Secure Sharing Model Based on Block Chain in Medical Cloud (Short Paper)

Tao Feng(✉), Ying Jiao, and Junli Fang

School of Computer and Communication,
Lanzhou University of Technology, Gansu 730050, China
fengt@lut.cn

Abstract. The cloud storage and sharing system are widely used in medical systems. The unique characteristics of cloud storage enable healthy data being efficiently delivered and retrieved. Nevertheless, traditional medical cloud system suffers two flaws. For one thing, centralized cloud servers are vulnerable to malicious attack and single point of failure. For another, these systems cannot offer a powerful capability to protect medical health data. Blockchain technology is considered to be one of vital technologies of Bitcoin. In this paper, we propose a security model which combines the cloud storage technology with blockchain technology. Our model adopts Delegate Proof of Stake (DPOS) consensus mechanism to ensure that all nodes have unified state in the network. Additionally, the CP-ABE scheme is introduced into the Proxy Re-encryption to store and share medical data which supports the keywords searching. Moreover, we rank medical institutions that different ranks have different duties. In our secure sharing models, there are no central nodes and it is a distributed environment. It not only can reduce the access overhead of the blockchain but also better resist the collusion attack. Furthermore, our security analysis indicates that the proposed scheme achieves provable security under the q-DBDHE assumption in the random oracle model. Then, the comparisons show that our model is more efficient and practical than previous ones.

Keywords: Medical cloud (MC) · Blockchain · DPOS consensus mechanism · Attribute-based Proxy Re-encryption (AB-PRE) · Privacy-preserving

1 Introduction

1.1 Background and Related Work

As everyone pays more attention to health, medical health data is becoming more and more important. Everyone expects the Medical Cloud (MC) to provide desirable health care in a near future. However, MC is still in many concerns remain to be solved for practical applications. In particularly, security storage and sharing issues of medical data have become the biggest concerns in MC. the traditional medical health system stored the user s data through the Semi Trusted Third Party server (DaSCE) in the cloud, which improves the efficiency of storage, retrieval and sharing. However, if DaSCE was attacked or some medical institutions are tempted by high-value sensitive information, the medical data in the DaSCE must be leaked. Researchers in the medical

X. Wang et al. (Eds.): CollaborateCom 2019, LNICST 292, pp. 429–438, 2019.
https://doi.org/10.1007/978-3-030-30146-0_30

cloud have recently explored this problem. Someone has proposed schemes based on medical cloud. He et al. [1] proposed a private cloud platform architecture which includes interoperability services with CCR standards according to the specific requirements, but the architecture has not secure and private. Kyazze's Health Ticket model [2] helps healthcare providers to access users' health data through the web applications and the model uses CP-ABE to protect the user's privacy, but the single encryption mechanism has been unable to protect user's privacy. Hong et al. [3] proposed a hybrid secret sharing scheme based on attribute encryption, which achieved more efficient access control with dynamic policy updating. Seo et al. [4] proposed a scheme which combines traditional proxy re-encryption with ABE, so a user is able to empower designated users to decrypt the re-encrypted ciphertext with the associated attributes of designated users. These solutions can protect medical health data well, but they have some obstacles in sharing data stage. Literature [5] proposed a searchable KP-ABE based proxy re-encryption, the scheme enables a data owner to efficiently share his data to a specified group of users matching a sharing policy and meanwhile, the data will maintain its searchable property, but its communication overhead is relatively large. These schemes are sound but encryption processes are all required to be carried out in the highly centralized cloud severs, which are vulnerable to malicious attack and the single point of failure. This could lead to sensitive health data breaches. Blockchain technology can solve these problems well. Literature [6] proposed a MedRec scheme, it is a novel, decentralized record management system to handle medical data by using the blockchain technology. MedRec use the features of the blockchain and POW consensus mechanisms for authentication and management, as well as ensuring the confidentiality of shared medical data. Fu et al. employed a better encryption algorithm from NTT Service Evolution Laboratory to enforce the decentralizing Privacy. Instead of using POW for protection, they employed Proof-of-Credibility Score to improve the previous system [7]. Shrier and Chang proposed to create a secure environment for storing and analyzing medical data with blockchain technology [8].

