Privacy-preserving Cloud-based Personal Health Record System Using Attribute-based Encryption and Anonymous Multi-Receiver Identity-based Encryption

Changji Wang
Cisco School of Informatics, Guangdong University of Foreign Studies, Guangzhou 510006, China
E-mail: wchangji@gmail.com

Xilei Xu, Dongyuan Shi and Jian Fang
School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510275, China

Keywords: personal health record, cloud computing, ciphertext-policy attribute-based encryption, anonymous multi-receiver identity-based encryption

Received: July 16, 2015

As an emerging patient-centric model of health information exchange, cloud-based personal health record (CB-PHR) system holds great promise for empowering patients and ensuring more effective delivery of health care. In this paper, we design a novel CB-PHR system. It allows PHR owners to securely store their health data on the semi-trusted cloud service providers, and to selectively share their health data with a wide range of PHR users. To reduce the key management complexity, we divide PHR users into two security domains named public domain and personal domain. PHR owners encrypt their health data for the public domain using ciphertext-policy attribute-based encryption scheme, while encrypt their health data for the personal domain using anonymous multi-receiver identity-based encryption scheme. Only authorized users whose credentials satisfy the specified ciphertext-policy or whose identities belong to dedicated identities can decrypt the encrypted health data. Extensive analytical and experimental results are presented which show that our CB-PHR system is secure, privacy-protected, scalable and efficient.

Povzetek: Predstavljen je sistem CB-PHR, tj. sistem za oblačne zdravstvene kartone.

1 Introduction

In recent years, personal health record system has emerged as a patient-centric model of health information exchange. It enables the patient to create and control their health data in a centralized place through web-based application from anywhere and at any time, which has made the storage, retrieval, and sharing of the health data more efficient. Due to the high cost of building and maintaining specialized data centers, as well as vigorous development of cloud computing in recent years, many PHR services are outsourced to third-party cloud service providers (CSPs), for example, Microsoft Health Vault, Google Health, Indivo and MyPHR.

Although cloud-assisted PHR services could offer a great opportunity to improve the quality of health care services and potentially reduce health care costs, there have been wide privacy concerns as personal health information could be exposed to those semi-trusted CSPs and to unauthorized parties. Health data can reveal very sensitive information, including fertility, surgical procedures, emotional and psychological disorders and diseases, etc. There exist health care regulations such as HIPAA which is recently amended to incorporate business associates, but CSPs are usually not covered entities. Moreover, due to the high value of health data, CSPs are often the targets of various malicious behaviors which may lead to exposure of health data. In addition, CSPs have significant commercial interest in collecting and sharing patients' health data with either pharmacy companies, research institutions or insurance companies.

To keep sensitive health data confidential against those semi-trusted CSPs and unauthorized parties in a CB-PHR system, a natural way is to store only the encrypted data in the cloud. While it is important to allow patients to selectively share their health data with a wide range of users, including staffs from health care providers and medical research institutions, and family members or friends, thus it is essential to provide fine-grained data access control mechanisms that work with semi-trusted CSPs.

1.1 Related work

Anonymous Multi-Receiver Identity-Based Encryption: Boneh and Franklin [1] proposed the first practical and secure identity-based encryption (IBE) scheme from bilinear pairings. Since then, IBE has attracted a lot of attention and a large number of IBE schemes and related

systems have been proposed.

Considering a situation where a sender would like to encrypt a message for t receivers, the sender must encrypt the message t time using conventional IBE schemes. To improve the performance, Baek et al. [2] first introduced the notion of multi-receiver IBE scheme, and proposed an efficient provably secure multi-receiver IBE scheme from bilinear pairings. Next, Boyen and Waters [3] proposed an anonymous IBE scheme to guarantee receiver's privacy, where the ciphertext does not leak the identity of the recipient. Later, Fan et al. [4] introduced the concept of anonymous multi-receiver IBE (AMRIBE) scheme, and proposed an AMRIBE scheme from bilinear parings. Fan et al. claimed that their AMRIBE scheme makes it impossible for an attacker or any other receiver to derive the identity of a message receiver such that the privacy of every receiver can be guaranteed. Unfortunately, Chien [5] showed that in Fan et al.'s AMRIBE scheme any selected receiver may extract the identities of the other selected receivers, and presented an improved AMRIBE scheme. However, only heuristic arguments for security proofs are presented. Recently, Tseng et al. [6] proposed an efficient AMRIBE scheme with complete receiver anonymity and proved that the scheme is semantically secure against adaptively chosen-ciphertext attacks.

Attribute-Based Encryption: In some scenarios, the recipient of the ciphertext is not yet known at the time of the encryption or there are more than one recipient who should be able to decrypt the ciphertext. To preserve data confidentiality and enforce fine-grained access control simultaneously, Sahai and Waters [7] first introduced the concept of attribute-based encryption (ABE), which is envisioned as an important tool for addressing the problem of secure and fine-grained data sharing and access control.

ABE has attracted lots of attention from both academia and industry in recent years, various ABE schemes have been proposed, such as [8–13]. There are two main types of ABE schemes in the literatures: Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE).

