Journal of Optimization in Soft Computing (JOSC)

Vol. 1, Issue 1, pp: (1-11), September-2023

Journal homepage: https://sanad.iau.ir/journal/josc

Paper Type (Research paper)

A New Identity-Based Encryption Scheme Using Blockchain for Electronic Health System

Fatemeh Alidadi Shamsabadi[1], Shaghayegh Bakhtiari Chehelcheshmeh[1*] and Majid Alipour[1]

[1]*Department of Computer, Faculty of Engineering, Shahrekord Branch, Islamic Azad University, Shahrekord, Iran.*

Article Info

Article History:
Received :2023/8/12
Revised :2023/8/21
Accepted 2023/9/1

Keywords:
Electronic Health System, Identity-Based Encryption, Blockchain, Cloud Computing.

**Corresponding Author's Email Address: sh.bakhtiari@iaushk.ac.ir*

Abstract

With the development of information technology, electronic health (e-health) systems are used as a common approach to recording patients' medical data. Given that medical information is an essential asset of individuals and the health system, there are severe concerns about secure sharing and preserving this information's privacy. In this paper, we propose a new identity-based encryption (IBE) method by bilinear pairings to ensure the confidentiality of patients' data and their privacy in cloud health systems; in this way, this plan also provides authentication for users using challenge-response mechanisms. In addition, the proposed scheme, using blockchain techniques, ensures integrity and precise access control for shared data. The correctness of the proposed protocol is verified, and its security is formally proven in the standard model. The implementation of our scheme is performed in Java, and the results show that the proposed scheme reduces the computational overhead compared to previous similar methods.

1. Introduction

Today, e-health systems are rapidly evolving and becoming operational because these systems increase the quality of health care by enabling the exchange of information between health centers and joint treatment decisions. They also prevent unnecessary tests, misdiagnosis, and repetitive treatments by strengthening links between healthcare institutions [1, 2].

One of the main challenges in developing and advancing electronic health systems is providing confidentiality service and privacy. Since any attack on these systems will lead to irreparable damage, in recent years, many schemes have been proposed to ensure the security and confidentiality of electronic health systems.

Many of these methods are based on public-key protocols. In traditional systems, the public key infrastructure (PKI) requires a trusted third party to issue digital certificates so that users can verify the authenticity of other users' public keys. In addition to increasing the system's complexity, this increases the cost of electronic health systems [3]. In an identity-based encryption system, the identity of users (such as email addresses) is used to generate the keys of users. Thus, there is no need to issue and verify a digital certificate in an identity-based cryptography system [4]. The use of identity-based encryption in electronic health systems makes users comfortable. And also significantly reduces the costs of these types of systems.

Re-encryption proxy is another encryption method that converts ciphertext using the first user's identity to another ciphertext using the second user's identity. Therefore, in addition to preserving the confidentiality of the message, the second user can decrypt the ciphertext. Since the electronic health system needs to provide encrypted information by the patient to other authorized departments using the ID of the medical team, the use of re-encryption proxies in these systems facilitates the patient service process. Also, it reduces the cost of cryptography [3].

In addition to security issues, sharing and synchronizing sensitive information in e-health systems is also very important. Patient information held by the medical team is not readily available to other health centers. As a result, duplicate medical records are created. In addition to being costly for the health care system, this poses other processes for patients, which wastes

their time and unnecessarily extra costs. Blockchain, meanwhile, allows healthcare professionals to share this information through a chain of non-tampering blocks rather than storing patient records in separate databases [5, 6].

However, using blocks as a storage place for all information requires a lot of storage space and is expensive. Therefore, the content of patients' data can be stored in encrypted form in the cloud medical providers. Only the access address and a brief description of that information in the cloud providers can be recorded in the blocks to be accessed when needed [7].

Therefore in this research, a new identity-based encryption scheme is presented; Solves issues related to digital certificate management and public key infrastructure complexity. The proposed IBE scheme uses bilinear pairings only in the decryption phase, and the pairing parameter used in the encryption phase is pre-calculated; for this reason, using the proposed IBE reduces the computational overhead in the electronic health system.

The proposed design also can be used in re-encryption and blockchain technology. Due to the high volume of information, the content of patients' medical records is stored as encrypted in cloud storage systems. The access address of each of them is placed in a blockchain to share better and manage this data.

In addition, the effective combination of this scheme and re-encryption proxy provides confidentiality, reduces costs, and increases accessibility in the health system. In this paper, the proposed scheme is proved both in the random oracle and standard models. Also, the implementation results show that the proposed method reduces the running time compared to similar schemes.

The subsequent sections of the paper are organized as follows: In Section 2, an overview of previous schemes is provided. Section 3 describes the requirements for the proposal. In Section 4, the system is presented. In Section 5, the security and efficiency of the scheme are proved and evaluated. Finally, Section 6 concludes the paper.

2. Related Works

E-health is an electronic and communication process aimed at supporting patients' health care, introduced in 1999 [8]. The Electronic Medical Record (EMR) is kept confidential in these systems. E-health records contain information about the health of individuals during their lifetime, which serves as a source of information for physicians, health care providers, and research centers. Using electronic health systems, physicians can easily change health records. Patients also have easy access to their medical records through user interfaces designed to view medical information; In addition, healthcare providers can access patient information in critical situations [9, 3].

However, confidentiality and privacy are the main challenges in developing the health system to record patients' health records [10].

There are currently many suggestions for using cryptography to provide confidentiality in health systems, including symmetric and Asymmetric key methods similar to the anonymous ID technique. A common belief for creating confidentiality and privacy in e-health systems is to encrypt e-health documents in these systems [3].

Thus, data, identifiers, and attribute data keys (metadata) must be encrypted before being stored in an authentication center or resource in the cloud. In addition, establishing access control and key management issues and the cost of its implementation are always the most vital issues of health systems. Hence, cryptographic techniques can implement secure access control mechanisms or key management properties [11–13].

Despite the capabilities of IBE in recent years, very few articles have used these techniques to create confidentiality and privacy in electronic cloud health systems. Therefore, in this section, works close to the subject are expressed.

