Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8859961, 11 pages
https://doi.org/10.1155/2020/8859961

Research Article

A Medical Data Privacy Protection Scheme Based on Blockchain and Cloud Computing

Liang Huang[1,2] **and Hyung-Hyo Lee**[2]

[1]*School of Mathematics & Computer Science, Shangrao Normal University, Shangrao 334001, China*
[2]*Department of Computer and Software Engineering, Wonkwang University, Iksan 54538, Republic of Korea*

Correspondence should be addressed to Liang Huang; 305108@sru.edu.cn

Received 29 June 2020; Revised 19 August 2020; Accepted 12 September 2020; Published 26 September 2020

Academic Editor: Hongju Cheng

With the features of decentralization and trustlessness and through distributed data storage, point-to-point transmission, and encryption algorithms, blockchain has shed new light on the security and protection of medical data, and it can resolve the contradiction between data sharing and privacy protection with proper security strategies. In this paper, we integrate the strengths of both blockchain and cloud computing and build the privacy protection scheme for medical data based on blockchain and cloud computing. This scheme introduces cloud computing and provides services to blockchain nodes with cloud server computing; meanwhile, it collects, analyzes, processes, and maintains medical data in the identity authentication interface and solves the insufficient computing abilities of some nodes in blockchain so as to verify the authenticity and reliability of data. The simulation experiment proves that the proposed scheme is effective. It can achieve the secure protection and integrity verification of medical data and address the problems of high computing complexity, data sharing, and privacy protection.

1. Introduction

Intelligent hospitals are having increasing demands for information security, and it has become extremely urgent to protect personal private data of patients. Currently, these hospitals have been focusing on how to use convenient internet medical services to prevent the medical information system from being attacked and personal information from being stolen [1]. As blockchain and cloud computing come to maturity, related techniques have achieved rapid development in medical and health services, including medical informatization, mobile healthcare, medical e-commerce, wearable devices, and online medical services. The blockchain connects the participants in a peer-to-peer manner. The participants jointly maintain a system and express the cooperation rules through consensus mechanism and smart contract, so as to achieve a more flexible cooperation mode [2]. The concept of smart contract appeared in 1994 and laid the foundation for bitcoin. A smart contract is a set of commitments defined in digital form, including agreements on which contract participants can execute these commitments [3]. In a broad sense, blockchain technology must include four aspects: point-to-point network design, application of encryption technology, implementation of distributed algorithm, and use of data storage technology. Others may involve distributed storage, machine learning, VR, internet of things, big data, etc. In a narrow sense, blockchain only involves data storage technology, database or file operation, etc. [4]. Apart from conventional encryption methods, proxy reencryption and attribute-based encryption (ABE) can also be used in medical data sharing and patient privacy protection [5]. In traditional encryption methods, the client first downloads and decrypts locally encrypted text data. Then, before sending to the specified client, the client encrypts the data with the public key of the specified client, who can decrypt the data, but it requires plenty of network overhead and operating costs and it also occupies the client's limited memory, multiplying the client's costs [6]. Proxy reencryption is to convert the ciphertext encrypted by A's public key into the ciphertext to be decrypted by B's private key so as

to realize password sharing. Proxy reencryption means that a client can decrypt the ciphertext of another associated client without leaking users' private key and plaintext, which is mainly end-to-end [7]. In ABE, a data owner can set an access strategy authority in data encryption, and only those clients that satisfy this authority can decrypt the text in order to accomplish data sharing and personal privacy protection, which is one-to-many [8]. Based on attribute-based encryption (ABE), the problem of private data sharing can be solved by reasonable configuration and sharing strategy. According to the embedded objects, ABE can be divided into KP-ABE (Key-Policy ABE) and CP-ABE (Ciphertext-Policy ABE). With the popularization of intelligent healthcare, the medical institutions can have the data stored in the cloud to save equipment cost and lower costs. For the sake of data security and personal privacy protection of patients, some medical establishments need to encrypt the data in advance to form ciphertexts. Besides, they need other medical institutions to share certain ciphertexts frequently and prevent anyone (including cloud service providers) from cracking these data ciphertexts. In blockchain and cloud computing, the combination of decentralization and tamper-proofing of blockchain with the nodes of distributed cloud computing can help health institutions to carry out security and privacy protection of patient data at a lower cost and achieve data interaction among medical organizations. These will have a profound impact on the development of future healthcare industry.

The special contributions of this paper include the following:

(i) Aiming at data sharing and patient privacy protection of intelligent hospitals, we explore in-depth conventional encryption methods, proxy reencryption, attributed-based encryption, and so forth. Additionally, we also investigate how to apply blockchain and cloud computing technology in intelligent medical scenarios

(ii) To overcome the highly complex computation brought by encryption, we adopt the proxy reencryption method and ABE method to provide a specific access control mechanism to users and design the data sharing and replacement and privacy protection rule participated by the cloud service side

(iii) We propose a distributed medical data privacy protection scheme, bring in a cloud computing pattern, and designed blockchain-based distributed data management architecture to strengthen the computing power of the user side. Meanwhile, we also use the private chain in blockchain to ensure the security of patient data information

(iv) The simulation experiment has verified the effectiveness of the method in this paper. With blockchain and cloud computing, not only healthcare data can be effectively shared among medical institutions, but also the privacy of patient information can be assured

The remainder of this paper is organized as follows. Section 2 discusses related works, and the use of proxy reencryption for authorization management and access control in cloud computing is outlined in Section 3. The medical data privacy protection scheme based on blockchain and cloud computing is presented in Section 4. Section 5 shows the experimental simulation results, and Section 6 concludes the paper with a summary and proposed direction for future research.

2. Related Work

Medical data has precisely recorded people's illnesses, and medical records and the secure storage and sharing of medical data and patient privacy protection have increasingly become a priority to build intelligent hospitals. Traditional data access control technology builds and implements a safety access strategy with a completely reliable server, making it difficult to get adapted to the distributed network environment in modern times. Featured by decentralization and trustlessness, blockchain has given people a brand-new idea through distributed data storage, reliable point-to-point transmission, a consensus mechanism, and encryption algorithms [9]. In the security demand under the cloud computing environment in recent years, ABE is an important technological means, and the ABE access control mechanism has been studied extensively in the computing environment. As an encryption mechanism that uses attribute as a public key, the mechanism, in essence, links users with ciphertexts through the attribute. Its flexibility of encryption and access control form has greatly ensured the security of cloud data storage [10]. In the meanwhile, it has also achieved fine-grained access and become the key technique for secure cloud storage access control. However, the traditional ABE mechanism fails to completely guarantee data confidentiality, effectively prevent collision attack, or satisfy the forward and backward security of attribute revocation and the huge computing costs caused by revocation. It will be a significant core of research to apply blockchain into cloud computing and use the security mechanism of blockchain to enhance the secure storage and performance of cloud computing. The integration of blockchain and cloud computing plus proper security strategy can solve the contradiction between data sharing and privacy [11].

