hides the tree access structure associated with the ciphertext by inner product function. Also, the proposed system adapts ciphertext policy IPE (CP-IPE) such that the data owner can expressively describe access control policies over ciphertext. Thus our biometric-based multi-authority CP-IPE scheme is ahead of existing multi-authority ABE schemes in bestowing data privacy, data integrity, and user privacy, and it also reduces user access rejection complexity.

The content of the paper is structured as follows. Section 2 lays out the preliminary definitions needed to construct biometric-based multi-authority IPE. Section 3 explains the overview of related work used to compare with the proposed scheme. The system model and the detailed construction of biometric-based multi-authority IPE is described in section 4. The implementation of the proposed scheme and the comparative analysis with other related schemes is explained in section 5. Finally, the conclusion of the paper is provided.

2. Preliminaries

In this section, the basic definitions in exploiting biometric-based multi-authority CP-IPE for EHR is discussed.

2.1. Elliptic curve

Cryptographers have been using elliptic curves over finite fields since 1985. The following equation defines the elliptic curve over the finite field Fq

$$Y^2 \bmod q = X^3 + aX + b \bmod q$$

where $4a^3 + 27b^2 \bmod p \neq 0$

Koblitz and Miller found discrete logarithmic problems over groups of points on the elliptic curve give good security, and they stated that with the elliptic curve, shorter keys could be generated [9].

2.2. Pairing based cryptography:

Definition

Let G1, G2, and GT be from the same prime order cyclic group. A bilinear map from G1 × G2 to GT is a function e: $G1 \times G2 \rightarrow GT$ such that for all $u \in G1$, $v \in G2$, $a, b \in Z$,

$$e(u^a, v^b) = e(u, v)^{ab}$$

The following properties must be satisfied by the bilinear map:

(i) Bilinear: if $e(a^P,b^Q) = e(P,Q)^{ab}$ for all P,Q ϵ G1 and for all a,b ϵ Z, then the map e: G1 × G2 → GT is said to be bilinear.

(ii) Non–degenerate: The map does not give all G1 x G1 pairs to G2 identity. Note that since G1, G2 are prime order groups, this means that if P is a G1 generator, then e(P, P) is a G2 generator.

(iii) Computable: An effective algorithm should be used to determine e(P, Q) for any P,Q ϵ G1 [10].

Bilinear maps are called pairing groups because it can pair elements from G1 and G2 to GT. Pairing based cryptography takes two points from elliptic curve G and outputs from multiplicative abelian group GT. The pairing group has a unique property called bi-linearity, which is suitable for cryptography.

2.3. Decisional Bilinear Diffie Hellman (DBDH)

Decisional bilinear Diffie-Hellman should determine $e(g,g)^{abc}$, and the decision is taken whether Z= $e(g,g)^{abc}$ where a, b and c are uniform random elements of Z_p. Where g is the G generator, e is the bilinear map, and Z is a random G_T element [9].

An adversary A's advantage in resolving DBDH is defined as

ADV(A) = $\{pr[A(g,g^a,g^b,g^c,Z) \to 1 \mid Z= e(g,g)^{abc}] - pr[A(g,g^a,g^b,g^c,Z) \to 1 \mid Z \text{ is random}]\}$

The conclusion says that the Decisional Bilinear Diffie-Hellman (DBDH) assumption holds in the pairing group if the advantage of any polynomial-time adversary is negligible in solving the DBDH hard problem.

2.4. Definition of Mahalanobis Distance

Let $x = (x1, x2, \cdots, xn)$ and $y = (y1, y2, \cdots, yn)$ be two n-length vector which is derived from attributes [11]. With the covariance matrix M, the two vectors are of the same distribution. The Mahalanobis distance is defined below as if the two vector values are from the real number space R.

$$d(x,y) = \sqrt{(x-y)M^{-1}(x-y)^T}$$

Where $x - y = (x1-y1, x2-y2, \cdots, xn - yn)$.

The inverse covariance matrix M^{-1} is defined as follows:

$$M^{-1} = \begin{pmatrix} m_{1,1} & m_{1,2} & \dots & m_{1,n} \\ m_{2,1} & m_{2,2} & \dots & m_{2,n} \\ \cdots & \cdots & \cdots & \cdots \\ m_{n,1} & m_{n,2} & \dots & m_{n,n} \end{pmatrix}$$

Mahalanobis distance can be rewritten as:

$$d(x,y) = \sqrt{\sum_{1 \le i,j \le n} m_{i,j}\,(x_i - y_i)(x_j - y_j)}$$

The values x, y, M are to be embedded in group exponent of pairing group, so all the values of x, y, and M should be integers. The Mahalanobis distance value d should also be an integer, so the value d is squared to get squared Mahalanobis distance.

The squared Mahalanobis distance is:

$$D = d^2(x,y) = \sum_{1 \le i,j \le n} m_{i,j}\,(x_i - y_i)(x_j - y_j)$$

2.5 Definition of biometric-based multi-authority IPE

The following five polynomial-time algorithms present in a biometric-based multi-authority CP-IPE scheme:

Setup (λ) $\to pp, msk$: The trusted authority runs this randomized algorithm. This algorithm takes the input parameter λ and generates public parameters pp and master secret key msk.

Authority key generation (N, n, GID, msk): The data owner runs this authority key generation algorithm. The algorithm takes $N, n, GID, and\ msk$ as inputs. It outputs secret key for authorities sk_a, where n is the length of GID, and N is the number of authorities and GID is biometric of authority.

User key generation (sk_a, GID, A^k, d): This algorithm run by each attribute authorities. The algorithm takes authorities secret key, GID of a user, threshold value d, and attributes A^k in their domain as input. The algorithm checks the inner product between GID and attributes in their domain and GID and attributes submitted by the user. If the inner product between the attributes is zero, then the attribute authority issues the secret key for the user sk_a^k. The user collects sk_a^k from all n authorities and forms secret key SK. Since GID is biometric, the inner product between GID cannot be zero, and there arises fuzziness. If the fuzziness is below the threshold value, the secret key is issued; otherwise, the null value is returned.