1.2 Our Contribution

In this paper, we efficiently address both security storage, sharing and data privacy issues in Medical cloud (MC) by introducing a security model. In our security model, we focus on the important issues mentioned above, i.e., Decentralization, Privacy-preserving, supporting keyword retrieval, collusion resistance, expressiveness and full Security. We simultaneously solve these issues by combined blockchain and MC with the attributed-based proxy re-encryption. In addition, the improved DPOS consensus mechanism is used to ensure that nodes in the network trust each other. Our rigorous security proofs and comprehensive comparisons with other schemes indicate that the secure sharing model is fully secure and efficient. Specifically, our model is characterized by the following attractive features.

2 System Model

In this section, we will illustrate the basic structure of the sharing model, its threat model and its security model.

2.1 Threat Model

In the proposed scheme, it is assumed that the medical institutions and patients in the alliance have valid identity information. Only the owners of medical data are fully trusted; the cloud server is honest but curious. It will abide by the protocol returning the searched ciphertext to the value node R, but it may steal the shared data and information; the shared requester can be malicious and collude with each other to decrypt the data that they don't have permissions.

2.2 System Architecture

System architecture is depicted in Figs. 1 and 2, There are four entities are involved in the scheme: data owner, cloud server, block chain, first-level medical node alliance group (HL1) and second-level medical node alliance group (HL2).

Data Owners: Patients and medical institutions in the alliance can store relevant medical data. Moreover, they need to encrypted data and set sharing permissions structure. When other medical institutions in the alliance wanted to get the data, they need to meet the permissions in order to decrypt the ciphertext and then achieve the original data.

HL1 and HL2:

1. Storage Phase: When the user started a storage request to the general node O_0 in HL1, O_0 broadcast the message to the entire network and the check node C_0 in HL2 verified the identity of user. If the verification steps are successful, O_0 encrypted the user's data using the ABE and stored it in its own database, and then O_0 broadcast the information about the original ciphertext in the entire network again.
   If over 1/3 of the nodes in the network received this information, O_0 returned to the user a message about accepted the storage request; O_0 send a message about stored the data to the current value node R at this time, R received the message and broadcast to the entire network again. After more than 1/3 of the nodes received the message, R begins to store the data.
2. Sharing Phase: If the medical institution in the alliance wanted to obtain medical data of the certain user. It needs to submit a sharing request to the current value node R at the moment; After received the request, R broadcasts the request information to the entire network, and in HL2, the check node C_1 verified the identity of the institution and determined whether the ciphertext sharing permission was satisfied; If the organization met the sharing permission and more than 1/3 of the nodes received the sharing request, then R use keyword to searched the medical data in the blockchain which was requested. Finally, R will find the corresponding TX block.

Blockchain and Cloud Server:

1. Storage Phase: The ciphertext *CT* of the original user's data was stored in the cloud server, and the cloud server returned the location information LM of the ciphertext; the public-key PK of *R* at this time, sharing permission (A, f), the original encryption key, the storage location information LM and the data digest are encrypted and stored in the TX block, then put them into the blockchain according to the structure of the Merkel tree.
2. Sharing Phase: the medical institution wanted to get the data in the alliance and the value node *R* need to find the corresponding TX block. By using proxy re-encryption for ciphertext CT' and sharing authority structure (A', f'), R can convert the information which is in the TX block and make it satisfied the medical institution. And then, *R* broadcast this conversion information in HL1. If more than 1/3 of the nodes received this information, it means that the medical data can be shared with the organization; Next, this institution get the CT', the location information LM of the data in the cloud server by decryption and ciphertext *CT* of the original data. Through these operations, the medical institution can get the plaintext data. In order to ensure the security of the medical data after sharing, the value node *R* can revoke the sharing request information at any time through the re-encryption algorithm.

