Journal of Medical Systems (2020) 44:97
https://doi.org/10.1007/s10916-020-01564-z

MOBILE & WIRELESS HEALTH

Efficient and Secure Attribute Based Access Control Architecture for Smart Healthcare

Saurabh Rana[1] · Dheerendra Mishra[1]

Received: 27 December 2019 / Accepted: 17 March 2020

Abstract

The smart health medical system is expected to enhance the quality of health care services significantly. These system keeps patients related record and provides the services over the insecure public channel which may cause data security and privacy concerns in a smart health system. On the other hand, ciphertext attribute-based encryption(CP-ABE) provides possible encrypted data security. There are some security flaws in CP-ABE, where the existing access policies are in the cleartext form for accessing encrypted sensitive data. On the other hand, it supports the small attribute universe, which restricts the practical deployments of CP-ABE. Moreover, outsider adversary observed the communication, which also creates a serious threat to CP-ABE model. To overcome security and privacy risk, efficient access control have been designed and devolved for medical services. Although we also demonstrate the security analysis of Zhang et al.'s scheme, which is vulnerable to inefficient security proof and man in the middle attack. In the proposed scheme, we proposed an efficient and security preserve scheme to overcome the weaknesses of Zhang's et al.'s system. The protocol satisfies the attribute values of the medical user with hidden access policies. It has been proved under the standard model, which ensure the security of the protocol. Moreover, performance analysis comparison shows that the proposed scheme is more efficient than the existing one.

Keywords Smart healthcare · Ciphertext attribute-based encryption · Medical data storage · Security · Privacy

Introduction

Nowadays, people continuously involve in the currently growing smart health technology and people expect to obtain more comprehensive health care. The medical data storing in the cloud has become the most significant trend in the modern medical system, which evoked the new challenges and opportunity for smart health users. However, the smart health system facilitates both the communication and data access authority in a very convenient way. Some sensitive kinds of medical data such as patient's private health records, hospital expertise, doctors related information could be valuable for relevant authority. Therefore, it should be fully trusted that can have the access policy over the cloud server. There are several existing solutions for secure access to the cloud storage system, attribute-based access control. In the smart health access control, we obtain the facility to access the health record from medical repository desk. The traditional ciphertext attribute-based encryption (CP-ABE) scheme has directly adapted to expressiveness access control on sensitive medical data. Thus, CP-ABE will incompatible for a smart health system until the access policy does not satisfy the set of attributes of the respective user.

In the smart medical services, each patient has identified by a collection of his attributes and corresponding trusted authority issue the secret key according to attributes. Then, CP-ABE gives the right to the data owner for choosing his access policy and outsourced the encrypted data to the cloud server. If any user wishes to access the data, it should fulfil predefined access policy. This mechanism restricts unauthorised access to outsourced data from a cloud server. Since attribute could be managed by single authority CP-ABE or multiauthority CP-ABE, however,

This article is part of the Topical Collection on *Mobile & Wireless Health*

✉ Dheerendra Mishra
dheerendra.mishra@lnmiit.ac.in

Saurabh Rana
saurabhrana.y16@lnmiit.ac.in

[1] The LNM Institute of Information Technology, Jaipur, India

multiauthority CP-ABE based schemes are depending on attribute universe, which shows that if a system satisfies the initial phase, then attribute universe has permanently fixed. Although this is not practically implemented because adding and removing users is a fundamental need for any system.

CP-ABE scheme also handles the policy hiding and large universe issues and it also ensures the security and efficiency in a smart health system. Moreover, policy hiding has two main phases, either it is partial or fully hiding policy. Here, fully hidden policy access structure expressed in term of user attributes and corresponding ciphertext. Those who know the full attribute information only those can access the encrypted outsourced data. As shows in Fig. 1, a hospital maintains his encrypted record on cloud server under specific access policy. Let patient information can only be accessed to a neurologist in Jaipur city max hospital and patient social security number. Thus, the only person who knows this information according to access policy can get access to a server. Otherwise, CP-ABE scheme will not execute the process and the respective user fails to access the content. Smart health care system makes a convenient and efficient connection between doctors at a clinical centre and patients at home. Its delivery of the telemedicine directly into the patients home via public networks. However, an adversary may have full control over the public channel which may increase security threat. Moreover, user relates information is used in these online services. The increasing amount of users' information availability raises privacy concerns. The smart card-based remote user authentication protocols have been designed in the response to privacy and security threat. These protocols try to present an efficient and secure way of communication over an insecure public channel

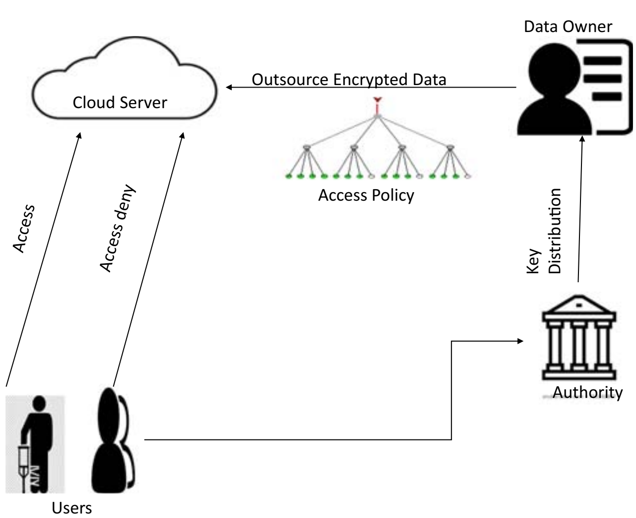

Fig. 1 system model

He and Hu [8] observed the Shao et al. [14] ID-based authentication scheme with access control mechanism for multiserver environment. Then He and Hu's cryptanalyse the Shao et al.'s scheme and found some serious flaws such as server spooning, password guessing attack, etc. Mukhopadhyay et al. [13] gave a brief overview of human condition monitoring through wireless sensors. They mentioned that the smart health system joins the activities of a human being through wearable devices continuously. Yan et al. [18] introduced an anonymous health records deduction technique. Xu et al. [17] gave an ideal for IoT based medical system, which collects the IoT based data and transfers to the needed user. However, mostly above discussed technique was not focusing on data security and privacy in a smart health system. Then researchers were starting the adoption of two kinds of attribute-based encryption schemes [3, 7]. Moreover, Li et al. [12] presented an abuse-free attribute-based access control system. Li et al. gave a very primitive idea to deal with the access control system. Zhang et al. [20] proposed cypher-text policy-based access control system, which enhances the accountability of both the communicating parties. However, Zhang et al.'s scheme only support the selective model for security. The number of communication messages or keys are also increasing the overhead of transmission messages. Amin et al. [1] analyzed the existing medical authentication protocol suffers from the smart card stolen attack. Moreover, Amin et al.'s cryptanalyses and design the improved protocol for telecare medical system. Thus, Gope and Amin [6] presented the situation based access policy mechanism for electronic patient health record.

For facilitate the medical system, Phuong et al. [15] proposed attribute-based policy-hiding scheme under a selective model. Jia et al. [10] introduced authentication and key establishment protocol for the smart healthcare system. Yang et al. [19] introduced a big data access control mechanism. However, the security of Yang et al.'s scheme enabled to validate security proof. Wang et al. [16] presented the new paradigm of CP-ABE multi-linear map with direct revocation. They claimed that the proposed scheme gives the novel direction in ciphertext revocation. Cui et al. [4] introduced a CP-ABE based partially hidden policy, which supports a linear secret sharing scheme(LSSS). Cui et al.'s scheme proved under a random oracle model. But, it does not obtain full security under the proposed model. Zhang et al. [23] proposed efficient big data access control scheme with leakage resilience framework. However, Zhang's et al. scheme does not resist against man in the middle attack. Although, it also have inefficient semi-functional and security verification phase. Zhou et al. [25] proposed a identity based continuous leakage-resilient(CLR). They prove the security of the scheme under a random oracle model. However, Zhou enables to prove in a standard model and it also not withstand with efficient access in the cloud.