Encryption (GID, M, T): The data owner runs this algorithm. The algorithm takes the public key, GID of attribute authorities, message M and access structure T as input and output the ciphertext CT.

Decryption (CT, SK): This algorithm run by a user takes CT and secret key SK as inputs and checks the inner product between the secret key related attributes and the ciphertext-related attributes. If the inner product between the attributes is zero, then outputs M; otherwise, outputs a null value.

3. Related Work

The massive advancement of digital technology replaced paper-based health records with electronic health records (EHR). There are numerous gaps in paper-based health records (PBHRs) [12]. Storing and transmitting PBHRs is expensive, and as it is hard to analyze. PBHRs are inefficient in providing quality healthcare delivery. So patient health record is stored digitally to provide global healthcare. Initially, medical organization adapted client-server based EHR system [13]. This technique uses local servers to store and maintain patient medical records. The major drawback of this technique is, the patient has to back up his medical records periodically to multiple locations in order to prevent his data from system failure. Moreover, the medical organization has to fix the server space and bandwidth before system implementation, and this affects scalability. The emergence of cloud computing overtook the disadvantages in the client server-based EHR system. The numerous benefits provided by cloud computing influenced medical organizations to store and maintain patient records in the cloud [14].

Storing patient sensitive and personal information to the cloud, which is a third-party service provider, leads to security concerns. Various encryption schemes were used to solve the security issues dealt with EHR outsourced to the cloud. Symmetric key encryption, public-key encryption, and identity-based encryption are the encryption techniques used to satisfy the security requirement of EHR. Symmetric key encryption falls with the drawback of key management. Public key encryption also falls with key management issues, and also it requires encryption of the same information multiple times each time for different user secret keys. Identity-based encryption also poses the former problem, and the management of certificates for each identity is cumbersome. So researchers found ABE well suited for encrypting EHR because it bestows flexibility, which makes encryption and key management more efficient. In this section, the overall ABE schemes developed using elliptic key cryptography, which is suitable for securing EHR, is discussed.

3.1. Single Authority ABE

ABE was initially introduced by Sahai and Waters as fuzzy identity-based encryption [3]. ABE is designed to support ciphertext encrypted for many users. A set of attributes is associated with both ciphertext and user secret key in ABE schemes. Only if the attributes related to the secret key meets the ciphertext related attributes, a user can able to decrypt the ciphertext. Researchers also developed access policy over attributes that can be embedded either in ciphertext or in secret key [4],[5]. ABE schemes are therefore categorized as KP-ABE and CP-ABE. The monotonic access structure is incorporated with the user secret key in KP-ABE, and in the ciphertext, the attribute sets are incorporated. The access policy in CP-ABE is embedded with ciphertext, and the attributes form the secret key of users. Yu et al. used ABE [15] to achieve EHR protection in the cloud. The proposed work used the dual encryption principle. Using symmetric key encryption, EHR is first encrypted, then with KP-ABE. The major disadvantage of the scheme is that the cloud server stores all user secret key components so user privacy falls. Moreover, KP-ABE does not allow data owners to enforce access policy over the ciphertext but over the key of the user, which lacks expressiveness. CP-ABE was created by Ibrami et al. [16] to provide access to EHR only for authorized users who comply with the access policy. This work separated EHR users into two categories: professional and social. This scheme addresses the issue of the expressiveness of the access policy. Narayan et al. [17] also developed an EHR security scheme based on CP-ABE. The drawback of the work is, the length of the ciphertext directly relates to the number of unrevoked users. With the following drawbacks, all ABE with single authority falls. First, it is overhead to maintain all attributes by a single authority. Secondly, by allowing the authority to decrypt all encrypted files, user privacy is lacking. Finally, ABE lacks the revocation of users on demand.

3.2. Multi Authority ABE

Researchers have therefore built ABE multi-authority to resolve all the drawbacks found in ABE single authority. Multi-authority ABE was initially developed by [6]. The users receive the public key and the secret key from various authorities. The central trusted authority shares public keys and secret keys to the attribute authorities, and the problem of collusion attack was resolved by having a global identifier. But the main problem is that the authorities can collide together to find the attributes of the user, which leads to a lack of user privacy. Without central trusted authority, Chase and Chow [7] developed multi-authority ABE by using distributed pseudorandom functions. Maintaining user privacy is achieved by using an anonymous key issuing protocol. The anonymous key issuing protocol resists authorities from knowing the global identifier of the user. The drawback of the scheme is user revocation is not realized efficiently, and access policy is incorporated in the user secret key, not on the ciphertext, which is not suitable to encrypt EHR. Li et al. [18] also promoted multi-authority ABE by splitting security domain to professional domain, and personal domain. The patient itself maintains a personal domain, and multiple attribute authorities maintain the professional domain, and EHR is encrypted using KP-ABE. This scheme used role-based access control techniques and key access policy to provide fine-grained access control over EHR for authorized users. Distinguishing each individual from a group is difficult in this scheme because of role-based access control. And naturally, KP-ABE is not suitable for securing EHR because the data owner is not specific with who can decrypt the ciphertext. According to [14], CP-ABE can be suitable for securing EHR because the authorized users attribute to satisfy the access policy related to the ciphertext that can decrypt the ciphertext. CP-ABE schemes with logically defined attribute set used to form secret key lacks flexibility and efficiency.