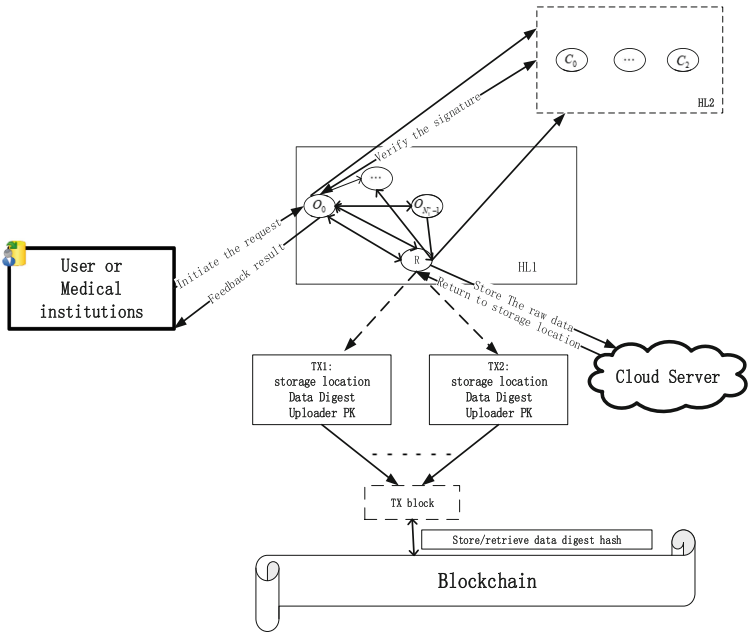

Fig. 1. Storage phase of the security model

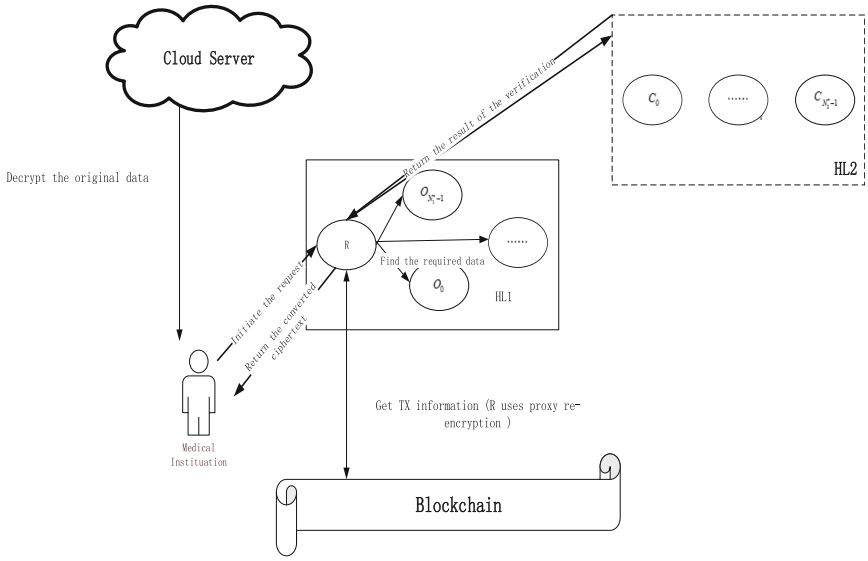

Fig. 2. Data sharing phase of the security model

2.3 Concrete Algorithm

In this section, we will give the specific algorithm construction of our proposed scheme:

1. **Setup** $Setup(\tau, U) \rightarrow (GP, PK, MSK)$: the security parameter of the preset system is τ, the attribute set of the medical institution in the alliance is U. There is a bilinear map $e : G \times G \rightarrow G_T$, G is the additive cyclic group of prime order p and the generator of G is g, $g_1 \in G$. There are the following Hash functions:

$$\begin{aligned} H_1 : (0,1)^{2k} \rightarrow Z_p; H_2 : (0,1)^{2k} \rightarrow G_T; H_3 : (0,1)^* \rightarrow G; \\ H_4 : (0,1)^* \rightarrow G_T; H_5 : (0,1)^k \rightarrow Z_p; H_6 : (0,1)^k \rightarrow G_T \end{aligned} \tag{1}$$