Gap analysis

In the real-life scenario, the user's attribute values have a significant sensitiveness rather than generic information of the respective user. In the last few years, many schemes have been proposed, such as as [4, 11, 21, 23, 24], which uses the partially hidden and leakage resilience policy. In [21] introduced an efficient decryption phase before final decryption, which helps to improve the efficiency in smart health search and send ciphertext to the user. Lai et al. [11] also introduced the decryption phase, which is inefficient in term of linearly expressed of bilinear operation for complexity. Cui et al. [4] proposed a partially hidden policy-based scheme, which has expensive ciphertext and keys length. Zhang et al. [23] proposed a scheme for leakage resilience, but it has inefficient proof of correctness and semi-function phase. Moreover, it does not resist any existing adversary in the middle. We observed the gap in existing system as follows:

1. Ensure the proof of correctness and security, which will be based on the property of bilinear pairings. However, updating the keys should not be an effect on the security of the scheme.
2. The large number of the secret key is a significant issue of trusted authority to handle and store safely.
3. The existing scheme also facing some serious threats from the outsider adversary, those observed all the communication through the public channel. They can impersonate or try to forge dialogue.
4. The attribute anonymity and privacy protection also have a major concern in existing CP-ABE schemes.
5. The confidentiality of encrypted data on the cloud server would also be a challenging task.

Motivation and our contribution

Recently, it has been observed that the emerging trend in smart medical system facilities the medical users. If any user wishes to access and use the encrypted medical data through his smart device, he must ensure the to satisfy the access policy for encrypted data. In this process, authority main concern about the security and privacy of user access policy and attribute. Moreover, a serious threat from outsider adversary also gives the challenge to the access control schemes. Then, we presented the efficient and secure policy hiding access control scheme for medical system. The contribution is as follows:

- Initially, we observed the security analysis of Zhang et al.'s scheme. In which, we mentioned the security flaws of Zhang's protocol for big data storage in cloud computing.
- Secondly, we proposed the secure encrypted medical data storage access control protocol, which also enabled the policy hiding policy corresponding the user attribute.
- The security of the proposed protocol has been proved under the standard model. That, ensure the proposed protocol is fully secure against any adversary.
- Finally, if we compared with the existing schemes. The security attribute comparison shows the significance of protocol. The leakage ratio comparison also enhance the proposed protocol. Thus, we claim that the proposed scheme is more suitable for the smart medical system.

Roadmap

The rest of the paper flow as follows: In "Preliminaries", we discussed some basic preliminaries. In "Review of Zhang et al.'s scheme", we demonstrates the review and analysis of the Zhang et al.'s scheme. In "Proposed scheme", we present the improve access control in detail. In "Security proof", we introduced our security model then give the security proof in standard model. In "Performance analysis and comparisons" evaluate the performance and comparison of proposed protocol and then "Conclusion" gives the conclusion.

Preliminaries

In this section, we briefly discussed some preliminaries and assumption, which we have used proposed work.

Bilinear pairing Let G_0, G_1 be two multiplicative cyclic group of prime order p. Let g be a generator of G_0 and e be a bilinear map, $e : G_0 \times G_0 \rightarrow G_1$. The bilinear map has following properties:

1. Bilinearity:- $\forall\ g \in G_0$ and $u, v \in Z_p$, we have $e(g^u, g^v) = e(g, g)^{uv}$
2. Non-degeneracy:- $e(g, g) \neq 1$
3. Computability:- There exist an efficient algorithm to compute $e : G_0 \times G_0 \rightarrow G_1$.

Access structures: Let J be the collection of total number of users. Then, the set of users $\mathbb{A} \subseteq 2^J$ is called an access structure. An $\mathbb{A}$ is called an monotone access structure if $\{\mathbb{C} \subseteq 2^J : C \subseteq \mathbb{C} for some C \in \mathbb{A}\} \subseteq \mathbb{A}$.

Linear secret sharing scheme: Let $\mathbb{A}$ be a monotonic access structure. A LSSS for $\mathbb{AS}$ over finite field Z_p is an $m \times n$ matrix $\mathbb{M}$(entries in Z_p) along with the row labeling function σ which associates each row i of $\mathbb{M}$

with an attribute $\sigma(i)$ in $\mathbb{AS}$ and associates an following two polynomial time algorithm:

1. Distribute($\mathbb{M}, \sigma, \alpha$): Gives a input $\mathbb{M}$, σ and secret value $\alpha \leftarrow Z_p$. Then generates an another samples as $b_2, b_3, ...b_n \in_R Z_p$ along with insert his secret value α and set $u = (\alpha, b_2, b_3, ...b_n) \in Z_p^n$. Its gives a set $\{\lambda_\sigma(i) = M_i.u\}_{i \in m}$, where M_i is the ith row of matrix $\mathbb{M}$. The share $\lambda_\sigma(i)$ belongs to the attribute σ_i.
2. Reconstruct($\mathbb{M}, \sigma, L$): This gives a input as $\mathbb{M}$, σ, authorized attribute set L. It secret reconstruction constants $\{w_i\}_{i \in I} \subset Z_p$, where $I = \{i \in l : \sigma(i) \in L\}$ satisfying $\sum_{i \in I}(w_i M_i) = (1, 0, 0, ...0)$. Hence $\sum_{i \in I}(w_i \lambda_{\sigma_i}) = \alpha$

From there, we can say that $I \in \{1, 2, 3, \dots, n\}$ fulfils $(\mathbb{M}, \sigma)$ and $\exists \{w_i \in I\}$ s.t $\sum_{i=I} w_i \mathbb{M} = (1, 0, 0...0)$.

Assumptions

The following static assumptions have been adopted for rest of the paper.

Assumption 1: Let $\mathscr{G}$ be a given generator of the group. Then, distribution of function defined as:

$(N = p_1, p_2, p_3, G_0, G_1, e) \leftarrow \mathscr{G}$, $g_1 \leftarrow G_{p_1}$, $X \leftarrow_R G_{p_3}$

$(\Pi_1 = X, g_1, G_0, G_1, e)$, $T_1 \leftarrow G_{p_1} \times G_{p_2}$, $T_2 \leftarrow_R G_{p_1}$, $(\Pi_1, g_1, X) \rightarrow I$ Then, the advantage(ADV) of any adversary $\Im$ to break the assumption

$$ADV_{G,\mathscr{A}1}(\Lambda) = |Pr[\Im(I_1, T_1) = 1] - Pr[\Im(I_1, T_2) = 1]|$$

Definition 1 If any polynomial time adversary $\Im$ has negligible $ADV_{G,\mathscr{A}}(\Lambda)$ for given security parameter Λ. Then assumption is adoptable.

Assumption 2: Let $\mathscr{G}$ be a given generator of the group. Then, distribution of function defined as:

$(N = p_1, p_2, p_3, G_0, G_1, e) \leftarrow \mathscr{G}$, $b_1, c_1 \leftarrow G_{p_1}$, $d_1 \leftarrow G_{p_2}$

$(\Pi_2 = b_1.d_1, c_1 G_0, G_1, e)$, $T_1 \leftarrow G_0$, $T_2 \leftarrow G_{p_1} \times G_{p_3}$, $(\Pi_2, b_1.d_1, c_1) \rightarrow I_2$ Then, the advantage(ADV) of any adversary $\Im$ to break the assumption

$$ADV_{G,\mathscr{A}}(\Lambda) = |Pr[\Im(I_2, T_1) = 1] - Pr[\Im(I_2, T_2) = 1]|$$

Definition 2 If any polynomial time adversary $\Im$ has negligible $ADV_{G,\mathscr{A}2}(\Lambda)$ for given security parameter Λ. Then assumption-2 is adoptable.

Assumption 3: Let $\mathscr{G}$ be a given generator of the group. Then, distribution of function defined as:

$(N = p_1, p_2, p_3, G_0, G_1, e) \leftarrow \mathscr{G}$, $s_1, s, s_2 \leftarrow \mathbb{Z}_N$, $b_1 \leftarrow G_{p_1}$, $Y \leftarrow G_{p_1} \times G_{p_2}$, $(\Pi_3 = {g_1}^{s_2}, e(g_1, g_1)^{s_1}, e(g_1, g_1)^{s_1 s}, G_0, G_1, e)$, $T_1 \leftarrow e(g_1, g_1)^{s_1 s}$, $T_2 \leftarrow G_1$, $(\Pi_3, {g_1}^{s_2}, e(g_1, g_1)^{s_1}, e(g_1, g_1)^{s_1 s}) \rightarrow I_3$. Then, the advantage(ADV) of any adversary $\Im$ to break the assumption

$$ADV_{G,\mathscr{A}}(\Lambda) = |Pr[\Im(I_3, T_1) = 1] - Pr[\Im(I_3, T_2) = 1]|$$

Definition 3 If any polynomial time adversary $\Im$ has negligible $ADV_{G,\mathscr{A}3}(\Lambda)$ for given security parameter Λ. Then assumption-3 is adoptable.