In a KP-ABE system, ciphertexts are labeled by the sender with a set of descriptive attributes, and users' private keys are issued by the trusted attribute authority are associated with access structures that specify which type of ciphertexts the key can decrypt. Goyal et al. [8] proposed the first KP-ABE scheme, which was very expressive in that it allowed the access policies to be expressed by any monotonic formula over encrypted data. While in a CP-ABE system, when a sender encrypts a message, they specify a specific access policy in terms of access structure over attributes in the ciphertext, stating what kind of receivers will be able to decrypt the ciphertext. Users possess sets of attributes and obtain corresponding secret attribute keys from the attribute authority, such a user can decrypt a ciphertext if his/her attributes satisfy the access policy associated with the ciphertext. Bethencourt et al. [9] constructed the first CP-ABE scheme, but its security was proved in the generic group model. Later, Waters [10] proposed an efficient CP-ABE scheme with expressive access policy described in general linear secret sharing scheme.

Several CB-PHR systems using ABE schemes have been developed in recent years. Ibraimi et al. [14] proposed a secure PHR management system using Bethencourt et al.'s CP-ABE scheme, which allows PHR owners to encrypt their health data according to an access policy over a set of attributes issued by two trusted authorities. Later, Li et al. [15] proposed a secure and scalable PHR sharing framework on semi-trusted storage servers under multi-owner settings by leveraging both KP-ABE and CP-ABE techniques.

1.2 Our contributions

As we all know, semantically secure against adaptive chosen-ciphertext attacks (IND-CCA) is the de facto level of security required for asymmetric encryption schemes used in practice. Access policy supported by Waters's CP-ABE scheme [10] is expressive. However, it is only proved to be semantically secure against chosen-plaintext attack (IND-CPA). Okamoto and Pointcheval [16] proposed a method named rapid enhanced-security asymmetric cryptosystems transform (REACT) for any asymmetric encryption schemes to achieve IND-CCA secure from IND-CPA secure. In this paper, we first apply REACT technique for Waters' CP-ABE scheme [10] to obtain an IND-CCA secure CP-ABE scheme in the random oracle model.

Tseng et al. [6] extended Boneh and Franklin's IBE scheme [1] to multiple recipients scenario and proposed an efficient AMRIBE scheme. To achieve IND-CCA secure, they adopted the Fujisaki-Okamoto transformation [17] for any asymmetric encryption schemes to achieve IND-CCA secure from one-way secure in the random oracle model. We note that k can play the same role as σ in the Fujisaki-Okamoto transformation of Tseng et al.'s AMRIBE scheme [6]. In this paper, we further improve Tseng et al.'s AMRIBE scheme without compromising security.

Finally, we propose a new CB-PHR system, which allows patients to securely store their health data on semi-trusted CSPs, and selectively share their health data with a wide range of users, including health care professionals like doctors and nurses, family members or friends. To reduce the key management complexity for PHR owners and PHR users, we divide the system into public domain (PUD) and personal domain (PSD). The PUD consists of users who make access based on their professional roles, such as doctors, nurses and medical researchers. The PSD consists of users who are familiar to the PHR owner, such as family members or close friends. PHR owners encrypt their health data for the PUD user using CP-ABE scheme, while they encrypt their health data for the PSD using AMRIBE scheme. Only authorized users whose credentials satisfy the specified ciphertext-policy or whose identities belong to dedicated identities can decrypt the encrypted health data, where ciphertext-policy or dedicated identities are embedded in the encrypted health data.

1.3 Paper organization

This paper is structured as follows. We review some necessary preliminary work in Section 2. Next, we describe our proposed CB-PHR system in Section 3. Then, we give security and efficiency analysis in Section 4. Finally, we conclude our paper and discuss our future work in Section 5.

2 Preliminaries

A prime order bilinear group generator $\mathcal{G}$ is an algorithm that takes as input a security parameter κ and outputs a bilinear group $(p, \mathbf{G}_1, \mathbf{G}_2, \hat{e}, g)$, where p is a prime of size 2^κ, $\mathbf{G}_1$ and $\mathbf{G}_2$ are p order cyclic groups, g is a generator of $\mathbf{G}_1$, and $\hat{e} : \mathbf{G}_1 \times \mathbf{G}_1 \to \mathbf{G}_2$ is a bilinear map with the following properties:

- Bilinearity: $\hat{e}(g^a, g^b) = \hat{e}(g, g)^{ab}$ for $a, b \overset{\$}{\leftarrow} \mathbf{Z}_p^*$. Here $x \overset{\$}{\leftarrow} \mathbf{S}$ is denoted by picking an element a uniformly at random from the set $\mathbf{S}$.
- Non-degeneracy: $\hat{e}(g, g)$ is a generator of $\mathbf{G}_2$.
- Computability: There is an efficient algorithm to compute $\hat{e}(g_1, g_2)$ for $g_1, g_2 \overset{\$}{\leftarrow} \mathbf{G}_1$.

The *bilinear Diffie-Hellman (BDH)* assumption in a prime order bilinear group $(p, \mathbf{G}_1, \mathbf{G}_2, \hat{e}, g)$ is that if a tuple (g, g^a, g^b, g^c) is given for unknown $a, b, c \overset{\$}{\leftarrow} \mathbf{Z}_p^*$, there is no probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ can compute $\hat{e}(g, g)^{abc}$ with non-negligible advantage.

The *decisional bilinear Diffie-Hellman (DBDH)* assumption in a prime order bilinear group $(p, \mathbf{G}_1, \mathbf{G}_2, \hat{e}, g)$ is that if a tuple (g, g^a, g^b, g^c, T) is given for unknown $a, b, c \overset{\$}{\leftarrow} \mathbf{Z}_p^*$ and $T \overset{\$}{\leftarrow} \mathbf{G}_2$, there is no PPT adversary $\mathcal{A}$ can decide whether $T = \hat{e}(g, g)^{abc}$ with non-negligible advantage.