This paper has brought forth a distributed medical data privacy protection scheme based on blockchain and cloud computing technology with an aim at the open-ended question brought by data sharing of intelligent hospitals and personal privacy protection of patients. Concretely, on the one hand, the scheme has introduced a cloud computing pattern and designed blockchain-based distributed data management architecture for intelligent hospitals, in which it uses a consortium chain in the blockchain and ensures the security of user information in order to guarantee the operating efficiency of blockchain and reduce the computing burden of the user side. Besides, to handle the highly complex computing caused by encryption, it has used proxy reencryption technology and ABE technology to offer specific access control mechanisms to users. The access of every user is based on condition and attribute, which provides a secure exchange

of patient information for every doctor. The response side encrypts all medical data. The cloud nodes process the medical data transmitted to get and return the final ciphertext to the request side. On the other hand, it has designed the data sharing and replacement as well as privacy protection rules with the participation of the cloud computing service side, and it can greatly solve the difficulties in secure storage and sharing of intelligent hospitals.

The underlying communication of blockchain generally adopts P2P communication. P2P technology makes the communication on the network easy and direct and reduces the dependence on the intermediate server to the minimum. P2P technology has the characteristics of decentralization, scalability, robustness, high cost performance, and load balancing. Consensus mechanism is the core of blockchain, which maintains the normal operation of blockchain. Consensus mechanism is an algorithm to reach consensus on the order of things in a period of time. Common consensus mechanisms include proof of work (POW), proof of stake (POS), and practical Byzantine fault tolerance (PBFT). Consensus mechanism ensures that the uniqueness of information and data cannot be tampered with. Taking advantage of this, blockchain technology can be widely used in intelligent asset management, such as intellectual property protection and domain name management, to ensure that the contract is not tampered with. At present, relevant researchers all over the world have been studying medical data sharing and privacy protection. He et al. has proposed a medical data sharing model of cloud storage, which adopts the distributed sharing mechanism and which meets the interoperability requirements of CCR standard [12]; however, there is still a huge gap with the data security and privacy protection as required by intelligent hospitals. Seyedmostafa et al. has built a portable medical system architecture, which supports data security and privacy protection through the CIA/HIPAA protocol, but which does not meet the requirement of interoperability [13]. Liang et al. have used the CCR standard and designed a solution—HealthVault, which is a web medical and health record system and which adopts the client-server pattern. All medical data are stored in a third-party server, so security and reliability cannot be guaranteed [14]. The Healthticket model designed by Kyazze et al. enables doctors to access medical data of patients through the web app [15]. This model ensures the private information of patients with CP-ABE mechanism, but the access requires multiple licenses. The security, privacy, and interoperability of all these models are difficult to meet the requirements of intelligent healthcare. However, blockchain technology completes permission validation through a third party, which has solved the above problems satisfactorily, balanced medical data sharing and privacy protection, eliminated central nodes, and improved access efficiency.

Proxy reencryption is a key conversion mechanism between ciphertexts and it was proposed by Cheng et al. Wang et al. has given its normative formal definition in the 2005 Network & Distributed System Security Symposium (NDSS) and the 2007 ACM Conference on Computer and Communications Security and constructed the one-way proxy reencryption algorithm [16, 17]. Based on the above two studies, Xu has constructed the first valid two-way proxy reencryption algorithm [18]. Afterward, Yang et al. have also constructed the secure one-way proxy reencryption scheme without bilinear pairing [19]. Ateniese et al. had configured the privacy proxy reencryption algorithm in line with CPA security. As for ABE, Fan et al. had constructed the KP-ABE algorithm to support monotonous access for the first time, and the ciphertext uses the attribute for encryption [20]. The key is tied to user access strategy and only when the access strategy of the key matches the attribute of the passphrase can the user correctly decrypt the passphrase. Willison et al. had raised a secure and unbounded ABE algorithm [21], the size of whose attribute set is not confirmed when initializing the public parameters. Moreover, the available attributes are infinite polynomial orders, and new attributes can be added in the specific implementation. Hakak et al. had improved the ABE algorithm, which had extended the decryption condition to the universal monotonous access control and adopted a fine-sorted access control key [22]. It has greatly expanded the coverage of the ABE algorithm [23]. Later, Hussein et al. had come up with an ABE algorithm approximate to actual access control, but loopholes still exist in the security [24]. Conti et al. had put forward an ABE algorithm for DBDH problems, but the access mode is merely a simple attribute operation without reaching universal access control [25]. Integrating blockchain and cloud computing in the research of secure storage of healthcare data has found a new direction for the relevant theoretical research of information security and promoted extended applications of blockchain in the fields, which involve sensitive data such as intelligent healthcare. In this sense, it has certain practical value [26].

3. Use of Proxy Reencryption for Authorization Management and Access Control in Cloud Computing

When a cloud hospital needs to share the data authorization with another hospital, it needs to get the other's public key. Thus, it needs to generate a corresponding switch key for every user and then sends it to the cloud. When a user requests access to these data resources, the cloud will return the encrypted text of data and the corresponding key ciphertext according to the user's public key after verifying the identity authentication and authorization authentication, and the user decrypts these two ciphertext files to get the original plaintext resources of the corresponding data [27].

The cloud needs to generate a reencrypted ciphertext for every authorized user, and those unauthorized users have no right to obtain the reencrypted ciphertext of other users [28]. Even if unauthorized users do get the reencrypted ciphertext, they cannot decrypt the corresponding plaintext data. When applying ABE in proxy reencryption, it can authorize more than one user with the same group of attributes at one time. The procedure of proxy reencryption is as follows:

(1) Hospital A requests the cloud service provider to generate its pair of public and private keys and encrypts

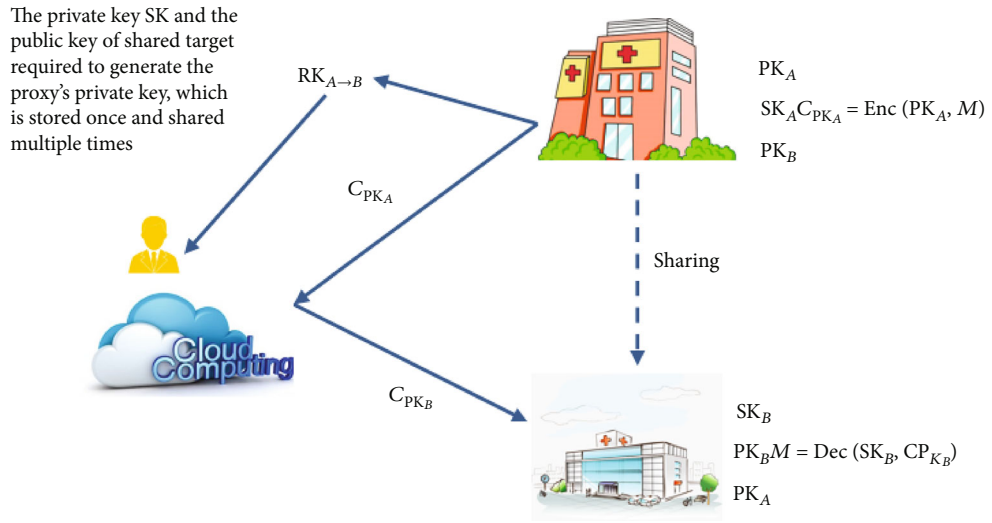

Figure 1: Sketch of proxy reencryption.

the plaintext M of medical data with its public key C_{PKa} to get the ciphertext C_{PKa} = Enc(PK_A, M). Here, M is what Hospital A wants to give to Hospital B.