Nobody can find collision of $h(x)$, where x is an arbitrary string.

Assumption 3: There are no any polynomial time adversary that can distinguish $(g^u, g^v, g^w, e(g, g)^{uvw})$ and $(g^u, g^v, g^w, e(g, g)^c)$ with non-negligible advantage. Then, it hard problem is called decision diffie-hellman problem.

Assumption 4: We assume that all the existing clock's are synchronized.

Threat model for medical system

The adversary($\Im$) threat model demonstrated through security assumptions. The $\Im$ have a potential to CP-ABE access control system for the smart medical system [5].

- Initially, the $\Im$ tries to retrieve private information from the smart health record in the cloud. $\Im$ does not disclose the information about the targeted encrypted data.
- In threat model, it has been assumed that $\Im$ can eavesdrop the stored encrypted medical data through the public channel.
- It is presumed that $\Im$ can extract the sensitive information about the attribute value of the user. Which modify, capture, and divert the communication over the open channel.
- $\Im$ may enter the access control system as a legitimate user. Then, it tries to retrieve the master key of a trusted server.

Network model

The presented model in this article involved four-phase and four entitled.

1. Data owner(DO) uploads encrypted files with a public parameter to the cloud server(CS).
2. If any user wishes to access the encrypted file from a cloud server, then it downloads the encrypted files to the local desk. Further, DO uses the attribute of the

respective user for encrypted data. Then, user decrypts the downloaded file; Otherwise, the user can not be able to decrypt the uploaded files.

3. Cloud server(CS) is responsible for storing the encrypted files. There are many encrypted files from different resources. It assumed that aggregate data is securely stored and compute in efficient manner.
4. The authority is the entity that computes the secret keys of the user. We assumed that authority is not needed to be fully trusted.

Case study of an access control architecture

Review of Zhang et al.'s scheme

For a smooth understanding of Zhang et al.'s scheme [23]. First, we describe efficient leakage resistance in cloud computing.

1. **Initialization Phase:** A trusted authority(TA) chooses the public parameters as $e, P_1, P_2, P_3, G_0, G_1$, where G_0, G_1 represents the composite order cyclic group. They are defining as $|G| = N$, where $N = P_1.P_2.P_3$. Then we can say that G_{p1}, G_{p2}, G_{p3} are three different cyclic group. Further, TA selects a_1, b_1, c_1 from G_{p1} and s_1, s_2 from $\mathbb{Z}_{\mathbb{N}}$. Thus, TA contract a public parameters $P_u = \{a_1, b_1, c_1, e(g_1, g_1)^{s_1 z}\}$ and $w = g_1{}^{s_2}$. In the initialization phase, we assume s_1 is a master secret key(Msk).
2. **Keygen:** The TA generates the private key corresponding to content sharing authority. Then keygen algorithm performs $(Pu, Msk, Id) \to sk$. To follows the corresponding approach TA randomly selects r_a from Z_N and $r_1, r_2, r_3....r_n$ are also belong to the Z_N. Further, TA selects an R_3, $R_3{}'$, R_{3i} with respect to the identity Id = $(id_1, id_2....id_n)$, where $i \in G_{p3}$. Then secret key will be calculated as $SK = (Sk_1, Sk_2, Sk_3)$, where
$$Sk_1 = g_1{}^{s_1}.w^{r_a}.R_3{}^{r_a}$$
$$Sk_2 = g_1{}^{r_a}.R_3{}'^{r_a}$$
$$Sk_3 = \prod_{n=i}^{n}(c_1{}^{id_i}.b_1)^{r_a}(R_{3i})^{r_i}$$
Due to the leakage of secret keys, content sharing user receives the encrypted files. Then U_i sends the request to the authority to generates a fresh private key.
3. **Key updating:** After receiving the request for updating the key of the user. TA runs the keyupdating phase $(Pu, SK, Id) \to Sk_i$, where $i \in \{1, 2, 3\}$. For performing keyupdate algorithm, TA selects random element $\Delta r_a{}'$ and $\Delta r_i{}' \in Z_N \;\forall\; i\{\in 1, 2, 3, 4, ...n\}$. Then updating key secret keys are $SK' = (Sk_1{}', Sk_2{}', Sk_3{}')$.
$$Sk_1{}' = g_1{}^{s_1}.w^{r_a+\Delta r_a{}'}.R_3{}^{(r_a+\Delta r_a{}')}$$
$$Sk_2{}' = g_1{}^{r_a+\Delta r_a{}'}.R_3{}'^{(r_a+\Delta r_a{}')}$$
$$Sk_3{}' = \prod_{i=1}^{n}(c_1{}^{id_i}, b_1).(R_{3i})^{(r_{a_i}+\Delta r_{a_i}{}')}$$
where $\Delta r_{a_i}{}'$ and Δr_{a_i} are choosing randomly from Z_N. We will also ensure that $r_a + \Delta r_a{}'$ and $r_{a_i} + \Delta r_{a_i}{}'$ are also randomly chosen values. So, we can conclude that new and old both secret keys have same distribution.
4. **Keygensf:** After generating regular secret keys Sk_1, Sk_2, Sk_3. TA further chooses $\delta_1, \delta_2, \delta_3, \phi_k \in Z_N$. TA generates the semi-function key as: $\widehat{SK} = (\widehat{Sk_1}, \widehat{Sk_2}, \widehat{Sk_3})$
$$\widehat{Sk_1} = Sk_1.g_2{}^{\delta_1}$$
$$\widehat{Sk_2} = Sk_2.g_2{}^{\delta_3.\phi_k}$$
$$\widehat{Sk_3} = Sk_3.g_2{}^{\delta_2}$$
.
5. **Enc:** Data owner uploads his encrypted files on the cloud. We describe the standard encryption algorithm as follows: For constructing the corresponding cipher text $Enc(P_u, Id, m) \to E_{sk}(m) = CPT$, where P_u is a public parameter, Id indicates the identity of the respective user, m is a randomly chosen message by user. CPT = (C_{i1}, C_{i2}, C_{i3}), where
$$C_{i1} = m \oplus e(g_1, g_1)^{s_1.z}$$
$$C_{i2} = w^z \prod_{i=1}^{n}(c_1{}^{id_i.b_1})^z$$
$$C_{i3} = g_1{}^z$$
6. **Encsf:** After generating general cipher text C_{i1}, C_{i2}, C_{i3}, TA chooses a random number s_1, $\phi_c \in Z_C$. Then, it sets the semi-function ciphertext as: $\widehat{CPT} = (\widehat{C_{i1}}, \widehat{C_{i2}}, \widehat{C_{i3}})$, where $\widehat{C_{i1}} = C_{i1}$
$$\widehat{C_{i2}} = C_{i2}g_2{}^{s_1}$$
$$\widehat{C_{i3}} = C_{i3}g_2{}^{s_1\phi_c}$$
7. **Dec:** U_i acquires his secret key from trusted authority. Then, by using the secret key U_i will able to retrieve corresponding plane text or message m. For decryption, U_i process as $Dec(Pu, CPT, SK) \to m$ and computes $e(Sk_1 Sk_3, C_{3i})e(Sk_2, C_{2i})^{-1}$ by impose the original secret keys or semi-functional keys.

Analysis of Zhang et al.'s scheme

After observing the Zhang et al. [23] protocol, we found that it faces some serious threats. The detail description of existing threats in Zhang et al.'s scheme describes as follows:

Main in the middle attack: In the proposed scheme, TA announced the public parameters as $\{a_1, b_1, c_1, e(g_1, g_1)^{s_1 z}\}$. Further, data owner upload his encrypted data C_1, C_2, C_3 in on the cloud server. If any adversary came in the middle and extract his private encrypted data from the cloud server. There encrypted messages are $C_{i1} = m \oplus e(g_1, g_1)^{s_1 . z}$, $C_{i2} = w^z \prod_{i=1}^{n} (c_1{}^{id_i . b_1})^z$, $C_{i3} = g_1{}^z$. If adversary knows the public parameter and the encrypted message collection, then it computes $m = C_{i1} \oplus e(g_1, g_1)^{s_1 z}$. Thus, transmitted message has been compromised. Since, any adversary have an capability to retrieve the transmit massage.