The *gap bilinear Diffie-Hellman (GBDH)* assumption in a prime order bilinear group $(p, \mathbf{G}_1, \mathbf{G}_2, \hat{e}, g)$ is that if a tuple (g, g^a, g^b, g^c) is given for unknown $a, b, c \overset{\$}{\leftarrow} \mathbf{Z}_p^*$, there is no PPT adversary $\mathcal{A}$ can compute $\hat{e}(g, g)^{abc}$ with the help of the DBDH oracle with non-negligible advantage. The DBDH oracle means that given a tuple (g, g^a, g^b, g^c, T), outputs 1 if $T = \hat{e}(g, g)^{abc}$ and 0 otherwise.

The *decisional q-parallel bilinear Diffie-Hellman exponent (q-DBDHE)* assumption is that if $X \overset{\$}{\leftarrow} \mathbf{G}_2$ and $\vec{y} =$

$$(g, g^s, g^a, \ldots, g^{(a^q)}, g^{(a^{q+2})}, \ldots, g^{(a^{2q})},$$
$$g^{s \cdot b_j}, g^{a/b_j}, \ldots, g^{(a^q/b_j)}, g^{(a^{q+2}/b_j)}, \ldots, g^{(a^{2q}/b_j)},$$
$$g^{a \cdot s \cdot b_k/b_j}, \ldots, g^{(a^q \cdot s \cdot b_k/b_j)}).$$

are given for unknown $a, s, b_1, \ldots, b_q \overset{\$}{\leftarrow} \mathbf{Z}_p^*$, where $1 \leq j \leq q$, $1 \leq k \leq q$ and $k \neq j$, there is no PPT adversary $\mathcal{A}$ can decide whether $X = \hat{e}(g, g)^{a^{q+1}s}$ with non-negligible advantage.

Let $\mathbf{\Omega} = \{\mathtt{attr}_1, \mathtt{attr}_2, \ldots, \mathtt{attr}_n\}$ be a set of attributes. A collection $\mathbb{A} \subseteq 2^{\mathbf{\Omega}}$ is monotone if for any set of attributes $\vec{\eta}$ and $\vec{\vartheta}$, we have that if $\vec{\eta} \in \mathbb{A}$ and $\vec{\eta} \subseteq \vec{\vartheta}$ then $\vec{\vartheta} \in \mathbb{A}$. An *access structure* (respectively, *monotone access structure*) is a collection (respectively, monotone collection) $\mathbb{A} \subseteq 2^{\mathbf{\Omega}} \setminus \{\emptyset\}$. The sets in $\mathbb{A}$ are called the authorized sets of attributes, and the sets not in $\mathbb{A}$ are called the unauthorized sets of attributes.

If a set of attributes $\vec{\omega}$ satisfies an access structure $\mathbb{A}$, we denote it as $\mathbb{A}(\vec{\omega}) = 1$. In this paper, we restrict our attention to monotone access structures. As stated in [18], any monotone access structure can be represented by a linear secret sharing scheme (LSSS). A secret sharing scheme Π for an access structure $\mathbb{A}$ over a set of attributes $\mathbf{\Omega}$ is called linear over $\mathbf{Z}_p$ if

- The shares for each attribute form a vector over $\mathbf{Z}_p$.
- There exists a matrix $\mathbf{M}_{\ell \times n}$ called the share generating matrix for Π. For all $i = 1, 2, \ldots, \ell$, we let the function ρ defined the attribute labeling row i of $\mathbf{M}_{\ell \times n}$ as $\rho(i)$. When we consider the column vector $\vec{v} = (s, r_2, \ldots, r_n)^\intercal$, where $s \in \mathbf{Z}_p$ is the secret to be shared, and $r_2, \ldots, r_n \overset{\$}{\leftarrow} \mathbf{Z}_p$, then $\vec{\alpha} = \mathbf{M}_{\ell \times n}\vec{v}$ is the vector of ℓ shares of the secret s according to Π. The share $\alpha_i = (\mathbf{M}_{\ell \times n}\vec{v})_i$ belongs to attribute $\rho(i)$.

Beimel [18] showed that every LSSS enjoys the linear reconstruction property: Suppose that Π is a LSSS for the access structure $\mathbb{A}$. Let $\vec{\omega} \in \mathbb{A}$ be any authorized set, and define $\mathbf{I} = \{i | \rho(i) \in \vec{\omega}\} \subset \{1, 2, \ldots, \ell\}$. If $\{\alpha_i\}$ are valid shares of any secret s according to Π, then there exist constants $\{\beta_i\}$ for $i \in \mathbf{I}$ such that $\sum_{i \in \mathbf{I}} \alpha_i \beta_i = s$, and these constants $\{\beta_i\}$ can be found in time polynomial in the size of $\mathbf{M}_{\ell \times n}$. For unauthorized sets, no such constants $\{\beta_i\}$ exist.

3 Our CB-PHR system

There are four participants involved in our CB-PHR system.

- A trusted authority (TA), who acts as the root of trust and is responsible for generating system parameters, issuing attribute-based private keys or identity-based private keys for PHR owners and PHR users.
- A semi-trusted CSP, who manages a cloud to provide data storage service. It is important to assume that CSP is semi-trusted, which means CSP will try to find out as much secret information in the stored health data as possible, but it will honestly follow the protocol in general.
- Multiple PHR users, who belong to PUD or PSD. PHR users in PUD make access based on their professional roles, such as doctors, nurses, and medical researchers, while PHR users in PSD make access based

on their identities, such as patients' family members or close friends.