3.3. Multi authority attribute set based encryption

Bobba et al. [19] developed a system to support flexibility. They proposed a multi-authority attribute set based encryption, which supports key structure organized in a recursive set structure. In order to provide more flexibility, a hierarchical structure to the cloud users is proposed in [14]. The flexibility is assured because an attribute can hold multiple values for users. Wang et al. [20] combined hierarchical IBE with CP-ABE to develop hierarchical ABE. Although it provides hierarchical structure to the system users, it is not as efficient as [14] because it does not support multiple value assignments and compound attributes. Qian et al. [21] also improvised CP-multi authority ABE of [18] to secure EHR, which provides the user/attribute lazy revocation. This scheme lacks in providing data integrity and data privacy. The hierarchical attribute set based encryption designed bestows greater flexibility and fine-grained access control over EHR. As attributes are exposed and attribute set based encryption support multiple values, an attacker can easily guess the attributes needed to decrypt the ciphertext. So, there is a need to hide the attributes associated with the ciphertext.

3.4. Inner Product Encryption

Hiding attributes associated with the ciphertext meet user privacy. IPE is adapted to provide data privacy, which hides the attributes associated with the ciphertext to the user. IPE states that the private key formed by a vector x can be used to decrypt a ciphertext encrypted with another vector y, only if the inner product between the two vectors is zero ($x.y = 0$). Initially, the IPE scheme was introduced by Katz et al. [8]. Hierarchical inner product encryption was also developed having inner product predicates having levels such as predicate or attributes and searching attributes from predicates [22,23, 24]. Abdalla et al. [25] developed simple inner product encryption using lattices. IPE was also developed for biometric identity, which has to provide fault tolerance. The difference between the biometric during the registration phase and the decryption phase of the user is measured using a distance metric [11]. If the distance value lies below the threshold value then the user can decrypt the message. All the IPE schemes developed were single authority, and the attributes hidden are organized in a logically unique set.

In this paper, the proposed work exploits a variant to Multi authority ABE schemes, which provides data integrity, data privacy, and user privacy. Data integrity is achieved by using biometric as a GID. The proposed biometric-based multi-authority inner product encryption system hides the monotonic attribute tree access structure associated with the ciphertext, and various attribute authorities maintain the attributes as in multi-authority ABE. Each attribute authority maintains a disjoint subset of attributes and issues keys to the user. Biometric is added as one of the attributes to enhance data integrity and to avoid impersonation attacks. Moreover, an additional NOT gate is added to the monotonic tree access structure so that the user access rejection time complexity is reduced.

4. Proposed System

In this section, the proposed biometric-based multi-authority IPE scheme for securing EHR outsourced to a cloud server is elaborated.

4.1 Problem Definition

Within cloud servers, the data owner stores the EHR. EHR includes the sensitive data of the patient that should be confidential, and the reliability of healthcare delivery should be maintained correctly. The data owner should have control over the full medical record. So, before being outsourced to the cloud, the owner of the EHR encrypts the data. The encryption scheme used to encrypt EHR should ensure the following security requirements.

Data Privacy

Unauthorized access to EHR results in the disclosure of sensitive data resulting in both technological error and financial loss. Access to EHR should only be available for users who possess the attributes that fulfil the access tree structure established by the data owner. EHR should remain in accessible to unauthorized users.

Data Integrity

The data entered in EHR should be correct. Since the data is exchanged between many users and is outsourced to third parties, the data may be intentionally or unintentionally changed. EHR outsourced to the cloud should ensure accuracy in order to deliver quality health care.

User Privacy

The authority who issues secret keys to the users can unlock all the confidential data received by the user, which leads to a lack of user privacy. So the encryption scheme should avoid key escrow.

Availability

EHR should provide up-to-date information which should be accurate, and it should be available at the appropriate time to provide effective treatment for the patient. The availability of health records is very crucial for effective healthcare delivery.

Fine-grained access control

The authorized users should be able to access the EHR outsourced to the cloud easily. The flexibility in accessing EHR by the authorized user can be promised by employing flexible access policies over EHR by the data owner.

4.2 Overview of our system

The notion of our scheme is to secure EHR by providing data integrity, data privacy, user privacy, and fine-grained access control over outsourced EHR. Figure 1. shows the system model of biometric-based multi-authority IPE. The scheme has multiple attribute authorities, each holding a disjoint subset of attributes, and each user is identified by a global identifier GID, which is the biometric of a user. By having multiple authorities, the problem key escrow is resisted. The attribute authorities receive the private key

