Hindawi
Security and Communication Networks
Volume 2017, Article ID 6426495, 12 pages
https://doi.org/10.1155/2017/6426495

Research Article

Secure and Privacy-Preserving Data Sharing and Collaboration in Mobile Healthcare Social Networks of Smart Cities

Qinlong Huang,[1,2] Licheng Wang,[1,2] and Yixian Yang[1,2]

[1] *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2] *National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China*

Correspondence should be addressed to Qinlong Huang; longsec@bupt.edu.cn

Received 18 May 2017; Accepted 6 July 2017; Published 3 August 2017

Academic Editor: Qing Yang

Mobile healthcare social networks (MHSN) integrated with connected medical sensors and cloud-based health data storage provide preventive and curative health services in smart cities. The fusion of social data together with real-time health data facilitates a novel paradigm of healthcare big data analysis. However, the collaboration of healthcare and social network service providers may pose a series of security and privacy issues. In this paper, we propose a secure health and social data sharing and collaboration scheme in MHSN. To preserve the data privacy, we realize secure and fine-grained health data and social data sharing with attribute-based encryption and identity-based broadcast encryption techniques, respectively, which allows patients to share their private personal data securely. In order to achieve enhanced data collaboration, we allow the healthcare analyzers to access both the reencrypted health data and the social data with authorization from the data owner based on proxy reencryption. Specifically, most of the health data encryption and decryption computations are outsourced from resource-constrained mobile devices to a health cloud, and the decryption of the healthcare analyzer incurs a low cost. The security and performance analysis results show the security and efficiency of our scheme.

1. Introduction

As an emerging paradigm, smart cities leverage a variety of promising techniques, such as Internet of Things, mobile communications, and big data analysis, to enable intelligent services and provide a comfortable life for local residents [1]. The smart city is an urbanized area where multiple sectors cooperate to achieve sustainable outcomes through the analysis of contextual, real-time information, which would produce massive opportunities for mobile healthcare social network (MHSN) [2]. MHSN extends the traditional centralized healthcare system, in which the patients stay at home or in hospital environment and the professional physicians in the healthcare center take responsibility of generating medical treatment. With the considerable development of wearable devices and body sensors in the smart city, MHSN serving as a mobile community platform for healthcare purposes improves healthcare efficiency and places great emphasis on social interactivities [3] and assists patients in dealing with certain emergency situations or helps in forwarding data and sharing patients' feelings.

Compared to traditional hospital-centric healthcare which not only lacks efficiency when dealing with identifying some serious diseases in early stages but also suffers from limited healthcare information [4], MHSN enables continuous health monitoring and timely diagnosis to the patients in the smart city. It relies on wearable devices and medical sensors to measure the patients' health conditions and sends health data to the processing unit for doctors' further diagnosis and analysis and provides easy access to a patient's historical comprehensive health information. Additionally, the patients wearing body sensors continuously monitoring their health conditions are assumed to walk outside, moving from time to time and place to place [5]. However, MHSN may suffer from a series of security and privacy threats due to the vulnerabilities of personal health and social data. The collected private information is stored and processed in the honest but curious health and social

cloud servers, which may be directly revealed during the storage and processing phases [6, 7]. Moreover, the adversary can intercept the sessions between patients to get their health and social data. Hence, the underlying security and privacy requirements, including confidentiality and access control, should be satisfied in MHSN [8–10].

Intelligent healthcare is another functionality that can be realized in MHSN, which would provide efficient diagnosis and health condition warning by analyzing the infectiousness in real time, such as infectious diseases analysis [11]. As we know, infectious diseases could be rapidly spread in the population via human-to-human contact. An old-fashioned approach to prevent the spread of disease is to isolate the susceptible people for a certain period. However, this approach is always not satisfactory, since people having frequent contact or strong social relationships with a patient are more easily infected from the perspectives of biomedicine and sociology. In general, the spread of infectious diseases depends on users' social contacts and health conditions in a high probability. Specifically, the effective infectious diseases analysis could take several key factors into consideration, that is, susceptibility of the infected patient and immunity strength of contacted user. However, the health and social data of patients are collected by multiple independent service providers, such as hospitals and social network vendors. Hence, the collaboration of these service providers is the key challenge of enabling this enhanced infection analysis in MHSN.

1.1. Our Techniques. In order to preserve the patient's data privacy and achieve data availability, encryption techniques must be adopted to make both health and social data invisible to the untrusted cloud servers. Any users without the authorization of the data owner should not be able to access the personal health and social data, and the collaboration of different untrusted cloud servers should be achieved via an authorized entity. Otherwise, patients may not be willing to share their health and social data such that the infection analysis would be disabled. In fact, attribute-based encryption (ABE) and identity-based broadcast encryption (IBBE) are widely adopted encryption algorithms [12]. Particularly, CP-ABE is conceptually closer to traditional access control models, to enforce fine-grained access control of encrypted data. By using CP-ABE, health data can be protected with access policy, and only the people who possess a set of attributes that satisfy the access policy can access data. IBBE scheme is a cryptographic mechanism in which data owners could broadcast their encrypted data to multiple receivers at one time and the public key of the user can be regarded as any valid strings, such as the email, unique ID, and username. In combination, these two mechanisms can be used to implement data protection in healthcare systems and social networks. In this paper, we propose a secure health and social data sharing and collaboration scheme in MHSN. The main contributions of our scheme are as follows:

(1) We realize secure and privacy-preserving health data and social data sharing with attribute-based encryption and identity-based broadcast encryption techniques, respectively, which protects the private data confidentiality.

(2) We provide a secure data collaboration construction from different independent cloud servers based on proxy reencryption (PRE), which allows the healthcare analyzers authorized by the data owner to access the reencrypted health data and social data for enhanced data analysis.

(3) We outsource most of the health data encryption and decryption computations from resource-constrained mobile devices to a health cloud, and the decryption of the healthcare analyzer incurs low cost. The extensive security and performance analysis results show that our scheme is secure and efficient.

1.2. Organization. This paper is structured as follows: we review related work in Section 2. We introduce the preliminaries in Section 3 and provide the system model, system definition, and security definition in Section 4. The detailed construction is given in Section 5. Then, we analyze the security and performance of our scheme in Sections 6 and 7, respectively. Finally, we conclude this paper in Section 8.

2. Related Work

Personal health records (PHRs) are the electronic records containing health and medical information of patients, which involves privacy information that patients are unwilling to disclose. Thus, the security and protection of PHR have been of great concern and a subject of research over the years [13]. Zhang et al. [14] proposed a PHR security and privacy preservation scheme by introducing consent-based access control, where the consent can only be generated by an authorized user based on PRE. Currently, there has been an increasing interest in applying ABE to protect PHR. ABE is a promising one-to-many cryptographic technique to realize flexible and fine-grained access control for sharing data [15], which was first introduced by Sahai and Waters as a new method for fuzzy identity-based encryption (IBE) [16]. It features a mechanism that enables access control over encrypted data using access policies and ascribed attributes among private keys and ciphertexts [17]. Narayan et al. [18] proposed an attribute-based infrastructure for PHR systems, where each patient's PHR files are encrypted using a broadcast variant of ciphertext-policy ABE. Li et al. [19] proposed a novel ABE-based framework for patient-centric secure sharing of PHRs in cloud computing environments. Au et al. [20] designed a general framework for secure sharing of PHR in cloud with CP-ABE, and it deploys attribute-based PRE (ABPRE) mechanism so that the ciphertext for doctor A can be transformed to the ciphertext for doctor B. However, the main complaint in CP-ABE scheme is the high computation overhead brought about by its complex computation. This problem will become even worse in the face of resource-limited wearable devices or mobile sensors in MHSN, since it needs to perform burdensome computation tasks for fine-grained data access control when adopting the ABE algorithm. In order to reduce the computational

overheads, Liu et al. [21] proposed an outsourced healthcare record access control system by moving the encryption computation offline and keeping online computation task very low. Yeh et al. [22] proposed a decryption outsourcing framework for health information access control in the cloud by utilizing CSP to check whether the attributes satisfy the access policy in ciphertext, which induces the outsourced encryption and decryption scheme introduced by Zhang et al. [23].