– Multiple PHR owners (patients), who encrypt and outsource their sensitive health data to CSP. Specifically, PHR owners encrypt their health data for PUD users using improved Waters' CP-ABE scheme, while they encrypt their health data for PSD users using improved Tseng et al.'s AMRIBE scheme.

Fig.1 illustrates the system architecture and workflow of our CB-PHR system, which is explained as follows.

3.1 Setup

TA first defines the universe $\mathbf{\Omega}$ of attributes, runs $\mathcal{G}(1^\kappa) \rightarrow (p, \mathbf{G}_1, \mathbf{G}_2, \hat{e}, g)$, chooses $x, y \xleftarrow{\$} \mathbf{Z}_p^*$, $h_i \xleftarrow{\$} \mathbf{G}_1$ for $1 \leq i \leq n$. Next, TA computes $h = g^x$ and $Y = \hat{e}(g,g)^y$, picks a semantically secure symmetric encryption scheme Γ with key space $\mathbf{K}$, encryption algorithm Enc and decryption algorithm Dec, respectively. TA then chooses a cryptographically secure message authentication code $\mathrm{MAC} : \mathbf{K} \times \{0,1\}^* \rightarrow \mathbf{Z}_p^*$, three cryptographically secure hash functions: $H_1 : \{0,1\}^* \rightarrow \mathbf{G}_1$, $H_2 : \mathbf{G}_2 \rightarrow \mathbf{K}$ and $H_3 : \mathbf{G}_2 \rightarrow \mathbf{Z}_p^*$. Finally, TA sets the master secret key $msk = \langle x, g^y \rangle$, and the system parameters $mpk = \langle \mathbf{\Omega}, p, \mathbf{G}_1, \mathbf{G}_2, \hat{e}, g, h, Y, \{h_i\}_{i=1}^n, \{H_i\}_{i=1}^3, \mathrm{MAC}, \Gamma \rangle$.

3.2 KeyGen

Given a user's identity ID, and a set $\vec{\omega} \subseteq \mathbf{\Omega}$ of attributes belonging to the user, TA chooses $z \xleftarrow{\$} \mathbf{Z}_p^*$, computes $g_{\mathsf{ID}} = H_1(\mathsf{ID})$, $D_{\mathsf{ID}} = g_{\mathsf{ID}}^x$, $K = g^{xz} g^y$, $L = g^z$, $K_i = h_i^z$ for all $\mathsf{attr}_i \in \vec{\omega}$. TA then sets user's private key $sk_{\mathsf{ID},\vec{\omega}} = \langle D_{\mathsf{ID}}, K, L, \{K_i\}_{\mathsf{attr}_i \in \vec{\omega}} \rangle$, and sends $sk_{\mathsf{ID},\vec{\omega}}$ to the user via a secure channel.

Note: If a user requests identity-based private key corresponding to an identity ID, then TA only needs to compute $sk_{\mathsf{ID}} = D_{\mathsf{ID}}$. If a user requests attribute-based private key corresponding to a set $\vec{\omega}$ of attribute, then TA only needs to compute $sk_{\vec{\omega}} = \langle K, L, \{K_i\}_{\mathsf{attr}_i \in \vec{\omega}} \rangle$.

3.3 Encrypt

Given an original health data m to be encrypted, a LSSS access structure $\mathbb{A} = (\mathbf{M}_{\ell \times n}, \rho)$ and a list of identities $\mathbf{ID}_R = \{\mathsf{ID}_i\}_{i=1}^t$, PHR owner performs the following steps.

1. Choose $s \xleftarrow{\$} \mathbf{Z}_p^*$, $u_1, \ldots, u_n, r_1, \ldots, r_\ell \xleftarrow{\$} \mathbf{Z}_p$, $U \xleftarrow{\$} \mathbf{G}_2$, and set $\vec{u} = (s, u_2, \ldots, u_n)^\intercal$.
2. Compute $k_1 = H_2(U)$, $E_1 = \mathrm{Enc}(k_1, m)$, $C' = g^s$, $C_1' = U \cdot \hat{e}(g,g)^{sy}$, $\alpha_i = (\mathbf{M}_{\ell \times n} \vec{u})_i$, $C_i = g^{x\alpha_i} h_{\rho(i)}^{-r_i}$, and $D_i = g^{r_i}$ for $1 \leq i \leq \ell$, $\lambda_1 = \mathrm{MAC}(k_1, m, E_1, C', C_1', C_1, D_1, \ldots, C_\ell, D_\ell)$.
3. Choose $k_2 \xleftarrow{\$} \mathbf{K}$, compute $E_2 = \mathrm{Enc}(k_2, m)$, $g_{\mathsf{ID}_i} = H_1(\mathsf{ID}_i)$ and $v_i = H_3(\hat{e}(g_{\mathsf{ID}_i}, h)^s)$ for $\mathsf{ID}_i \in \mathbf{ID}_R$.
4. Construct the polynomial $f(x) = \prod_{i=1}^t (x - v_i) + k_2 = c_0 + c_1 x + \cdots + c_{t-1} x^{t-1} + x^t \bmod p$, compute $\lambda_2 = \mathrm{MAC}(k_2, m, E_2, C', c_0, c_1, \ldots, c_{t-1})$.
5. Set the ciphertext $CT = \langle C', C_1', \{C_i, D_i\}_{i=1}^\ell, \{c_i\}_{i=0}^{t-1}, E_1, E_2, \lambda_1, \lambda_2 \rangle$.
6. Finally, PHR owner uploads the ciphertext to CSP along with a description of access policy $(\mathbf{M}_{\ell \times n}, \rho)$ and a set of identities of designated recipients $\mathbf{ID}_R$.