   With choosing the random number $\alpha, \beta \in Z_p$, calculate: $H_x = g^\beta, x \in U$.
   Global parameter: $GP = (p, g, g_1, g^\alpha, e(g,g)\alpha, H_1, \cdots, H_6)$.
   Public key: $PK = (g, g_1, g^\alpha, e(g,g)^\alpha, H_x)$.
   Master key: $MSK = (g^\alpha, \alpha)$
2. **KeyGen** $keyGen(GP, PK, MSK, u_i) \rightarrow (PK_i, SK_i)$: the value node R input *GP, PK, MSK*, data owner's attribute set $u_i \subseteq U$ and the medical institution attribute set $u_l \subseteq U$, R selects random number $\lambda \in Z_p$. The public-private key pair is calculated as follows:

$$SK_i = (u_i, K_i = g^\alpha g^{\alpha\lambda}, P_i = g^\lambda, (K_i = H_3(u_i^n)^\lambda)_{u_i^n \in U})(SK_l \text{ same argument}) \tag{2}$$

$$PK_i = g^{SK_i}(PK_l \text{ same argument}) \tag{3}$$

3. **Re-KeyGen** Re $keyGen(GP, SK_i, (A_l, f_l), PK_l) \rightarrow rk_{i\rightarrow l}$: When the value node R selects the integers $\theta \in Z_p$ and the g^{θ}, g_1^{θ} is calculated; R makes up the shared structure $(A_l^{'}, f_l^{'})$ according to attribute set $u_l \subseteq U$ of the medical institution and the LSSS secret sharing scheme; the re-encryption key is created as:

$$\left\{\begin{array}{l} rk_1 = g^{\alpha} g^{\alpha\lambda} g_1^{\theta} \\ rk_2 = g^{\theta} \\ rk_3 = g^{\lambda H_5(\delta)} \\ rk_4 = C^{'}_{(u_l^{'}, f^{'})} \\ R_i = K_i^{H_5(\delta)} \end{array}\right\} \tag{4}$$

$$rk_{i\rightarrow l} = (u_i, rk_1, rk_2, rk_3, rk_4, R_i) \tag{5}$$

Where $A_l^{'}$ is a $a \times b$ matrix over Z_p, function $f^{'}(a)$ is the attribute of the shared organization; By selecting a row vector $\vec{y} = (d, y_1, \cdots, y_n)$, and $d, y_1, \cdots, y_n \in Z_p$. $\vec{\xi}_{a_m} = \vec{y} \cdot A^{'}_{a_m}$ can be calculated. Among them, d represents the shared data information, $A^{'}_{a_m}$ is the m-th row vector of $A_l^{'}$, and $U_l = \left\{l : f^{'}(a) \subseteq U, 1 \le m \le a\right\}$ is the attribute set in $(A_l^{'}, f^{'})$.

4. **Encrypt the Medical Data:**
   (1) Encrypt the original data $Enc_1(D, (A_i, f_i), PK_i) \rightarrow CT_i$: The value node R use CP-ABE to encrypt the user's public key, the original medical data and the shared permission structure, and then the ciphertext CT_i is generated and store it in the cloud server.
   (2) Encrypt Data digest and other information $Enc_2(PK, LM, D_i, t, (A_i, f_i), k_i) \rightarrow CT_i^{'} \rightarrow TX_i$: The system public key PK, the shared structure (A_i, f_i), the storage location LM of the original data in the cloud, the data digest D_i and the key k_i of the decrypt original data is encrypted by R, and then generate the ciphertext $CT_i^{'}$. R put the $CT_i^{'}$ into the TX block.
5. **Re-Encrypt** $CT_i \mathrm{Re}Enc(rk_{i\rightarrow l}, CT_i, PK_l, (A_l^{'}, f^{'})) \rightarrow CT_l$: The check node C verifies the identity of the medical institution in the alliance which need to get the shared data, and if the verification is successful, R performs the following calculations:

$$CT_l = (X_1, X_2, (A_l^{'}, f^{'}), (Y_l, Z_l)_{l=1}^{N_1^*-1}, \mu) \tag{6}$$

Among them:

$$X_1 = \zeta \cdot e(g, g)^{\alpha \cdot d}, X_2 = g^d, X_3 = g_1^d, \zeta \in G_T \tag{7}$$

$$Y_1 = \frac{(g^{\alpha})^{\xi_{a_1}}}{H_1(f^{'}(1))}, \cdots, Y_l = \frac{(g^{\alpha})^{\xi_{a_1}}}{H_1(f^{'}(N_1^* - 1))} \tag{8}$$

$$Z_l = g^{\tau_1}, \cdots, g^{\tau_l}, \tau_l, \cdots, \tau_l \in Z_p \tag{9}$$

$$\mu = \frac{e(X_1, rk_1) \cdot e(X_2, rk_2)}{\Pi_{l \in U}(e(Y_l, rk_3) \cdot e(Z_l, R_{f(1)}))^{w_l}}, w_l \in Z_p \text{ and } \prod_{l \in U} w_l \cdot \xi_{a_l} = d \tag{10}$$

6. **IndexGen** $Index(GP, D_i^{'}) \rightarrow ID_i$ and ID_l: When R utilizes the global parameter GP, the data digest D_i of original data, and then the MAC_i is calculated; similarly, we can get MAC_l, ID_i and ID_l in Re-encrypt ciphertext.
7. **Re-Decrypt** Re $Dec(SK_l, CT_l) \rightarrow CT_i$: the value node R checks whether the attribute set u_l matches the shared structure (A_l, f_l); If there is a match, the medical institution can decrypt CT_l uses the CP-ABE to get CT_i, and then the decryption keys k_i can be calculated:

$$k_i = \frac{X_1}{\gamma^{\frac{1}{H(v)}}}, \gamma \text{ is the part of ciphertext } v \in G_T \tag{11}$$

$$CT_i = \frac{A_1 \cdot e(A_3, g^{\theta})}{\gamma}, \theta \in Z_p \tag{12}$$

8. **Decrypt the original data ciphertext** $Dec(CT_i, k_i, GP) \rightarrow d$: Using the formula

$$d = \frac{A_1}{\Pi_{i \in U}(e(Y_l, g^{\lambda}) e(X_2, R_{f(1)}))^{w_i}} \tag{13}$$

3 Security Proof

In this section, the security of proposed sharing model is proved in the random oracle model that it is against chosen plaintext attacks (CPA).

Lemma 4.1: Based on the q-DBDHE assumption, if the scheme in [9] is secure against chosen plaintext attacks (CPA) in the random oracle model, our scheme is secure against CPA.

Proof: Suppose there exists a probabilistic polynomial time adversary A can attack our scheme with a non-negligible advantage ε. We prove that the following q-DBDHE game can be solved by the challenger B with the advantage $\frac{\varepsilon}{2}$.

Initialization: Challenger B randomly picks $x, y \in Z_p$ and multiple hash functions $H_1, H_2, H_3, H_4, H_5, H_6$ to calculate $e(g,g)^z = e(g,g)^x e(g,g)^y$. The global parameters $GP = (p, g, g_1, g^{\alpha}, e(g,g)\alpha, H_1, \cdots, H_6)$ and $PK = (g, g_1, g^{\alpha}, e(g,g)^{\alpha}, H_x)$ are sent to the adversary A.

Inquiry 1:

(1) **Private Key Query:** The adversary A queries for the private key SK_U according to the attribute set U and shared permission structure (A_*, f). If U satisfies the shared permission structure (A_*, f), challenger B chooses to output a value at $\{0,1\}$ and the game ends; If U is not satisfied, Challenger B picks a set of data to make $m = (m_1, \cdots, m_n) \in Z_p, m_1 = -1, m \cdot A_* = 0$.