Intelligent healthcare, which is one of the intelligent services in the smart city, contains various health-related applications in MHSN, such as home care and emergency alarm [24]. Wang et al. [25] designed a secure health cloud system framework based on IBE, in which the assistant doctor can access the health data for enhanced analysis with authorization from the data owner based on identity-based PRE (IBPRE). In particular, by analyzing the collected social data together with real-time health data, accurate infection analysis can be achieved. The secure collaboration of healthcare and social network service providers is the key challenge of intelligent healthcare, since different service providers may adopt different techniques to protect data privacy. Zhang et al. [11] introduced some challenges of security and privacy in MHSN of smart cities and proposed the first secure data collaboration framework of healthcare and social network service providers. However, this scheme does not give the implementation construction. Liang et al. [26] proposed PEC, an ABE-based emergency call scheme for MHSN, which combines location data with health data to guarantee that emergency information is sent to nearby physicians. Jiang et al. [27] proposed EPPS, a personal health information sharing scheme based on ABE by combining the mobile social network with a healthcare center. Patients with geographical proximity can constitute a group to exchange health conditions, healthcare experiences, and medical treatments with the authorized physician. But in this scheme, the physicians in the healthcare center must have many attribute secret keys for each attribute to dock with patients in different groups. Moreover, these two schemes above do not consider the data collaboration (e.g., infectious diseases analysis) with health and social data.

3. Preliminaries

3.1. Bilinear Pairing. Let $\mathbb{G}_0$ and $\mathbb{G}_T$ be two multiplicative groups of prime order p. A bilinear map is a function $e : \mathbb{G}_0 \times \mathbb{G}_0 \to \mathbb{G}_T$ with the following properties:

(1) *Computability*. There is an efficient algorithm to compute $e(g, h) \in \mathbb{G}_T$, for any $g, h \in \mathbb{G}_0$.

(2) *Bilinearity*. For all $g, h \in \mathbb{G}_0$ and $a, b \in \mathbb{Z}_p$, we have $e(g^a, h^b) = e(g, h)^{ab}$.

(3) *Nondegeneracy*. If g is a generator of $\mathbb{G}_0$, then $e(g, g)$ is also a generator of $\mathbb{G}_T$.

3.2. Ciphertext-Policy Attribute-Based Encryption. The CP-ABE is a cryptography prototype for one-to-many secure communication, which consists of the following algorithms [17].

(1) $Setup(1^\lambda)$. The setup algorithm takes as input the security parameter λ and outputs a public key PK and a master secret key MK.

(2) $KeyGen(\text{PK}, \text{MK}, S)$. The key generation algorithm takes as input the public key PK, the master secret key MK, and a set S of attributes and outputs an attribute key AK.

(3) $Enc(\text{PK}, M, T)$. The encryption algorithm takes as input the public key PK, a message M, and an access policy T and outputs a ciphertext CT.

(4) $Dec(\text{PK}, \text{AK}, \text{CT})$. The decryption algorithm takes as input the public key PK, an attribute key AK, and a ciphertext CT with an access policy T. If $S \in T$, it outputs the message M.

3.3. Identity-Based Broadcast Encryption. The IBBE can be seen as an extension of the IBE, by allowing one to encrypt a message once for many receivers. The definition of IBBE is as follows [28].

(1) $Setup(1^\lambda, N)$. The setup algorithm takes as input a security parameter λ and the maximal size N of a set of receivers and outputs a pair of public key PK and master secret key MK.

(2) $KegGen(\text{PK}, \text{MK}, \text{ID})$. The key generation algorithm takes as input the public key PK, the master secret key MK, and a user's identity ID and outputs a secret key SK_{ID} for the user.

(3) $Enc(\text{PK}, M, U)$. The encryption algorithm takes as input the public key PK, a message M, and a set U of receivers' identities; the algorithm outputs a ciphertext CT for U.

(4) $Dec(\text{PK}, \text{CT}, \text{SK}_{\text{ID}}, \text{ID})$. The decryption algorithm takes as input the public key PK, a ciphertext CT, a secret key SK_{ID}, and an identity ID; the algorithm outputs the message M if $\text{ID} \in U$.

4. The Proposed Scheme

4.1. System Model. In MHSN, the fusion of health data and social data facilitates a novel paradigm of authorized infection analysis. Our scheme focuses on the secure sharing and collaboration of these data. As shown in Figure 1, the system model of our scheme consists of central authority, health cloud, social cloud, users, healthcare provider, and healthcare analyzer.

(1) *Central Authority*. The central authority is a fully trusted party which is in charge of generating system parameters as well as private keys for each user.

(2) *Health Cloud*. The health cloud is a semitrusted party which provides health data storage service. It is also responsible for helping encrypt health data for mobile healthcare sensors and decrypt the ciphertext for healthcare providers and reencrypt ciphertext for healthcare analyzers.

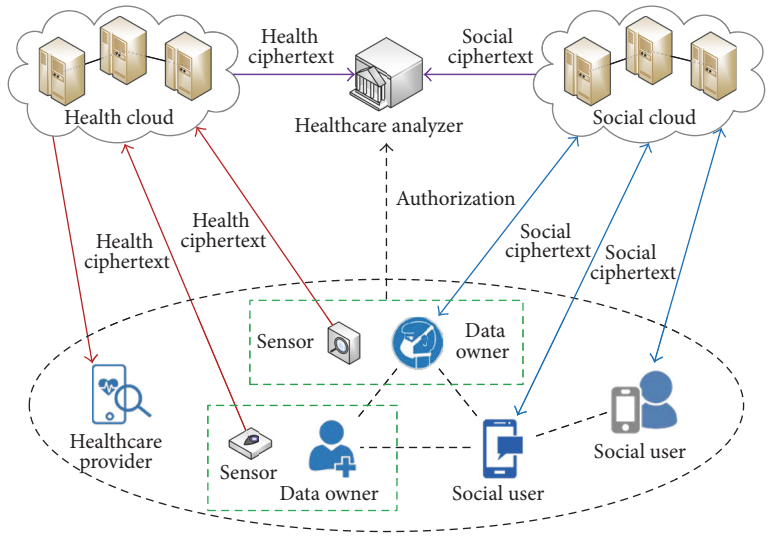

Figure 1: System model of our scheme.

(3) *Social Cloud*. The social cloud is also a semitrusted party which provides social data storage service and is in charge of reencrypting social ciphertext for healthcare analyzers.

(4) *Data Owner*. The data owners generate a great amount of health data through the mobile healthcare sensors and upload them to the health cloud by defining access policy and also upload their social data to the social cloud for sharing.

(5) *User*. The user is the ciphertexts' receiver and is able to decrypt the ciphertexts if he is the intended receiver defined by the data owners.

(6) *Healthcare Provider*. The healthcare providers are the intended receivers of health ciphertext stored in the health cloud. If a healthcare provider's attribute set satisfies the access policy in the ciphertext, he is able to decrypt the patient's health data from the ciphertext.

(7) *Healthcare Analyzer*. The healthcare analyzer is the authorized receiver of both health ciphertext and social ciphertext for data collaboration and analysis.

4.2. System Definition. Based on the system model, our scheme consists of the following algorithms.

(1) *Setup*$(1^{\lambda}, N)$. The central authority takes as input a security parameter λ and the maximal size of receiver set N and outputs a system public key PK and a master secret key MK.