Note: If a PHR owner wants to share his/her health data with PHR users from the PUD, then the PHR owner only needs to perform step 1 and step 2. If a PHR owner wants to share his/her health data with PHR users from the PSD, then the PHR owner only needs to perform step 3, step 4 and compute $C' = g^s$.

3.4 Decrypt

Given a ciphertext CT along with a description of access policy $\mathbb{A} = (\mathbf{M}_{\ell \times n}, \rho)$ and a set $\mathbf{ID}_R$ of identities, a PHR user performs different steps depending on whether the PHR user is from the PUD or from the PSD.

– If the PHR user is from the PUD, and he owns credentials corresponding to a set $\vec{\omega}$ of attributes such that $\mathbb{A}(\vec{\omega}) = 1$, then the PHR user computes

$$\begin{aligned}
\widetilde{U} &= C_1' \cdot \frac{\prod_{i \in \mathbf{I}} (\hat{e}(C_i, L) \hat{e}(D_i, K_{\rho(i)}))^{\beta_i}}{\hat{e}(C', K)} \\
\widetilde{k}_1 &= H_2(\widetilde{U}) \\
\widetilde{m} &= \mathrm{Dec}(\widetilde{k}_1, E_1) \\
\widetilde{\lambda}_1 &= \mathrm{MAC}(\widetilde{k}_1, \widetilde{m}, E_1, C', C_1', \{C_i, D_i\}_{i=1}^\ell)
\end{aligned}$$

where $\rho(i), \beta_i$ and $\mathbf{I}$ are defined in Section 2. Finally, PHR user tests whether $\widetilde{\lambda}_1 = \lambda_1$ or not. If it holds, PHR user accepts the message $\widetilde{m} = m$ and outputs $\perp$ otherwise.

– If the PHR user is from the PSD, and his identity ID_i belongs to the set $\mathbf{ID}_R$ of identities of designated recipients, then the PHR user computes

$$\begin{aligned}
\widehat{v}_i &= H_2(\hat{e}(D_{\mathsf{ID}_i}, C')) \\
\widehat{k}_2 &= f(\widetilde{v}_i) \\
&= c_0 + c_1 \widetilde{v}_i + \ldots + c_{t-1} \widetilde{v}_i^{t-1} + \widetilde{v}_i^t \bmod p \\
\widehat{m} &= \mathrm{Dec}(\widehat{k}_2, E_2), \\
\widehat{\lambda}_2 &= \mathrm{MAC}(\widehat{k}_2, \widehat{m}, E_2, C', c_0, c_1, \ldots, c_{t-1})
\end{aligned}$$

Finally, PHR user tests whether $\widehat{\lambda}_2 = \lambda_2$ or not. If it holds, PHR user accepts the message $\widehat{m} = m$ and outputs $\perp$ otherwise.

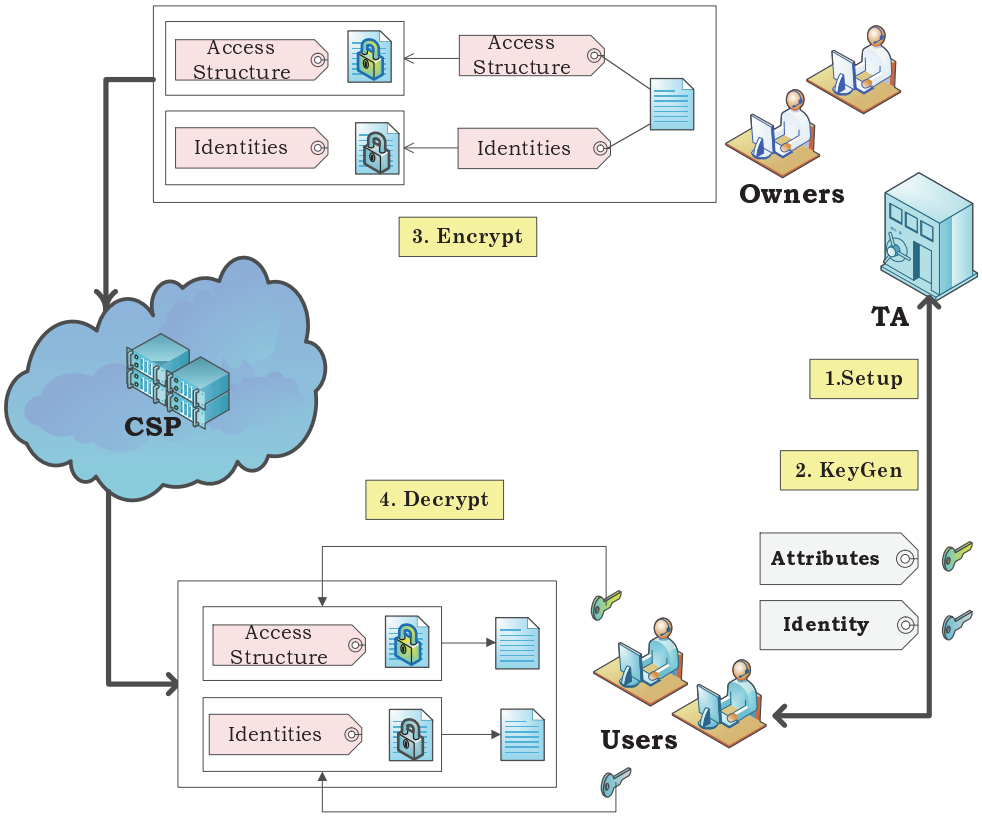


Figure 1: Architecture and workflow of our CB-PHR system.