Benaloh et al. (2009) explored the challenges of protecting patients' privacy in the electronic health record system, arguing that security in such systems should be provided using encryption and access control. They also discussed using cryptography to record electronic medical records, ensuring confidentiality by a patient-controlled cryptography model [14]. In this scheme, the patient can generate and store the cryptographic key; So that the patient's privacy in the computer data center is not compromised. In the same year, Xue et al. proposed an authentication system using identity-based encryption to protect the confidentiality of electronic health networks [15].

In 2011, Barua et al. proposed a plan for the confidentiality and control of patient-centered access to electronic health systems in the cloud [16]. In this scheme, to ensure the privacy of personal health information, the EDPAC technique has been introduced, which enables the system to give data requesters different levels of access based on their role in the system.

In 2012, Guo et al. introduced an authentication system with feature-based confidentiality in the e-health system [17]. In this scheme, to protect patients' personal information while receiving medical services, a framework called PAAS has been proposed to authenticate the attribute of users in the process of authentication of users in the electronic health system to preserve privacy.

In 2013, Li et al. proposed the scalable and secure sharing of personal health records in the cloud using feature-based encryption [18]. This design presents a

new patient-centric model with a set of data access control mechanisms for storing personal health documents using the feature-based encryption technique in semi-trusted providers.

In 2016, Yan et al. proposed a new access plan to implement secure access control of personal health documents in electronic health systems based on the original feature-based encryption scheme [19].

According to studies, the schemes [3, 7] increase access to medical records and are considered to be the most relevant plans to the proposed health system. Now, these schemes will be reviewed.

In 2017, Wang et al. presented a new identity-based encryption scheme for utilization in the health system. They explained how to use this scheme to reduce the disadvantages of the methods used in the e-health system. This identity-based encryption scheme can be used in a re-encryption proxy. However, the extensive use of bilinear pairing functions and extended general parameters increases the computational cost in the encryption and decoding phases [3].

In 2018, Wang and Song implemented a hybrid encryption scheme in blockchain technology to share e-health records securely. The use of two attribute-based signature schemes and identity-based encryption in this method dramatically increases the computational overhead and overshadows the scalability of this system [7].

3. Prerequisites for the Proposed Scheme

In this paper, we first introduce a new method for identity-based encryption. The proposed method is then combined with a re-encryption proxy, blockchain technology, and cloud storage systems for electronic health systems. For this purpose, cryptographic methods based on identity are examined in this section, and other concepts related to the proposed design are described.

3.1. Identity-Based Encryption

As the name implies, identity-based encryption uses the user ID (such as Email Address) as the public key in this type of encryption. In this encryption method, Key Generation Center (KGC) is responsible for the authentication of users. The identifiers are registered; KGC creates the private key corresponding to the ID and delivers it to the users. It also creates some public parameters and makes them known to everyone.

The user who intends to send the message first encrypts the message with the recipient's public key obtained directly from her ID and the public parameters provided by the key generation center. The message recipient decrypts the ciphertext using its private key and the public parameters from the key generation center [20]. Shamir first proposed this cryptographic design in 1984 as an identity-based signature (IBS) method [21].

However, Shamir failed to introduce identity-based encryption until Boneh and Franklin 2001 introduced the first practical structure of identity-based encryption based on bilinear pairing groups with proof in the random oracle model [4]. Due to the reasonable length of the key and the cost of computations for the key generation center, this design became the basis for creating IBE methods.

In 2003, Boneh and Franklin introduced another identity-based encryption. This design was presented with slight changes from their first design, such as asymmetric bilinear pairing and the use of two hash functions as a public parameter of the key generation center with proof in the random oracle model [22].

Subsequently, other methods with relatively different structures were proposed, among which the IBE and IBS methods of Sakai and Kasahara 2003 [23] and the IBE method of Boneh and Boyen 2004 [24] were more effective. The reason for this better efficiency was not to use bilinear pairing at encryption, which reduced costs.

In 2006, Gentry introduced an identity-based encryption scheme based on the Boneh and Boyen method, which required the calculation of further pairings in the form of parameters pre-calculated by the key generation center [25]. Gentry design has more resistance than Boneh and Boyen's scheme. Still, it is less efficient than the Sakai and Kasahara designs and the non-random oracle version of Boneh and Boyen, and it also requires complex assumptions [20].

In 2011, Boneh and Boyen introduced an identity-based encryption system. Their system was not based on the random oracle model, and it provided resistance against the chosen-identity attack. This structure did not need to calculate bilinear pairing in the encryption phase. It is only required to calculate two pairing functions in the decryption phase [26]. In 2010, Galindo proposed an identity-based encryption design. It provided chosen-ciphertext security with constant-size ciphertexts under computational Diffie-Hellman's bilinear assumptions in the standard model [27].

In 2015, Park et al. proposed an identity-based encryption scheme with chosen-ciphertext security. They aimed to obtain tight security in the bilinear Diffie Hellman problem [28]. In 2015, Susilo et al. presented an identity-based encryption scheme with a dynamic threshold and constant-size ciphertext. In their design, the sender, by selecting the number of receivers, provides constant-size ciphertext so that it is possible to decrypt only in the presence of all receivers [29].

In 2017, Bakhtiari and Hosseinzadeh introduced an identity-based encryption method that, in addition to encryption, can also use for signing messages. They used their method for proposing a certificateless authentication scheme [30]. In the same year, Wang et al. introduced the e-health system using an identity-

based cryptographic scheme that was efficient [3]. This method is optimized for use in re-encryption proxies. The disadvantages of this method are the long public parameters and the use of many bilinear pairing functions in encryption and decryption.

3.2. Re-Encryption Proxy

The concept of re-encryption proxy was introduced in 1998 by Blaze et al. [31]. In this scheme, a semitrusted proxy with information such as a re-encryption key converts the ciphertext into another ciphertext using the public key of the first delegate; So that it is possible to decryption the ciphertext by the private key of the second delegate. In this scheme, the proxy will not access the message's plaintext.

3.3. Blockchain Technology

The first blockchain was introduced in 2008 by Nakamoto to create a consistent database among all members of a decentralized network [32]. Here is an example of its application in the health system to better understand blockchain technology.