Inefficient semi-functional encryption phase: TA chooses a random number s_1, $\phi_c \in Z_C$. Then, it sets the semi-function ciphertext $(\widehat{C_{i1}}, \widehat{C_{i2}}, \widehat{C_{i3}})$, where $\widehat{C_{i1}} = C_{i1}$, $\widehat{C_{i2}} = C_{i2} g_2{}^{s_1}$, $\widehat{C_{i3}} = C_{i3} g_2{}^{s_1 \phi_c}$. Here, TA's uses his master key s_1 as random number in semi-functional encryption phase, which will work for the decryption phase.

Inefficient correctness proof phase: The correctness proof of proposed scheme will not work. The details of correctness proof is shown as follows:

$$\frac{e(Sk_1 \cdot Sk_3, C_{i3})}{e(Sk_2, C_{i2})}$$

$$= \frac{e(g_1{}^{s_1} g_1{}^{s_2 r} R_3{}^r \cdot \prod_{i=1}^{n} (c_{1t}{}^{t_i} . b_1)(R_{3i})^{r_i}, g_1{}^z)}{e(g_1{}^r R_3{}'^r, g_1{}^{s_2 z} \prod_{i=1}^{n} (u_t{}^{t_i} b_1)^z)}$$

$$= \frac{e(g_1{}^z, g_1{}^{s_1}) e(g_1{}^z, g_1{}^{r . s_2}) e(g_1{}^z, R_3{}^r . \prod_{i=1}^{n} (c_{1t}{}^{t_i} b_1) R_{3i}{}^{r_i})}{e(g_1{}^r, g_1{}^{z s_2}) e(g_1{}^r, \prod_{i=1}^{n} (c_{1t}{}^{t_i} b_1)^z}$$

$$\neq e(g_1, g_1)^{s_1 z}$$

According to the above computation, it has been proved that the correctness of proof is inefficient.

Proposed scheme

For deploying the smart health facility, trusted medical authority(TMA) selects a security parameter Λ, which is $G(1^{\Lambda})$. Further, TMA chooses the public parameters $(p_1, p_2, p_3, N, G_0, G_1, e)$. The universe set of attribute selects from $\mathbb{U} = \mathbb{Z}_{N = p_1 p_2 p_3}$.

[Setup(1^{Λ}):] TMA chooses uniformly random $s_1, s_2 \in \mathbb{Z}_{\mathbb{N}}$, $a_1, b_1, c_1 \in G_{p_1}$, $d_1 \in G_{p_2}$ and $X \in G_{p_3}$. Then, TMA computes $Z = e(g_1, g_1)^{s_1}$, $Y = b_1 . d_1$. Then, TMA includes some essential public parameter Pu = $(N, g_1, g_1{}^{s_2}, Z, Y, c_1)$ and announce the master key $MK = (s_1, b_1, X)$.

Keygen(Pu, MK, S): If any data user has an set of attribute (I_s, S), where $S = \{att_i\}_i \in I_s$ and $I_s \in \mathbb{Z}_N$. After verifying the set of attribute, TMA generates the keys for further communication. TMA uniformly chooses $r \in \mathbb{Z}_N$ and R, $R_1, R_{1i} \in G_{p3}$ for $i \in I_s$. Form these credential, TM generates secret keys SK = $(S, Sk, Sk_1, Sk_{i1} 1 \in I_s)$, where $Sk = g_1{}^{s_1} g_1{}^{s_2} r R$, $Sk_1 = g_1{}^r . R_1$, $Sk_{i1} = (g^{att_i} b_1)^r R_{1i}$.

Enc(Pu, $\mathbb{M}$, $\mathbb{A}$): Data owners(DO) uploads his encrypted medical data on the clouds server. DO selects AES encryption scheme to encrypt his medical records. Then, DO public the access policy $=(\mathbb{M}, \sigma, T)$, where $\mathbb{M}$ is an $n \times m$ matrix, σ is a map from each row Rw_x of $\mathbb{M}$, and $T = (r_{\sigma(1)}, r_{\sigma(2)}, r_{\sigma(3)}, \ldots, r_{\sigma(n)}) \in \mathbb{Z}_{\mathbb{N}}{}^n$. Then, it encrypt the original $M \in G_1$ with the suitable access policy. In this process, DO chooses the two vectors v_i, $v_j \in \mathbb{Z}_N^m$, where $v_i = (s, b_2, b_3, \ldots, b_m)$, $v_j = (s', b_2{}', b_3{}', ...b_m{}')$. DO again chooses uniformly D_1, $D_{1x}, D_{2x}, D_{3x} \in G_{p2}$ and t_x from $\mathbb{Z}_N$ for $1 \leq x \leq n$. Further, ciphertext will be calculated as: CPT = $(\mathbb{M}, \sigma)$, C_1, $C_1{}'$, $\{C_{1,x}\}_{1 \leq x \leq n}$, and C_2, $C_2{}'$, $\{C_{2,x}, C_{2,x}{}'\}_{1 \leq x \leq n}$, where $C_1 = Z^{s'}$, $C_1{}' = g_1{}^{s'} . D_1$,

$$C_{1,x} = g_1{}^{s_2 Rw_x v_j} (g_1{}^{r_{\sigma(x)}} . Y)^{-s'} D_{1,x}$$

$$C_2 = M . Z^s$$

$$C_2{}' = g_1{}^s$$

$$C_{2,x} = g_1{}^{s_2 Rw_x v_i} (g_1{}^{r_{\sigma(x)}} . Y)^{-t_x} D_{2,x}$$

$$C_{2,x}{}' = g_1{}^{t_x} . D_{3,x}$$

Then, DO uploads details on the cloud server. If data user wishes to get the health record from a cloud server, he required to obtain the plaintext message M by the Decryption algorithm. But, the proposed protocol essentially requires to verifying the underlying user attribute as follows:

- For accessing the data user input CPT, Pu. User first set the minimum subset of attributes $\{I_{\mathbb{M}, \sigma(i)}\}_1 \leq i \leq n$ from $\mathbb{M}, \sigma$. Then, user attribute exists $\{I_{\mathbb{M}, \sigma(i)}\}$ and checks weather $\{\sigma(i) | i \in I\} \subseteq S$, where $S = \{att_i\}_i \in I_s$. If user attains all the existing attributes. Then, user must go through from the verifying phase.
- For cross verifying the user, it takes minimum subset of I_S and retrieve the secret key of user SK = $(S, Sk, Sk_1, Sk_{i1i} \in I_s)$, (I_s, S), where $S = \{att_i\}_i \in I_s$ and $I_s \in \mathbb{Z}_N$. After that it calculates

$$C_1{}^* = \frac{e(C_1{}', Sk)}{\prod_{i \in I} (e(C_{1,i}, Sk_1) e(C_1{}', Sk_{\sigma i}))^{w_i}}$$

$$= \frac{e(g^{s'} D_1, g_1{}^{s_1} g_1{}^{s_2 r R})}{\prod_{i \in I} (e(g_1{}^{s_2 Rw_i . v_j} (g_1{}^{r_{\sigma(i)}} Y)^{-s'} D_{1,i}, g_1{}^r R_1)}$$

$$e(g_1{}^{s'} D_1, (g^{S_{\sigma i}} b_1)^r R_{\sigma(i)}))^{w_i}$$

$$= \frac{e(g_1{}^{s'}, g_1{}^{s_1} g_1{}^{s_2 r})}{\prod_{i \in I} (e(g_1{}^{s_2 Rw_i} v_j, g_1{}^r))^{w_i}}$$

$$= \frac{e(g_1{}^{s'}, g_1{}^{s_1} g_1{}^{s_2 r})}{e(g_1{}^{s_2}, g^r)^{(\sum_{i \in I} w_i Rw_i)} v_i}$$

$= e(g_1, g_1)^{s_1 s'}$

$= C_1$

, it satisfies if and only if $r_\sigma(i) = s_\sigma(i)$ for $i \in I$. Otherwise $C_1{}^* \neq C_1$, which indicates the proposed scheme does not satisfies the partially hidden policy.