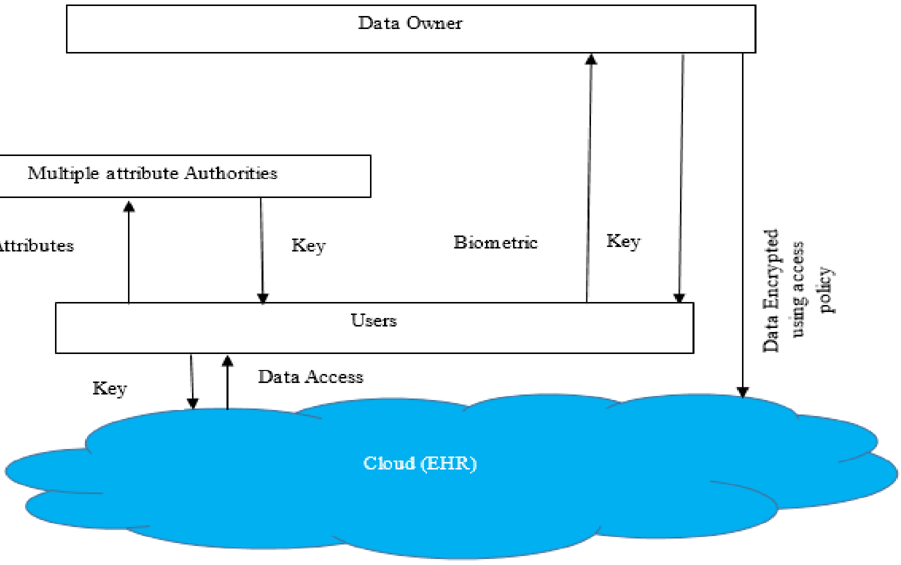

Figure 1. The proposed biometric based multi-authority IPE framework

from the data owner. The user submits GID along with other attributes to these attribute authorities. Each attribute authority checks the inner product between the attributes provided by them and attributes managed by them. If the inner product between the attributes is zero, then the attribute authority issue secret key to the user. The user collects a part of the secret key from all attribute authorities, and form a secret keys to decrypt a message. If the inner product between the attributes associated with the secret key created by the user and the attributes related to the access structure of ciphertext is zero, the user can decrypt the message. Since GID is biometric in the proposed scheme, there arises fuzziness between the biometric submitted by the user and the biometric maintained by the authorities. This fuzziness is measured by distance metric called Mahalanobis distance. If the distance value measured lies below the threshold value, the secret key is issued; otherwise, a null value is returned.This fuzziness is measured by distance metric called Mahalanobis distance. If the distance value measured lies below the threshold value, the secret key is issued; otherwise, a null value is returned.

4.3 System Description

In this section, the detailed construction of the proposed system is discussed. There are five polynomial-time algorithms in the system.

System Setup

The system first forms the universe of attributes and collects biometric of attribute authorities and users. The attributes are personal details, medical history, occupation details, medication, etc. Then this algorithm takes an input security parameter λ and the key structure depth d and outputs public parameters pp and master secret key msk. In this paper, key structure depth is considered to be two, and it can be extended. Moreover, as biometric is utilized, the inner product of the biometric at different times of the user may not be zero. In order to make the inner product zero, a vector transformation is done as in [11] with respect to Mahalanobis distance.

Let p be the prime number, G, G_T are the two cyclic group of same order p, e is the bilinear map $e: G \times G \rightarrow G_T$ and g be the group G generator. Then the algorithm chooses randomly $a_i, b_{i,j} \in z_p$ for $i = 1 to\ d, k = 1\ to\ m,$ and $j = 1\ to\ n,$ where m be the number of attribute sets and n be the number of attributes in the attribute set. Then the setup algorithm computes group element $g_{k,j} = g^{b_{k,j}}$. The public parameters and the master secret key is defined as follows:

$$pp = (G, G_T, p, g, u = e(g, g)^{\gamma}, f_i = g^{\frac{1}{a_i}}, h_i = g^{a_i})$$
$$msk = (a_i, b_{k,j}, \gamma)$$

Authority key Generation

There are N authorities, each maintaining a disjoint subset of attributes. This algorithm takes $N,$ the biometric, attributes of authorities M and msk as input and output secret keys for authorities. It chooses randomly $r, r_k, and\ r_{k,j} \in z_p$ and computes private key for authorities as:

$$sk_{AA} = (D = g^{\frac{\gamma+r}{a_1}}, D_1 = g^{\gamma+r_k} . \sum b_{k,j} . (M_{k,j})^{r_{k,j}}, D_2 = g^{k,j}, D_3 = g^{\frac{r+r_k}{a_2}})$$

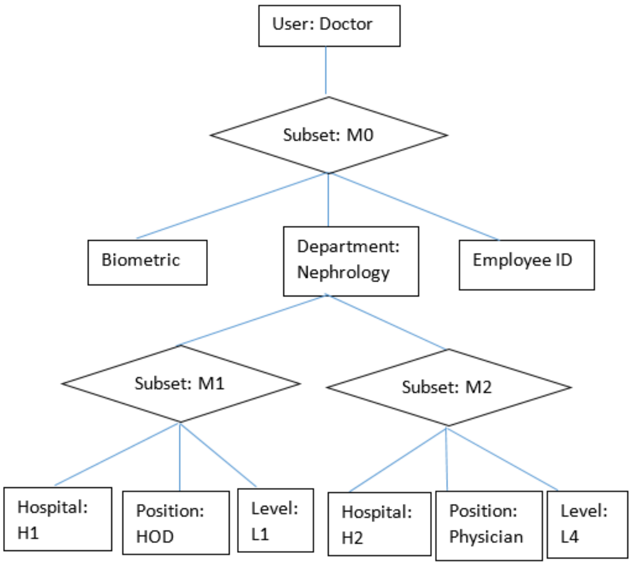

Figure 2. Example Key Structure

An example key structure of the users is shown in figure 2. The structure forms a recursive set. The recursion level in the recursive set is the depth of the key structure. The components in depth 1 may either be attributes or sets for depth two key structures, but only attributes constitute the set of components in depth 2. In Figure 2 {Hospital: H1, Position: HOD, Level: 1}, {Hospital: H2, Position: Physician, Level: 4} forms the key structure at depth 2. Indexing the sets in depth two as 1 to m can represent the key structure as M = {M0, M1, M2, ……., Mm}, where M0 is the sets at depth1. In Figure 2, {Biometric, Department: Nephrology, Employee ID}, {Hospital: H1, Position: HOD, Level: 1}, {Hospital: H2, Position: Physician, Level: 4} corresponds to M0, M1 and M2 respectively.

User Key Generation

Each user submits the biometric and the attributes to authorities. If the inner product between the biometric and attributes submitted by the user and the biometric and attributes maintained by authorities are zero, the authorities will issue the secret key to the user. The inner product between the biometric submitted by the user and the biometric maintained by authorities will not be zero. So the difference between the biometrics is measured using the distance metric called Mahalanobis distance. If the distance value lies within the threshold value t set by the data owner, then the user is accepted. To make the inner product zero, correspondence to Mahalanobis distance, and the threshold value, the biometric vectors are transformed as in [11]. This algorithm takes $GID,$ private key of authority sk_{AA} , subset of users attributes $M = M_0, \dots \dots \dots, M_m$ and generate secret key for users. Each attribute authority chooses $r', r'_k, and\ r'_{k,j} \in z_p$ and computes sk_n^k as:

$$sk_u = (D' = D.f_1^{r'}, D'_1$$
$$= D_1 . g^{r'k} . \sum \left(b_{k,j} (M_{k,j})^{r'k,j} \right) . D'_2$$
$$= D_2 . g^{r'k,j}, D'_3 = D_3 . f_2^{r'+r'k})$$

The user combines all the secret key issued by attribute authorities to form SK_u.