(2) The cloud service provider generates a pair of public and private keys and returns them to Hospital A. After sending C_{PKa} to the cloud service provider, Hospital A also calculates for the cloud service provider and generates the specific key $RK_{A\to B}$.

(3) The intermediate proxy uses the key $RK_{A\to B}$ generated by Hospital A to change the ciphertext C_{PKa} into the encrypted text C_{PKb}, which can also be decrypted, by the private key of Hospital B. Here, the proxy only provides conversion service, and it cannot get the original plaintext data resources.

(4) Later, the proxy will send the encrypted text data C_{PKb} to Hospital B.

(5) After receiving the ciphertext from the proxy, Hospital B decrypts and gets the plaintext data M of medical data, secretly shared by Hospital A.

The sketch of proxy reencryption is shown in Figure 1.

The above proxy reencryption process has released the burden of Hospital A, which only needs to generate the key of the proxy while the transmission of specific medical data, the encrypted conversion of data, and the file storage are all completed by the cloud service provider. Proxy reencryption can achieve the sharing of ciphertext medical data in the cloud without leaking the decryption key of the data owner. The data can be stored once and shared many times, and only the shared key needs to be generated for the control of authority [29].

4. Medical Data Privacy Protection Scheme Based on Blockchain and Cloud Computing

4.1. Proxy Reencryption Based on Paillier and RSA. We adopt the proxy reencryption of Paillier homomorphism and the RSA algorithm to prevent shared medical data from leaking. If an encrypted function only satisfies the addition homomorphism, it can only be added and subtracted; if an encrypted function only satisfies multiplicative homomorphism, it can only perform multiplication and division. The Paillier algorithm is homomorphic to addition, and the RSA algorithm is homomorphic to multiplication. In an untrusted cloud storage, when the confidentiality of data cannot be guaranteed, the proxy reencryption part is used for reencryption, and the part is used for authorization. In the untrusted open environment of the third party, it can ensure the confidentiality of sensitive data in cloud storage. In homomorphic encryption, the private key encrypts medical data and only the client has the public key. In the keys generated by using proxy reencryption, even if a malicious attacker gets one of them, the attacker still needs another different key for decryption. If the attacker gets all these encrypted data, he cannot decrypt and get the original plaintext data between the client and the server. This also makes sure that even the processor cannot access the information of the data [30]. The algorithms begin with initialization and outputs from the central authentication center the pair of public and key keys, the master key of the center, the public key of the system, and the common parameters. Below are the specific implementation steps.

Step 1. Generate a pair of public and private keys.

Hospital A and Hospital B request the cloud service provider to generate their public keys and private keys, respectively. After the provider generates a pair of a public key and private key for Hospital A and Hospital B separately, the cloud service provider will return to Hospital A and Hospital B.

Step 2. Randomly choose two relatively big and independent prime numbers p, q to make

$$(pq, (p-1)(q-1)) = 1. \quad (1)$$

Step 3. Calculate

$$n = pq\,\varphi(n) = (p-1)(q-1),$$
$$e \text{ makes } \mathrm{Gcd}(e, \varphi(n)) = 1, \tag{2}$$

$$c = m^e \bmod n, \tag{3}$$

$$\lambda = cm(p-1, q-1), \tag{4}$$

in which m is the information to be encrypted.

Step 4. Choose a random integer g to make $g \in Z_n^*$.

Step 5. Use Equation (4) below and calculate the existence of modularized multiplicative inverse to determine n and separate the sequence of g.

$$\mu = (L(c\lambda \bmod n_2)) - 1 \bmod n, \tag{5}$$

in which, function L is defined as the following equation:

$$L(w) = w - \frac{1}{n}. \tag{6}$$

Step 6. The public key is (n, g) and the private key is (λ, μ).

Step 7. Generate the encrypted file.

Hospital A first uses RSA encryption to calculate and encrypt data to generate the encrypted file C1. Then, Hospital A encrypts according to the second layer, encrypts the key of RSA with its public key, and generates the encrypted file C2. Finally, Hospital A uploads two encrypted files: C1 and C2 into the server.

$$\text{Encrypt} \longrightarrow \mathrm{Enc}(m, pk). \tag{7}$$

$$c = gm \cdot n^r \bmod n^2. \tag{8}$$

Step 8. Make m the information to be encrypted and $m \in Z_n$.

Step 9. Randomly select r and make $r \in Z_n^*$.

Step 10. Calculate the ciphertext:

Step 11. Construct the key of proxy reencryption.

Hospital A requests the public key of Hospital A from the cloud service provider. The provider will return this public key to Hospital A. Hospital A uses the public key of Hospital B and its private key to generate the reencryption key, and then Hospital A uploads the newly generated reencryption key into the server.

Step 12. Calculate the public key and private key (Rsk, Rpk).

Step 13. The Paillier algorithm generates the reencrypted ciphertext and the public key (Rpk) is sent to the cloud computing server.

For a given public key(Rpk) and the second-layer ciphertext, this algorithm can use the reencryption key and generate the first-layer ciphertext of the public key (Rpk). The server uses the reencryption key and the ciphertext uploaded by Hospital A to conduct proxy reencryption computing and generates new ciphertext.

Step 14. Hospital B requests data and decrypts $\longrightarrow \mathrm{Dec}(c, sk)$.

Hospital B requests the cloud server to decrypt the data and the corresponding ciphertext. The cloud server sends the reencrypted text to Hospital B. Hospital B decrypts the ciphertext, gets the key, and uses RSA for decryption to get the original plaintext data.

Step 15. Ciphertext $c \in Z_n^*$.

Step 16. Compute the information.

$$m = \frac{L(c\lambda \bmod n^2)}{L(g\lambda \bmod n^2)} \bmod n. \tag{9}$$

4.2. Measurement of Ability of This Scheme against Malicious Attacks. Firstly, make the client set to implement the encryption task ρ_T. For the ith responder in ρ_T, its encrypted data is a m-dimensional vector, represented by s_i. So, $s_i = \{s_{i,j}, j = 1, \cdots, m\}$. After receiving the encrypted data, the cloud node EN_T will request ρ_T the credibility of every client in the response side to the central authentication center.