(2) **Re-encrypt Key Query:** Select the attribute set u_l to determine whether it conforms to the shared permission structure (A_l,f). If u_l meets the shared permission structure (A_l,f), challenger B chooses to output the value at $\{0,1\}$, the game ends. Instead, the private key SK_l is obtained; the re-encrypt key $rk_{i\to l} = (u_i, rk_1, rk_2, rk_3, rk_4, R_i)$ is calculated and sent it to the adversary A.

Challenge: The adversary A selects two data digests D_1, D_2 which has equal length and sends them to the challenger B. The challenger B selected one bit attributes from $\theta \in (0,1)$ and encrypt it with the shared permission structure (A_*,f). Then B gets the ciphertext CT_* and sent CT_* to the adversary A. If $e(g,g)^{\alpha^{q+1}s}$ and T are equal, CT_* is a valid ciphertext.

Inquiry 2: Repeat Phase 1 adaptively.

Guess: The adversary A submits the guess θ' of θ. When $\theta' = \theta$, the simulator represented challenger B outputs $T = e(g,g)^{\alpha^{q+1}s}$; when $\theta' \neq \theta$, the simulator represented challenger B outputs $T \neq e(g,g)^{\alpha^{q+1}s}$. In the game, the advantage of the adversary A is $\left|\Pr[\theta' = \theta] - \frac{1}{2}\right|$; if $\theta = 0$, it means that the advantage A can't get any useful information and the probability of guessing correctly is 1/2. When $\theta = 1$, it means that the adversary A can get all the information about the ciphertext and the original data, so the advantage is $1/2 + \varepsilon$. Therefore, the advantage of the probabilistic polynomial time adversary in the q-DBDHE game is $\Pr(\theta' = \theta) - \frac{1}{2} = \frac{1}{2}\left(\frac{1}{2} + \varepsilon\right) + \frac{1}{2}\cdot\frac{1}{2} - \frac{1}{2} = \frac{\varepsilon}{2}$. To conclude, if the adversary has non-negligible advantage ε in the constructed game, he can solve the q-DBDHE problem with the non-negligible advantage $\frac{\varepsilon}{2}$. Based on the q-DBDHE assumption, there is no adversary has significant advantage in our security game and our scheme is secure.

4 Analysis and Comparison

1. **Privacy Analysis of Medical Data Content**

In order to protect medical health data while sharing and storing, our scheme uses DPOS to rank the medical institutions. Moreover, the scheme adopts a combination of the CP-ABE algorithm and the proxy re-encryption algorithm to store and share medical data, which is safer than the symmetrical encryption. The data owners presets the shared permission structure of the medical data, They use the attribute-based proxy Re-encryption algorithm stores the complete ciphertext of original data in the cloud server, and stores important information such as storage location and data digest in the blockchain in order to facilitate the searching and sharing of the medical data. The requesters want to obtain the medical data, they need to find the corresponding block by the keyword searching in blockchain, and then they can find the ciphertext in the cloud server. In our security model, the ciphertext is stored separately, so our model realizes the privacy of medical data content.

2. **Collusion Resistance**

When the value node R generates the re-encryption key, R could verify the attribute set $u_l \subseteq U$ and share permission structure (A_l, f) of medical institutions through the X_2. In our model, rk_3, rk_4, R_i and $\delta \in G_T$ are associated; rk_1, rk_2, rk_4 and $\theta \in Z_p$ are associated; $\delta \in G_T$ is encrypted by rk_4, shared permissions (A_i, f) and $\theta \in Z_p$. Therefore, when rk_1, rk_2, rk_3, R_i is hacked lead to the original data is changed, the re-encrypted ciphertext will also be invalid according to the above relationship. If the attribute sets, sharing permissions, and rk_4 are tampered, you can verify it by calculating the following formula:

$$e(X_2, H_6(X_1, X_2, (Y_l, Z_l)_{l=1}^{N_1^*-1}, u_i, (A_i, f))) = e(g, g) \tag{14}$$