(2) *AKeyGen*(PK, MK, S). The central authority takes as input PK and MK and a set of attributes S of user or healthcare provider and outputs the attribute key AK.

(3) *SKeyGen*(PK, MK, ID). The central authority takes as input PK and MK and an identity ID of user or healthcare analyzer and outputs the secret key of user SK.

(4) *Cloud.Encrypt*(PK, T). The health cloud takes as input PK and an access policy T and outputs an outsourced health ciphertext CT'.

(5) *Health.Encrypt*(PK, m_h, CT'). The health data owner takes as input PK, health data m_h, and an outsourced health ciphertext CT' and outputs a health ciphertext CT_h.

(6) *Cloud.Decrypt*(PK, CT_h, AK'). The health cloud takes as input PK, a health ciphertext CT_h, and an outsourced attribute key AK' and outputs a partial decrypted health ciphertext CT_r if the attributes in AK' satisfy the access policy in the ciphertext.

(7) *Health.Decrypt*(CT_r, AK). The healthcare provider takes as input a partial decrypted health ciphertext CT_r and an attribute key AK and outputs the health data m_h.

(8) *Social.Encrypt*(PK, m_c, U). The social data owner takes as input PK, social data m_c, and a set U of receivers' identities and outputs a social ciphertext CT_c.

(9) *Social.Decrypt*(PK, CT_c, ID, SK). The social receiver takes as input PK, a social ciphertext CT_c, a receiver's identity ID, and its secret key SK and outputs the social data m_c if ID and SK are valid.

(10) *Health.ReKeyGen*(PK, AK, ID'). The health data owner takes as input PK, attribute key AK, and a healthcare analyzer's identity ID' and outputs a health reencryption key RK_h.

(11) *Health.ReEnc*(CT_h, RK_h). The health cloud takes as input a health ciphertext CT_h and a heath reencryption key RK_h and outputs a reencrypted health ciphertext RT_h.

(12) *Social.ReKeyGen*(PK, SK, ID'). The social data owner takes as input PK, a secret key SK, and a healthcare

analyzer's identity ID′ and outputs a social reencryption key RK_c.

(13) *Social.ReEnc*(CT_c, RK_c). The social cloud takes as input a social ciphertext CT_c and a social reencryption key RK_c and outputs a reencrypted social ciphertext RT_c.

(14) *Analyzer.Decrypt*(RT_h, RT_c, SK′). The healthcare analyzer takes as input a reencrypted health ciphertext RT_h, a reencrypted social ciphertext RT_c, and a secret key SK′ and outputs health data m_h and social data m_c.

In the registration phase, the central authority runs *Setup* algorithms to generate system public key and master secret key. Meanwhile, it also uses *AKeyGen* and *SKeyGen* algorithm to generate attribute keys and secret keys of users in the system. For the health data, the health cloud first runs *Cloud.Encrypt* algorithm to encrypt data with an access policy, and then the data owner runs *Health.Encrypt* algorithm to finish the encryption. When accessing the health data, the health cloud first uses the *Cloud.Decrypt* algorithm to partially decrypt the ciphertext, and then the user can use the *Health.Decrypt* algorithm to recover the data. For the social data, the data owner runs *Social.Encrypt* algorithm to encrypt data for a set of receivers, and the user can use the *Social.Decrypt* algorithm to recover the social data. Furthermore, the data owner could run *Health.ReKeyGen* and *Social.ReKeyGen* algorithms, respectively, to generate reencryption keys containing their own attribute keys and secret keys. Receiving the reencryption keys, the health cloud and social cloud would run *Health.ReEnc* and *Social.ReEnc* algorithms to transform the initial ciphertexts to the reencrypted ciphertexts. Hence, the healthcare analyzer can run *Analyzer.Decrypt* algorithm to decrypt the reencrypted health and social ciphertexts.

4.3. Security Definition. In our scheme, we assume that the health cloud and social cloud are honest but curious, which means they carry out computation and storage tasks but may try to learn information about the private data [29]. Specifically, the security model covers the following aspects.

(1) *Data Confidentiality*. The unauthorized users that are not the intended receivers defined by the data owner should be prevented from accessing the health and social data. The healthcare analyzer should not be able to access the reencrypted data without the authorization of the data owner.

(2) *Fine-Grained Access Control*. The data owner can customize an expressive and flexible access policy so that the health data only can be accessed by the healthcare providers whose attributes satisfy these policies.

(3) *Collusion Resistance*. If each of the users' attributes in the set cannot satisfy the access policy in the ciphertexts alone, the access of ciphertext should not successful.

5. Construction

5.1. System Setup. The central authority runs *Setup* algorithm to select a bilinear map $e : \mathbb{G}_0 \times \mathbb{G}_0 \to \mathbb{G}_T$, where $\mathbb{G}_0$ and $\mathbb{G}_T$ are two multiplicative groups with prime order p and g is the generator of $\mathbb{G}_0$. Then, the central authority chooses the maximum number of receivers N, randomly chooses $g, h, u, v, w \in \mathbb{G}_0$ and $\alpha, \beta \in \mathbb{Z}_p$, chooses cryptographic hash function $H_1 : \{0,1\}^* \to \mathbb{Z}_p^*$, $H_2 : \mathbb{G}_T \to \mathbb{G}_0$, and finally outputs a system public key $PK = (g, g^\beta, e(g,g)^\alpha, h, u^\alpha, v, v^\alpha, \ldots, v^{\alpha^N}, e(u,v), w)$ and a master secret key $MK = (u, \alpha, \beta)$.

5.2. Key Generation. The central authority runs *AKeyGen* algorithm to select a random $\gamma \in \mathbb{Z}_p$, which is a unique secret assigned to each user. Then, the central authority chooses random $\varepsilon, \varphi \in \mathbb{Z}_p$ and random r_j for each attribute $j \in S$, where S is the attribute set of the user, and outputs the attribute key AK.

$$\begin{aligned} AK = \Big(& D = g^{(\alpha+\gamma)/\beta},\ D_1 = g^\gamma h^\varepsilon,\ D_2 = g^\varepsilon,\ D_3 \\ & = g^{1/\varphi},\ D_4 = g^{\varphi\alpha},\ D_5 \\ & = w^{\varphi\alpha},\ \left\{ \widetilde{D}_j = g^\gamma H_1(j)^{r_j},\ \widetilde{D}'_j = g^{r_j} \right\}_{j \in S} \Big). \end{aligned} \tag{1}$$

For each user in the system, the central authority runs *SKeyGen* algorithm to select a random $\pi \in \mathbb{Z}_p$ and output the secret key SK for the user with identity ID.

$$\begin{aligned} SK = \Big(& K = g^{1/(\alpha + H_1(ID))},\ K_1 = u^{1/\pi},\ K_2 = v^\pi,\ K_3 \\ & = w^\pi \Big). \end{aligned} \tag{2}$$

5.3. Secure Health Data Sharing

5.3.1. Health Data Encryption. The mobile healthcare sensors of the data owner could collect a wide range of real-time health data (e.g., blood pressure, heart rate, and pulse), for further diagnosis or specialist analysis. Before uploading the data to the health cloud, the data owner first chooses a random $HK \in \mathbb{Z}_p$ and encrypts the health data m_h with HK using a symmetric encryption algorithm, denoted as $C = SE_{HK}(m_h)$. Then, the data owner defines an access policy T, to ensure that only users satisfying this policy can access data, and then sends to the health cloud.

Then, the health cloud runs *Cloud.Encrypt* algorithm to perform the outsourced encryption. For each node x in the access policy tree T, the health cloud chooses a polynomial p_x. These polynomials are chosen in the following way in a top-down manner, starting from the root node R. For each node x in the tree, set the degree d_x of the polynomial p_x to be one less than the threshold value k_x of that node; that is, $d_x = k_x - 1$. Starting with the root node R, the algorithm chooses a random $s \in \mathbb{Z}_p$ and sets $p_R(0) = s$. Then, it chooses d_R other points of the polynomial p_R randomly to define it completely. For any other node x, it sets $p_x(0) = p_{\text{parent}(x)}(\text{index}(x))$ and chooses d_x other points randomly to completely define p_x.