Dec(Pu, CPT, SK): After verifying the policy attribute, U_i can decrypt the corresponding ciphertext for getting the health record. It initiates the following process:

$$M = \frac{C_2}{B}$$

, where

$$B = \frac{e(C_2, Sk)}{\prod_{i \in I}(e(C_{2,i}, Sk_1)e(C_{2,i}{}', Sk_{\sigma i}))^{w_i}}$$

For the decryption S satisfies access structure $\mathbb{A}$ then $\exists$ an eligible set I. Then, it consists $\{w_i\}_{i \in I}$ such that $\sum_{i \in I} w_i Rw_i = (1, 0, 0....0)$, $r_\sigma(i) = s_\sigma(i)$ for $i \in I$.

$$= \frac{e(C_2, Sk)}{\prod_{i \in I}(e(C_{2,i}, Sk_1)e(C_{2,i}{}', Sk_{\sigma i}))^{w_i}}$$

$$= \frac{e(g_1{}^s, g_1{}^{s_1} g_1{}^{s_2 r} R)}{\prod_{i \in I}(e(g_1{}^{s_2 Rw_i v_i}(g_1{}^{r_\sigma(i)Y})^{-t_i} D_{2,i}, g_1{}^r R_1)}$$

$$e(g_1{}^{t_i} D_{3,i}, (g_1{}^{s_\sigma(i) b_1})^r R_{1,i}))^{w_i}$$

$$= \frac{e(g_1{}^s, g_1{}^{s_1} g_1{}^{s_2 r})}{\prod_{i \in I}(e(g_1{}^{s_2 Rw_i v_i}, g_1{}^r))^{w_i}}$$

$$= \frac{e(g_1{}^s, g_1{}^{s_1} g_1{}^{s_2 r})}{(e(g_1{}^{s_2}, g_1{}^r))^{(\sum_{i \in I} w_i Rw_i) v_i}} = Z^s$$

$$= \frac{M.Z^s}{Z^s}$$

$$= M$$

Security proof

First, introduce the security model and then establishes the proposed scheme.

Security model:- In this model, we briefly introduced the security model for proposed scheme. It defines the game between $\Im$ and challenger ($\mathscr{C}$) for security challenge. This game will process, which defined as follows [2, 9].

1. Setup: In setup phase, $\mathscr{C}$ invokes Setup$(1^\Lambda, U_i) \rightarrow (Pu, MK)$. Then, it gives Pu to $\Im$ and stores MK as a secret parameter.
2. Phase-1: The $\Im$ adaptively generates the polynomially number of queries to the oracle ($\wr$).
   (a) The $\Im$ provides the set of attributes $S = \{att_i\}_{i \in I_s}$ to $\mathscr{C}$. Then, $\mathscr{C}$ runs $SK \leftarrow KeyGEN(Pu, MK, S)$. It gives the M to $\Im$.
3. Challenge: After the phase-1, challenger $\mathscr{C}$ sends the messages $\{M_0, M_1\}$ to the $\Im$, which has equal length. Then, it also submits the $\mathbb{AS}_1 = (M, \sigma, S_1)$, $\mathbb{AS}_2 = (M, \sigma, S_2)$. But, there are restrictions on access policies, which will be defined in phase-1. Then, $\mathscr{C}$ flips the random coin $C \in \{0, 1\}$, $Enc(Pu, M_c, \mathbb{AS}) \rightarrow CPT_{\mathbb{AS}_c}$. Further, it sends $CPT_{\mathbb{AS}_c}$ to $\Im$ as a challenging ciphertext.
4. Phase-2: The $\Im$ invokes the adaptive quires to the $\mathscr{C}$ for retrieve the SK. Then, it also verifies the set of attributes for corresponding access structure $\mathbb{AS}_1$ and $\mathbb{AS}_2$ with restrictions. Thus, $\Im$ identifying the users, which does not the access policy.
5. Guess: The $\Im$ guess and sends a bit $c' \in \{0, 1\}$ U_j. $\Im$ will win the game if its holds c = c'. Thus, adversary have an advantage to win this game, which is defines as: $|Pr[c' = c] - \frac{1}{2}|$. Here, we take a probability on the chosen random bits with corresponding $\Im_{Ad}$ and $\mathscr{C}$.

Let $Succ(\Im)$ successfully guessing the value of a bit c, which is selected from 6th(Test) phase. The advantage held by the $\Im_{Ad}$ against specific access control scheme. Defined as:

$$\Im_{Adv_{A,P}}(k) = |2.Pr[Succ(\Im_{Ad})] - 1|$$

Definition 4 The ciphertext attribute based encryption scheme is fully secure for partially hidden policy. If any adversary must have the negligible advantage to win the security game.

Theorem 1 *If all the statical assumptions holds. Then, proposed CP-ABE is fully secure in given security model.*

Proof In our proposed scheme, we process our proof through the semi-function ciphertext(SFC) and keys(SFK). These parameters will not work as original cipher or keys. But, these are necessary for proceed the game.

Let g be a generator of the group G. Then, SFC will have been generated by any challenger. It chooses two numbers x, x' from $\mathbb{Z}_N$ and corresponding two vectors v, v' from $\mathbb{Z}_N^m$. Moreover, chooses a random number z_i, which associated with a existing set of attributes and $a_x, a_x{}' \in_R \mathbb{Z}_N$, with respect to Rw_x. Then, the normal output ciphertext would be $SFCPT_{\mathbb{M}} = (\mathbb{M}, \sigma)$, Cf_1, $Cf_1{}'$, $\{Cf_{1,x}\}_{1 \le x \le m}$, and Cf_2, $Cf_2{}'$, $\{Cf_{2,x}, Cf_{2,x}{}'\}_{1 \le x \le m}$

$Cf_1 = Z^{s'}$, $Cf_1{}' = g_1{}^{s'} g^{x'}.D_1$

$$Cf_{1,x} = g_1{}^{s_2 Rw_x v_j}(g_1{}^{r_\sigma(x)}.Y)^{-s'} D_{1,x} g^{Rw_x r_1{}' + a_x{}' z_\sigma(x)}$$

$$Cf_2 = M.Z^s$$

$$Cf_2{}' = g_1{}^s g^x$$

,

$$Cf_{2,x} = g_1{}^{s_2 Rw_x v_i}(g_1{}^{r_\sigma(x)}.Y)^{-t_x} D_{2,x} g^{Rw_x v + a_x z_{\sigma x}}$$

$Cf_{2,x}{}' = g_1{}^{t_x}.D_{3,x}g^{-a_x}$
In this process, SFK would be re-generated and challenger chooses the random number $n, n' \in \mathbb{Z}_N$ and $\{n_i \in \mathbb{Z}_N\}_{i \in I_s}$. Then, all those parameter will take as a secret output as semi-functional key(SFK). It shows in basically three type of $Sfk = g_1{}^{s_1}g_1{}^{s_2}rRg^n$, $Sfk_1 = g_1{}^r.R_1g^{n'}$, $\{Sfk_{i1} = (g^{att_i}b_1)^r R_{1i}g^{n'z_i}\}_{i \in I_s}$. Now, the second type of SFK will be $g_1{}^{s_1}g_1{}^{s_2}rRg^n$, $Sfk_1 = g_1{}^r.R_1$, $\{Sfk_{i1} = (g^{att_i}b_1)^r R_{1i}$. In this manner third type of SFK $g_1{}^{s_1}g_1{}^{s_2}rRg^n$, $Sfk_1 = g_1{}^r.R_1g^{n'}$, $\{Sfk_{i1} = (g^{att_i}b_1)^r R_{1i}g^{n'_i}\}_{i \in I_s}$. Then, we will prove the security of game by hybrid arguments of sequences of game. Where first game security depends on the normal ciphertext and keys, which is denoted as $Game_{real}$. In the another game, we would choose the normal keys and semi functional ciphertext, which is denotes as $Game_{chall}$. □

Let $\Im$ invokes the $q_{i\,1 \leq q}$ many queries, then adversary plays the following game as follows:

1. $Game_{k,0}$: Initially, $\Im$ plays the game with challenging semi-functional ciphertext. Moreover, $k-1$ number number of challenging keys are type three and behave like a semi-functional. kth key is SFK of type one and others are normal keys.
2. $Game_{k,1}$: In this play phase, $\Im$ plays the game with challenging semi-functional ciphertext. In which, first $k-1$ number of keys are SF of type three and kth is SFK of type two. Others are normal.
3. $Game_{k,2}$: The $\Im$ plays the game with SF challenging ciphertext, in which k number of keys are type three and the other keys are normal. On the other hand, if challenging ciphertext is SF then all keys are SF of type three.
4. $Game_{k,3}$: $\Im$ invokes the SF encryption of random messages m_0, m_1, which will be the challenging ciphertext. However, all the existing keys are SF of type three.
5. $Game_{k,4}$: $\Im$ gives the challenge $C_{1,x}$, $C_{2,x}$ as a random ciphertext, which is distinguish from T_0 and T_1. Then, we can say that $\Im$ has an negligible advantage to win the game.