The reliability measurement s_i is weighed through the difference between s_i and the final result s_T. Here, we have defined the extent of difference between s_i and s_T as the square of Euclidean distance between s_i and s_T, which can be calculated through the following equation:

$$d_i = \sum_{j=1}^{m} \left(s_{i,j} - s_{T,j}\right)^2, \tag{10}$$

in which, the smaller the value of d_i, the higher the credibility of s_i. The degree of difference is the extent of difference among the values of variables, and it is used to measure the safety risk.

When the central authentication center receives the $\{d_i : i \in \rho_T\}$ from the cloud node EN_T, it needs to find the median of difference $\widehat{d}$. Introduce the adjustment parameter δ, and for the response side of the ith encryption task, if the difference of encrypted data is $d_i \le \widehat{d} + \delta$, the credibility of this user will increase. Besides, the smaller the d_i, the more the increase of the credibility. If $d_i > \widehat{d} + \delta$, then the credibility of this client decreases. In addition, the bigger the value of $d_i - \widehat{d}$, the more the reduction of the credibility. After getting the credibility r_i before implementing the current encryption task of the ith client in ρ_T,

Table 1: Attributes of different dimensions of encrypted medical data.

No.	Item name	Unit	Ref	No.	Item name	Unit	Ref
1	White blood cell	10^9/L	4–10	16	Monocyte number	10^9/L	0–0.8
2	Red blood cell	10^{12}/L	3.5–5.5	17	Eosinophil number	10^9/L	0.05–0.5
3	Hemoglobin	g/L	110–160	18	Basophil number	10^9/L	0–0.1
4	Hematocrit	%	36–50	19	Red cell distribution width-coefficient variation	10^9/L	10.9–15.3
5	Mean corpuscular volume	fL	82–100	20	Red cell distribution width-standard deviation	%	37–54
6	Mean corpuscular hemoglobin	pg	26–32	21	Platelet distribution width	fL	9–17
7	Mean corpuscular hemoglobin concentration	g/L	320–360	22	Mean platelet volume	fL	9–13
8	Platelets	10^9/L	100–300	23	Plateletcrit	%	0.17–0.3
9	Lymphocyte percentage	%	20–40	24	Platelet-larger cell ratio	%	13–43
10	Neutrophil percentage	%	50–70	25	Erythrocyte sedimentation rate		0–15
11	Monocyte percentage	%	3–8				
12	Eosinophil percentage	%	0.5–5				
13	Basophil percentage	%	0–1				
14	Lymphocyte number	10^9/L	0.8–4				
15	Neutrophil number						

the central authentication center has the following equation to calculate the credibility of this client:

$$r_{i+1} = r_i + \frac{\operatorname{sign}\left(\widehat{d} + \delta - d_i\right) + 1}{2} \cdot (1 - r_i) \cdot \exp\{-u \cdot d_i - \gamma\} + \frac{\operatorname{sign}\left(\widehat{d} + \delta - d_i\right) - 1}{2} \cdot r_i \cdot \left(1 - \exp\left\{-v \cdot \left(d_i - \widehat{d}\right) - \eta\right\}\right), \tag{11}$$

in which, u, γ, v, and η are the parameters to confirm r_{i+1}, and their values are all bigger than 0. sign (x) is a sign function, and it is defined as follows: if $x > 0$, sign $(x) = 1$; if $x = 0$, sign $(x) = 0$; and if $x < 0$, sign $(x) = -1$. By selecting the proper value of δ, $d_i < \widehat{d} + \delta$ always sustains when the user accesses normally, and it can eliminate malicious accesses and attacks from the client set with increased difference.

After getting $d_i'(i \in \rho_T)$, first, find the median $\widehat{d}'$ in the sequence of differences. It can be learned from Equation (11) that parameters γ and η have decided the rates at which the credibility converges to 0 and 1, respectively.

For the i user in ρ_T, if $d_i' < \widehat{d}'$, it is deemed as normal access. At this time, we introduce the adjustment parameter δ', and its value is a positive integer. The credibility iteration formula has become the following from Equation (11):

$$r_{i+1} = \begin{cases} r_i + (1 - r_i) \cdot \exp\left\{-u' \cdot d_i' - \gamma\right\}, & \text{if } d_i' < \widehat{d}', \\ r_i, & \text{if } \widehat{d}' \le d_i' \ge \widehat{d}' + \delta', \\ r_i \cdot \exp\left\{v' \cdot \left(d_i' - \widehat{d}'\right) - \eta\right\}, & \text{if } d_i' > \widehat{d}' + \delta', \end{cases} \tag{12}$$

in which, u' and v' are two new parameters. u' is smaller than u, and a smaller u' can avoid too much difference in the client's credibility during the iteration of Equation (12). Likewise, v' should also be smaller than v.

5. Simulation Experiment and Analysis

When conducting a simulation experiment, we use the data of the patient's routine medical checks. The data is a 25-dimensional vector, and the numerical value of every dimension can be seen in Table 1. In order to complete every encryption task τ, the processor of the encryption task ρ_T will firstly receive a 25-dimensional medical data vector. Then, it encrypts every element in the vector and sends the encrypted result to the cloud node EN_T where it is located. As this scheme uses the frameworks of Hadoop and Spark in the side of cloud computing, it has higher storage and computing abilities. It can respond in a timely manner to the requests of users and complete the uploading, computing, and downloading operations of users, so it can achieve the purpose of dynamic sharing and patient privacy protection.

For every client, its credibility is initialized as 0.5 and according to Equations (11) and (12), the client's credibility increases when providing the accurate data and the credibility decreases when providing wrong data.

The impact of different values of the parameter γ on credibility can be reflected from the changes in the client's credibility when n increases. Make n represent the number of encryption tasks to be implemented by the client. As shown in Figure 2, if the client can constantly provide correct data, thenγdecides the speed at which its credibility is converged to 1. Besides, the bigger the value of γ, the faster its credibility is converged to 1. However, when the value γ is too big, it can be easily attacked internally and externally. Therefore, γ should not be too big, and normally, it is set $\gamma \in [2, 3]$.