Let Y be the set of leaf nodes in T; the health cloud outputs an outsourced ciphertext CT' as

$$\begin{aligned}\mathrm{CT}' &= \left(T,\ C_3' = g^s,\ C_4' = h^s,\ C_7\right.\\ &\left.= \left\{\widetilde{C}_y = g^{p_y(0)},\ \widetilde{C}_y' = H_1\left(\mathrm{attr}_y\right)^{p_y(0)}\right\}_{y\in Y}\right).\end{aligned} \tag{3}$$

The health cloud returns CT' to the data owner. The data owner runs *Health.Encrypt* algorithm to select $t \in \mathbb{Z}_p$ at random and computes $C_1 = \mathrm{HK}\cdot e(g,g)^{\alpha t}$ with HK and computes $C_2 = g^{\beta t}$, $C_3 = C_3'\cdot g^t$, $C_4 = C_4'\cdot h^t$, $C_5 = (D_4)^t$, $C_6 = (D_5)^t$. Finally, the data owner outputs the ciphertext CT_h as

$$\begin{aligned}\mathrm{CT}_h &= \left(T,\ C = \mathrm{SE}_{\mathrm{HK}}\left(m_h\right),\ C_1 = \mathrm{HK}\cdot e\left(g,g\right)^{\alpha t},\ C_2\right.\\ &= g^{\beta t},\ C_3 = g^{s+t},\ C_4 = h^{s+t},\ C_5 = g^{\varphi\alpha t},\ C_6\\ &= w^{\varphi\alpha t},\ C_7\\ &\left.= \left\{\widetilde{C}_y = g^{p_y(0)},\ \widetilde{C}_y' = H_1\left(\mathrm{attr}_y\right)^{p_y(0)}\right\}_{y\in Y}\right).\end{aligned} \tag{4}$$

5.3.2. Health Data Decryption. If the attributes of the healthcare provider satisfy the access policy T, he can decrypt CT_h successfully by informing health cloud and obtaining the symmetric key. The health cloud runs *Cloud.Decrypt* algorithm with the ciphertext and outsourced attribute key $\mathrm{AK}' = (D_1, D_2, \{\widetilde{D}_j, \widetilde{D}_j'\}_{j\in S})$ from the healthcare provider. The health cloud first runs *DecryptNode* algorithm which can be described as a recursive algorithm. This algorithm takes the ciphertext CT_h, AK', and a node x from the access tree T as input.

(1) If the node x is a leaf node, then we let $z = \mathrm{attr}_x$ and compute as follows. If $z \in S$, then

$$\begin{aligned}\mathit{DecryptNode}\left(\mathrm{CT}_h, \mathrm{AK}', x\right) &= \frac{e\left(\widetilde{D}_z, \widetilde{C}_x\right)}{e\left(\widetilde{D}_z', \widetilde{C}_x'\right)}\\ &= \frac{e\left(g^{\gamma}H_1\left(z\right)^{r_z}, g^{p_x(0)}\right)}{e\left(g^{r_z}, H_1\left(\mathrm{attr}_x\right)^{p_x(0)}\right)} = e\left(g,g\right)^{\gamma p_x(0)}.\end{aligned} \tag{5}$$

If $z \notin S$, then $\mathit{DecryptNode}(\mathrm{CT}_h, \mathrm{AK}', x) = \perp$.

(2) If the node x is a nonleaf node, the algorithm $\mathit{DecryptNode}(\mathrm{CT}_h, \mathrm{AK}', x)$ proceeds as follows: for all nodes n that are children of x, it calls $\mathit{DecryptNode}(\mathrm{CT}_h, \mathrm{AK}', n)$ and stores output as F_n. Let S_x be an arbitrary k_x-sized set of child nodes n such that $F_n \neq \perp$. If no such set exists, then the node is not satisfied and the function returns $\perp$. Otherwise, the function defines $j = \mathrm{index}(n)$ and $S_x' = \{\mathrm{index}(n) : n \in S_x\}$ and returns the result.

$$\begin{aligned}F_x &= \prod_{n\in S_x} F_n^{\Delta_{j,S_x'}(0)}\\ &= \prod_{n\in S_x}\left(e\left(g,g\right)^{r\cdot p_{\mathrm{parent}(n)}(\mathrm{index}(n))}\right)^{\Delta_{j,S_x'}(0)}\\ &= \prod_{n\in S_x} e\left(g,g\right)^{r\cdot p_x(j)\cdot\Delta_{j,S_x'}(0)} = e\left(g,g\right)^{r p_x(0)}.\end{aligned} \tag{6}$$

If the access policy tree T is satisfied by S, we set the result of the entire evaluation for the access tree T as F, such that

$$\begin{aligned}F &= \mathit{DecryptNode}\left(\mathrm{CT}_h, \mathrm{AK}', R\right) = e\left(g,g\right)^{\gamma p_R(0)}\\ &= e\left(g,g\right)^{\gamma s}.\end{aligned} \tag{7}$$

Then, the health cloud computes

$$\begin{aligned}B &= \frac{e\left(D_1, C_3\right)}{e\left(D_2, C_4\right)} = \frac{e\left(g^{\gamma}h^{\varepsilon}, g^{s+t}\right)}{e\left(g^{\varepsilon}, h^{s+t}\right)} = e\left(g,g\right)^{\gamma(s+t)},\\ A &= \frac{B}{F} = \frac{e\left(g,g\right)^{\gamma(s+t)}}{e\left(g,g\right)^{\gamma s}} = e\left(g,g\right)^{\gamma t}.\end{aligned} \tag{8}$$

Finally, the health cloud sends the partial decrypted health ciphertext $\mathrm{CT}_r = (C = \mathrm{SE}_{\mathrm{HK}}(m_h), C_1 = \mathrm{HK}\cdot e(g,g)^{\alpha t}, C_2 = g^{\beta t}, A = e(g,g)^{\gamma t})$ to the healthcare provider. After receiving CT_r from the health cloud, the healthcare provider runs *Health.Decrypt* algorithm to obtain the symmetric key.

$$\mathrm{HK} = \frac{C_1\cdot A}{e\left(C_2, D\right)} = \frac{\mathrm{HK}\cdot e\left(g,g\right)^{\alpha t}\cdot e\left(g,g\right)^{\gamma t}}{e\left(g^{\beta t}, g^{(\alpha+\gamma)/\beta}\right)}. \tag{9}$$

Thus, $\mathrm{SE}_{\mathrm{HK}}(m_h)$ can be decrypted with HK by applying the symmetric decryption algorithm, and the healthcare provider can access the data owner's health data for diagnosis.