4 Security proofs and efficiency analysis

Theorem 1. *Our CB-PHR system is correct.*

Proof. The correctness can be verified as follows.

$$\frac{\hat{e}(C', K)}{\prod_{i\in\mathbf{I}}(\hat{e}(C_i, L)\hat{e}(D_i, K_{\rho(i)}))^{\beta_i}}$$
$$= \frac{\hat{e}(g^s, g^{xz}g^y)}{\prod_{i\in\mathbf{I}}[\hat{e}(g^{x\alpha_i}h_{\rho(i)}^{-r_i}, g^z)\hat{e}(g^{r_i}, h_{\rho(i)}^z)]^{\beta_i}}$$
$$= \frac{\hat{e}(g,g)^{sy}\hat{e}(g,g)^{sxz}}{\prod_{i\in\mathbf{I}}\hat{e}(g,g)^{xz\alpha_i\beta_i}} = \frac{\hat{e}(g,g)^{sy}\hat{e}(g,g)^{sxz}}{\hat{e}(g,g)^{xz\sum_{i\in\mathbf{I}}\alpha_i\beta_i}}$$
$$= \frac{\hat{e}(g,g)^{sy}\hat{e}(g,g)^{sxz}}{\hat{e}(g,g)^{sxz}} = \hat{e}(g,g)^{sy}$$

$$H_2(\hat{e}(D_{\mathsf{ID}_i}, C')) = H_2(\hat{e}(g_{\mathsf{ID}_i}^x, g^s))$$
$$= H_2(\hat{e}(g_{\mathsf{ID}_i}, h)^s) = v_i$$

$$f(x) = c_0 + c_1x + \cdots + c_{t-1}x^{t-1} + x^t$$
$$= \prod_{i=1}^{t}(x - v_i) + k_2 \bmod p$$
$$= (x - v_i)F(x) + k_2 \bmod p$$
$$\Rightarrow f(v_i) = c_0 + c_1v_i + \ldots + c_{t-1}v_i^{t-1} + v_i^t$$
$$= (v_i - v_i)F(v_i) + k_2 \bmod p = k_2$$

This completes the proof. □

Theorem 2. *Our CB-PHR system satisfies receiver anonymity in the random oracle model under the GBDH assumption.*

Proof. PHR owners encrypt their health data for receivers in the PUD using an improved Waters's CP-ABE scheme, where REACT technique [16] is applied to achieve IND-CCA secure. Intended receivers are specified through attributes owned by receivers instead of receivers' identities, and these attributes are potentially able to be shared by unlimited number of PHR users. Thus receiver anonymity is satisfied for PHR users in the PUD.

PHR owners encrypt their health data for PHR users in the PSD using an improved Tseng et al.'s AMRIBE scheme [6]. We improved Tseng et al.'s AMRIBE scheme [6] without compromising security by removing σ and related operations, because k plays the same role as σ in the Fujisaki-Okamoto transformation of Tseng et al.'s AMRIBE scheme [6]. Tseng et al.'s AMRIBE scheme is proved to satisfy receiver anonymity in the random oracle model under the GBDH assumption, thus receiver anonymity is satisfied for PHR users in the PSD. □

Table 1: Efficiency analysis of our CB-PHR system

	Private key size	Encrypt cost	Decrypt cost
PHR Owner	$\times$	$N_{\mathrm{R}}t_p + (2\ell+1)t_m + t_e + 2t_E + N_{\mathrm{R}}t_H$	$\times$
A PUD User	$(N_{\mathrm{A}}+2)\lvert\mathbf{G}_1\rvert$	$\times$	$(2+N_{\mathbf{I}})t_p + N_{\mathbf{I}}t_e + t_D$
A PSD User	$\lvert\mathbf{G}_1\rvert$	$\times$	$t_p + t_D$

Theorem 3. *Our CB-PHR system is IND-CCA secure in the selective model under the q-DBDHE assumption and GBDH assumption.*

Proof. PHR owners encrypt their health data for PHR users in the PUD using our improved IND-CCA secure CP-ABE scheme, which is obtained by applying REACT transformation for Waters' CP-ABE scheme [10]. Waters' CP-ABE scheme is proved to be IND-CPA secure in the selective model under the q-DBDHE assumption, and REACT transformation is a generic method for any asymmetric encryption schemes to achieve IND-CCA secure from IND-CPA secure, thus our improved CP-ABE scheme is IND-CCA secure in the selective model under the q-DBDHE assumption. For detailed proofs, we recommend you refer to [10] and [16].

PHR owners encrypt their health data in the PSD using our improved Tseng et al.'s AMRIBE scheme. We improved Tseng et al.'s AMRIBE scheme [6] without compromising security by removing σ and related operations, because k plays the same role as σ in the Fujisaki-Okamoto transformation of Tseng et al.'s AMRIBE scheme [6]. Tseng et al.'s AMRIBE scheme is proved to be IND-CCA secure in the selective model under the GBDH assumption, thus our improved AMRIBE scheme is IND-CCA secure in the selective model under the GBDH assumption. For detailed proofs, we recommend you refer to [6].