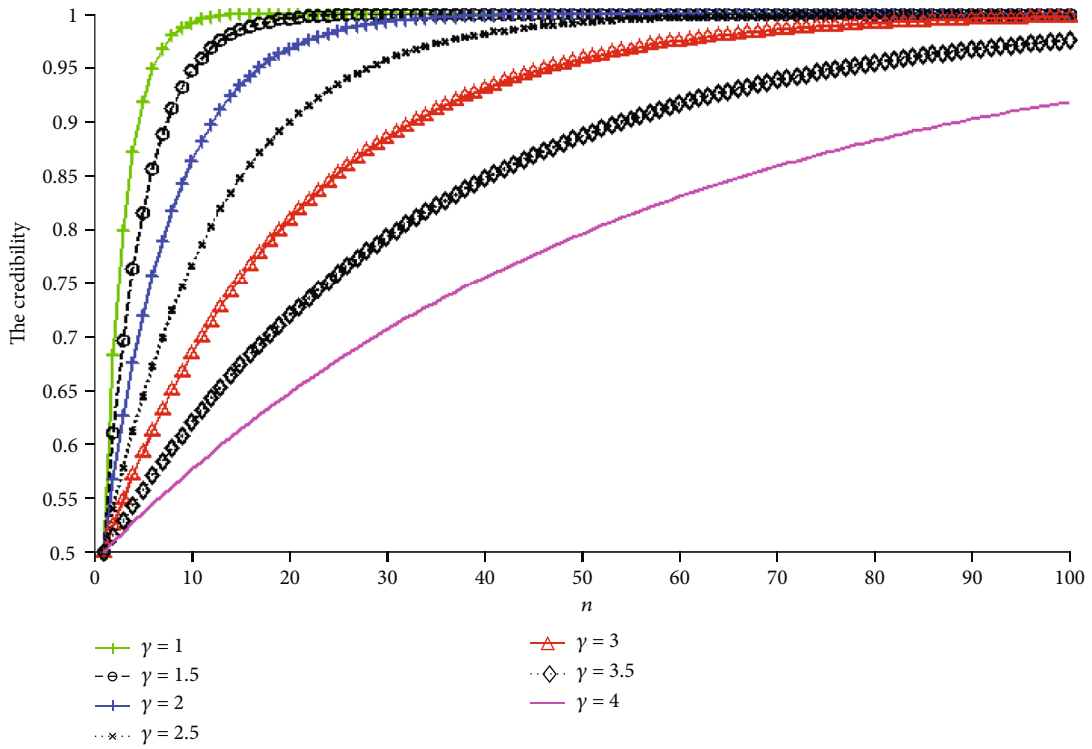

Figure 2: Impact of γ on credibility.

The value of η changes from the initial value of 0.03 to 0.28 at a step-length of 0.05. As indicated in Figure 3, η determines the speed at which that client's credibility is converged to 0. Besides, the value of η cannot be too big; otherwise, the credibility will drop too fast when the client generates wrong data due to various accidental factors, which should be avoided. Moreover, the value of η cannot be too little, either; otherwise, it will give too little punishment to the credibility of dishonest clients and lead to further attacks. The values of γ and η shall meet the requirement of $\exp\{-\gamma\} < 1 - \exp(-\eta)$. In this paper, it is set as follows: $\eta = 0.13$.

In order to analyze the impact of parameters u, v, u', and v' on updated credibility, this paper has set the scenario, which includes 100 encryption tasks. These 100 client sides need to handle 100 encryption tasks. In the initial stage, the initial credibility of every client handling the encryption task is 0.5. In all encryption processing, we assume that there exist 10 dishonest clients and set $\delta = 0.15$.

When analyzing the impact of parameter u on credibility update, we randomly select a normal client and observe the change of credibility over the number of tasks n. Here, the values of u include 5, 20, 50, 80, and 100. For every value of u, we experiment 100 times and summarize the changes of the mean value of that client's credibility when n increases from 1 to 100. As can be seen from Figure 4, the smaller the value of u, the faster the client's credibility is converged to 1. When updating the credibility through Equation (12), the smaller the value of u, the bigger the value of $\exp\{-u \cdot d_i - \gamma\}$ and the more the increase in the client's credibility after giving one correct data. When u is 0, the increase of credibility is completely decided by γ and it cannot filter different clients. Therefore, the value u cannot be too small; otherwise, the client can easily get higher credibility and cause potential security risks. Generally, it is set $u \in [50, 100]$.

Likewise, the impact of v credibility update is analyzed. The values of v are 0.001, 0.005, 0.01, 0.05, and 0.1. In particular, the value of v is much smaller than that of u because the difference in data of normal clients is usually very close and approximates to 0. As indicated in Figure 5, the bigger the value of v, the faster the credibility of dishonest clients is converged to 0. According to Equation (12), when v approximates 0, the decrease of credibility is determined by parameter η. In order to avoid the client's credibility falling too much due to the occasional provision of few wrong data, the value of v cannot be too small, and generally, it is set as $v \in [0.005, 0.01]$.

When analyzing the impact of u' on credibility, its values are set as 0.001, 0.005, 0.01, 0.05, and 0.1, and meanwhile, make $\delta' = 35$. Generally, the value u' is smaller. Figure 6 has shown the changes of credibility when u' takes different values. It can be seen that the impact of u' is similar to that of u; in other words, the smaller the u', the faster the credibility is converged to 1. Considering the difficulty to set credibility, the value u' cannot be too small, and normally, it is as follows: $u' \in [0.01, 0.05]$.

Figure 7 shows the changes of credibility when v' is given the values of 0.001, 0.005, 0.01, 0.05, and 0.1. The bigger the value of v', the faster the credibility is converged to 0. After all medical data are normalized, within the range of $[0, 1]$, the credibility is arranged according to the order of difference

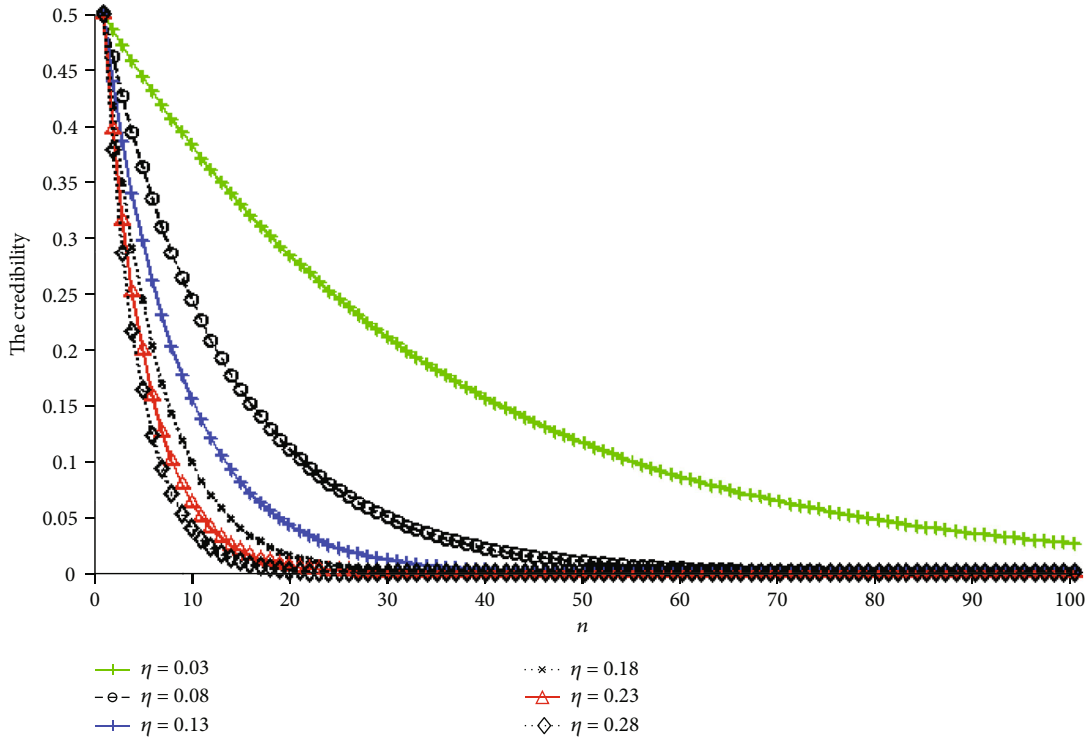

Figure 3: Impact of η on credibility.