People often go to different hospitals and medical centers during their lives, and each time they go, they provide specific and various medical information to these institutions. Hospitals must share patients' medical information confidentially with other authorized institutions to provide accurate, fast, and effective medical services [33]. In addition, they need to address concerns about patients' privacy, mistrust between healthcare providers, scalability, and how to control access to medical information [34, 35].

For this purpose, blockchain technology is used as a suitable solution. Blockchain technology allows the information stored in the blocks to be shared among all network members, making it almost impossible to manipulate the recorded data using cryptographic methods. In addition, access control can be achieved more efficiently by implementing blockchain. When this system is used for large volumes of data, health professionals will be well aware of how accurate the management of this new trend can be [36, 5].

4. Proposed Scheme

In this section, a new identity-based encryption scheme based on bilinear pairings is first proposed. Then, the model of the re-encryption proxy system is presented according to the proposed cryptographic scheme. Finally, the cloud health system for medical information sharing using blockchain technology is described. Table 1 describes the symbols used in the proposed scheme.

Table 1: Symbols of the proposed scheme

Symbol	Definition
$h()$	Hash function
G, G_T	Cyclic group
$e: G \times G \to G_T$	Function bilinear pairing on the elliptic curve
ID_i	Identity-related to the *i*th user
$msk = \{\}$	KGC's private key
g_1, g_2	Public parameters
Z_P	The prime group to measure p
$Z^*{}_p$	The prime group, which contains all positive integers, is smaller than p.
g	Generator of group $Z^*{}_p$
d_i	Private key related to the *i*th user
m	Plaintext
CT	Ciphertext
SE	Symmetric cryptographic element
δ	One-time digital signature pattern

4.1. Proposed Identity-Based Encryption

The focus of the proposed identity-based encryption scheme is to maintain flexibility while providing security so that the proposed IBE is independent in other applications. In the proposed IBE, the computational overhead is significantly reduced by shortening the parameters used in the cryptographic phases and pre-calculated pairing in the encryption phase. In addition, the strength of the proposed IBE is its ability to be used in a re-encryption proxy system and blockchain technology.

Thus, by reducing the calculations of bilinear pairings in the phases of encryption and decryption, the amount of computations is significantly reduced compared to previous methods; as a result, the computational overhead of the system is reduced.

System Setup Phase: First, the algorithm $\mathcal{G}(1^n)$ is executed to obtain a tuple of (G, G_T, e). In this system, g is the generator element for the bilinear group G modulus p, and the identity ID is assumed to be an element of the group Z_p^*. The ciphertext is also considered an element in the group G_T. To generate public parameters and the master key, the key generation center chooses two random numbers $a_1, a_2 \in Z_p^*$. The public parameters of the system and the master key are then defined by the key generation center as Eq. (1).

$$\begin{aligned} &g_1 = g^{a_1} \\ &g_2 = g^{a_2} \\ &Vo = e(g, g_2) \\ &params = \{g, g_1, g_2, Vo, G, G_T, e, h\} \\ &msk = \{a_1, a_2\} \end{aligned} \quad (1)$$

Key Generation Phase: With the public parameters $(params)$, master key msk, and identity ID, the key

generation center selects a random number r and generates the private key as Eq. (2).

$$d_{ID} = (d_1, d_2, d_3) = \left((a_1 ID + a_2)^{-1}, {g_1}^{ID^r}, {g_1}^r\right) \quad (2)$$

Encryption Phase: A random number s is selected to encrypt plaintext $m \in G_1$ using identifier $ID \in Z_p^*$. The ciphertext C_T is calculated as Eq. (3).

$$C_T = (C_1, C_2, C_3) = \left((g_1{}^{ID} g_2)^s, mVo^s, g^{ID^s}\right) \quad (3)$$

Decryption Phase: The end-user decrypts the ciphertext.$C_T = (C_1, C_2, C_3)$ using her private key and public parameters and does the Eq. (4).

$$M = \frac{C_2 e(C_3, d_3)}{e\left({C_1}^{d_1}, g_2 d_2\right)} \quad (4)$$

The correctness of the above condition is as Eq. (5).

$$M = \frac{C_2 e(C_3, d_3)}{e\left({C_1}^{d_1}, g_2 d_2\right)} = \frac{mVo^s e\left(g^{ID^s}, {g_1}^r\right)}{e\left((g_1{}^{ID} g_2)^{s^{(a_1 ID + a_2)^{-1}}}, g_2 {g_1}^{ID^r}\right)} = \frac{me(g, g_2)^s}{e(g^s, g_2)} = M \quad (5)$$

4.2. Proposed Re-Encryption Proxy

This section describes how to apply the proposed IBE to the re-encryption proxy system for use in blockchain technology.

System setup: First, the algorithm $\mathcal{G}(1^n)$ is run to obtain tuples (G, G_T, e). The generator g is then generated for the bilinear group G modulus p. Next, a one-time digital signature δ and symmetric encryption element SE are chosen. Also, three hash functions, $G: \{0,1\}^* \to Z_p^*$. $H_1: S \to G$ and $H_2: G_T \to K$ are selected in which K is the SE's keyspace. Here the ciphertext is assumed to be an element in group G_T. Random numbers $a_1, a_2, f, f' \in Z_p^*$ are selected to generate public parameters $params$ and the master key msk. The public parameters of the system and the master key are then defined by the key generation center as Eq. (6).

$$g_1 = g^{a_1}, \quad g_2 = g^{a_2}, \quad Vo = e(g, g_2), \quad \mathcal{A} = g^f, \quad params = \{g, g_1, g_2, Vo, G, G_T, e, h\}, \quad msk = \{a_1, a_2, f, f'\} \quad (6)$$

Key Generation: With the public parameters ($params$), the master secret key msk, and the identity ID, the key generation center selects the random numbers $r, r', n, n', z, \mathfrak{n} \in Z_p^*$ and generates the users' private key sk_{ID} as Eq. (7).