5.4. Secure Social Data Sharing

5.4.1. Social Data Encryption. For the private social data denoted as m_c, the data owner runs *Social.Encrypt* algorithm to encrypt it and then outsource the ciphertext to the social cloud. First, the data owner chooses a set U of receivers' identities (where $|U| \leq N$) and a random $\mathrm{CK} \in \mathbb{Z}_p$ which is used to encrypt the data based on the symmetric encryption algorithm. The data owner randomly picks $k \in \mathbb{Z}_p^*$ and outputs a social ciphertext CT_c.

$$\begin{aligned}\mathrm{CT}_c &= \left(C = \mathrm{SE}_{\mathrm{CK}}\left(m_c\right),\ C_1 = \mathrm{CK}\cdot e\left(u,v\right)^k,\ C_2\right.\\ &= v^{k\cdot\prod_{\mathrm{ID}_i\in U}(\alpha+H_1(\mathrm{ID}_i))},\ C_3 = v^{\pi k},\ C_4 = w^{\pi k},\ C_5\\ &\left.= u^{-\alpha k}\right).\end{aligned} \tag{10}$$

5.4.2. Social Data Decryption. The user with identity ID runs *Social.Decrypt* algorithm to decrypt the social ciphertext. If

ID $\in U$, the user computes

$$\begin{aligned} I &= \left(e\left(C_5, v^{\Delta_\alpha(\mathrm{ID},U)}\right)\cdot e\left(K, C_2\right)\right)^{1/\prod_{\mathrm{ID}_i\in U\wedge \mathrm{ID}_i\neq \mathrm{ID}} H_1(\mathrm{ID}_i)} = \left(e\left(u^{-\alpha k}, v^{\Delta_\alpha(\mathrm{ID},U)}\right)\cdot e\left(u^{1/(\alpha+H_1(\mathrm{ID}))}, v^{k\cdot\prod_{\mathrm{ID}_i\in U}(\alpha+H_1(\mathrm{ID}_i))}\right)\right)^{1/\prod_{\mathrm{ID}_i\in U\wedge \mathrm{ID}_i\neq \mathrm{ID}} H_1(\mathrm{ID}_i)} \\ &= \left(e\left(u^{-\alpha k}, v^{\alpha^{-1}\cdot\left(\prod_{\mathrm{ID}_i\in U\wedge \mathrm{ID}_i\neq \mathrm{ID}}(\alpha+H_1(\mathrm{ID}_i))-\prod_{\mathrm{ID}_i\in U\wedge \mathrm{ID}_i\neq \mathrm{ID}} H_1(\mathrm{ID}_i)\right)}\right)\cdot e\left(u, v\right)^{k\cdot\prod_{\mathrm{ID}_i\in U\wedge \mathrm{ID}_i\neq \mathrm{ID}}(\alpha+H_1(\mathrm{ID}_i))}\right)^{1/\prod_{\mathrm{ID}_i\in U\wedge \mathrm{ID}_i\neq \mathrm{ID}} H_1(\mathrm{ID}_i)} \\ &= \left(e\left(u^k, v\right)^{\prod_{\mathrm{ID}_i\in U\wedge \mathrm{ID}_i\neq \mathrm{ID}} H_1(\mathrm{ID}_i)-\prod_{\mathrm{ID}_i\in U\wedge \mathrm{ID}_i\neq \mathrm{ID}}(\alpha+H_1(\mathrm{ID}_i))+\prod_{\mathrm{ID}_i\in U\wedge \mathrm{ID}_i\neq \mathrm{ID}}(\alpha+H_1(\mathrm{ID}_i))}\right)^{1/\prod_{\mathrm{ID}_i\in U\wedge \mathrm{ID}_i\neq \mathrm{ID}} H_1(\mathrm{ID}_i)} = e\left(u, v\right)^k, \end{aligned} \tag{11}$$

where

$$\Delta_\alpha(\mathrm{ID}, U) = \alpha^{-1}\cdot\left(\prod_{\mathrm{ID}_i\in U\wedge \mathrm{ID}_i\neq \mathrm{ID}}(\alpha + H_1(\mathrm{ID}_i)) - \prod_{\mathrm{ID}_i\in U\wedge \mathrm{ID}_i\neq \mathrm{ID}} H_1(\mathrm{ID}_i)\right). \tag{12}$$

Then, the user computes CK with I.

$$\mathrm{CK} = \frac{C_1}{I} = \frac{\mathrm{CK}\cdot e(u,v)^k}{e(u,v)^k}. \tag{13}$$

Finally, the user recovers message m_c with CK using the symmetric encryption algorithm.

5.5. Authorized Data Analysis

5.5.1. Health Data Reencryption. In order to analyze the healthcare data, the health data owner runs *Health .ReKeyGen* algorithm to choose a healthcare analyzer's identity ID′, randomly pick $t', b \in \mathbb{Z}_p$, and compute the following with attribute key AK:

$$\begin{aligned} R_1 &= D_3\cdot w^b = g^{1/\varphi}\cdot w^b, \\ R_2 &= v^{t'\cdot(\alpha+H_1(\mathrm{ID}'))}, \\ R_3 &= H_2\left(e(u,v)^{t'}\right)\cdot g^b. \end{aligned} \tag{14}$$

Then, the health data owner outputs the health reencryption key $\mathrm{RK}_h = (R_1, R_2, R_3)$. When receiving the reencryption key, the health cloud runs *Health.ReEnc* algorithm to reencrypt the initial health ciphertext. The health cloud computes

$$\begin{aligned} C_1' &= \frac{C_1}{e\left(R_1, C_5\right)} = \frac{\mathrm{HK}\cdot e(g,g)^{\alpha t}}{e\left(g^{1/\varphi}\cdot w^b, g^{\varphi\alpha t}\right)} \\ &= \mathrm{HK}\cdot e\left(w^b, g^{-\varphi\alpha t}\right). \end{aligned} \tag{15}$$

Finally, the health cloud outputs a reencrypted health ciphertext.

$$\begin{aligned} \mathrm{RT}_h = \Big(&C' = C = \mathrm{SE}_{\mathrm{HK}}(m_h),\ C_1' = \mathrm{HK} \\ &\cdot e\left(w^b, g^{-\varphi\alpha t}\right),\ C_2' = R_2 = v^{t'\cdot(\alpha+H_1(\mathrm{ID}'))},\ C_3' = R_3 \\ &= H_2\left(e(u,v)^{t'}\right)\cdot g^b,\ C_4' = C_6 = w^{\varphi\alpha t}\Big). \end{aligned} \tag{16}$$

5.5.2. Social Data Reencryption. The social data is also used to analyze healthcare, such as infectious diseases. The data owner runs *Social.ReKeyGen* algorithm to choose a healthcare analyzer's identity ID′, randomly pick $k', l \in \mathbb{Z}_p$, and compute the following with secret key SK:

$$\begin{aligned} R_1 &= K_1\cdot w^l = u^{1/\pi}\cdot w^l, \\ R_2 &= v^{k'\cdot(\alpha+H_1(\mathrm{ID}'))}, \\ R_3 &= H_2\left(e(u,v)^{k'}\right)\cdot v^l. \end{aligned} \tag{17}$$

Then, the data owner outputs the social reencryption key $\mathrm{RK}_c = (R_1, R_2, R_3)$. Then, receiving the reencryption key, the social cloud runs *Social.ReEnc* algorithm to reencrypt the initial social ciphertext. The social cloud computes

$$\begin{aligned} C_1' &= \frac{C_1}{e\left(R_1, C_3\right)} = \frac{\mathrm{CK}\cdot e(u,v)^k}{e\left(u^{1/\pi}\cdot w^l, v^{\pi k}\right)} \\ &= \mathrm{CK}\cdot e\left(w^l, v^{-\pi k}\right). \end{aligned} \tag{18}$$

Finally, the social cloud outputs a reencrypted social ciphertext.

$$\begin{aligned} \mathrm{RT}_c = \Big(&C' = C = \mathrm{SE}_{\mathrm{CK}}(m_c),\ C_1' = \mathrm{CK} \\ &\cdot e\left(w^l, v^{-\pi k}\right),\ C_2' = R_2 = v^{k'\cdot(\alpha+H_1(\mathrm{ID}'))},\ C_3' = R_3 \\ &= H_2\left(e(u,v)^{k'}\right)\cdot v^l,\ C_4' = C_4 = w^{\pi k}\Big). \end{aligned} \tag{19}$$