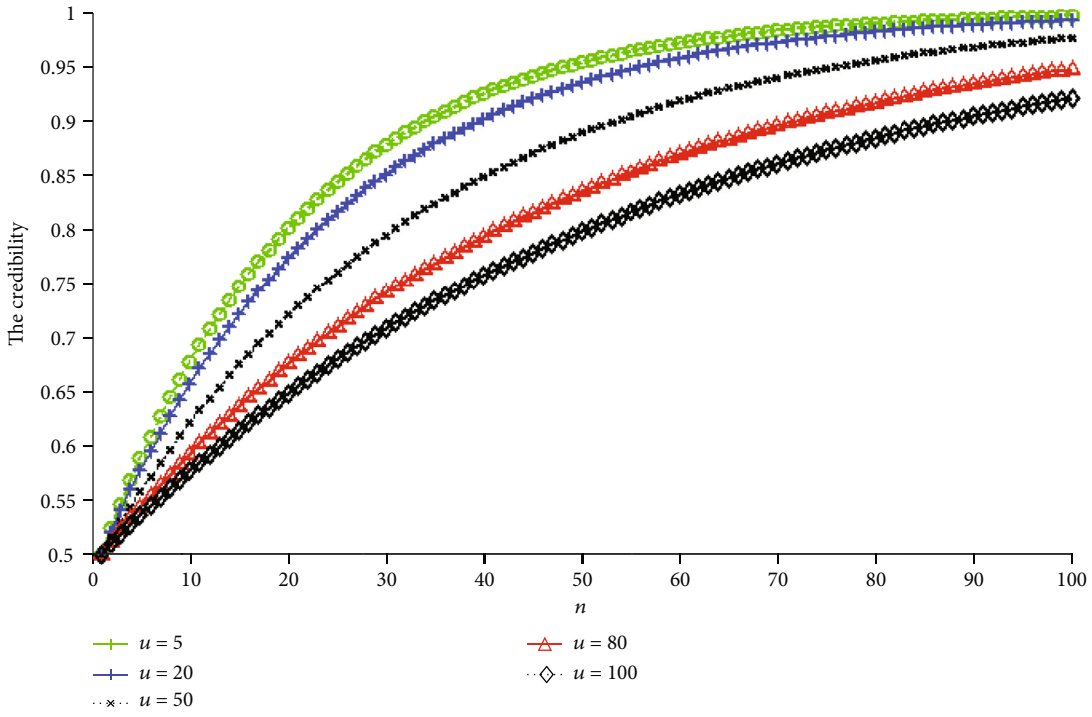

Figure 4: Impact of different values of u on credibility.

of encrypted data. With the changing trend of credibility, the value of v' is smaller than that of v. Besides, to prevent credibility from falling too quickly, the value of v' cannot be too big. Generally, we have set $v' = 0.05$.

With the help of the powerful storage ability of the cloud platform, the client will store the ciphertext in the cloud after the client uses the RSA method to encrypt the data, by encrypting the public key of the client-side, uploading, and

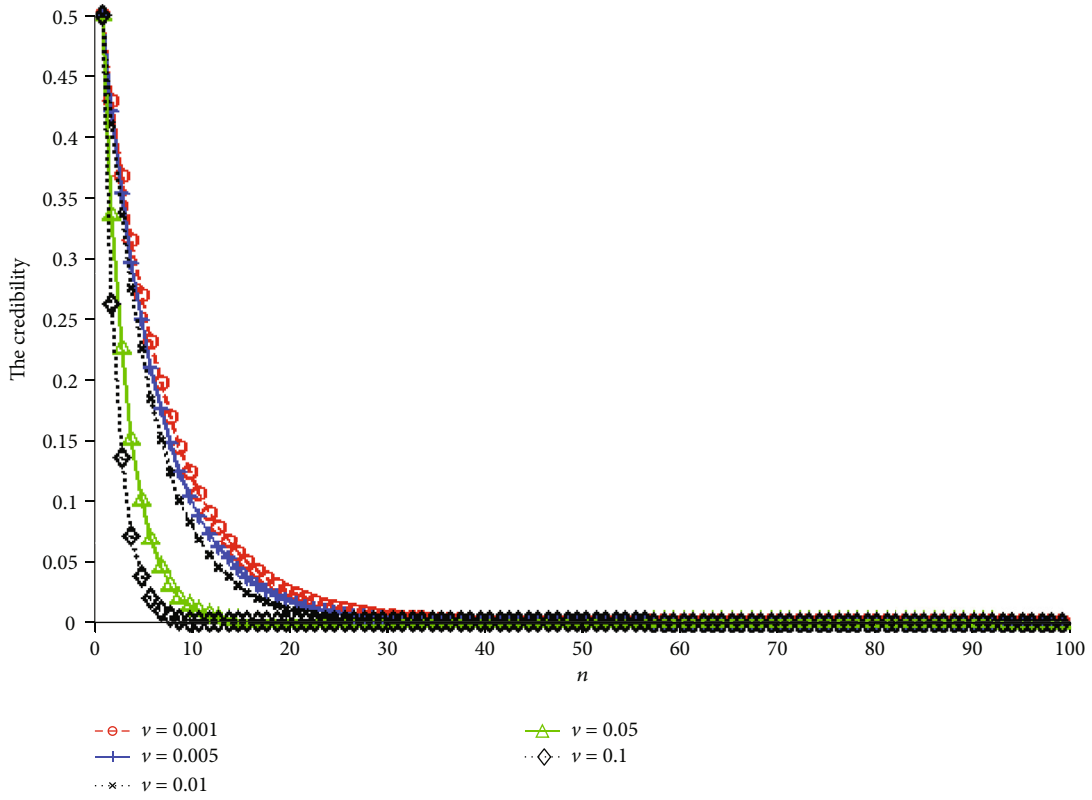

Figure 5: Impact of value of v on credibility.