In summary, our CB-PHR system is IND-CCA secure in the selective model under the q-DBDHE assumption and GBDH assumption. □

Table 1 shows the computational cost of each participant in our CB-PHR system. Denote by t_p, t_m, t_e, t_H, t_E, t_D, the computation cost of a bilinear pairing in $(\mathbf{G}_1, \mathbf{G}_2)$, a multiplication in $\mathbf{G}_1$, an exponentiation in $\mathbf{G}_2$, a map-to-point hash function H_1, an encryption and a decryption in Γ, respectively. Other operations are omitted in the following analysis since their computation cost is trivial. Denote by N_{R}, N_{A}, $N_{\mathbf{I}}$, $|m|$, $|\mathbf{G}_1|$ and $|\mathbf{Z}_q^*|$ the number of receivers in the PSD, the number of attributes owned by a user in the PUD, the number of attributes in the set $\mathbf{I}$, the bit-length of a plaintext, an element in group $\mathbf{G}_1$, and an element in group $\mathbf{Z}_q^*$, respectively.

In order to evaluate the performance of our CB-PHR system, we implement the corresponding algorithms in our CB-PHR system based on Charm Crypto Framework (version 0.42) [19] and pairing-based crypto (PBC) library [22]. Figure 2 shows the performance of our CB-PHR system, where times are measured in seconds (averaged over 30 iterations) and were computed on an Intel processor with 2GB RAM and hosted on 2.40GHz.

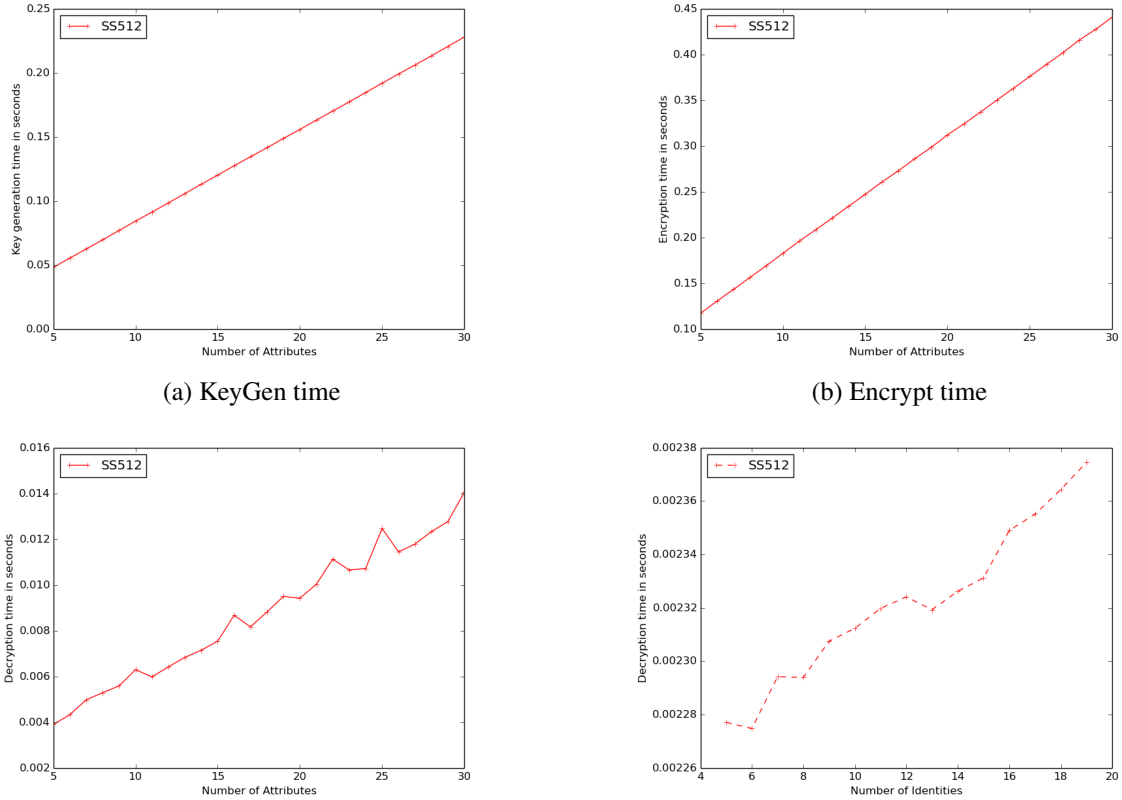
We test on SS512-type elliptic curves with symmetric bilinear pairings, 512 bytes plaintext, AES-256 symmetric encryption algorithm, and the number of attributes and identities are chosen from 5 to 30 and from 5 to 15, respectively. Figure 2(a) illustrates the relationship between the running time for attribute-based private key generation and the number of attributes. Figure 2(b) illustrates the relationship between the running time for encryption and the number of attributes, where we fix the number of receivers 15. Figure 2(c) illustrates the relationship between the running time for decryption for a PHR user in the PUD and the number of attributes. Figure 2(d) illustrates the relationship between the running time for decryption for a user in the PSD and the number of designated receivers.