We will prove that all the existing game are indistinguishable. Hence, $\Im$ can never have non-negligible advantage to breaking the proposed scheme.

Lemma 1 *Any probabilistic polynomial-time $\Im$ satisfies the Assumption-1. The ciphertext along with the keys has real security in the first security game. Then, the ciphertext is SFC then it also obtains real security.*

Proof Let $\exists$ an adversary $\Im_A$, which has negligible advantage $|Pr[\Im_A(Game_{real})(ADV) - \Im_A(Game_{chall}(ADV)]| = \epsilon$. Then, we adopts the simulator $\mathscr{S}$ with $ADV_{\mathscr{S},\Im_A}(\Lambda) = \epsilon$ for break the Assumption-1. The $\mathscr{S}$ gives the input as g_1, X, c_1, T. Then, it simulates $Game_{real}$ or $Game_{chall}$ with the $\Im_A$.

Setup: The $\mathscr{S}$ selects a random numbers $s_1, s_2, s_3 \in \mathbb{Z}_\mathbb{N}$ and $d_1 \in G_{p_2}$. Further, it computes $Z = e(g_1, g_1)^{s_1}$, $b_1 = g_1{}^{s_3}$, and $Y = b_1.d_1$. Then, $\mathscr{S}$ send the public parameters($N, g_1, g_1{}^{s_3}, Z, Y, d_1$) to the $\Im_A$.

Phase 1: The $\mathscr{S}$ offers the normal keys to the $\Im_A$ by key generation algorithm. It also have a master key as MK = (s_1, b_1, X).

Challenge: After $\Im_A$ submitting the two messages M_0, M_1 to the corresponding $\mathscr{C}$. Along with this, they also provide the two different access policies $\mathbb{AS}_{\not\models} = (\mathbb{M}, \sigma, T_0)$ and $\mathbb{AS}_{\not\models} = (\mathbb{M}, \sigma, T_1)$. There will also be a restriction on both the access policies, in which no one can hold the required attributes. Let $T_c' = (r_\sigma(1), r_\sigma(2), r_\sigma(3)....r_\sigma(n))$, where c' can be chosen from $c' \in \{0, 1\}$. $\mathscr{S}$ also follows:

1. Initially, generates the vector $v_i = (1, b_2, b_3, \ldots, b_m)$, $v_j{}' = (1, b_2{}', b_3{}', \ldots, b_m{}')$ and $v_{\triangle v} = (0, v_{\triangle b2}, v_{\triangle b3}, \ldots, v_{\triangle bm})$, where $v_i, v_j{}', v_{\triangle b} \in \mathbb{Z}_N$
2. After that, $\mathscr{S}$ chooses t_x from $\mathbb{Z}_N$ and $s_x = (s_3 + r_\sigma(x))^{-1}$ and $D_1, D_{1x}, D_{2x}, D_{3x} \in G_{p2}$, where $1 \leq x \leq n$
3. Then, simulator selects the secret parameter $s \in Z_N$ and computes $C_1 = e(g_1{}^{s'}, T^s)$, $C_1{}' = T^{s'}.D_1$, $C_{1,x} = T^{(ss_2Rw_xv_j)}T^{(Rw_xv_\triangle)(s_2s_x - s.s_3 + r_\sigma(x))}D_{1,x}$, $C_2 = M_{c'}.e(g_1{}^s, T)$, $C_2{}' = T$, $C_{2,x} = T^{s_2Rw_xv_i}T^{(s_3+r_{\sigma(x)})^{-t_x}}D_{2,x}$, $C_{2,x}{}' = T^{t_x}.D_{3,x}$, where $1 \leq x \leq n$.
4. $\mathscr{S}$ give the challenge on the ciphertext $CPT_{\mathbb{M}'}$ and forward to the $\Im_A$. $CPT_{\mathbb{M}'} = (\mathbb{M}, \sigma)$, C_1, $C_1{}'$, $\{C_{1,x}\}_{1 \leq x \leq m}$, and $C_2, C_2{}', \{C_{2,x}, C_{2,x}{}'\}_{1 \leq x \leq m}$. Then, $T = g_1{}^s g^c$ and $C_1 = Z^{s'}$, $C_1{}' = g_1{}^{s'}.D_1.g^{c'}$, $C_{1,x} = g_1{}^{s_2Rw_xv_j}(g_1{}^{r_{\sigma(x)}}.Y)^{-s'}D_{1,x}g^{v'Rw_x + a_x{}'z_\sigma(x)}$, where $z_\sigma(x) = s_3 + r_\sigma(x)$, $v_1{}' = s'$, $D_{1,x} = Y^{s'}D_{1,x}$, $a_x{}' = c((Rw_x \cdot v_\triangle)s_2s_x - s)$. Further, computes $C_1 = M_{c'}Z^s$, $C_1{}' = g^s.g_1{}^c$, $C_{2,x} = T^{s_2Rw_xv_i}T^{(s_3+r_{\sigma(x)})^{-t_x}}D_{2,x}g^{Rw_x + a_x{}'z_\sigma(x)}$, $C_{2,x}{}' = T^{t_x}.D_{3,x}g^{-a_x}$, where $v = sv'$ with $v_1 = s$. Therefore, it has been considered $r_x = sr_x{}'$, $D_{2,x} = D^{sr_x}D_{3,x}{}'$, $z_\sigma(x) = s_3 + r_\sigma(x)$, $a_x = -c'r_x{}'$. Which proves that the challenging $\mathbb{CPT}$ is a normal ciphertext. Moreover, $\mathscr{S}$ simulate the $Game_{chall}$. Further, $G_{p_1} \rightarrow T$, which will be the normal ciphertext with simulation queries on $Game_{real}$.

Phase 2: As $\mathscr{S}$ plays a phase-1, in which access policies $\mathbb{AS}_{\not\models}$ and $\mathbb{AS}_{\not\models}$ are not satisfied the any set of attributes. These policies has restriction on the attribute set. If

Table 1 Security attributes comparison

S/A	Npub	Ncpt	Npk	Security model
Cui et al. [4]	12	9	7	Standard model
Zhang et al. [20]	9	7	10	Selective security model
Li et al. [12]	9	5	4	Standard model
Zhou et al. [25]	6	5	4	Standard model
Zhang et al. [22]	8	6	7	Random oracle
Proposed	6	6	4	Standard model

adversary chooses $T \leftarrow G_{p_1} \times G_{p_2}$ and $\mathscr{S}$ simulates the game $Game_0$. On the other hand if $\Im_A$ chooses $T \leftarrow G_{p_1}$, $\mathscr{S}$ can simulate the all queries for $Game_{real}$. Hence, $\mathscr{S}$ uses the output result of the $\Im_A$ for distinguish T. Thus, it has a negligible advantage $ADV1_{\mathscr{S},\Im_A}(\Lambda) = \epsilon$. □

Lemma 2 *Any probabilistic polynomial-time $\Im$ satisfies the Assumption-2. The $Game_{k-1,3}$ and $Game_{k,1}$ games are indistinguishable. Then, the ciphertext is SFC then it also obtains real security.*

Proof Let $\exists$ an adversary $\Im_A$, which has negligible advantage $|Pr[\Im_A(Game_{k-1,3})(ADV) - \Im_A(Game_{k,1}(ADV)]| = \epsilon$. Then, we adopts the simulator $\mathscr{S}$ with $ADV_2\mathscr{S}, \Im_A(\Lambda) = \epsilon$ for break the Assumption-2. The $\mathscr{S}$ gives the input as g, p_1p_2, q_1q_2, X, d_1 , T c_1, T. Then, it simulates $Game_{k-1,3}$ or $Game_{k,1}$ with the $\Im_A$.

Setup: The $\mathscr{S}$ selects a random numbers $s_1, s_2, s_3 \in \mathbb{Z}_{\mathbb{N}}$ and $d_1 \in G_{p_2}$. Further, it computes $Z = e(g_1, g_1)^{s_1}$, $b_1 = {g_1}^{s_3}$, and $Y = b_1.d_1$. Then, $\mathscr{S}$ send the public parameters$(N, g_1, {g_1}^{s_3}, Z, Y, d_1)$ to the $\Im_A$. Where the master secret key are MK = (s_1, b_1, X).