Encryption

Before the encryption process is done, the access structure for the users should be formed. An example tree access structure adopted in the proposed system is shown in figure 3. The tree access structure consists of interior nodes, which are threshold gates, and of leaf nodes which represent attributes [21]. Let the number of children of a node x is represented as n_x, and 0 to n_x be the range of threshold values. The threshold value of all the leaf nodes is 1. The various functions that can be executed with tree access structure are the parent(x), which output the node x parent, the att(x), which output leaf node x attribute that holds and the index(x), which refers to the number which defines node x. The patient medical record is hierarchically arranged so that the data owner can bestow access only to some portions in medical records according to the category of user [26].

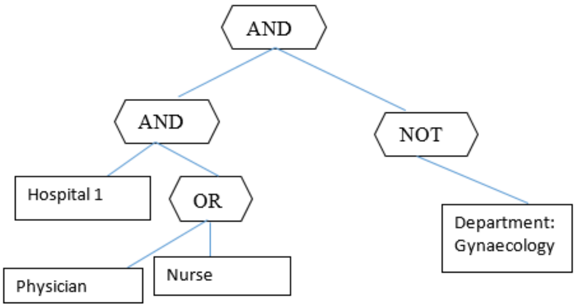

Figure 3. Tree access structure

The encryption algorithm takes GID of each attribute authority as input, and it encrypts the message M under specified access tree structure T. First the algorithm chooses polynomial P_x for each and every node x in the access structure T. The degree of the P_x is $t_x - 1,$ where t_x is the threshold value of node x. The t_x value of the leaf nodes is zero. Then the algorithm randomly chooses $s \in z_p$ and set $P_R(0) = s,$ where R represents the root node of the access structure T. The polynomial P_R is set by randomly choosing other t_R points. For other non-root nodes, $P_x(0) = P_{parent(x)}(index(x))$ and the polynomial P_x is set by randomly choosing other t_x points.

$$CT = msg.u^r, C = h_1^{\ r}, C_1 = h_2^{\ r}, C_l = g_r^{P_y(0)}, C_x$$
$$= h_2^{P_x(0)}, g_{1,1}^{s.w_{1,1}}, \dots \dots \dots, g_{k,j}^{s.w_{k,j}}$$

where l relates to the set of leaf node, x relates to the set of translating nodes and w relates to the value of each node in the tree access structure.

Decryption

The data owner encrypts the EHR according to the access structure and outsources it to the cloud. Authorized users who pose the key satisfying the access structure can access the EHR. The inner product between the attributes used to generate key and the attributes used to form the access structure should be zero. The algorithm checks the inner product between the attributes associated with SK_u and the attributes associated with CT. If the inner product is zero, then the algorithm output the original message; otherwise, a null value is returned.

5. Implementation and Comparative Analysis

5.1 Implementation

The system environment to implement biometric-based multi-authority inner product encryption for EHR providing data integrity, data privacy, user privacy, and fine-grained access control is set up using Intel i3 CPU 2.30 GHz, 4GB RAM, 64-bit Windows operating systems and 1TB hard drive. The Pairing based cryptography library is used to implement inner product encryption. An open-source software pairing-based cryptography library implemented in C language based on GNU multiple precision arithmetic libraries [27] is used in our scheme. Our scheme is compared with other related schemes through implementation and simulation. First, multi-authority ABE [7] is implemented, and then the proposed system is integrated into a prototype PHR system [28].

5.2 Comparing proposed system with similar existing systems

In this subsection, the comparison of the proposed biometric-based multi-authority IPE scheme with former ABE schemes designed for securing EHR is discussed. Table 1. shows the comparison between the proposed system and similar existing approaches in securing EHR. The comparison is made based on the mechanisms used to construct the scheme and the security requirement of EHR satisfied by each scheme. The security features found in our scheme are discussed below.

User Privacy

As the attributes are hidden to the attribute authorities through inner product function, user privacy is enhanced compared with other ABE schemes.

Data Privacy

Compared with other systems, data privacy through patient-centric EHR is strengthened. Since the attribute authorities receive the key from the data owner, the data owner has full control over the EHR. Thus our scheme provides more security to EHR outsourced to the cloud.

Data Integrity

Most of the existing ABE schemes used to secure EHR does not ensure data integrity. As biometric is used as GID, masquerading attack is almost avoided because biometric traits cannot be forged easily. The authorized users can only be able to access the information stored in EHR. If the data changed by the authorized user, it can be easily traceable.

Resist identity guessing attack

IPE hides the attributes associated with the ciphertext to the users. The attribute hiding property resists the adversaries from guessing the attributes needed to decrypt the ciphertext. So it is difficult for adversaries to get the secret key needed to decrypt the ciphertext. Thus our scheme provides more security to EHR outsourced to the cloud.

Fine-grained access control

As the proposed system adapted ciphertext-policy IPE, the data owners can establish access policy over the EHR effectively. Also, a hierarchical structure to the data and to the attributes used to form the key structure is generated. The hierarchical structure offers more flexibility in accessing the data in EHR, allowing access to specific data in EHR to specific authorized users.