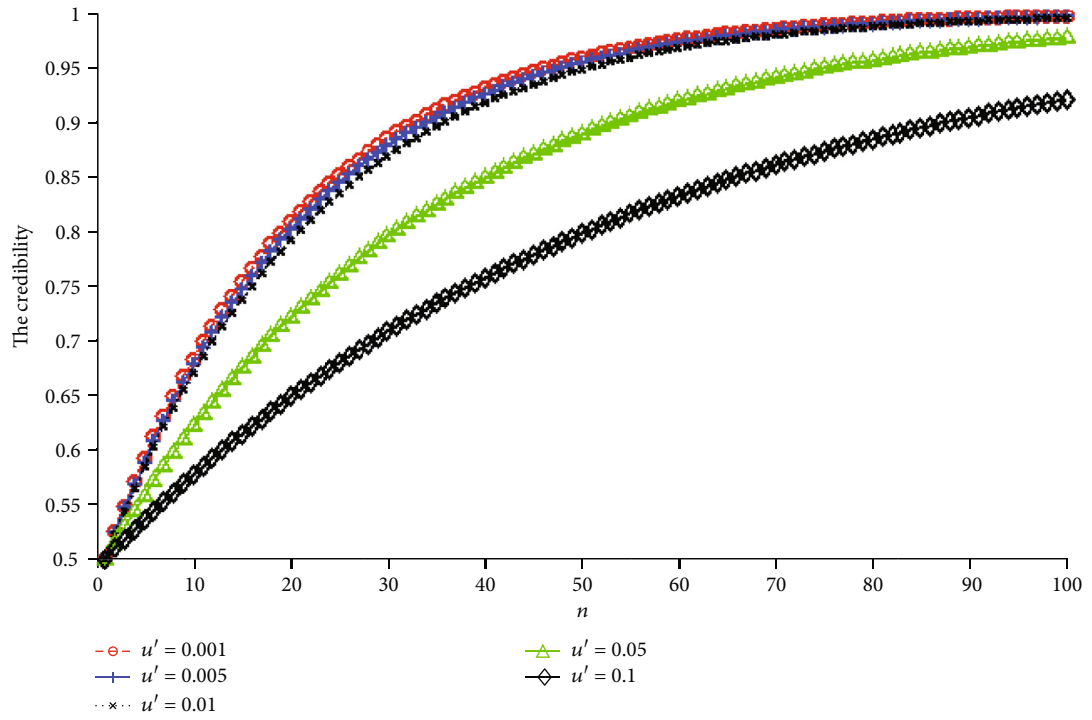

Figure 6: Impact of u' value on credibility.

storing the ciphertext to the cloud. When the client wants to share the data with another person, the client generates a reencryption key according to its decryption key and the encryption key of the other person and sends it to the cloud. The cloud server uses its strong computing power, integrates the reencryption key, proceeds with the reencryption, and

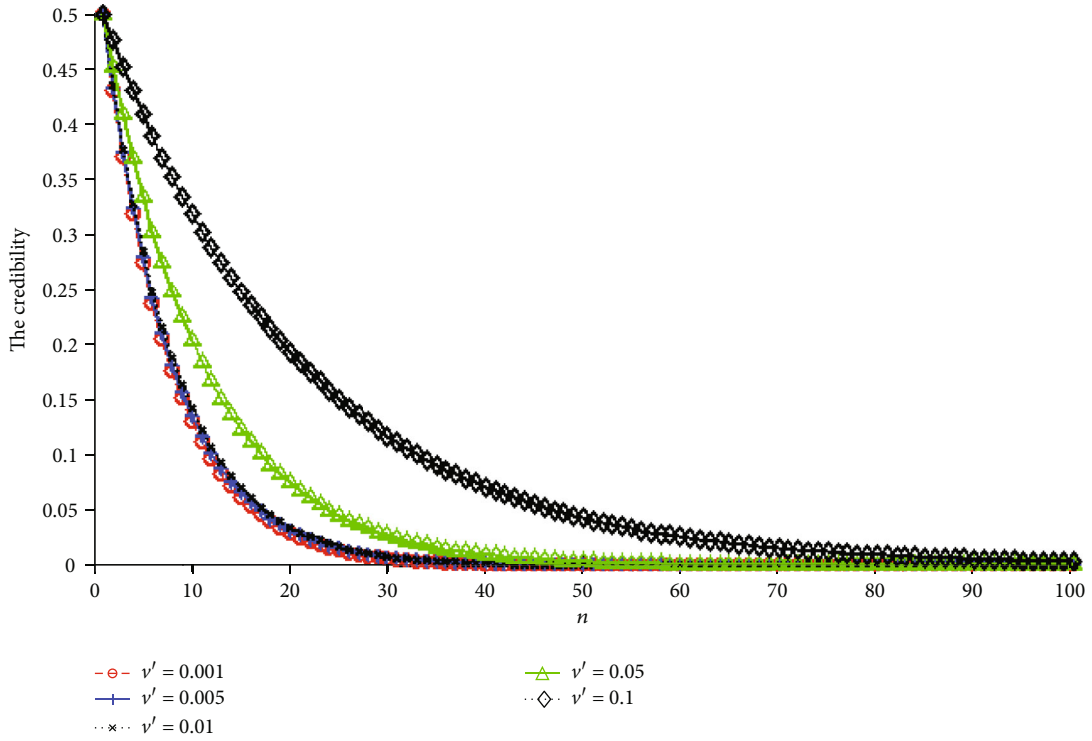

Figure 7: Impact of v' value on credibility.

stores the ciphertext in the cloud. Then, the other person downloads from the cloud server, decrypts with his private key, and gets the original plaintext with RSA decryption. In this way, the ciphertext is shared and the private key of the client is not leaked in this entire process. The medical data privacy protection scheme based on blockchain and cloud computing designed in this paper solves the problems of medical data storage and point-to-point data transaction, meets the needs of users for data management, and provides a new idea for solving the problem of data privacy security. Compared with the traditional technology, this scheme does not need an additional trusted third party nor does it need to rely on the "challenge response" mechanism, that is, the cloud does not need to provide special interface support, and the blockchain does not need to construct special transactions for the technical solution.

6. Conclusion

Blockchain is a brand-new decentralized distributed database, and it is a series of data blocks by using cryptographic methods. In this paper, we combined two encryption methods: proxy reencryption and attribute-based encryption and built key technical solutions for cloud computing based on blockchain to be applied in security and privacy protection of distributed medical data. It can not only achieve integrity testing of cloud data but also achieve broader security encryption computing. Intelligent hospitals only need to give the proxy key to the cloud server, which can convert medical data into the encrypted text in the designated format. The fixed client can access these shared data resources with their private key at any time. Even if the cloud server has the proxy key, it cannot get these data resources and the client does not need to download these resources. The proposed scheme can help solve such problems in that healthcare data are easy to be monopolized and tampered with and difficult to share and that the third party is not trustworthy to achieve the purpose of secure sharing and storage of distributed, decentralized, traceable, and unalterable healthcare data. In the future, we will consider improving the consensus mechanism, studying how to achieve fine-grained control of cloud data and how to reduce the storage overhead of redundant data, so that the performance of the blockchain can meet more needs of intelligent hospitals.