$$sk_{ID} = (d_{ID}^A, d_{ID}^B, d_{ID}^C)$$
$$d_{ID}^A = (d_1, d_2, d_3, d_4, d_5, d_6) = \begin{pmatrix} (a_1 ID + a_2)^{-1}, {g_1}^{ID^r}, g^{ID^r}, \mathfrak{n} + fr, \\ {g_1}^n, \mathcal{A}^r (g_1{}^{ID} g_2)^{-n} g^{\mathfrak{n}} \end{pmatrix}$$
$$d_{ID}^B = (d'_1, d'_2, d'_3) = \left(\frac{fr'}{a_1 ID + a_2}, {g_1}^{n'} g^{f' ID}, \mathcal{A}^{r'} (g_1{}^{ID} g_2)^{-n'}\right)$$
$$d_{ID}^c = (d_7, d_8) = g_2{}^{a_1{}^{-1}} (g_1{}^{ID} g_2)^{zID}, {g_1}^{zID} g^{f' ID} \quad (7)$$

Encryption and Signature: To encrypt the plaintext $m \in G_T$ using the $ID \in Z_p^*$, a random number s and an on-time digital signature in time are selected using the private key ssk and public key svk, and the ciphertext C_{ID} is obtained as Eq. (8).

$$C_{ID} = (C_1, C_2, C_3, C_4, C_5, C_6) = \begin{pmatrix} (g_1{}^{ID} g_2)^s, SE.Enc(h_2(V_o)^s, m), \\ {g_1}^s, h_1(svk)^s, svk, \sigma \end{pmatrix}$$
$$\sigma = \delta.sig(ssk, C_1, C_2, C_3, C_4, C_5) \quad (8)$$

Message Validation: The Eq. (9) verification is checked to ensure the message's validity using the ciphertext $C_{ID} = (C_1, C_2, C_3, C_4, C_5, C_6)_{ID}$, and public parameters.

$$\delta.Verify(C_5, C_6) = Yes\ , e(g_1, C_4) = e\left(C_3, h_1(C_5)\right) \quad (9)$$

Re-Key Generation: The first recipient with the identity ID is the only person who has access to the information encrypted with his ID. Upon receipt of the decryption request from the second receiver with the ID', the first receiver generates the re-encryption key for the proxy; The proxy encrypts the information with the re-encryption key without being informed of the ciphertext content. New encrypted data can be decrypted once and only by the decryption key of the second user.

In the above phases, two points are essential: first, the re-encryption key $rk_{ID \to ID'}$ is sent to the re-encryption proxy using IBE in a provided platform; Second, the proxy re-encrypts the information that it is not aware of its contents, and the risk of a re-encryption key alone does not compromise information security.

In addition, since the re-encryption key is only intended for re-encryption and does not apply to the unencrypted message, the attacker can not achieve the message content only by the re-encryption key and without the private key of the message's receiver. To

generate a re-encryption key, the recipient, after selecting a random number k generates the re-encryption key $rk_{ID\to ID'}$ as Eq. (10) and provides it to the re-encryption proxy.

$$
\begin{aligned}
&rk_{ID\to ID'} = (rk_1, rk_2, rk_3)\\
&rk_1 = \frac{1}{k}\left((d_1 d_4)ID' + d'_1\right)\\
&= \frac{\mu ID' + f(rID' + r')}{k(a_1 ID + a_2)}\\
&rk_2 = {d_5}^{ID'} d'_2 = g^{f' ID} {g_1}^{(nID'+nr)}\\
&rk_3 = {d_6}^{ID'} d'_3 = \frac{g^{f(rID'+r')} g^{f\mu ID'}}{{g_1}^{ID}\,{g_2}^{(nID'+nr)}}\\
&rk_4 = {g_1}^{k}
\end{aligned}
\tag{10}
$$

Re-Encryption: The re-encryption proxy with the option of ciphertext $C_{ID} = (C_1, C_2, C_3, C_4, C_5, C_6)_{ID}$ and public parameters, re-encrypt the ciphertext as Eq. (11).

$$
\begin{aligned}
&\hat{C}_{ID} = (C'_1, C'_2, C'_3, C'_4, C'_5, C'_6)\\
&= \left(C_1, C_2, C_3, e\left({C_1}^{rk_1}, rk_4\right), rk_2, rk_3\right)
\end{aligned}
\tag{11}
$$

Decryption 2: The recipient of the message will decrypt the message by having the ciphertext $C_{ID} = (C_1, C_2, C_3, C_4, C_5, C_6)_{ID}$ that is encrypted using his ID and the private key $sk_{ID} = (d_{ID}^A, d_{ID}^B, d_{ID}^C)$ that is in it $sk_{ID}^A = (d_1, d_2, d_3, d_4, d_5, d_6)$, and the public parameters are as Eq. (12).

$$
\begin{aligned}
&K = h_2\left(\frac{e({C_1}^{d_1}, g_2 d_2)}{e(C_3, d_3)}\right)\\
&SE.Dec(K, C_2) = m.
\end{aligned}
\tag{12}
$$

Finally, using the properties of element SE, plaintext m is verified.

Decryption 1: In this phase, user B, with the public parameters and the private key $d_{ID}^C = (d_7, d_8)$, decrypts the re-encrypted ciphertext $\hat{C}_{ID} = (C'_1, C'_2, C'_3, C'_4, C'_5, C'_6)$ as Eq. (13).

$$
\begin{aligned}
&K = h_2\left(\frac{e(C'_1, C'_5)\, e(C'_3, C'_6)\, e(C'_1, d_7)}{C'_4\, e(C'_1, d_8)}\right)\\
&SE.Dec(K, C_2) = m.
\end{aligned}
\tag{13}
$$

4.3. Proposed Blockchain-Based E-Health

As shown in Figure 1, five entities play a role in the proposed e-health system, including patients, the medical team, the key generation center, the re-encryption proxy, and the health service provider. Using a re-encryption proxy in blockchain technology and combining it with the proposed encryption scheme in the cloud health system, we have the following scenario (It should be noted that all steps in this scenario are performed by Section 5.2):

0. The key generation center generates the public parameters of the system and the public and private keys of each entity and provides them. This process takes place after registering the identity of each entity in the health system and authenticating them.
1. Patient A visits the medical team for the first time. The medical team sends their ID (the public key) to the patient so that both can use identity-based encryption and agree on a symmetric key to encrypt the patient's medical records.
2. The patient encrypts his electronic health documents to provide confidentiality using the agreed symmetric key and AES encryption (or similar). Then, according to the system model, it outsources these medical documents to the cloud, along with the symmetric agreement key encrypted in identity-based encryption.
3. Members of a blockchain network extract encrypted data from the cloud and execute a verification algorithm to message validation. Then, by performing a consensus protocol, they select the bookkeeping member.
4. The bookkeeping member sends the encrypted data to the cloud re-encryption proxy and obtains the data access address from the cloud.