Phase 1: Now, let us know that how $\mathscr{S}$ responds for the jth secret query for $S = (I_s, S)$ where $S = \{s_i\}_{i\in I}$

1. If any jth query j ¡k, $\mathscr{S}$ selects the $\hat{t}, \hat{d}, \hat{d}' \in \mathbb{Z}_N$ with $\{\hat{d}_i \in \mathbb{Z}_N\}$, where $i \in I_S$. Further, it creates SFK as: $Sfk = {g_1}^{s_1} g^{s_2\hat{t}}(q_1q_2)^{\hat{d}}$, $Sfk' = {g_1}^{t}(q_1q_2)^{\hat{d}}$, $Sfk_i = ({g_1}^{s_i}b_1)^{\hat{t}}$, where $i \in I_s$. Which is properly distributed semi-functional key.
2. If j¿k, $\mathscr{S}$ generates the normal keys through the key generate algorithm. Then, it will know as master secret keys as s_1, b_1, X.
3. $\mathscr{S}$ chooses the $\hat{R}_1, \hat{R}_1{}', \hat{R}_i$ from G_{p3}. Then, it responds to the kth queries. Further, it calculates $Sk = {g_1}^{s_1}T^{s_2}\hat{R}_1$, $Sk' = T\hat{R}_1{}'$, $Sk_i = T^{\{s_3 + s_i\}}\hat{R}_i$, where $i \in I_S$. It has been observed that it $T \leftarrow G_{p1} \times G_{p3}$ and $T = {g_1}^t g^d \hat{R}$, $Sfk = {g_1}^{s_1} g^{s_2\hat{t}}(q_1q_2)^{\hat{d}}$, $Sfk' = {g_1}^t g^{\hat{d}\hat{R}}$, $Sfk_i = ({g_1}^{s_i}b_1)^{\hat{t}\hat{R}_i {g_1}^{z_i}}$, where $i \in I_s$. where $d = s_2d'$, $R_i = \hat{R}^{s_1+s_i}\hat{R}_i$, $z_i = s_1 + s_i$. If T has been chosen from $G_{p1} \times G_{p2} \times G_{p3}$ then it is properly distributed in normal form.

Challenge: $\Im_A$ submits the two messages M_0, M_1 to the corresponding $\mathscr{C}$. Along with this, they also provide the two different access policies $\mathbb{AS}_{\not{k}} = (\mathbb{M}, \sigma, T_0)$ and $\mathbb{AS}_{\not{k}} = (\mathbb{M}, \sigma, T_1)$. There will also be a restriction on both the access policies, in which no one can hold the required attributes. Let $T_c' = (r_\sigma(1), r_\sigma(2), r_\sigma(3)....r_\sigma(n))$, where c' can be chosen from $c' \in \{0, 1\}$. $\mathscr{S}$ also follows:

1. Initially, generates the vector $v_i = (1, b_2, b_3, \ldots, b_m)$, $v_j{}' = (1, b_2{}', b_3{}', \ldots, b_m{}')$ and $v_{\triangle v} = (0, v_{\triangle b2}, v_{\triangle b3}, \ldots, v_{\triangle bm})$, where $v_i, v_j{}', v_{\triangle b} \in \mathbb{Z}_N$
2. After that, $\mathscr{S}$ chooses t_x from $\mathbb{Z}_N$ and $s_x = (s_3 + r_\sigma(x))^{-1}$ and $D_1, D_{1x}, D_{2x}, D_{3x} \in G_{p2}$, where $1 \le x \le n$
3. Then, simulator selects the secret parameter $s \in Z_N$ and computes $C_1 = e({g_1}^{s'}, (p_1p_2)^s)$, $C_1{}' = (p_1p_2)^{s'}.D_1$, $C_{1,x} = (p_1p_2)^{(ss_2Rw_xv_j)}(p_1p_2)^{(Rw_xv_\triangle)(s_2s_x - s.s_3 + r_\sigma(x))}D_{1,x}$, $C_2 = M_{c'}.e({g_1}^s, (p_1p_2))$, $C_2{}' = p_1p_2$, $C_{2,x} = (p_1p_2)^{s_2Rw_xv_i}T^{(s_3+r_\sigma(x))^{-t_x}}D_{2,x}$, $C_{2,x}{}' = (p_1p_2)^{t_x}.D_{3,x}$, where $1 \le x \le n$.
4. $\mathscr{S}$ give the challenge on the ciphertext $CPT_{\mathbb{M}'}$ and forward to the $\Im_A$. $CPT_{\mathbb{M}'}$ = $(\mathbb{M}, \sigma)$, C_1, $C_1{}'$, $\{C_{1,x}\}_{1\le x\le m}$, and $C_2, C_2{}', \{C_{2,x}, C_{2,x}{}'\}_{1\le x\le m}$. Then, $p_1p_2 = {g_1}^s g^c$ and $C_1 = Z^{s'}$, $C_1{}' = {g_1}^{s'}.D_1.g^{c'}$, $C_{1,x} = {g_1}^{s_2Rw_xv_j}({g_1}^{r_{\sigma(x)}}.Y)^{-s'}D_{1,x}g^{v'Rw_x + a_x{}'z_\sigma(x)}$, where $z_\sigma(x) = s_3 + r_\sigma(x)$, $v_1{}' = s'$, $D_{1,x} = Y^{s'}D_{1,x}$, $a_x{}' = c((Rw_x \cdot v_\triangle)s_2s_x - s)$. Further, computes $C_1 = M_{c'}Z^s$, $C_1{}' = g^s.{g_1}^c$, $C_{2,x} = (p_1p_2)^{s_2Rw_xv_i}(p_1p_2)^{(s_3+r_{\sigma(x)})^{-t_x}}D_{2,x}g^{Rw_x + a_x{}'z_\sigma(x)}$, $C_{2,x}{}' = (p_1p_2)^{t_x}.D_{3,x}g^{-a_x}$, where $v = sv'$ with $v_1 = s$. Therefore, it has been considered $r_x = s{r_x}'$, $D_{2,x} = D^{sr_x}D_{3,x}{}', z_\sigma(x) = s_3 + r_\sigma(x), a_x = -c'{r_x}'$. Which proves that the challenging $\mathbb{CPT}$ is a normal ciphertext. Moreover, $\mathscr{S}$ simulate the $Game_{chall}$.

Table 2 Total Leakage ratio and security comparison

Schemes	Leakage ratio(LR)	Informal security
Cui et al. [4]	1/5	Strong
Zhang et al. [20]	1/2	Weak
Li et al. [12]	1/2	Conditional
Zhou et al. [25]	1/2	Very weak
Zhang et al. [22]	1/3	Strong
Proposed	1/3	Strong

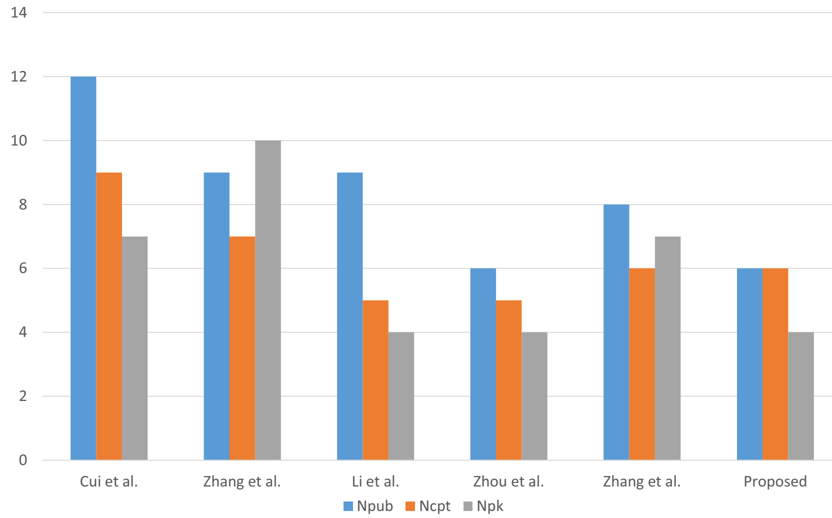

Fig. 2 Comparison of communication messages size

Further, $G_{p_1} \rightarrow T$, which will be the normal ciphertext with simulation queries on $Game_{real}$.