Table 1. Comparing proposed system with similar approaches

Scheme	Yu et al [14]	Ibrami et al [15]	Chase [4]	Chase and Chow [5]	Li et al[4]	Qian et al [7]	Wan et al [8]	Proposed scheme
Encryption	Single authority ABE	Single authority ABE	MA-ABE	MA-ABE	MA-ABE	MA-ABE	MA-ABE	MA-IPE
Access control mechanism	Attribute based	Attribute based	–	–	Role based	Role based	Hierarchical attribute set based	Attribute based
Access Policy	KP	CP	_	_	CP	KP	CP	CP
Central Authority	Yes	Yes	Yes	No	No	No	Yes	Yes
Attribute hiding to authority	No	No	No	No	No	No	No	Yes
Attribute hiding to user	No	No	No	No	No	No	No	Yes

User Privacy	No	No	No	Yes	Yes	Yes	No	Yes
Data Privacy	Yes	Yes	No	No	No	No	Yes	Yes
Data Integrity	No	No	No	No	No	No	No	Yes
Key Escrow	Yes	Yes	Yes	No	No	No	Yes	No
Selective identity attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

5.3 Comparison of computational cost

Table 2. Comparison of computational complexity

Operations	Yu [14]	Li [6]	Wan [8]	Qian [7]	Proposed scheme
System setup	O(R)	O(R)	O(1)	O(R)	O(1)
File deletion	O(1)	O(1)	O(1)	O(1)	O(1)
Encryption	O(I)	O(I)	O(2R+X)	O(I)	O(2R+X)
Authority Key Generation	–	O(R)	O(2K+P)	O(R)	O(2K+d)
New user key generation	O(R)	O(R)	O(2K+P)	O(R)	O(2K+d)
Decryption	O(max(R,A))	O(R)	O(2R+X+Q))	O(R)	O(2R+X+Q)

Through implementation and simulation, the computational complexity of each algorithm is computed for the proposed scheme. The computational cost of each algorithm is calculated based on the number of exponentiations done to generate the output of the algorithm. The computational cost of the proposed system is compared with the existing systems and is shown in Table 2. Comparing with other systems, our scheme provides less computational cost in generating user keys.

where A relates to the total number of attributes in Universe, I relates to the attributes needed to encrypt the data file, d refers to the depth of key structure, R relates to the number of leaf nodes, K relates to the number of attributes in the key structure, P relates to the total number of attribute sets in a key structure, X relates to the number of translating nodes from each leaf node to the root node and Q relates to the number of nodes in the track of leaf node to the root node. The computational cost for each operation in our scheme is discussed below.

System setup:

There are only several exponential operations in calculating, and so the computational cost for selecting random numbers, bilinear group, and exponentiation operations are O(1). Setup time depends on the depth of the key structure.

Encryption:

The computation cost of encryption a data file relates to number of leaf nodes and to the number of translating nodes in tree access structure. To generate ciphertext, for each leaf node, there are two exponentiation operations, and for each translating node, there is one exponentiation operation. So the computational complexity for encrypting a data file is O(2R+X).

Authority key generation:

The computational cost of authority key generation relates to the number of attributes and the key structure depth. The authority key generation computation has two exponentiation for each attribute and one exponentiation for each depth. Therefore, the computational complexity for generating authority key generation is O(2K+d).

User key generation:

The computational cost of user key generation is associated with the number of attribute M involved in the key structure of a user and the depth of the key structure. Therefore, the computational complexity for user key generation of our scheme is O(2K+d).

Decryption:

The computational cost of decrypting a ciphertext relates to the number of attributes in the key structure and tree access structure. In the decryption algorithm, two pairing operations for every leaf node satisfying the tree and one pairing operation for every translating nodes is presented. As the size of the key structure and tree structure varies, the computational complexity of our decryption algorithm is O(2R+X)).

File Deletion:

As per the request of data owner EHR is deleted from the cloud. The cloud server confirms whether the offer is from the valid data owner. Therefore, the computational complexity is O(1).

User Access Rejection

If the user is not an authorized user, the access for EHR is rejected immediately because of NOT gate in the access tree structure. If there is no NOT gate, the user access rejection time complexity is equal to the complexity of decryption. The computational complexity is O(1).

Figure 4 shows the computational time for the setup phase, key generation phase, decryption and, user access rejection. The proposed scheme assumes that the key structure consists of one subset with 10, 20, 30, 40, and 50 attributes. The input to setup algorithm is the depth of the key structure. The input to the key generation algorithm is the attributes present in the key structure of the user. The time taken to generate a key is calculated with the number of attributes present in the key structure of the user. The input to the decryption algorithm is the ciphertext embedded with access tree structure and the secret key of the user. Figure 4. shows that the key generation time increases linearly with the number of attributes present in the key structure, and the setup time increases linearly with the depth of the key structure. The user access rejection time depends on the NOT gate present in the access tree structure and the level of the access tree structure. Decryption time depends on the way the key structure satisfies the access structure embedded in the ciphertext due to the subsets of attributes present in the key structure.