5.5.3. Authorized Decryption. For the reencrypted health and social ciphertext, the healthcare analyzer with identity ID′ runs *Analyzer.Decrypt* algorithm to decrypt. For the health data, the healthcare analyzer first computes

$$\begin{aligned} K' &= e\left(K, C_2'\right) = e\left(u^{1/(\alpha+H_1(\mathrm{ID}'))}, v^{t'\cdot(\alpha+H_1(\mathrm{ID}'))}\right) \\ &= e(u,v)^{t'}. \end{aligned} \tag{20}$$

Then, the healthcare analyzer computes

$$Z = \frac{C_3'}{H_2(K')} = \frac{H_2\left(e(u,v)^{t'}\right)\cdot g^b}{H_2\left(e(u,v)^{t'}\right)} = g^b. \tag{21}$$

Finally, the healthcare analyzer computes the HK and recovers the health data m_h.

$$\begin{aligned} \mathrm{HK} &= C_1' \cdot e\left(Z, C_4'\right) \\ &= \mathrm{HK} \cdot e\left(w^b, g^{-\varphi\alpha t}\right) \cdot e\left(g^b, w^{\varphi\alpha t}\right). \end{aligned} \tag{22}$$

For the social data, the healthcare analyzer can compute v^l with secret key and then compute CK and recover the social data m_c.

$$\mathrm{CK} = C_1' \cdot e\left(v^l, C_4'\right) = \mathrm{CK} \cdot e\left(w^l, v^{-\pi k}\right) \cdot e\left(v^l, w^{\pi k}\right). \tag{23}$$

Therefore, the healthcare analyzers can access both the reencrypted health data and the social data for collaboration and analysis with authorization from the data owner.

6. Security Analysis

The sharing data in our scheme is encrypted with CP-ABE and IBBE techniques, which are secure against chosen plaintext attack since the DBDH assumption holds [23, 28]. We analyze the security properties of our scheme as follows [29].

(1) *Data Confidentiality*. The health data is encrypted using access policy, and the confidentiality of health data can be guaranteed against users who do not hold a set of attributes that satisfy the access policy. In the encryption phase, though the health cloud performs encryption computation for the data owner, it still cannot access the data without the attribute key. During the decryption phase, since the set of attributes cannot satisfy the access policy in the ciphertext, the health cloud server cannot recover the value $A = e(g, g)^{\gamma t}$ to further get the desired value HK. Therefore, only the users with valid attributes that satisfy the access policy can decrypt the health ciphertext. The social data is encrypted with a random symmetric key CK, and then CK is protected by IBBE. Since the symmetric encryption and IBBE scheme are secure, the confidentiality of outsourced social data can be guaranteed against unauthorized users whose identities are not in the set of receivers' identities defined by the data owner.

(2) *Fine-Grained Access Control*. The fine-grained access control allows flexibility in specifying differential access policies of individual health data. To enforce this kind of access control, we utilize CP-ABE to escort the symmetric encryption key of health data. In the health data encryption phase of our scheme, the data owner is able to enforce an expressive and flexible access policy and encrypt the symmetric key which is used to encrypt the health data. Specifically, the access policy of encrypted data defined in access tree supports complex operations including both AND and OR gate, which is able to represent any desired access conditions.

(3) *Collusion Resistance*. The users may intend to combine their attribute keys to access the data which they cannot access individually. In our scheme, the central authority generates attribute keys for different users; the attribute key is associated with random γ, which is uniquely related to each user and makes the combination of components in different attribute keys meaningless. Suppose two or more users with different attributes combine together to satisfy the access policy; they cannot compute $F = e(g, g)^{\gamma s}$ in the outsourced decryption phase. Thus, the proposed scheme is collusion-resistant.

7. Performance Analysis

7.1. Functionality Comparisons. We list the key features of our scheme in Table 1 and make a comparison of our scheme with several data sharing schemes in MHSN in terms of health data confidentiality, health data access control, outsourced encryption and decryption, data authorization, and social data collaboration. In order to achieve fine-grained access control, most of these schemes adopt the ABE technique. From the comparison, we can see that only EPPS [27] and our scheme achieve health data outsourced decryption considering the low computing power of resource-constrained mobile devices or healthcare sensors. Zhang et al. [14], Wang et al. [25], Au et al. [20], and our scheme support data authorization by deploying PRE mechanism so that the semitrusted server could reencrypt the ciphertext to data requester for research and analysis purposes without acquiring any plaintext. Further, PEC [26] combines social data with healthcare record for emergency call, and EPPS [27] divides the mobile patients into different groups according to social data. However, both PEC [26] and EPPS [27] only utilize location information of social data and ignore other valuable data in social networks, which makes extensive social data needed in-depth healthcare analysis (e.g., infectious diseases analysis) impossible.

Moreover, the health and social data may be collected and protected by different independent service providers adopting different encryption techniques, such as ABE and IBBE. Thus, to achieve data collaboration of these service providers, data authorization in these different service providers must be supported. Our scheme proposes an efficient CP-ABE construction with outsourced encryption and decryption to achieve efficient fine-grained access control of health data and provides a secure solution for the collaboration of different service providers by transforming the ABE-encrypted health data and IBBE-encrypted social data into an IBE-encrypted one that can only be decrypted by an authorized healthcare analyzer such as specialists, since IBE is more suitable to be employed on resource-constrained mobile devices in MHSN.

7.2. Performance Comparisons. We analyze the performance efficiency of health data encryption, decryption, reencryption key generation, and reencryption by comparing our scheme with several secure health data sharing schemes; the result is shown in Table 2. Let T_r be the computation cost of a single pairing, T_0 be the computation cost of an exponent

Table 1: Functionality comparison of data sharing schemes in MHSN.

	Zhang et al. [14]	Wang et al. [25]	Au et al. [20]	PEC [26]	EPPS [27]	Our scheme
Health data confidentiality	PKE	IBE	CP-ABE	CP-ABE	CP-ABE	CP-ABE
Health data access control	Consent-based	Identity-based	Attribute-based	Attribute-based	Attribute-based	Attribute-based
Outsourced encryption	—	No	No	No	No	Yes
Outsourced decryption	—	No	No	No	Yes	Yes
Data authorization	Yes	Yes	Yes	No	No	Yes
Social data collaboration	No	No	No	Yes	Yes	Yes

Table 2: Comparison of computation overhead for health data sharing.

Schemes	Data encryption	Data decryption	Data reencryption key generation	Data reencryption
Yeh et al. [22]	$T_r + (2N_c + 1)T_0 + T_t$	$2T_r + T_t$	—	—
EPPS [27]	$(3N_c + 1)T_0 + T_t$	T_t	—	—
Au et al. [20]	$(3N_c + 2)T_0 + T_t$	$(2N_c + 1)T_r + N_cT_t$	$(3N_r + 1)T_0 + T_t$	$(2N_r + 2)T_r + N_rT_t$
Wang et al. [25]	$2T_0 + 2T_t$	$2T_r$	$3T_0$	$T_r + T_0$
Our scheme	$5T_0 + T_t$	T_r	$3T_0 + T_t$	T_r

Table 3: Computation overhead of social data sharing.

Data encryption	Data decryption	Data reencryption key generation	Data reencryption	Data authorized decryption
$(N_u + 4)T_0 + T_t$	$2T_r + (N_u - 1)T_0 + T_t$	$4T_0 + T_t$	T_r	$2T_r$

operation in $\mathbb{G}_0$, T_t be the time for an exponent operation in $\mathbb{G}_T$, N_c be the number of attributes in a ciphertext, N_r be the number of attributes in a reencrypted ciphertext, and N_u be the total number of receivers in social networks. We ignore the simple multiplication, hash, and symmetric encryption and decryption operations.