4.1. It also writes a brief description that includes encrypted data and its cloud address as a specific format in the blockchain.

5. Whenever the medical team needs patient A's electronic health records, they review the blockchain's contents and obtain the data address they want.

5.1. The medical team receives the relevant encrypted documents from the cloud and, with a pre-shared symmetric key, decrypts the documents easily.

6. We assume that user A becomes ill again sometime later and needs the services of another medical center. The health service provider needs the information of user A to diagnose the disease better and take action. Therefore, they find the address of information of patient A in the blockchain.

6.1. The health service provider sends the address of information of patient A in the blockchain and their ID to the medical team.

7. The medical team, having its private key and the ID of the health service provider, generates a re-encryption key by running the re-key generation algorithm in the re-encryption proxy system. It also provides the address of information of patient A and the re-encryption key to the re-encryption proxy.

7.1. In addition, it sends the decryption key of the first-level encrypted text to the requester for information on user A.

8. The re-encryption proxy re-encrypts the pre-shared symmetric key that has already been encrypted using the identity-based encryption scheme and sends it to the health service provider.
9. The health service provider decrypts patient A's medical information using the key provided to them by the medical team during the re-key generation key phase and the pre-shared symmetric key that has been re-encrypted by the proxy and sent to themThis section describes how to apply the proposed IBE to the re-encryption proxy system for use in blockchain technology.

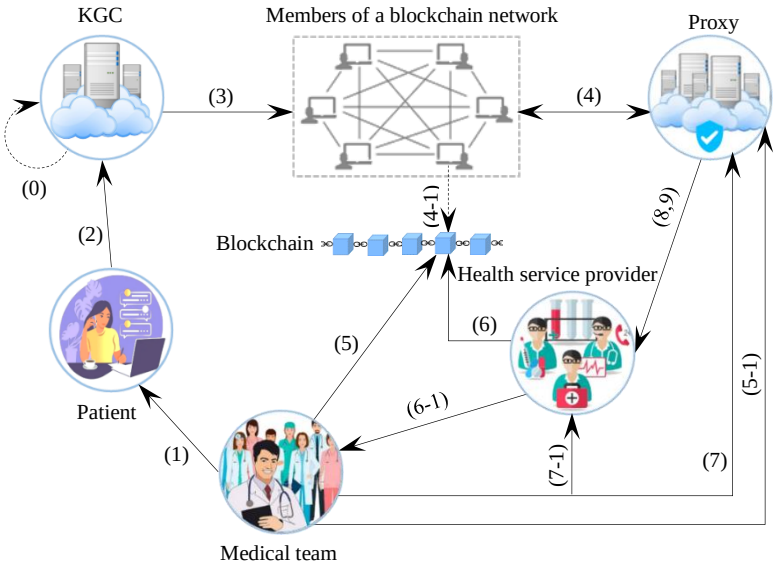

Figure 1. The framework of the proposed e-health system

5. The Proposed Scheme Analysis

In this section, the proposed identity-based encryption scheme is evaluated in terms of security and performance. First, the security of the proposed scheme is proved in the standard model, and it is shown that this method has provable security in the random oracle model. Then, the efficiency of the proposed scheme is compared with other identity-based encryption methods.

5.1. Security Analysis

The IND-ID-CCA security model is used here to prove the proposed IBE formally. This security model is based on a game between the challenger and the attacker in 5 steps (setup, phase 1, challenge, phase 2, and guess). According to theorm1, the proposed method is secure against the IND-ID-CCA attacker. In the following, we explain the mentioned steps.

- **Theorm1:** If the hypotheses of Bilinear Decisional Diffie-Hellman (BDDH) are valid in the tuple (G, G_T, e), the proposed identity-based encryption scheme is secure against the IND-ID-CCA attacker.
- **Proof:** Suppose attacker α can attack the proposed scheme. In this case, we show that a structure called Algorithm β can solve the BDDH problem in the tuple (G, G_T, e). Algorithm β has multiple (g, g^a, g^b, g^c, T). T is a random number or equal to $e(g,g)^{acb}$. The purpose of Algorithm β is to generate the bit 1 if the equation $T = e(g,g)^{abc}$ is satisfied; If T equals a random number, the bit 0 is generated as the output. Suppose $a = a_1$ and $b = a_2$. Algorithm β interacts with attacker α to solve the problem ahead. The game of the selective identity begins with the first output of the identity ID^* that attacker α intends to attack as the following:

- **Setup:** To generate system parameters, Algorithm β selects two random numbers, a and b, and generates the public parameters $params = \{g, g_1, g_2, Vo\}$, and passes them to attacker α.
- **Phase 1:** In this phase, the attacker α selects identities adaptively. It then uses these identities to issue private key generation or decryption requests. Algorithm β provides a valid decrypted text related to the attacker's requested ciphertext and a private key associated with the attacker's desired ID.
- **Challenge:** After the attacker α decides to end phase one, it sends two plaintexts m_1, m_2 with equal length and an identity ID_* to the algorithm β. Algorithm β then selects the random bit $\gamma \in \{0, 1\}$ and generates the ciphertext $CT_* = (g_1{}^{ID_*} g_2)^c, M \cdot T, g^{ID_*{}^c}$. It then sends the ciphertext CT_* as a challenge to attacker α. Note that algorithm β does not know the value of c; But receiving the value of g^c is considered as one of the inputs to the BDDH problem.