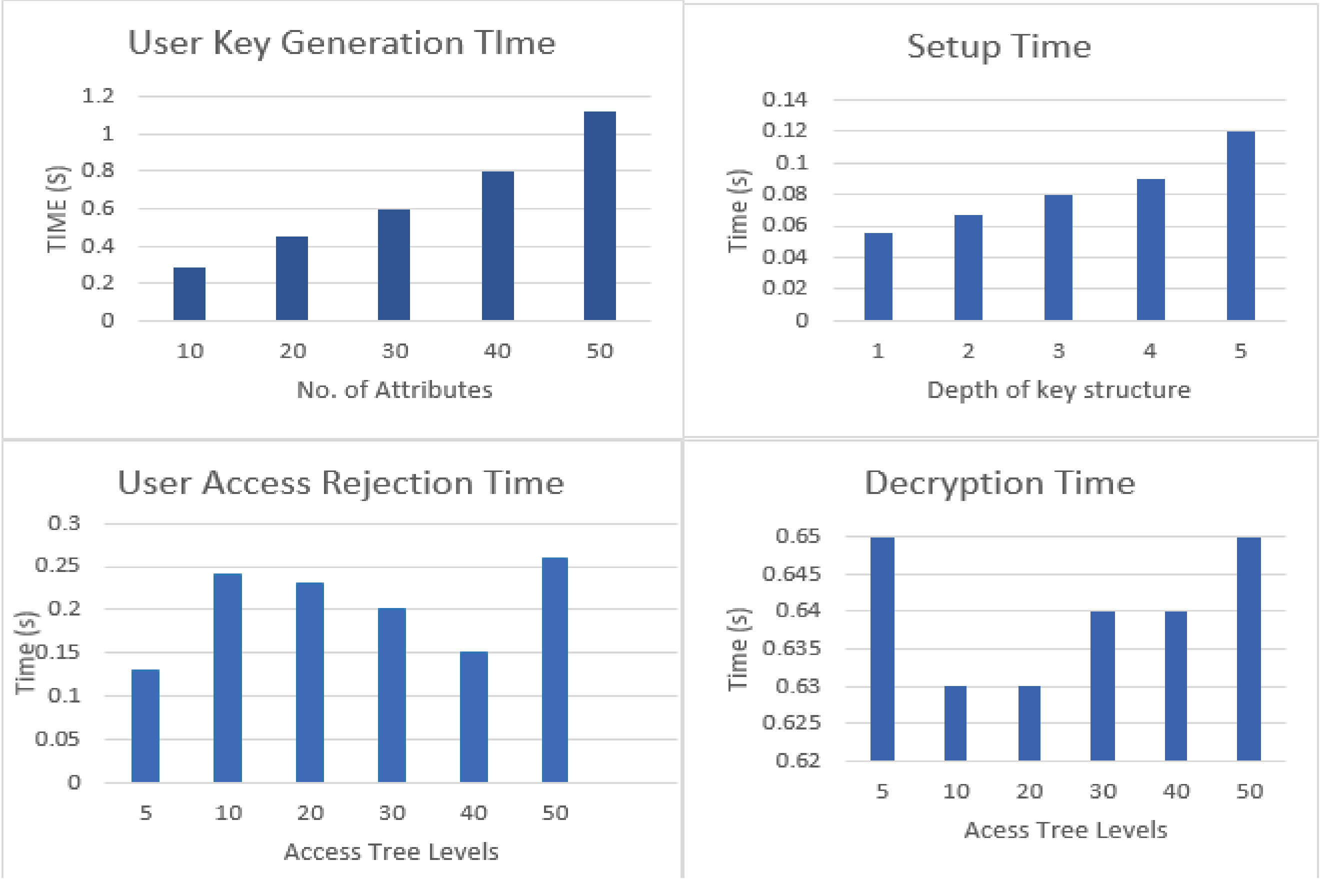

Figure 4. Experiments on Computational complexity of system setup, key generation, decryption and, user access rejection

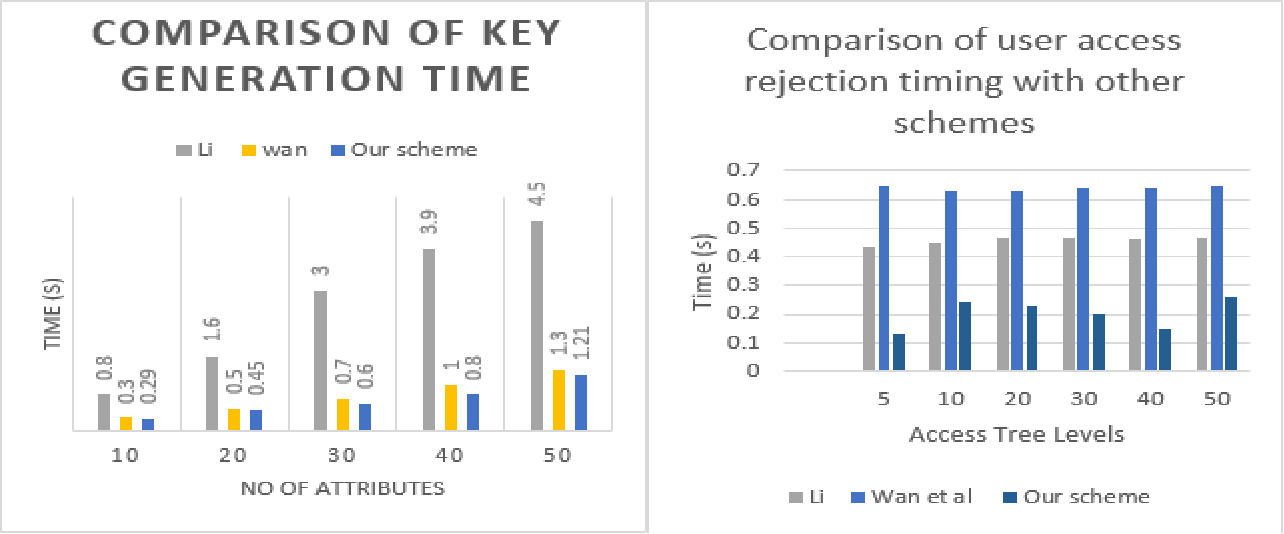

Figure 5. Comparison of key generation time and user access rejection time with other schemes

Figure 5 shows the computational complexity comparison of the proposed scheme with other existing schemes. The comparison result shows that the user access rejection time is decreased compared with other schemes. Because user access rejection time depends on the presence of NOT gate in the access tree structure and the level of access structure, where the NOT gate is present. The key generation time of user or attribute authority is slightly reduced compared with other schemes. Because the attribute is hidden, and only the inner product value is checked to generate the key.