Data Availability

The raw/processed data required to reproduce these findings cannot be shared at this time as the data also forms part of an ongoing study.

Conflicts of Interest

The authors declare that they have no competing interests.

References

[1] H. Liang, J. Zou, K. Zuo, and M. J. Khan, "An improved genetic algorithm optimization fuzzy controller applied to the wellhead back pressure control system," *Mechanical Systems and Signal Processing*, vol. 142, p. 106708, 2020.

[2] R. He, N. Xiong, L. T. Yang, and J. H. Park, "Using multimodal semantic association rules to fuse keywords and visual features automatically for web image retrieval," *Information Fusion*, vol. 12, no. 3, pp. 223–230, 2011.

[3] H. Zheng, W. Guo, and N. Xiong, "A kernel-based compressive sensing approach for mobile data gathering in wireless sensor network systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 12, pp. 2315–2327, 2018.

[4] Z. Wan, N. Xiong, N. Ghani, A. V. Vasilakos, and L. Zhou, "Adaptive unequal protection for wireless video transmission over IEEE 802.11e networks," *Multimedia Tools and Applications*, vol. 72, no. 1, pp. 541–571, 2014.

[5] H. Liang, J. Zou, Z. Li, M. J. Khan, and Y. Lu, "Dynamic evaluation of drilling leakage risk based on fuzzy theory and PSO-SVR algorithm," *Future Generation Computer Systems*, vol. 95, pp. 454–466, 2019.

[6] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *Journal of Information Security and Applications*, vol. 50, no. 2, p. 102407, 2020.

[7] A. Farouk, A. Alahmadi, S. Ghose, and A. Mashatan, "Blockchain platform for industrial healthcare: vision and future opportunities," *Computer Communications*, vol. 154, no. 15, pp. 223–235, 2020.

[8] S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, "Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain," *Information Sciences*, vol. 485, no. 6, pp. 427–440, 2019.

[9] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: research challenges and opportunities," *Journal of Network and Computer Applications*, vol. 135, pp. 62–75, 2019.

[10] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Generation Computer Systems*, vol. 95, pp. 511–521, 2019.

[11] N. Islam, Y. Faheem, I. U. Din, M. Talha, M. Guizani, and M. Khalil, "A blockchain-based fog computing framework for activity recognition as an application to e-healthcare services," *Future Generation Computer Systems*, vol. 100, no. 11, pp. 569–578, 2019.

[12] C. He, X. Fan, and Y. Li, "Toward ubiquitous healthcare services with a novel efficient cloud platform," *IEEE Transactions on Biomedical Engineering*, vol. 60, no. 1, pp. 230–234, 2013.

[13] S. Safavi and Z. Shukur, "Conceptual privacy framework for health information on wearable device," *PLoS One*, vol. 9, no. 12, article e114306, 2014.

[14] L. Huang, X. Chen, and X. Lai, "Network security prediction method based on Kalman filtering fusion decision entropy theory," *International Journal of Security and its Applications*, vol. 10, no. 12, pp. 347–358, 2016.

[15] M. Kyazze, J. Wesson, and K. Naude, "The design and implementation of a ubiquitous personal health record system for South Africa," *Studies in Health Technology & Informatics*, vol. 206, no. 206, pp. 29–41, 2014.

[16] H. Cheng, D. Feng, X. Shi, and C. Chen, "Data quality analysis and cleaning strategy for wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, 11 pages, 2018.

[17] S. Wang, X. Wang, F. Meng, R. Yang, and Y. Zhao, "Investor behaviour monitoring based on deep learning," *Behaviour & Information Technology*, pp. 1–12, 2020.

[18] C. Xu, "A novel recommendation method based on social network using matrix factorization technique," *Information Processing & Management*, vol. 54, no. 3, pp. 463–474, 2018.

[19] R. Yang, L. Yu, Y. Zhao et al., "Big data analytics for financial market volatility forecast based on support vector machine," *International Journal of Information Management*, vol. 50, no. 1, pp. 452–462, 2020.

[20] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," *IET Communications*, vol. 12, no. 5, pp. 527–532, 2018.

[21] D. J. Willison, M. K. Kapral, P. Peladeau, J. A. Richards, J. Fang, and F. L. Silver, "Variation in recruitment across sites in a consent-based clinical data registry: lessons from the Canadian Stroke Network," *BMC Medical Ethics*, vol. 7, no. 1, p. 6, 2006.

[22] S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, and N. Guizani, "Securing smart cities through blockchain technology: architecture, requirements, and challenges," *IEEE Network*, vol. 34, no. 1, pp. 8–14, 2020.

[23] H. Cheng, N. Xiong, A. V. Vasilakos, L. T. Yang, G. Chen, and X. Zhuang, "Nodes organization for channel assignment with topology preservation in multi-radio wireless mesh networks," *Ad Hoc Networks*, vol. 10, no. 5, pp. 760–773, 2012.

[24] A. F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J. M. R. S. Tavares, and V. H. C. de Albuquerque, "A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform," *Cognitive Systems Research*, vol. 52, no. 12, pp. 1–11, 2018.

[25] A. Conti, P. Delbon, L. Laffranchi, C. Paganelli, and F. De Ferrari, "HIV-positive status and preservation of privacy: a recent decision from the Italian Data Protection Authority on the procedure of gathering personal patient data in the dental office," *Journal of Medical Ethics*, vol. 38, no. 6, pp. 386–388, 2012.

[26] F. Holotiuk, F. Pisani, and J. Moormann, "Radicalness of blockchain: an assessment based on its impact on the payments industry," *Technology Analysis and Strategic Management*, vol. 31, no. 8, pp. 915–928, 2019.

[27] Z. Liu, B. Hu, B. Huang, L. Lang, H. Guo, and Y. Zhao, "Strategies of Haze Risk Reduction Using the Tripartite Game Model," *Complexity*, vol. 2020, Article ID 2145951, 11 pages, 2020.

[28] F. Hu and G. Wu, "Distributed error correction of EKF algorithm in multi-sensor fusion localization model," *IEEE Access*, vol. 8, pp. 93211–93218, 2020.

[29] Z. Liu, B. Hu, Y. Zhao et al., "Research on intelligent decision of low carbon supply chain based on carbon tax constraints in human-driven edge computing," *IEEE Access*, vol. 8, pp. 48264–48273, 2020.

[30] L. Huang, J. Zheng, and G. Tan, "Research on task scheduling convergence non-dominated sorting method in cloud computing," *International Journal of Grid Distribution Computing*, vol. 8, no. 1, pp. 237–246, 2015.