- **Phase 2:** This phase is similar to phase 1; the difference is that the attacker cannot request a private key for the identity ID^* and a request for decryption CT_*.
- **Guess:** In the final, attacker α guesses the value $\gamma' = \{0, 1\}$. If the equation $\gamma' = \gamma$ is true, Algorithm β displays the value 1 as the output. This means $T = e(g, g)^{acb}$; Otherwise, it represents the value 0, which means T is a random number. If the equation $T = e(g, g)^{acb}$ is satisfied, attacker α can defeat the proposed scheme, which means that algorithm β must exist and solve the hard problem of BDDH. As a result, as long as no algorithm β can solve the hard BDDH problem, the proposed encryption scheme will be IND-ID-CCA secure.

5.2. Security Comparison

Table 2 shows a comparison between the proposed method and other methods from a security point of view. Protocols that benefit from encryption, digital signature, re-encryption proxy, and blockchain are more secure. Also, IBE methods whose security has been proven in the standard model are more reliable.

Table 2: Security comparison

Schemes	Security Properties							
	Confidentiality	Traceability	Authentication	Non-repudiation	Integrity	Optimized in re-encryption proxy	Access control with blockchain	Proof security in the standard model
Boneh and Franklin [4]	✓	✓	×	×	×	×	×	×
Boneh and Franklin [22]	✓	✓	×	×	×	×	×	×
Sakai and Kasahara [23]	✓	✓	✓	✓	✓	×	×	×
Boneh and Boyen [24]	✓	✓	×	×	×	×	×	✓
Gentry [25]	✓	✓	×	×	×	×	×	✓
Boneh and Boyen [26]	✓	✓	×	×	×	×	×	✓
Bakhtiari and Hosseinzadeh [30]	✓	✓	✓	✓	✓	×	×	×
Wang et al. [3]	✓	✓	✓	✓	✓	✓	×	✓
Wang and Song [7]	✓	✓	✓	✓	✓	×	✓	✓
Proposed scheme	✓	✓	✓	✓	✓	✓	✓	✓

5.3. Performance Evaluation

Less use of bilinear pairing in identity-based encryption schemes reduces computational overhead. Therefore, Table 3 shows the number of bilinear pairing functions used in the three phases of key generation, encryption, decryption in IBE schemes, and their comparison with the proposed method.

Table 3: Efficiency comparison

Schemes	Need to bilinear pairing		
	KGC	Encryption	Decryption
Boneh and Franklin [4]	×	✓	✓
Boneh and Franklin [22]	×	✓	✓
Sakai and Kasahara [23]	✓	×	✓
Boneh and Boyen [24]	✓	×	✓
Gentry [25]	✓	×	✓
Boneh and Boyen [26]	✓	×	✓
Bakhtiari and Hosseinzadeh [30]	×	✓	✓
Wang et al. [3]	×	✓	✓
Wang and Song [7]	✓	✓	✓
Proposed scheme	✓	×	✓

Then, the superior methods with the least use of bilinear pairings are compared with the proposed method in running time. We obtained the listed results by implementing the mentioned schemes using the JPBC library in the programming language of Java [37] and an environment with specifications stated in Table 4.

Table 4: System specifications for implementation

Platform	Specifications
Integrated development environment	Eclipse
The operating system	Ubuntu 16.04
CPU	Intel Core i7 3.5GHz
RAM	8GB

Figure 2 shows the running time of the setup and key generation phases of the considered methods in milliseconds. This type is known as type A in the JPBC library. This part of the system, which includes generating public parameters and the master key, is calculated only once in a cryptographic method. The pre-calculated parameters are used in the setup phase in the next times of the key generation, encryption, and decryption phases.

Figure 3 shows the encryption and decryption running time in identity-based encryption schemes. Some identity-based encryption methods also use the bilinear pairing function in the encryption phase. In this case, with each running of the encryption phase, there is a need to calculate bilinear pairing functions.

This increases the cost of an IBE system. For this reason, IBE methods that use bilinear pairing calculations only in the decryption phase significantly reduce the computational cost.

As shown in Figure 2, the proposed IBE has a similar running time in setup and key generation phases compared to the method of Boneh and Boyen [24]. Figure 3 also shows that the proposed method in the encryption phase has a 13-millisecond advantage over Boneh and Boyen [24]; But in the decryption phase, the method of Boneh and Boyen [24] has a 3-millisecond advantage over the proposed method.

In this way, in total, the running time of encryption and decryption of the proposed IBE has a shorter running time (about 10 milliseconds), which reduces the cost of the system.

In addition, the proposed IBE method, compared to the IBE method of Wang et al. [3], shows significant changes in reducing the running time of each of the three phases of key generation, encryption, and decryption. Figure 4 compares the running time of the proposed re-encryption proxy with the re-encryption proxy Wang et al. [3]. As the implementation results show, the proposed method reduces the cost of the re-encryption proxy scheme by reducing the computational overhead and improving the running time. In addition, the proposed scheme offers high flexibility and scalability due to the use of blockchain technology.