3. **Scheme Comparison**

In this paper, we compared the proposed scheme with some of classic cloud storage schemes, as is shown in Table 1. Among the schemes, the scheme of Akinyele [10] and Hong [3] are the single attribute-based encryption cloud storage scheme. The schemes of Seo [4], Shi [11], and Luo [12] use attribute-based proxy re-encryption, but they rely on third parties to complete storage and sharing. In particular, the Seo's solution required multiple data centers, so it is difficult to ensure that the medical data has not tampered during data is transported and stored. Moreover, except for the Shi's solution, other schemes which the ciphertext are not searchable, these schemes have hindered the data sharing. Our solution can realize all the functions on the table at the same time, and select the required information according to the actual situation, so it is more suitable for the practical application of sharing.

Table 1. Comparison of sharing schemes.

Scheme	Key-word search	Attribute encryption	Proxy re-encryption	Attribute-based Proxy re-encryption	Blockchain technology	No third party
[10]	×	√	×	×	×	×
[3]	×	√	×	×	×	×
[4]	×	√	√	√	×	×
[11]	√	√	√	√	×	×
[12]	×	√	√	√	×	×
our	√	√	√	√	√	√

5 Conclusion

In order to ensure the security of medical health data in the process of storage and sharing, we proposed a way to combine blockchain and cloud storage; the attribute-based encryption was introduced into the proxy re-encryption which supports the

keywords searching to store and share the medical data in the security situation. This way avoids the problem that some share requesters want to secondary forward shared data. The ciphertext of original data and ciphertext of re-encrypted are stored separately, which has the possibility of preventing the collusion. Through the security proof and privacy preserving analysis, our model has practicality. Compared with other existing models, the proposed model gives a better performance in terms of sharing medical data and privacy preserving.

References

1. He, C., Fan, X., Li, Y.: Toward ubiquitous healthcare services with a novel efficient cloud platform. IEEE Trans. Biomedical Eng. **60**(1), 230–234 (2013)
2. Kyazze, M., Wesson, J., Naude, K.: The design and implementation of a ubiquitous personal health record system for South Africa. Stud. Health Technol. Informatics **206**(206), 29–41 (2014)
3. Cheng, H., Min, Z., Deng-Guo, F.: Achieving efficient dynamic cryptographic access control in cloud storage. J. Commun. **32**(7), 125–132 (2011)
4. Seo, H.J., Kim, H.W.: Attribute-based proxy re-encryption with a constant number of pairing operations. J. Inf. Commun. Convergence Eng. **10**(1), 53–60 (2012)
5. Liang, K., Susilo, W.: Searchable attribute-based mechanism with efficient data sharing for secure cloud storage. IEEE Tran. Inf. Forensics Secur. **10**(9), 1981–1992 (2017)
6. Azaria, A., Ekblad, A., Vieira, T.: MedRec: using blockchain for medical data access and permission management. In: 2nd International Conference on Open and Big Data (OBD), pp. 25–30. IEEE (2016)
7. Fu, D., Fang L.: Blockchain-based trusted computing in social network. In: IEEE International Conference on Computer & Communications, pp. 19–22. IEEE (2017)
8. Kuo, T., Ohno-Machado, L.: Model chain: decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. Int. J. Netw. Secur. Appl. **1802**, 01746 (2018)
9. Liang, K., Susilo, W.: Searchable attribute-based mechanism with efficient data sharing for secure cloud storage. IEEE Trans. Inf. Forensics Secur. **10**(9), 1981–1992 (2017)
10. Akinyele, J.A., et al.: Securing electronic medical records using attribute-based encryption on mobile devices. In: 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, pp. 75–86. ACM (2011)
11. Yanfeng, S., Jiqiang, L., Zhen, H.: Attribute-based proxy re-encryption with keyword search. PLoS ONE **9**(12), 116325 (2014)
12. Luo, S., Hu, J., Chen, Z.: Ciphertext policy attribute-based proxy re-encryption. In: Soriano, M., Qing, S., López, J. (eds.) ICICS 2010. LNCS, vol. 6476, pp. 401–415. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-17650-0_28