Phase 2: As $\mathscr{S}$ plays a phase-1, in which access policies $\mathbb{AS}_{\not\models}$ and $\mathbb{AS}_{\not\models}$ are not satisfied the any set of attributes. These policies has restriction on the attribute set. If adversary chooses $T \leftarrow G_{p1} \times G_{p3}$ and $\mathscr{S}$ simulates the game $Game_{k,1}$. On the other hand, if $\Im_A$ chooses $T \leftarrow G_{p1} \times G_{p2} \times G_{p3}$, $\mathscr{S}$ can simulate the all queries for $Game_{k-1,3}$. Hence, $\mathscr{S}$ uses the output result of the $\Im_A$ for distinguish T. Thus, it has a negligible advantage $ADV2_{\mathscr{S},\Im_A}(\Lambda) = \epsilon$. □

Performance analysis and comparisons

In general, mostly existing CP-ABE has restricted computation, complexity and storage capacity. Therefore, the access control protocol focus on efficient-computing and parameters must address the issue of resource restraints in smart devices. We compare the performance and security attributes of proposed scheme with related scheme such as Cui et al. [4], Zhang et al. [20], Li et al. [12], Zhou et al. [25], Zhang et al. [22] (Table 1).

In this section, we observed the leakage resilience of the existing scheme and also provide the concept of leakage ratio. Then, we compute the leakage ration of the $L_{ratio} = \frac{l}{|sk|}$, where l represents the size of leakage and —sk— represents the size of a secret key. In the proposed scheme leakage size represents as $l \leq logp2$, Cui et al.'s has $l \leq logq$ and Zhou et al. has $l \leq 2logq$. Then, we calculates as $L_{ratio} = \frac{l}{|sk|} = \frac{logp2}{logN} = 1/3$. This leakage makes a significant distinguishable to secret-functional key between all the executed games. The proposed scheme also supports the policy hiding attribute. In Table 2 represents the security comparison between all the comparative schemes, which denotes the security model comparison. We use the standard model to prove the security of the proposed scheme. Hence, the protocol effectively occurs the security threats in comparison to selective and random oracle models.

The existing scheme's estimating the communication overhead for various operations such as: N_{pub}, N_{cpt}, N_{pk}. In these symbols called respectively number of public key, number of ciphertext size, number of secret key. All operations are practically affects among all the communication. As shown in the Table 1, some comparative scheme has less number of transmitted messages. However, proposed scheme is much better than among other platform. Our proposed scheme also support the attributes hiding policy, which the computation cost is linear in the size of user attributes. In Fig. 2 demonstrates the enhancement of communication messages in medical system.

Conclusion

This paper design a secure and efficient CP-ABE based access control system for a smart medical system with policy hiding characteristic. We have also demonstrated the failure of Zhang et al.'s schemes to present efficient big data storage with leakage resilience. In order to improve the Zhang et al.'s scheme, we have proposed an access control protocol. The proposed protocol includes the policy hiding technique. The attribute values of access policies are hidden in a specific encrypted form. Moreover, the proposed scheme security has been proved under the standard model, which ensure security. The study on proposed protocol performance and its comparison with related results are provided, which shows that the proposed scheme is able to resist active and passive attacks and improve efficiency.

Compliance with Ethical Standards

Informed Consent All the authors have agreed to this submission.

Research involving human participants and/or animals This article does not contain any studies with human participants or animals performed by any of the authors.

Disclosure of potential conflicts of interest All authors declare that they have no conflict of interest.

References

1. Amin, R., Islam, S. H., Biswas, G., Khan, M. K., and Obaidat, M. S., Design and analysis of an enhanced patient-server mutual authentication protocol for telecare medical information system. *Journal of medical systems* 39(11):137, 2015.
2. Bellare, M., Pointcheval, D., and Rogaway, P., Authenticated key exchange secure against dictionary attacks. In: *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 139–155: Springer, 2000.
3. Bethencourt, J., Sahai, A., and Waters, B., Ciphertext-policy attribute-based encryption. In: *IEEE Symposium on Security and Privacy-SP'07*, pp. 321–334: IEEE, 2007.
4. Cui, H., Deng, R. H., Lai, J., Yi, X., and Nepal, S., An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures, revisited. *Computer Networks* 133:157–165, 2018.
5. Dolev, D., and Yao, A. C., On the security of public key protocols. *IEEE Trans. Inform. Theory* 29(2):198–208, 1983.
6. Gope, P., and Amin, R., A novel reference security model with the situation based access policy for accessing ephr data. *J. Med. Syst.* 40(11):242, 2016.
7. Goyal, V., Pandey, O., Sahai, A., and Waters, B., Attribute-based encryption for fine-grained access control of encrypted data. In: *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 89–98: ACM, 2006.
8. He, D., and Hu, H., Cryptanalysis of a dynamic id-based remote user authentication scheme with access control for multi-server environments. *IEICE Trans. Inform. Syst.* 96(1):138–140, 2013.
9. Jakobsson, M., and Pointcheval, D., Mutual authentication for low-power mobile devices. In: *International Conference on Financial Cryptography*, pp. 178–195: Springer, 2001.
10. Jia, X., He, D., Kumar, N., and Choo, K. K. R., Authenticated key agreement scheme for fog-driven iot healthcare system. *Wireless Networks* 25(8):4737–4750, 2019.
11. Lai, J., Deng, R. H., and Li, Y., Expressive cp-abe with partially hidden access structures, 2012.
12. Li, J., Ren, K., and Kim, K., A2be: Accountable attribute-based encryption for abuse free access control. *IACR Cryptology ePrint Archive* 2009:118, 2009.
13. Mukhopadhyay, S. C., Wearable sensors for human activity monitoring: a review. *IEEE Sensors Journal* 15(3):1321–1330, 2014.
14. Shao, M. H., and Chin, Y. C., A privacy-preserving dynamic id-based remote user authentication scheme with access control for multi-server environment. *IEICE Trans. Inform. Syst.* 95(1):161–168, 2012.
15. Tran, P. V. X., Yang, G., and Susilo, W., Hidden ciphertext policy attribute-based encryption under standard assumptions, 2016.
16. Wang, H., He, D., Shen, J., Zheng, Z., Yang, X., and Au, M. H., Fuzzy matching and direct revocation: a new cp-abe scheme from multilinear maps. *Soft Comput.* 22(7):2267–2274, 2018.
17. Xu, B., Da Xu, L., Cai, H., Xie, C., Hu, J., and Bu, F., Ubiquitous data accessing method in iot-based information system for emergency medical services. *IEEE Trans. Ind. Inform.* 10(2):1578–1586, 2014.
18. Yan, H., Xu, L. D., Bi, Z., Pang, Z., Zhang, J., and Chen, Y., An emerging technology–wearable wireless sensor networks with applications in human health condition monitoring. *Journal of Management Analytics* 2(2):121–137, 2015.
19. Yang, K., Han, Q., Li, H., Zheng, K., Su, Z., and Shen, X., An efficient and fine-grained big data access control scheme with privacy-preserving policy. *IEEE Internet of Things Journal* 4(2):563–571, 2016.
20. Zhang, X., Jin, C., Li, C., Wen, Z., Shen, Q., Fang, Y., and Wu, Z., Ciphertext-policy attribute-based encryption with user and authority accountability. In: *International Conference on Security and Privacy in Communication Systems*, pp. 500–518: Springer, 2015.
21. Zhang, Y., Chen, X., Li, J., Wong, D. S., and Li, H., Anonymous attribute-based encryption supporting efficient decryption test. In: *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, pp. 511–516: ACM, 2013.
22. Zhang, Y., Li, J., Zheng, D., Chen, X., and Li, H., Towards privacy protection and malicious behavior traceability in smart health. *Pers. Ubiquit. Comput.* 21(5):815–830, 2017.
23. Zhang, Y., Yang, M., Zheng, D., Lang, P., Wu, A., and Chen, C., Efficient and secure big data storage system with leakage resilience in cloud computing. *Soft Comput.* 22(23):7763–7772, 2018.
24. Zhang, Y., Zheng, D., and Deng, R. H., Security and privacy in smart health: Efficient policy-hiding attribute-based access control. *IEEE Internet of Things Journal* 5(3):2130–2145, 2018.
25. Zhou, Y., Yang, B., and Mu, Y., Continuous leakage-resilient identity-based encryption without random oracles. *Comput. J* 61(4):586–600, 2018.