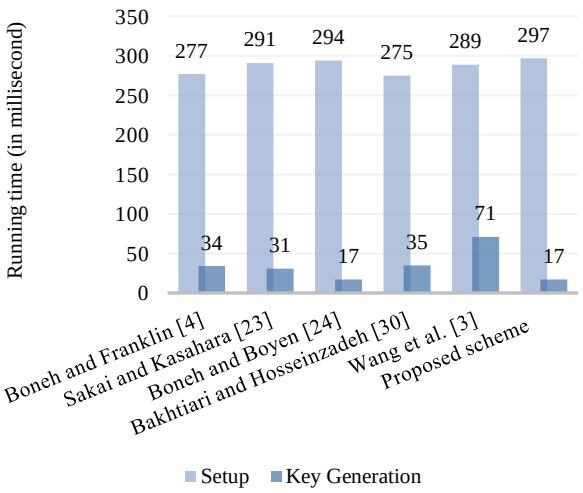

Figure 2. Compare of running times of setup and key generation phases

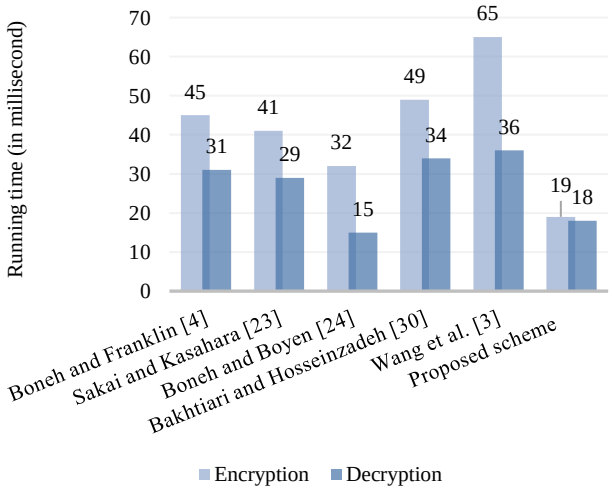

Figure 3. Compare of running times of encryption and decryption phases

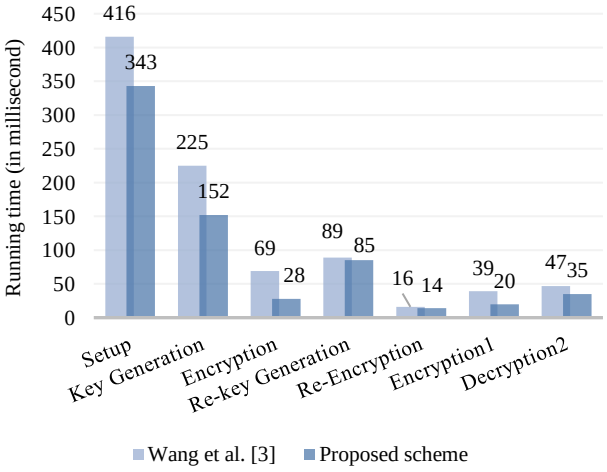

Figure 4. Compare of running times of the re-encryption proxy

6. Conclusion

In this paper, a secure and efficient cloud health system is proposed for sharing medical data between patients, hospitals, and other healthcare centers. The system includes a new identity-based encryption scheme with improvements in the re-encryption proxy. It can also be used in blockchain technology.

In the proposed method, the content of medical records is stored in the cloud servers, and their access address is located in the blockchain. This work has led to improved memory usage of blocks and more efficient medical data management during sharing. In addition, patients' medical records are encrypted and provided to the members of a blockchain network and the proxy in the cloud; No entity other than authorized users will be able to access the content of patients' medical information.

Also, in the proposed identity-based encryption scheme, bilinear pairing is used only in the decryption

phase, and the pairing parameter used in the encryption phase is a predetermined parameter. Another strength of the proposed approach is shortening the sending parameters while preserving system security.

The security analysis showed that the proposed scheme provides more security properties than similar schemes. In this regard, we also proved the security of the proposed IBE in the standard model. In addition, the implementation results showed that the proposed scheme has better running time and lower computational cost than previous similar schemes.

Acknowledgment

The authors sincerely thank this journal for giving chances to proposing the scheme.

References

[1] H. Toral-Cruz, D. He, A.D. Mihovska, K.K. Raymond Choo, and M.K. Khan, Reliable and Secure e-Health Networks. Wireless Personal Communications, (2021), 117, 1–6. https://doi.org/10.1007/s11277-021-08104-z.

[2] W. Hsin-Te, and T. Chun-Wei, Toward Blockchains for Health-Care Systems: Applying the Bilinear Pairing Technology to Ensure Privacy Protection and Accuracy in Data Sharing. IEEE Consumer Electronics Magazine, 7 (2018), 65-71. https://doi.org/10.1109/MCE.2018.2816306.

[3] X.A. Wang, J. Ma, F. Xhafa, M. Zhang, and X. Luo, Cost-Effective, Secure E-Health Cloud System Using Identity-Based Cryptographic Techniques. Future Generation Computer Systems, 67 (2017), 242–254. https://doi.org/10.1016/j.future.2016.08.008.

[4] D. Boneh, and M. Franklin, (2001, August). Identity-Based Encryption from the Weil Pairing. In Annual International Cryptology Conference (pp. 213–229). Springer, Berlin. https://doi.org/10.1007/3-540-44647-8_13.

[5] P. Patil, M. Sangeetha, and V. Bhaskar, Blockchain for IoT Access Control, Security and Privacy: A Review. Wireless Personal Communications, 117 (2021), 1815–1834. https://doi.org/10.1007/s11277-020-07947-2.

[6] P. Pandey and R. Litoriya, Securing E-health Networks from Counterfeit Medicine Penetration Using Blockchain. Wireless Personal Communications, 117 (2021), 7–25. https://doi.org/10.1007/s11277-020-07041-7.

[7] H. Wang and Y.J. Song, Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. Journal of Medical Systems, 42(8) (2018), 152:1–152:9. https://doi.org/10.1007/s10916-018-0994-6.

[8] V. Della Mea, What Is E-Health (2): The Death of Telemedicine? Journal of Medical Internet Research, 3(2) (2001). https://doi.org/10.2196/jmir.3.2.e22.

[9] O. Enaizan, A.A. Zaidan, N.H.M. Alwi, B.B. Zaidan, M.A. Alsalem, O.S. Albahri, and A.S. Albahri, Electronic Medical Record Systems: Decision Support Examination Framework for Individual, Security and Privacy Concerns Using Multi-Perspective Analysis. Health and Technology, 10 (2020), 795–822. https://doi.org/10.1007/s12553-018-0278-7.

[10] J. O'donoghue, and J. Herbert, Data Management within M-Health Environments: Patient Sensors, Mobile Devices, and Databases. Journal of Data and Information Quality, 4 (2012), 1–20. https://doi.org/10.1145/2378016.2378021.

[11] L. Neuhauser, and G.L. Kreps, Online Cancer Communication: Meeting the Literacy, Cultural and Linguistic Needs of Diverse Audiences. Patient Education and Counseling, 71 (2008), 365–377. https://doi.org/10.1016/j.pec.2008.02.015.