First, we discuss the computation cost of health data encryption and decryption. Since Yeh et al. [22], EPPS [27], and Au et al. [20] all perform standard ABE algorithm locally in the encryption phase, their encryption computation costs are $T_r + (2N_c + 1)T_0 + T_t$, $(3N_c + 1)T_0 + T_t$, and $(3N_c + 2)T_0 + T_t$, respectively, which grow linearly with the number of attributes in access policy. In our scheme, the users with mobile sensors only need to perform $5T_0 + T_t$ to encrypt the data, which is constant, the same as Wang et al. [25] and less than these schemes. In the data decryption phase, receivers in Au et al.'s study [20] use secret keys corresponding to matched attributes to recursively decrypt the health ciphertext, and the computation cost is $(2N_c + 1)T_r + N_cT_t$. In Yeh et al.'s study [22], EPPS [27], and our scheme, most of the decryption computations are outsourced to the cloud server. In particular, users in our scheme only need to perform one pairing operation to decrypt the ciphertext.

Further, in the data authorization phase, Au et al. [20] adopted ABPRE to reencrypt ciphertext for authorized users, and the computation costs of reencryption key generation and data reencryption are both related to the number of attributes of new access policy. Our scheme transforms ABE-encrypted health data to IBE-encrypted health data for analysis purposes, and the computation costs in these two phases are $3T_0 + T_t$ and T_r, which is constant and efficient as in Wang et al.'s study [25].

We also evaluate the computation overhead of social data sharing when the ciphertexts in different service providers need to collaborate together. From Table 3, we can observe that the social data encryption cost on the data owner is $(N_u + 4)T_0 + T_t$ based on IBBE. If the user is one of the desirable receivers, he can perform $2T_r + (N_u - 1)T_0 + T_t$ cost to decrypt ciphertext. Moreover, our scheme also has high efficiency for the social data authorized phase, in which the IBBE-encrypted social data can be reencrypted to IBE-encrypted one by semitrusted social cloud with reencryption key generated by the data owner. The computation cost of generating reencryption key is $4T_0 + T_t$, and the semitrusted social cloud needs to take T_r cost to finish the social data reencryption. At last, the authorized healthcare analyzer needs to perform $2T_r$ to obtain the social data or health data which are both protected by IBE.

7.3. Experimental Evaluation. We conduct experiments on a Linux system with an Intel Core 2 Duo CPU with 2.53 GHz processor and 4 GB memory. The experimental prototype is written in C language with the assistance of cpabe toolkit and pairing-based cryptography library [30]. We use a pairing-friendly type A 160-bit elliptic curve group based on the supersingular curve over a 512-bit finite field. The Advanced Encryption Standard (AES) is chosen as the symmetric key encryption scheme.

We analyze the time cost of the data encryption and decryption by comparing our scheme with Yeh et al. [22], EPPS [27], Au et al. [20], and Wang et al. [25]. In the data encryption phase, the data owner in these schemes encrypts a file with an access policy and posts the encrypted file to the cloud server. Figure 2 shows the computation time on data owners during this phase. The encryption time on data

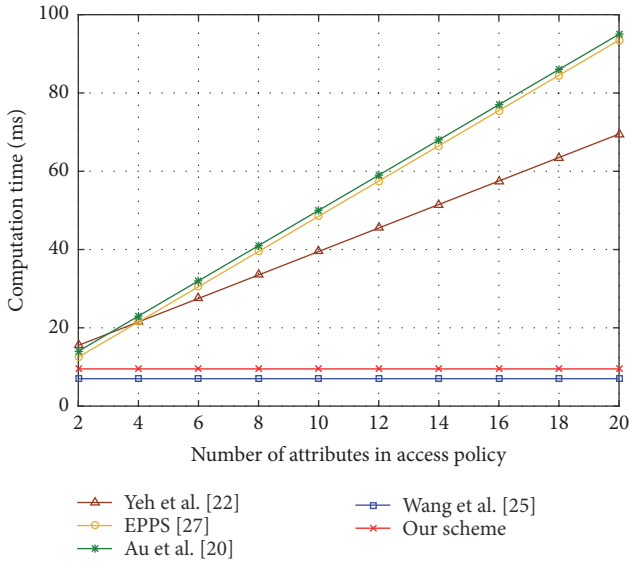

Figure 2: Computation cost of health data encryption.

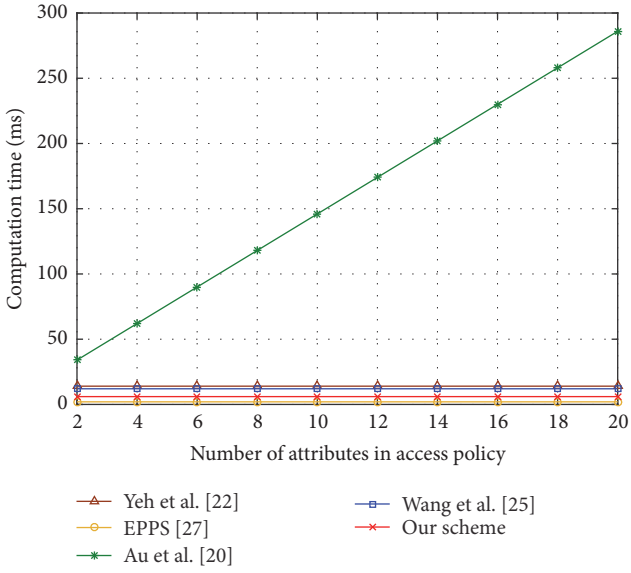

Figure 3: Computation cost of health data decryption.

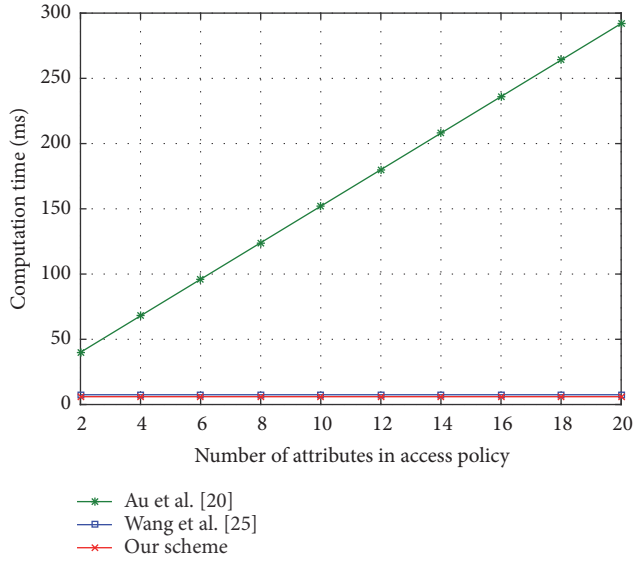

Figure 4: Computation cost of health data reencryption.

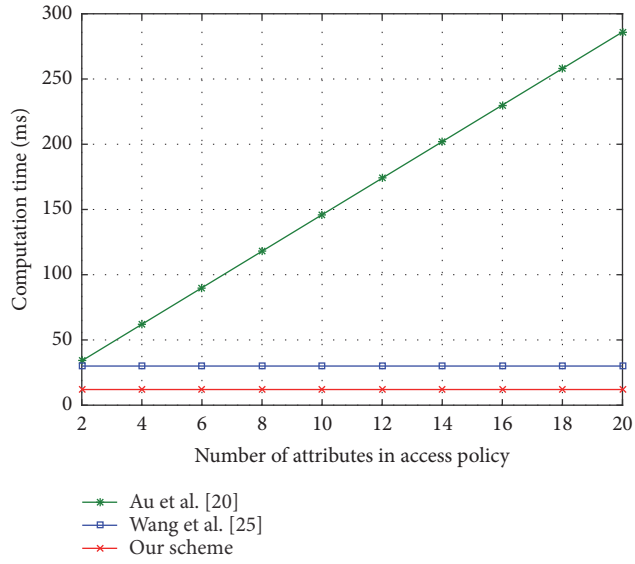

Figure 5: Computation cost of health data authorized decryption.

owners grows with the number of attributes in access policy in Yeh et al. [22], EPPS [27], and Au et al. [20], while it stays constant in our scheme. In the data decryption phase, Figure 3 shows the computation time on healthcare providers for decryption versus the number of attributes in access policy of ciphertext. Compared to Au et al. [20], we can see that the decryption times of Yeh et al. [22], EPPS [27], and our scheme are almost the same, which are constant since most of the laborious decryption operations are delegated to the cloud server.

Furthermore, we evaluate the computation time cost in health data reencryption phase and health data authorized decryption phase, and the results are shown in Figures 4 and 5, respectively. We compare our scheme with that of Au et al. [20] which utilizes ABPRE to support a general framework for secure sharing of PHR and that of Wang et al. [25] which adopts IBPRE. We can observe that the experimental results in Au et al. [20] approximately follow a linear relationship as the number of attributes increases. In our scheme, the data owner generates reencryption keys for authorized healthcare analyzers so that the ABE-based ciphertext can be reencrypted to an IBE-based one and then be decrypted with a secret key, which is independent of the number of attributes in access policy as in Wang et al. [25].

8. Conclusion

In this paper, we focus on the secure health data and social data sharing and collaboration in MHSN for smart cities and propose a detailed construction based on ABE and

IBBE. Our scheme allows the data owner to authorize the healthcare analyzers to access data by reencrypting both ABE-protected health data and IBBE-protected social data to IBE-protected one, which provides a solution for the collaboration of different service providers. In order to reduce the computation overhead of resource-constrained mobile devices, outsourced encryption and decryption construction is adopted in our scheme, which can delegate most of the computation cost to a cloud server. Finally, we analyze the performance of our scheme with the existing schemes in MHSN and conduct experiments. The results have shown that our scheme is secure and efficient.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Key Research and Development Program of China under Grant no. 2016YFB0800605, the National Natural Science Foundation of China under Grant no. 61572080, and the CCF and Venustech Research Program under Grant no. 2016012.

References

[1] M. S. Hossain, G. Muhammad, W. Abdul, B. Song, and B. Gupta, "Cloud-assisted secure video transmission and sharing framework for smart cities," *Future Generation Computer Systems*, 2017.

[2] B. Tang, Z. Chen, G. Hefferman et al., "Incorporating intelligence in fog computing for big data analysis in smart cities," *IEEE Transactions on Industrial Informatics*, no. 99, 2017.

[3] J. Zhou, Z. Cao, X. Dong, X. Lin, and A. Vasilakos, "Securing m-healthcare social networks: challenges, countermeasures and future directions," *IEEE Wireless Communications*, vol. 20, no. 4, pp. 12–21, 2013.

[4] K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen, and H. H. Luo, "Security and privacy for mobile healthcare networks: from a quality of protection perspective," *IEEE Wireless Communications*, vol. 22, no. 4, pp. 104–112, 2015.

[5] H. Huang, T. Gong, N. Ye, R. Wang, and Y. Dou, "Private and secured medical data transmission and analysis for wireless sensing healthcare system," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 3, pp. 1227–1237, 2017.

[6] X. Liang, M. Barua, R. Lu, X. Lin, and X. Shen, "HealthShare: achieving secure and privacy-preserving health information sharing through health social networks," *Computer Communications*, vol. 35, no. 15, pp. 1910–1920, 2012.

[7] J. Zhou, Z. Cao, X. Dong, N. Xiong, and A. V. Vasilakos, "4S: a secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks," *Information Sciences*, vol. 314, pp. 255–276, 2015.

[8] L. Chen, Z. Cao, R. Lu, X. Liang, and X. Shen, "EPF: an event-aided packet forwarding protocol for privacy-preserving mobile healthcare social networks," in *Proceedings of the 54th Annual IEEE Global Telecommunications Conference (GLOBECOM '11)*, Kathmandu, Nepal, December 2011.

[9] L. Guo, C. Zhang, J. Sun, and Y. Fang, "A privacy-preserving attribute-based authentication system for mobile health networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 9, pp. 1927–1941, 2014.

[10] W. Yu, Z. Liu, C. Chen, B. Yang, and X. Guan, "Privacy-preserving design for emergency response scheduling system in medical social networks," *Peer-to-Peer Networking and Applications*, vol. 10, no. 2, pp. 340–356, 2017.

[11] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: challenges and solutions," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 122–129, 2017.

[12] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Healing on the cloud: secure cloud architecture for medical wireless sensor networks," *Future Generation Computer Systems*, vol. 55, pp. 266–277, 2016.

[13] T.-L. Chen, Y.-T. Liao, Y.-F. Chang, and J.-H. Hwang, "Security approach to controlling access to personal health records in healthcare service," *Security and Communication Networks*, vol. 9, no. 7, pp. 652–666, 2016.

[14] A. Zhang, A. Bacchus, and X. Lin, "Consent-based access control for secure and privacy-preserving health information exchange," *Security and Communication Networks*, vol. 9, no. 16, pp. 3496–3508, 2016.

[15] Q. Huang, Y. Yang, and M. Shen, "Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing," *Future Generation Computer Systems*, vol. 72, pp. 239–249, 2017.

[16] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT '05)*, pp. 457–473, Springer, Aarhus, Denmark, May 2005.

[17] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, Berkeley, Calif, USA, May 2007.

[18] S. Narayan, M. Gagné, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," in *Proceedings of the ACM Workshop on Cloud Computing Security Workshop (CCSW '10)*, pp. 47–52, Chicago, Ill, USA, October 2010.

[19] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.

[20] M. H. Au, T. H. Yuen, J. K. Liu et al., "A general framework for secure sharing of personal health records in cloud system," *Journal of Computer and System Sciences*, 2017.

[21] Y. Liu, Y. Zhang, J. Ling, and Z. Liu, "Secure and fine-grained access control on e-healthcare records in mobile cloud computing," *Future Generation Computer Systems*, 2017.

[22] L.-Y. Yeh, P.-Y. Chiang, Y.-L. Tsai, and J.-L. Huang, "Cloud-based fine-grained health information access control framework for lightweight IoT devices with dynamic auditing and attribute revocation," *IEEE Transactions on Cloud Computing*, no. 99, 2015.

[23] P. Zhang, Z. Chen, J. K. Liu, K. Liang, and H. Liu, "An efficient access control scheme with outsourcing capability and attribute update for fog computing," *Future Generation Computer Systems*, 2016.

[24] A. Zanella, N. Bui, A. P. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014.

[25] X. A. Wang, J. Ma, F. Xhafa, M. Zhang, and X. Luo, "Cost-effective secure E-health cloud system using identity based cryptographic techniques," *Future Generation Computer Systems*, vol. 67, pp. 242–254, 2017.

[26] X. Liang, R. Lu, L. Chen, X. Lin, and X. Shen, "PEC: a privacy-preserving emergency call scheme for mobile healthcare social networks," *Journal of Communications and Networks*, vol. 13, no. 2, pp. 102–112, 2011.

[27] S. Jiang, X. Zhu, and L. Wang, "EPPS: Efficient and privacy-preserving personal health information sharing in mobile healthcare social networks," *Sensors*, vol. 15, no. 9, pp. 22419–22438, 2015.

[28] Y. Zhou, H. Deng, Q. Wu, B. Qin, J. Liu, and Y. Ding, "Identity-based proxy re-encryption version 2: making mobile access easy in cloud," *Future Generation Computer Systems*, vol. 62, pp. 128–139, 2016.

[29] Q. Huang, L. Wang, and Y. Yang, "DECENT: secure and fine-grained data access control with policy updating for constrained IoT devices," *World Wide Web*, pp. 1–17, 2017.

[30] B. Lynn, The pairing-based cryptography library, http://crypto.stanford.edu/pbc/.