5 Conclusion

In this paper, we propose a novel patient-centric framework for secure sharing of personal health records in cloud computing. It allows patients to securely store their health data on the semi-trusted cloud service providers, and to selectively share their health data with a wide range of users, including health care professionals such as doctors and nurses, family members or friends. To reduce the key management complexity for patients and users, we divide the users into public domain and personal domain. Different from existing cloud-based personal health record system, patients encrypt their health data for the public domain using ciphertext-policy attribute-based encryption scheme, and encrypt their health data for the personal domain using anonymous multi-receiver identity-based encryption scheme in our cloud-based personal health record system. Extensive analytical and experimental results show that our cloud-based personal health record system is secure, privacy-protected, scalable and efficient. In future work we will design cloud-based personal health record system supporting efficient data utilization services, such as data retrieval and data statistics.

Acknowledgement

This paper is jointly supported by the National Natural Science Foundation of China (Grant No. 61173189), the



(a) KeyGen time

(b) Encrypt time

(c) Decrypt time for PUD users

(d) Decrypt time for PSD users

Figure 2: Performance test of CB-PHR system.

Foundation for Innovative Research Team of Yunnan University, Guangdong Province Information Security Key Laboratory Project, Yunnan Province Software Engineering Key Laboratory Project (Grant No. 2015SE203).

References

[1] D. Boneh and M. Franklin (2001) Identity-based encryption from the Weil pairing, *CRYPTO 2001*, LNCS 2139, Springer Berlin Heidelberg, pp. 213–229.

[2] J. Baek, R. Safavi-Naini and W. Susilo (2005) Efficient Multi-receiver Identity-Based Encryption and Its Application to Broadcast Encryption, *PKC 2005*, LNCS 3386, Springer Berlin Heidelberg, pp.380–397.

[3] X. Boyen and B. Waters (2006) Anonymous hierarchical identity-based encryption (without random oracles), *CRYPTO 2006*, LNCS 4117, Springer Berlin Heidelberg, pp. 290–307.

[4] C.I. Fan, L.Y. Huang and P.H. Ho (2010) Anonymous multireceiver identity-based encryption, *IEEE Transactions on Computers*, Vol. 59, No. 9, pp. 1239–1249.

[5] H.Y. Chien (2012) Improved anonymous multi-receiver identity-based encryption, *The Computer Journal*, Vol. 55, No. 4, pp. 439–445.

[6] Y.M. Tseng, Y.H. Huang and H.J. Chang (2012) CCA-secure anonymous multi-receiver ID-based encryption, *26th International Conference on Advanced Information Networking and Applications Workshops*, IEEE, pp. 177–182.

[7] A. Sahai and b. Waters (2005) Fuzzy identity-based encryption, *EUROCRYPT 2005*, LNCS 3494, Springer Berlin Heidelberg, pp. 457–473.

[8] V. Goyal, O. Pandey, A. Sahai and B. Waters (2006) Attribute-based encryption for fine-grained access control of encrypted data, *CCS 2006*, ACM, New York, pp. 89–98.

[9] J. Bethencourt, A. Sahai and B. Waters (2007) Ciphertext-policy attribute-based encryption, *IEEE Symposium on Security and Privacy*, IEEE, pp. 321–334.

[10] B. Waters (2011) Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization, *PKC 2011*, LNCS 6571, Springer Berlin Heidelberg, pp. 53–70.

[11] J. Li, Q. Wang, C. Wang and R. Kui (2011) Enhancing attribute-based encryption with attribute hierarchy, *Mobile Network Application*, Vol. 16, No. 5, pp. 553–561.

[12] C.J. Wang and J.F. Luo (2013) An efficient key-policy attribute-based encryption scheme with constant ciphertext length, *Mathematical Problems in Engineering*, Hindawi, Vol. 2013, pp. 1–7.

[13] J. Li, X.Y. Huang, J.W. Li, X.F. Chen and Y. Xiang (2014) Securely outsourcing attribute-based encryption with checkability, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 25, No. 8, pp. 2201–2210.

[14] L. Ibraimi, M. Asim and M. Petkovic (2009) Secure management of personal health records by applying attribute-based encryption, *6th International Workshop on Wearable Micro and Nano Technologies for Personalized Health (pHealth)*, IEEE, pp. 71–74.

[15] M. Li, S.C. Yu, Y. Zheng, K. Ren and W.J. Lou (2013) 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.

[16] T. Okamoto and D. Pointcheval (2001) REACT: rapid enhanced-security asymmetric cryptosystem transform, *CT-RSA 2001*, LNCS 2020, Springer Berlin Heidelberg, pp. 159–174.

[17] E. Fujisaki and T. Okamoto (2011) Secure integration of asymmetric and symmetric encryption schemes, *Journal of Cryptology*, Vol. 26, No. 1, pp. 80–101.

[18] A. Beimel (1996) Secure schemes for secret sharing and key distribution, *PhD Thesis*, Israel Institute of Technology, Technion, Haifa, Israel.

[19] J.A. Akinyele, et al. (2013) Charm: a framework for rapidly prototyping cryptosystems, *Journal of Cryptographic Engineering*, Vol. 3, No. 2, pp. 111-128.

[20] M. Green and J.A. Akinyele (2014) The functional encryption library, *Online, accessed 18-July-2014*, `http://code.google.com/p/libfenc/`.

[21] E. Young and T. Hudson (2014) The openssl project, *Online, accessed 18-July-2014*, `http://www.openssl.org/`.

[22] B.Lynn (2014) The pairing-based cryptography library, *Online, accessed 18-July-2014*, `http://crypto.stanford.edu/pbc/`.