5.3 Limitations

This sub-section discusses the various limitations of the proposed scheme. They are,

(i) The computational complexity of the algorithm for decryption differs from how the key meets the configuration of the access tree embedded in the ciphertext, because the user key structure may contain different subsets with many values for attributes. This could have only little impact on the scalability of the scheme as decryption takes place on the user side.

(ii) The size of the key for the user also varies according to the number of subsets and to the number of attributes in each set in the key structure. The size of the key shows little impact on the scalability of the entire scheme.

(iii) As the proposed scheme is implemented using Elliptic curve cryptography (ECC) there are potential attacks such as side channel attack. Moreover, ECC is prone to quantum attacks.

5.4 Recommendations

The following are the list of recommendations to overcome the limitations found in the proposed scheme,

(i) The size of the key and computational complexity of decryption algorithm show little effect on the scalability of the entire scheme. The impact can be neglected as the scheme provides more flexibility and more security compared to the existing systems.

(ii) As ECC is prone to quantum attacks lattice based cryptography can be applied in our proposed scheme.

6. Conclusion

In this paper, a novel multi-authority IPE system is proposed to secure EHR outsourced to the cloud server by providing data privacy, data integrity, and user privacy. The proposed scheme claim that in multi-authority settings, the data owner should have full control of the EHR outsourced to the cloud. So data owners as the central authority who issue part of secret keys to EHR users and to multiple attribute authorities are adopted in this paper. EHR users also receive part of their key from these multiple authorities and combine them to form the secret key. Inner product encryption is utilized to bestow additional security of hiding access tree structure associated with the ciphertext to the users. This property of attribute hiding prevents adversaries from injecting selective identity attacks. Also, biometric is utilized as GID for users to bestow data integrity, which prevents the masquerading attack. The user privacy is maintained in our multi-authority IPE scheme by hiding the attributes of users submitted to attribute authorities. Moreover, key issuing complexity and user access rejection complexity is reduced in our scheme. As ECC is prone to quantum attacks, this work can be further extended to resist quantum attacks by adopting lattice-based cryptography.

References

[1] Doyle, J., & Lon, J. (1994). Guardian Angel : Patient-Centered Health Information Systems.

[2] Lemke, J. (2013). Storage and security of personal health information. OOHNA J, 32(1), 25-26.

[3] Sahai, A., & Waters, B. (2005, May). Fuzzy identity-based encryption. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 457-473). Springer, Berlin, Heidelberg.

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

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

[6] Chase, M. (2007, February). Multi-authority attribute based encryption. In Theory of cryptography conference (pp. 515-534). Springer, Berlin, Heidelberg.

[7] Chase, M., & Chow, S. S. (2009, November). Improving privacy and security in multi-authority attribute-based encryption. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 121-130). ACM.

[8] Katz, J., Sahai, A., & Waters, B. (2013). Predicate encryption supporting disjunctions, polynomial equations, and inner products. Journal of Cryptology, 26(2), 191–224. https://doi.org/10.1007/s00145-012-9119-4.

[9] Chatterjee, S., & Sarkar, P. (2011). Identity based encryption. Springer Science & Business Media.

[10] Boneh, D., & Franklin, M. (2001, August). Identity-based encryption from the Weil pairing. In Annual international cryptology conference (pp. 213-229). Springer, Berlin, Heidelberg.

[11] Guo, F., Susilo, W., & Mu, Y. (2016). Distance-based encryption: How to embed fuzziness in biometric-based encryption. IEEE Transactions on Information Forensics and Security, 11(2), 247–257. https://doi.org/10.1109/TIFS.2015.2489179.

[12] Stausberg, J., Koch, D., Ingenerf, J., & Betzler, M. (2003). Comparing paper-based with electronic patient records: lessons learned during a study on diagnosis and procedure codes. Journal of the American Medical Informatics Association, 10(5), 470-477.

[13] Bahga, A., & Madisetti, V. K. (2013). A cloud-based approach for interoperable electronic health records (EHRs). IEEE Journal of Biomedical and Health Informatics, 17(5), 894-906.

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

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

[16] Ibraimi, L., Asim, M., & Petković, M. (2010). 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.

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

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

[19] Bobba, R., Khurana, H., & Prabhakaran, M. (2009). 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, 587–604. https://doi.org/10.1007/978-3-642-04444-1_36.

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

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

[22] Okamoto, T., & Takashima, K. (2016). Adaptively attribute-hiding (hierarchical) inner product encryption. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E99A(1), 92–117. https://doi.org/10.1587/transfun.E99.A.92

[23] Lewko, A., Okamoto, T., Sahai, A., Takashima, K., & Waters, B. (n.d.). Fully Secure Functional Encryption : Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. 02(subaward 641), 62–91.

[24] Zhang, L., Wang, Z., Mu, Y., & Hu, Y. (2015). Fully Secure Hierarchical Inner Product Encryption for Privacy Preserving Keyword Searching in Cloud. Proceedings - 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 3PGCIC 2015, 449–453. https://doi.org/10.1109/3PGCIC.2015.63.

[25] Abdalla, M., Bourse, F., De Caro, A., & Pointcheval, D. (2015). Simple functional encryption schemes for inner products. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9020, 733–751. https://doi.org/10.1007/978-3-662-46447-2_33.

[26] Benaloh, J., Chase, M., Horvitz, E., & Lauter, K. (2009). Patient controlled encryption: Ensuring privacy of electronic medical records. Proceedings of the ACM Conference on Computer and Communications Security, 103–114. https://doi.org/10.1145/1655008.1655024.

[27] LYNN, & B. (n.d.). PBC library-Pairing-based cryptography. Http://Crypto.Stanford.Edu/Pbc/. Retrieved from http://ci.nii.ac.jp/naid/10030667938/en/.

[28] Zheng, Y. A. O. (2011). Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption.