Int. j. inf. tecnol. (January 2024) 16(1):121–130
https://doi.org/10.1007/s41870-023-01625-9

ORIGINAL RESEARCH

Hybrid blockchain based medical data sharing with the optimized CP-ABE for e-Health systems

Anil Kumar Mishra[1] · **Yogomaya Mohapatra**[2]

Received: 31 July 2023 / Accepted: 6 November 2023 / Published online: 9 December 2023

Abstract While e-Health systems must prioritise security and privacy, sharing medical data can help improve diagnostic accuracy. Because of its immutability, Blockchain (BC) is now being suggested as an exciting solution for sharing Personal Health Information (PHI). However, sharing PHI must improve patient privacy and security. As a result, this paper describes a secure medical data sharing system. Private BC, Consortium BC (CBC), and optimized cryptography are all included in the proposed system. To ensure patient privacy, PHI is encrypted using optimised ciphertext policy attribute based encryption (CP-ABE). In particular, replicated attributes amendment (RAA) is proposed to improve CP-ABE performance. For each replicated attribute, this RAA achieves a single share value. PHI ciphertexts are stored as blocks in the hospital's private BC. Furthermore, the PHI keyword is saved to the CBC. By validating the keyword and getting access to the private BC, the doctor may retrieve all patient's PHI. The article's findings show that the proposed system achieves lower storage overhead, encryption time, and decryption time.

Keywords e-Health system · Blockchain (BC) · CBC · Replicated attributes amendment

✉ Anil Kumar Mishra
aanil1mishra@gmail.com

Yogomaya Mohapatra
yogomaya.mohapatra@cgu-odisha.ac.in

[1] School of Computer Science and Engineering, Trident Academy of Technology, Bhubaneswar, Odisha, India

[2] Department of Computer Science and Engineering, C.V. Raman Global University, Bhubaneswar, Odisha, India

1 Introduction

In the name of e-health, medical services are delivered using digital technologies. The focus of e-Health research is on how to track and assess patients using computerized health information. A patient's healthcare team may consist of internists, experts, and general healthcare doctors [1–3]. Since data security and privacy are important considerations, the research community is now paying more focus to the sharing of medical records. By increasing the power and capability of healthcare organizations to exchange data and collaborate on treatment plans, e-Health raises the standard of medical care.

An electronic health record, or EHR, is a gathering of all of a patient's medical data accumulated over their lifetime. EHRs provide for the use of health information and physical care services inside the health sector with proper organisation and standards while preserving privacy standards [4, 5]. Effective nursing management, healthcare cooperation, and improved patient health and treatment all depend on the electronic sharing of medical records that is safe and secure. By providing accurate health information, rapid and safe data exchange eliminates planning mistakes in patient care, enabling medical experts to improve the treatment method and recognize patients' requirements to provide the optimal therapy [6–8]. Medical record could readily erase, changed, or even seized. During such situations, it's possible that medical information won't be adequately documented or preserved, delaying the healing process or possibly endangering the life and security of a patient.

BC has recently been proposed because it is an effective solution to the traditional privacy issues in e-Health systems since it can hold an expanding number of information in a shared and consistent fashion [9]. A patient could consult several healthcare entities in an e-Health system, every one of which has its very own record. It is predicted that a PHI sharing system built on BC technique will offer safe medical record transmission [10–14]. However, patient privacy and the security of medical data sharing must be improved further. In order to achieve these objectives, in this work, the contributions listed below are given.

- Each patient's PHI in a hospital is first encrypted using an optimized CP-ABE method. To enhance the performance of CP-ABE, RAA is presented. Using this RAA, optimized single share value of each replicated attribute is attained.
- Although the CBC maintains track of the safe indices of the PHI, the encrypted PHI would be kept in confidential BC.
- The ability to view a patient's health history is restricted to licensed physicians, thus precludes subsequent retrieval of information.

Below is an overview of the entire text in the article: Sect. 2 discusses current studies on secure medical data exchange. Hybrid BC Based Medical Data Sharing with the Optimized CP-ABE for E-Health Systems is proposed in Sect. 3. Section 4 analyzes the suggested scheme's efficiency. Section 5 of the paper describes the research's outcome.

2 Related works

This section reviews latest literatures that present safe medical related data sharing. Several researchers have offered numerous methods to increase privacy when sharing health information. By way of illustration, Fulong Chen et al. [15] offered BC-based Medical Cyber Physical Systems to show how the authentication method must adhere to security standards. This method used intractable problems and bilinear mapping to solve the security threat in the authentication process. The proposed scheme avoided the issue of third-party credibility. Moreover, 2-way authentication between the hospital and the BC node got accomplished. The authors achieved optimised computing and storage overhead by presenting the proposed scheme.

Secured sharing using the Tree Parity Machine, often known as TPM, was introduced by Arindam and Moumita Sarkar [16] to overcome the drawbacks of existing secret sharing techniques. The proposed technique generated the shares based on the outcome of a simple mask. The authors introduced the concept of privileged share in their approach. The patients were considered to have a particular right to provide the original data for the notion. Without special access, they were unable to put the real data back together. Furthermore, they were successfully completed secret sharing in response to the Man-In-The-Middle-Attack. In addition, to gain similar inputs and exchange outputs, 2 neural networks were used.The authors improved those framework's reliability and efficiency as a result of the performance of the proposed scheme.

Pournaghi et al. [17] sought out to manage medical information usage and solve the memory issue. The authors introduced MedSBA, and unique attribute-based encryption utilizing BC technique, to achieve their objective. They had securely recorded and stored medical data by proposing this scheme. Furthermore, user privacy was protected, and The General Data Protection Regulation makes patient data accessible for precise access management. The use of private BC in MedSBA improved access revocation. The article's proposed scheme reduced both computational complexity and storage overload.

In order to increase data security, M. Lilly Florence and Dhina Suresh [18] introduced a novel access control architecture termed encryption depending on user actions. Using a time frame, usage was mapped as a credential to each private attribute. Data users could only decrypt a hardened attribute if the credentials associated with the attribute matched. The feature extraction strategy and searchable encryption technique allowed for reliable routing of ciphertext characteristics. The privacy of important records been improved through multi credential routing. Furthermore, to safeguard the privacy of the data user, the authors developed a trustworthy overlay privacy-preserving protocol. The authors had achieved a reasonable communication overhead as a result of the proposed scheme.

In a closed system, each affirms its own database. This approach weakens data security and diminishes the success of healthcare delivery. As a result, Chen et al. [19] employed the method of BC. By proposing this idea, the authors demonstrated how to create a completely secure environment that is resistant to single-point assaults. Furthermore, they introduced BC-based medical information sharing in order to integrate each hospital's resources. In contrast to existing BC methods, their suggested BC technique categorised and managed individual requests to provide medical data. They classified distributing between hospitals into two categories: they are equal stage sharing, different stage sharing. The authors improved the system's security as a result of the proposed scheme.

Data retrieval in an e-Health framework based on BC is inefficient due to the basic structure of BC. Though BC offers great throughput and scalability, it could be open to rollback attacks and open a door to confidentiality leaking. For these concerns, Lv et al. [20] proposed a new e-Health system encompassing medical data sharing using BC while also maintaining safety. For rapid access, patient's electronic medical records were kept in conventional keys and microblocks. The authors proposed a proxy re-encryption method to achieve privacy preservation. The suggested scheme gained higher throughput while having a low storage overhead.

Health 4.0 and medical cyber-physical systems (MCPS) has recently been the target of cyberattacks that have put data security and end-user privacy at risk. Instead of being built for system function, conventional cryptographic algorithms were created for data protection. Data security and privacy are affected when such cryptographic methods move data security to key security. As a result, Qiu et al. [21] introduced a sharing strategy and safe data storage. This method uses a mix of dispersion, selective encryption, and then fragmentation. Although transmission media and keys were affected, the suggested methodology protected data privacy and security. The authors improved the framework's security as a result of the proposed scheme.

3 Hybrid blockchain based medical data sharing with the optimized CP-ABE for e-Health systems

3.1 Overview

With this method, the PHI of every hospital patient is digitized and kept on the hospital database. The doctor retrieves the PHI keyword and sends it to the server together with the PHI. PHI of each patient is encrypted using optimised CP-ABE to enhance patient privacy. To be specific, RAA is presented to improve the performance of CP-ABE. This RAA achieves a single share value for each replicated attribute. The PHI keyword is then stored as in CBC along with the encrypted PHI record as a block in the appropriate private BC by the server. The doctors are able to get a patient's PHI from the CBC by looking up that patient's PHI in the data generator's ID. They obtain the ciphertext of the patient's PHI by accessing the private BC. The optimised CP-ABE is then used to decrypt the PHI ciphertext.

3.2 System model

Figure 1 depicts the proposed medical data sharing system model. Three main entities are included in the model, as seen in the figure: patients, hospitals, and the system manager.

System manager (SM): It is in charge of the overall framework. This SM is where all patients and doctors register their information. For CBC, it also creates a consensus vector (a).

Medical service providers (MSPs): This represents hospitals as well. Each hospital includes a variety of computer servers and clients, as seen in Fig. 1. With the computer client, the doctor keeps a PHI record for each patient. Such clients then produce blocks for patient records containing PHI and transfer it towards the hospital's private BC. Then this server records the registrations of physicians and patients. Moreover, it verifies physicians who practice outside of the private BC before granting them entry to a patient's PHI there. Also, it tests fresh blocks for CBC.

Patients: The Patients seeking services in hospitals. Before patients can see a doctor, they must first register with the hospital server. Following registration, from the server, every patient gets a token. The token must be kept absolutely confidential until the patient reports to the hospital and then must be shown to the doctor. Beacons act as proof of the doctor relationship and allow the doctor to make PHI decisions on behalf of the patient. After then, the PHI would be kept in the hospital's secure BC. Furthermore, the CBC receives block keywords from hospitals in private BC.

3.3 Encryption using optimized CP-ABE

The doctor uses computer clients to record the patient's PHI after their hospital visit. Some visitors submit the data to the hospital's private BC in a block. The PHI is encrypted with the optimised CP-ABE to protect the patient's privacy. Specifically, RAA-based CP-ABE is presented for encryption. The PHI of the patient is encrypted using RAA-CP-ABE in this method, and RAA is utilized to optimize CP-ABE by getting a single share value for each replicated attribute. Figure 2 illustrates the basis operations of the proposed CP-ABE. The following describes how encryption works:

Preliminary: For prime order p, take two multiplicative cyclic groups G_0 and G_1. Therefore e is a bilinear map and g is a generator of G_0, i.e., $e : G_0 \times G_0 \rightarrow G_1$. The following is a description of the important characteristics of a bilinear map:

Bilinearity: $e\left(x^a, y^b\right) = e(x, y)^{ab}, \quad x, y \in G_0 \quad and \ a, b \in Z_p$.

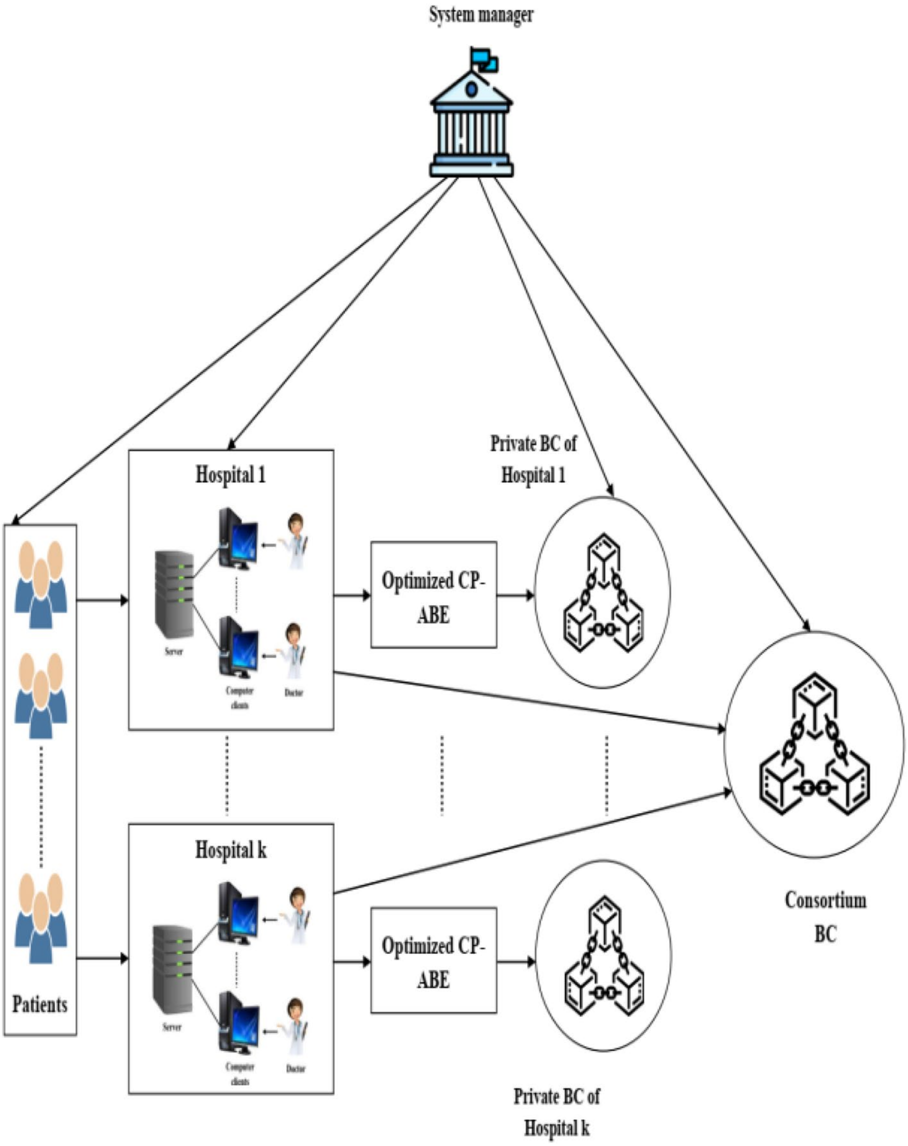
1. Non-degeneracy: $e(g,\ g) \neq 1$
2. Ability for computation: $e\left(g_1,\ g_2\right)$ is able to compute for all $g_1,\ g_2 \in G_0$

Access policy structure: The collection of user's attributes is denoted by $\left\{U_1, \ldots.., U_n\right\}$.A collection $C \subseteq 2^{\left\{U_1,\ldots,U_n\right\}}$ is called as monotonous, for $\forall X,\ Y$, if $X \in C$ and $X \subseteq Y$, there is $Y \in C$. The subset of collection C is referred to as an access structure. When C is present, the collection is referred to as the set of authorization, and when C is absent, the collection is referred to as the set of unauthorized. This work transforms the structure of access into a Boolean function.

3.4 The proposed CP-ABE's fundamental operations

Four procedures are included in the planned CP-APE: setup, key generation, encryption, decryption, and delegation. These operations are based on the following principles:

Fig. 1 The proposed medical data sharing system model



Setup $(G, \vartheta) \rightarrow (PK, MSK)$: This algorithm's setup is carried out by the AA. AA is the key centre from which SK and PK emerge. Both PK and SK are given to the doctors and MSP, respectively. It grants different levels of access to doctors based on their attributes. The global attribute G and the security parameter ϑ are treated as input parameters in this configuration. The output parameters PK and master SK (MSK) can be obtained by using these input parameters.

KeyGen $(PK, MSK, A) \rightarrow SK$**:** The SK, or private key, is produced by the AA. For SK generation, the following variables are used: PK, MSK, and doctor attribute set A. The doctor's SK may be established once the key generation method has been executed.

Encrypt$(PK, F, \rho) \rightarrow CT$: The MSP applies the encryption algorithm to the data that will be stored in private BC as a block. The encryption algorithm is executed by using input parameters like data F, PK,and access policy ρ. Finally, MSP receives encrypted data or cipher text (CT).

Decrypt $(CT, SK) \rightarrow F$: The decryption algorithm is run by the doctor. During this stage, the doctor uses SK to decrypt the CT. To decrypt the search data F, the doctor's attribute set A must first match the defined access policy ρ. Otherwise, the decryption algorithm will be decommissioned.

Delegate$\left(SK, A'\right) \rightarrow SK'$: For the collection of attributes A, SK stands for secret key or private key. If the subset of attribute A′ satisfied $A' \subseteq A$, delegate function generates the secret key SK′. This function is used to make AA longer.

In conventional CP-ABE methods, data access is contingent on the sense of accomplishment of every attribute set A in the policy. As a result, many users with different sets of attributes and then satisfying various A_i in policies

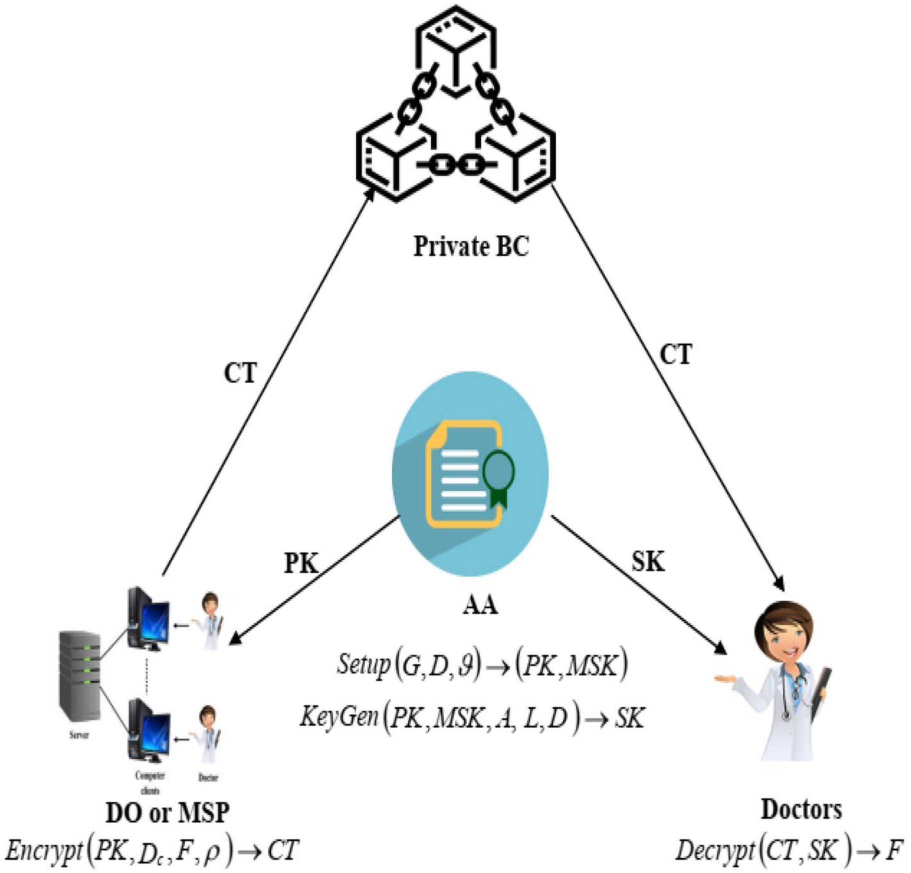

Private BC
CT
CT
PK
SK
AA
$Setup(G,D,\vartheta)\rightarrow(PK,MSK)$
$KeyGen(PK,MSK,A,L,D)\rightarrow SK$
Server
Computer clients
Doctor
DO or MSP
$Encrypt(PK,D_c,F,\rho)\rightarrow CT$
Doctors
$Decrypt(CT,SK)\rightarrow F$

Fig. 2 The proposed CP-ABE's fundamental operations

will possess permit to the similar data, as a single secret s is distributed to all the different A_i in policies.

RAA: RAA automatically re-randomizes a few share values in order to optimize the evaluated attribute shares using the secret reconstruction feature $\sum \vartheta_x c_x \in A_i = s$, here, s defines the shared secret, ϑ_x defines the valid secret shares and c_x is the constant parameter. This characteristic is utilized in optimization because the user's satisfaction of every attribute set Ai of a policy leads in the reconstruction of an identical secret s and provisional entry to an identical collection of data. The repeated characteristics by altering a few share values from various attribute sets of the policy, while keeping the secret s constant for all Ai, certain share values from distinct attribute sets are optimized, and after tuning, they join to reassemble the secret s. The goal of optimization is to minimize the communication and computation costs for an irreducible policy between both replicated and non-replicated characteristics in a certain attribute set.

In this RAA algorithm, the following parameters are taken as input during the encryption of CP-ABE.

- LSSS (Linear secret share scheme) matrix M which is the conversion of access policy. For a set of parties U, a SSS is linear if a vector over Z_p is built by incorporating shares from all U. Furthermore, there is a share accumulating matrix M with *m* rows and *n* columns,in which the xth row in matrix M relates to party U(x).
- γ denotes the map of rows of M to the attributes.
- γ' denotes the non-replicated distinct attributes list from γ.
- The value of secret share ϑ_x is computed as $\vartheta_x = M_x \cdot v$, here, v denotes the column vector with the length n and has s as its initial entry and M_x denotes the x^{th} row of M.
- Calculate $z_x = M_x \cdot z$, here, z denotes the random vector and secret s' = 0 for its initial entry.
- The amount of attribute sets A_i in policy.

The process of RAA based CP-ABE algorithm is explained as follows:

1. The relation (1) computes the coefficients c_x relative to attributes $\gamma(x)$ corresponding to all attribute sets A_i in policy.

$$\sum_x M_x \cdot c_x = (1,\ 0, ..., 0) \tag{1}$$

2. For all different non-replicated attributes from γ ′, the counter variable $(C_{\gamma'(t)})$ is assumed to zero. The instances

of all attributes given in attribute sets $C_{\gamma'(t)}$ are measured by raising the $\gamma(x) \in A_i$ variables starting with the first attribute set and continuing through all of them. This is used to keep track of traits that recur across many $\mathrm{A_i}$.

3. Variable S_i is assumed to 0 for each policy attribute set A_i and is increased with $C_{\gamma'(t)}$ for $\gamma(x) \in A_i$ and $\gamma(x) == \gamma'(t)$ achieves the Eq. 2:

$$S_i = \left(\sum_{\gamma(x)\in A_i} C_{\gamma'(t)} \quad if\ \gamma(x) == \gamma'(t) \right) \tag{2}$$

4. To enhance process of optimization, RAA chooses the $A_{l\max}$ which denotes the largest value of S_i or larger repetition count. After assessing $A_{l\max}$, it is necessary to convert its actual attributes shares ϑ_x, z_x values to optimised values $\vartheta_{x-optimized}$, $z_{x-optimized}$, and added to array K. Then the optimized-shares values replace the actual ϑ_x in all other attribute sets $\mathrm{A_i}$ that contain these replicated attributes.
5. The following relations (3) and (4) are used to optimise all other-shares attributes $\vartheta_{x-other}$, $z_{x-other}$ in another distinct $\mathrm{A_i}$ (not for $\mathrm{A_{lmax}}$):

$$\vartheta_{x-other} = \left(s - \sum_{x\in A_i, K} \vartheta_x c_x \right)\left(\frac{1}{c_{x-other}} \right) \tag{3}$$

$$\vartheta_{x-other} = \left(s - \sum_{x\in A_i, K} z_x c_x \right)\left(\frac{1}{c_{x-other}} \right) \tag{4}$$

Array K is appended with each new $\vartheta_{x-optimized}$, $z_{x-optimized}$. When all attribute shares have been optimised, the optimization process is completed.

6. All of the optimised values in $\gamma'(t)$ that correspond to attribute names are given to ϑ_t and z_t.

Following that, it calculates the CT (for optimised new shares ϑ_t, z_t) as defined in Eq. (5)

$$CT = \left\{ C_0 = F \cdot e(g,g)^s,\ C_{1,t} = e(g,g)^{\vartheta_t} \cdot e(g,g)^{\alpha_{\gamma'(1)} z_t},\ C_{2,t} = g^{r z_t} \quad for\, i = \{1, 2, ..., n'\} \right\} \tag{5}$$

Here, r denotes the random value chosen by each AA and α denotes the random value chosen by the AA for each attribute.

This CT is forwarded to the private BC along with (M, γ, γ'), where M, γ refers to the LSSS matrix denoting the actual policy together with replicated attributes and γ' refers to optimised non-replicated attributes used for CT calculation. Conventional CP-ABE schemes map M,γ and CT to each other; however, because we have removed the replicated attribute occurrences in CT while still imposing an irreducible policy, here A is mapped to γ, and γ' is mapped to CT.

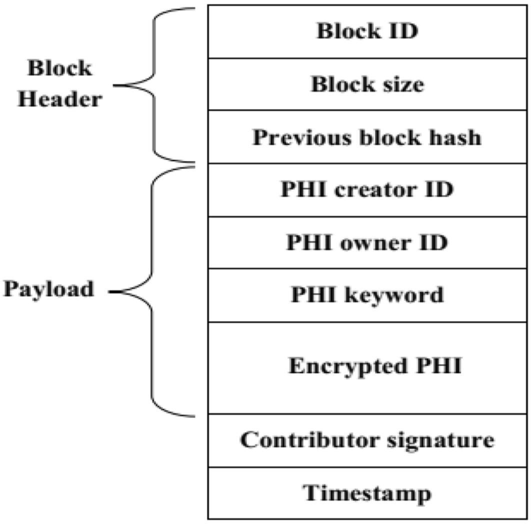


Fig. 3 A hospital's private BC block structure

3.5 Sharing encrypted PHI Using Private BC and CBC

The MSPs forward the CTs of PHI to the private BC as a block. These MSPs also send the keywords associated with the PHI blocks to the CBC. The following describes the operations of private BC and CBC:

Figure 3 depicts the structure of block of a hospital's private BC. The block header, payload, contributor signature, and timestamp are all part of this block structure. The block header contains the block ID, block size, and the previous block's hash. The payload contains the ID of the PHI creator or doctor, the ID of the PHI owner or patient, the PHI keyword, and the encrypted PHI hash. The contributor signature is employed to identify the block's creator. The timestamp indicates the time when the block was created. The consensus mechanism (CM) is used in private BC to ascertain the validation of new blocks. Proof of conformance is regarded as the CM in this approach for both private BC and CBC. The block's validation is determined using the proof of conformance. After registering with the hospital, a secure token can be created for the user to use as a CM. When the user visits the doctor, he or she displays the token to the doctor. The doctor can then generate a user ID by using a secure token. Other clients verify to determine whether the doctor is permitted to generate patient data when they receive a new transaction created by this client. If a new transaction

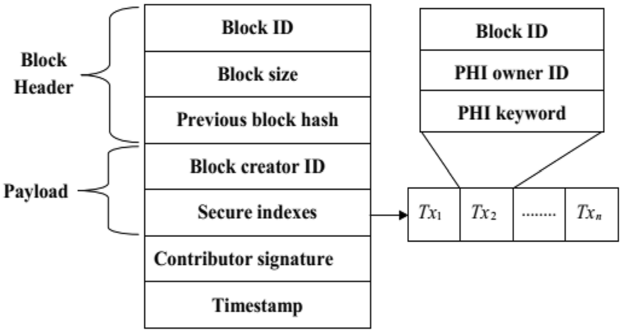


Fig. 4 The block structure of CBC

is approved by more than two or three clients, it is accepted as a new approval block in the private BC.

Figure 4 depicts the CBC block structure. CBC, like private BC, has a block header, a payload, a contributor signature, and a timestamp. The payload in this block contains the block creator ID and secures indexes. A secure index is made up of n transactions, denoted as $Tx_1, Tx_2, ..., Tx_{1n}$, here $n \geq 1$. Furthermore, each transaction contains a secure index for a patient's PHI, which includes the block ID, the ID of the PHI owner, and the PHI keyword. Because the CBC allows users to conduct keyword searches, the keywords stored in the BC must be consistent. Because keywords define a patient's symptoms or diagnosis, they correspond to standard medical descriptions in the system. Keywords are typically bound to a predetermined list so that users can search for them on the BC. The CM verifies the keywords chosen from the predetermined list denoted as Ω.

The doctor solves $Tx_i = \left(ID_C, ID_O, C_i(PHI)\right)$ to recover the patient's PHI associated with the keyword k'. Here, ID_C represents the PHI creator's ID, ID_O represents the PHI owner, and $C_i(PHI)$ represents the PHI CTs. By validating the ID_C, the doctor gains access to the hospital's private BC and obtains the CTs. The doctor then decrypts the CT in order to obtain the patient's PHI.

3.6 Decryption phase of optimized CP-ABE

Because the doctors know the contributor's signature, they rehash the blocks from the server. They get the CT (PHI) from the blocks. Then the CT is decrypt using the proposed CP-ABE algorithm. Namely, at first, the doctor evaluates which of his attributes achieve the policy, as well as the index of CT components that correspond to those attributes.

The RAA check algorithm considers the following attributes as input those are M, γ, γ', A_i in policy and decryption doctor attribute set U_{att}.

Table 1 Comparison with previous literature

References	Methods	Encryption time (ms)	Decryption time (ms)
[16]	Tree Parity Machine (TPM)	123	129
[17]	MedSBA	15.8	89
[18]	ABE with keyword search	98	110
Our	CP-ABE with RAA	15	81

If any policy attribute set A_i is a subset of doctor attribute set U_{att}, then the user attributes qualifying the policy must be those of that specific A_i; otherwise, the policy is not satisfied, and the doctor is not authorised to access data.

Calculate and return the coefficients c_x from the relation $\sum_x M_x \cdot c_x = (1, 0, ..., 0)$ for doctor attributes U'_{att} that satisfy the policy.

In order to satisfy policy, it will first look for the condition $\gamma(x) == \gamma'(t)$, and then the associated value of t in $\gamma'(t)$ will expose the position of each attribute in CT.

The doctor will then combine his attribute keys $K_{\gamma'(t),GID} = H(GID)^{1/r} \cdot g^{\alpha_{\gamma'(t)}/r}$ with CT to decrypt as defined in Eq. (6).

$$\prod_t \left(\frac{C_{1,t}}{e\left(K_{\gamma'(t),GID}, C_{2,t}\right)} \right)^{c_x} = \prod_t \left(\frac{e(g, g)^{\vartheta_t}}{e(H(GID), g)^{z_t}} \right)^{c_x} = e(g, g)^s \tag{6}$$

After determining $e(g, g)^s$, the algorithm divides this by the value of C_0 to get F or PHI of a patient.

4 Results and discussion

The suggested method's simulation is implemented in Python. The proposed approach is used on an EHR dataset from the Kaggle data repository (https://www.kaggle.com/datasets/saurabhshahane/patient-treatment-classification). The dataset was obtained from a private hospital in Indonesia using EHR Predicting. It includes the patient's laboratory test results, which are used to establish the patient's next course of therapy, whether they are in- or out-patients. The performance of the proposed approach is evaluated in terms of attack level, security level, encryption time, decryption time, key generation time, memory usage on encryption and decryption. Besides, the execution of the proposed RAA-CP-ABE is compared with that of the existing CP-ABE, Rivest-Shamir-Adleman (RSA), Diffie Hellman and ElGamal. Table 1 illustrates the overall performance of medical data sharing with different cryptography algorithms Fig. 5 illustrates the comparison of attack level and security level of different cryptography algorithms. As illustrated in the figure, security level of CP-ABE is attained to 94.82% than RSA,

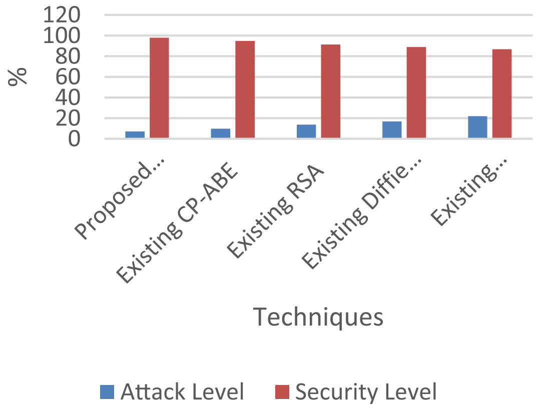


Fig. 5 The comparison of attack level and security level of different cryptography algorithms

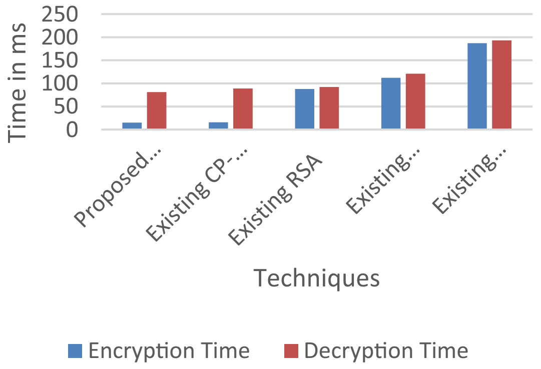


Fig. 6 The comparison of encryption time and decryption time of different cryptography algorithms

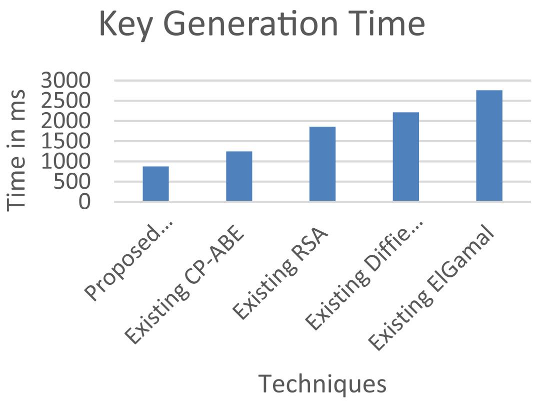


Fig. 7 The comparison of key generation time of different cryptography algorithms

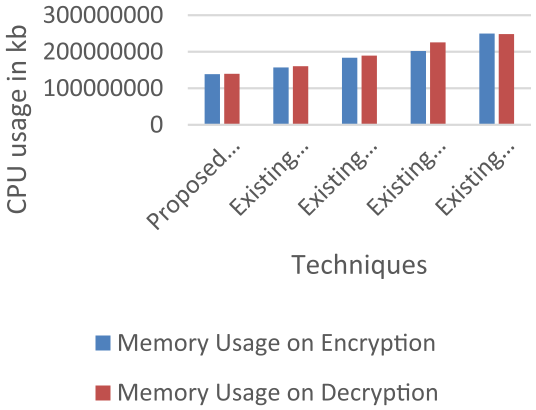


Fig. 8 The comparison of memory usage of different cryptography algorithms on encryption and decryption

Diffie Hellman and ElGamal. Nevertheless, the proposed RAA-CP-ABE security level is achieved to 97.85%. Namely, compared to existing CP-ABE, security level of RAA-CP-ABE is increased by 3.2% as the attributes of CP-ABE are optimized using RAA. As the CP-ABE allows the users to access the data in terms of attributes, attack level can be reduced. Besides, due to the optimization of CP-ABE using RAA, attack level of RAA-CP-ABE is reduced to 27%, 48%, 57% and 67% than that of CP-ABE, RSA, Diffie Hellman and ElGamal respectively.

The comparison of encryption time and decryption time of different cryptography algorithms is depicted in Fig. 6. Compared to CP-ABE, RSA, Diffie Hellman and ElGamal, encryption time of RAA-CP-ABE is decreased to 37%, 56%, 66% and 78% respectively. Likewise, as illustrated in the figure, decryption time of the RAA-CP-ABE is decreased to 40%, 57%, 67% and 98% than that of CP-ABE, RSA, Diffie Hellman and ElGamal respectively.

Figure 7 illustrates the comparison of key generation time of different cryptography algorithms. Compared to RSA, Diffie Hellman and ElGamal, key generation time of existing CP-ABE is decreased to 33%, 43% and 55% respectively. As the optimization of replicated attributes using RAA, key generation time of CP-ABE can be reduced further. Namely, compared to existing CP-ABE, key generation time of RAA-CP-ABE is decreased to 30%.

The comparison of memory usage of different cryptography algorithms on encryption and decryption is illustrated in Fig. 8. As depicted in the figure, memory usage of RAA-CP-ABE on encryption is decreased to 12%, 24%, 31% and 44% than that of existing CP-ABE, RSA, Diffie Hellman and ElGamal respectively. Besides, compared to CP-ABE, RSA, Diffie Hellman and ElGamal, memory usage of RAA-CP-ABE on decryption is decreased to 13%, 26%, 38% and 43% respectively.

4.1 Comparison with previous literature

Table 1 illustrates the comparison of the proposed scheme with the previous literature. As depicted in the figure, the methods are compared in terms of encryption time and decryption time. Compared to [20] and [11], the proposed method in [21] achieves better encryption time and decryption time. Namely, [21] obtained encryption time of 15.8 ms and decryption time 89 ms. However, our proposed scheme achieves better performance than [21]. The proposed scheme obtains encryption time of 15 ms and decryption time of 81 ms.

5 Conclusion

This paper presents a hybrid BC based e-Health system to improve the security and privacy of each patient's PHI during the medical sharing process. In this system, the PHI of each hospital patient is encrypted using the RAA-CP-ABE algorithm. The hospital server saved the CTs of the PHI and the AES key as a block to the private BC and the keyword of the relating PHI to the CBC. By checking the ID of the data generator, the doctors were able to recover the PHI of a patient associated with the keyword from the CBC. They obtained the CT of the patient's PHI by accessing the private BC. They then used the optimised CP-ABE to decrypt the PHI's CT. The proposed RAA-CP-ABE with BC-based e-Health system reduced encryption and decryption times by 78% and 98%, respectively. In future, we focus to improve data confidentiality by presenting efficient attack detection.

Author contributions All authors read and approved the final manuscript.

Funding The authors declare that they have competing interests and funding.

Availability of data and material Data sharing is not applicable to this article because of proprietary nature.

Code availability Code sharing is not applicable to this article because of proprietary nature.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Schiza E, Kyprianou T, Petkov N, Schizas C (2019) Proposal for an eHealth based ecosystem serving national healthcare. IEEE J Biomed Health Inform 23(3):1346–1357
2. Firouzi F, Farahani B, Ibrahim M, Chakrabarty K (2018) Keynote Paper: from EDA to IoT e-Health: promises, challenges, and solutions. IEEE Trans Comput Aided Des Integr Circuits Syst 37(12):2965–2978
3. Lin X, Lu R, Shen X, Nemoto Y, Kato N (2009) Sage: a strong privacy-preserving scheme against global eavesdropping for e-Health systems. IEEE J Select Areas Commun 27(4):365–378
4. Tsang G, Zhou S, Xie X (2021) Modeling large sparse data for feature selection: hospital admission predictions of the dementia patients using primary care electronic health records. IEEE J Transl Eng Health Med 9:1–13
5. Shickel B, Tighe P, Bihorac A, Rashidi P (2018) Deep EHR: a survey of recent advances in deep learning techniques for electronic health record (EHR) analysis. IEEE J Biomed Health Inform 22(5):1589–1604
6. Xia Q, Sifah E, Asamoah K, Gao J, Du X, Guizani M (2017) MeDShare: trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 5:14757–14767
7. Kassem J, De Laat C, Taal A, Grosso P (2020) The EPI framework: a dynamic data sharing framework for healthcare use cases. IEEE Access 8:179909–179920
8. Ma H, Zhang R, Yang G, Song Z, He K, Xiao Y (2020) Efficient fine-grained data sharing mechanism for electronic medical record systems with mobile devices. IEEE Trans Depend Secure Comput 17(5):1026–1038
9. Hyla T, Pejaś J (2019) eHealth integrity model based on permissioned blockchain. Future Internet 11(3):76
10. Zhang X, Poslad S, Ma Z (2018) Block-based access control for blockchain-based electronic medical records (EMRs) query in e-Health. In: 2018 IEEE Global Communications Conference (GLOBECOM), pp 1–7. IEEE
11. Khanday AMUD, Rabani ST, Khan QR, Rouf N, Din MMU (2020) Machine learning based approaches for detecting COVID-19 using clinical text data. Int J Inform Technol 12:731–739
12. Manoj-Kumar T, Karthigaikumar P (2020) A novel method of improvement in advanced encryption standard algorithm with dynamic shift rows, sub byte and mixcolumn operations for the secure communication. Int J Inform Technol 12:825–830
13. Anjana, Singh A (2019) Security concerns and countermeasures in cloud computing: a qualitative analysis. Int J Inform Technol 11:683–690
14. Shaikh TA, Ali R (2019) Big data for better Indian healthcare. Int J Inform Technol 11:735–741
15. Cheng X, Chen F, Xie D, Sun H, Huang C (2020) Design of a secure medical data sharing scheme based on blockchain. J Med Syst 44(2):52
16. Sarkar A, Sarkar M (2021) Tree parity machine guided patients' privileged based secure sharing of electronic medical record: cybersecurity for telehealth during COVID-19. Multimed Tools Appl 80(14):21899–21923
17. Pournaghi S, Bayat M, Farjami Y (2020) MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption. J Ambient Intell Humaniz Comput 11(11):4613–4641
18. Florence M, Suresh D (2017) Enhanced secure sharing of PHR's in cloud using user usage based attribute based encryption and signature with keyword search. Clust Comput 22(6):13119–13130
19. Chen C, Deng X, Kumar S, Kumari S, Islam S (2021) Blockchain-based medical data sharing schedule guaranteeing security of individual entities. J Ambient Intell Humaniz Comput. https://doi.org/10.1007/s12652-021-03448-7
20. Zou R, Lv X, Zhao J (2021) SPChain: Blockchain-based medical data sharing and privacy-preserving e-Health system. Inf Process Manag 58(4):102604

21. Qiu H, Qiu M, Liu M, Memmi G (2020) Secure health data sharing for medical cyber-physical systems for the healthcare 4.0. IEEE J Biomed Health Inform 24(9):2499–2505
22. Patel K (2019) Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files. Int J Inf Technol 11:813–819