[12] L. Neuhauser, and G.L. Kreps, E-Health Communication and Behavior Change: Promise and Performance. Social Semiotics, 20 (2010), 9–27. https://doi.org/10.1080/10350330903438386.

[13] G.L. Kreps, Strategic Use of Communication to Market Cancer Prevention and Control to Vulnerable Populations. Health Marketing Quarterly, 25 (2008), 204–216. https://doi.org/10.1080/07359680802126327.

[14] J. Benaloh, M. Chase, E. Horvitz and K. Lauter, Patient-Controlled Encryption: Ensuring the Privacy of Electronic Medical Records. In Proceedings of the 2009 ACM Workshop on Cloud Computing Security 2009, 103–114. https://doi.org/10.1145/1655008.1655024.

[15] Y. Xue, X. Mao, Y. Guo, and S. Lv,The Research Advance of Facial Expression Recognition in Human-Computer Interaction. Journal of Image and Graphics, 5 (2009), 764–772.

[16] M. Barua, X. Liang, R. Lu and X. Shen, ESPAC: Enabling Security and Patient-Centric Access Control for E-Health in Cloud Computing, International Journal of Security and Networks, 6 (2011), 67–76. https://doi.org/10.1504/IJSN.2011.043666.

[17] L. Guo, C. Zhang, J. Sun and Y. Fang, Paas: A Privacy-Preserving Attribute-Based Authentication System for E-Health Networks. IEEE Transactions on Mobile Computing, 13 (2012), 1927-1941. https://doi.org/10.1109/ICDCS.2012.45.

[18] M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou, Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. IEEE Transactions on Parallel and Distributed Systems, 24 (2013), 131–143. https://doi.org/10.1109/TPDS.2012.97.

[19] H. Yan, J. Li, X. Li, G. Zhao, S.Y. Lee and J. Shen, Secure Access Control of E-Health System with Attribute-Based Encryption. Intelligent Automation & Soft Computing, 22 (2016), 345–352. https://doi.org/10.1080/10798587.2015.1132586.

[20] X. Boyen, A Tapestry of Identity-Based Encryption: Practical Frameworks Compared. International Journal of Applied Cryptography, 1 (2008), 3–21. https://doi.org/10.1504/IJAC T.2008.017047.

[21] A. Shamir, Identity-Based Cryptosystems and Signature Schemes. Lecture Notes in Computer Science, 84 (1984), 47–53. https://doi.org/10.1007/3-540-39568-7_5.

[22] D. Boneh and M. Franklin, Identity-Based Encryption from the Weil Pairing. SIAM Journal on Computing, 32(3) (2003), 586–615. https://doi.org/10.1137/S0097539701398521.

[23] R. Sakai and M. Kasahara, ID-Based Cryptosystems with Pairing on Elliptic Curve. IACR Cryptology ePrint Archive. 2003.

[24] D. Boneh and X. Boyen, Efficient Selective-ID Secure Identity-Based Encryption without Random Oracles. In International Conference on the Theory and Applications of Cryptographic Techniques, 2004, 223–238. https://doi.org/10.100 7/978-3-540-24676-3_14.

[25] C. Gentry, Practical Identity-Based Encryption without Random Oracles. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2006, 445–464. https://doi.org/10.1007/11761679_27.

[26] D. Boneh and X. Boyen, Efficient Selective Identity-Based Encryption without Random Oracles. Journal of Cryptology, 24 (2011), 659–693. https://doi.org/10.1007/s00145-010-9078-6.

[27] D. Galindo, Chosen-Ciphertext Secure Identity-Based Encryption from Computational Bilinear Diffie-Hellman. In International Conference on Pairing-Based Cryptography, 2010, 367–376. https://doi.org/10.1007/978-3-642-17455-1_23.

[28] J.H. Park, K. Lee and D.H. Lee, New Chosen-Ciphertext Secure Identity-Based Encryption with a Tight Security Reduction to the Bilinear Diffie-Hellman Problem. Information Sciences, 325 (2015), 256–270. https://doi.org/10.1016/j.in s.2015.07.011.

[29] W. Susilo, F. Guo and Y. Mu, Efficient Dynamic Threshold Identity-Based Encryption with Constant-Size Ciphertext. Theoretical Computer Science, 609 (2015), 49–59. https://doi.org/10.1016/j.tcs.2015.09.006.

[30] S. Bakhtiari-Chehelcheshmeh and M. Hosseinzadeh,A New Certificateless and Secure Authentication Scheme for Ad-Hoc Networks. Wireless Personal Communications, 94 (2017), 2833–2851. https://doi.org/10.1007/s11277-016-3721-y.

[31] M. Green and G. Ateniese, Identity-Based Proxy Re-Encryption. In International Conference on Applied Cryptography and Network Security, 2007, 288–306. https://doi.org/10.100 7/978-3-540-72738-5_19.

[32] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System,2012.

[33] N. Kshetri, Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy. Telecommunications Policy, 41 (2017), 1027-1038. https://doi.org/10.1016/j.telpol.2017.09.003.

[34] X. Yue, H. Wang, D. Jin, M. Li and W. Jiang, Healthcare Data Gateways: Found Healthcare Intelligence on the Blockchain with Novel Privacy Risk Control. Journal of Medical Systems, 40 (2016), 218. https://doi.org/10.1007/s10916-016-0574-6.

[35] M. Banerjee, J. Lee and K.K. Raymond Choo,A Blockchain Future for the Internet of Things Security: A Position Paper. Digital Communications and Networks, 4 (2018), 149-160. https://doi.org/10.1016/j.dcan.2017.10.006.

[36] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, Medrec: Using Blockchain for Medical Data Access and Permission Management. Open and Big Data (OBD), International Conference on IEEE, 2016, 25-30. https://doi.org/10.1109/OB D.2016.11.

[37] A. De Caro, V. Iovino and A. Renato, JPBC : Java Pairing Based Cryptography. IEEE Symposium on Computers and Communications, 2011, 850–855. https://doi.org/10.1109/IS CC.2011.5983948E.