PSMPA: Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System

Jun Zhou, Xiaodong Lin, *Senior Member, IEEE*, Xiaolei Dong, and Zhenfu Cao, *Senior Member, IEEE*

Abstract—Distributed m-healthcare cloud computing system significantly facilitates efficient patient treatment for medical consultation by sharing personal health information among healthcare providers. However, it brings about the challenge of keeping both the data confidentiality and patients' identity privacy simultaneously. Many existing access control and anonymous authentication schemes cannot be straightforwardly exploited. To solve the problem, in this paper, a novel authorized accessible privacy model (AAPM) is established. Patients can authorize physicians by setting an access tree supporting flexible threshold predicates. Then, based on it, by devising a new technique of attribute-based designated verifier signature, a patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA) realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system is proposed. The directly authorized physicians, the indirectly authorized physicians and the unauthorized persons in medical consultation can respectively decipher the personal health information and/or verify patients' identities by satisfying the access tree with their own attribute sets. Finally, the formal security proof and simulation results illustrate our scheme can resist various kinds of attacks and far outperforms the previous ones in terms of computational, communication and storage overhead.

Index Terms—Authentication, access control, security and privacy, distributed cloud computing, m-healthcare system

1 Introduction

Distributed m-healthcare cloud computing systems have been increasingly adopted world wide including the European Commission activities, the US Health Insurance Portability and Accountability Act (HIPAA) and many other governments for efficient and high-quality medical treatment [1], [2], [3]. In m-healthcare social networks, the personal health information is always shared among the patients located in respective social communities suffering from the same disease for mutual support, and across distributed healthcare providers (HPs) equipped with their own cloud servers for medical consultant [28], [29]. However, it also brings about a series of challenges, especially how to ensure the security and privacy of the patients' personal health information from various attacks in the wireless communication channel such as eavesdropping and tampering [5], [26].

As to the security facet, one of the main issues is access control of patients' personal health information, namely it is only the authorized physicians or institutions that can recover the patients' personal health information during the data sharing in the distributed m-healthcare cloud computing system. In practice, most patients are concerned about the confidentiality of their personal health information since it is likely to make them in trouble for each kind of unauthorized collection and disclosure. Therefore, in distributed m-healthcare cloud computing systems, which part of the patients' personal health information should be shared and which physicians their personal health information should be shared with have become two intractable problems demanding urgent solutions. There has emerged various research results [8], [9], [10], [11], [15], [16], [18], [19] focusing on them. A fine-grained distributed data access control scheme [9] is proposed using the technique of attribute based encryption (ABE). A rendezvous-based access control method [10] provides access privilege if and only if the patient and the physician meet in the physical world. Recently, a patient-centric and fine-grained data access control in multi-owner settings is constructed for securing personal health records in cloud computing [30]. However, it mainly focuses on the central cloud computing system which is not sufficient for efficiently processing the increasing volume of personal health information in m-healthcare cloud computing system. Moreover, it is not enough for [30] to only guarantee the data confidentiality of the patient's personal health information in the honest-but-curious cloud server model since the frequent communication between a patient and a professional physician can lead the adversary to

- *J. Zhou is with Shanghai Key Lab for Trustworthy Computing, East China Normal University, Shanghai, China, 200062, and Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China, 200240. E-mail: zhoujun_tdt@sjtu.edu.cn.*
- *X. Dong and Z. Cao are with Shanghai Key Lab for Trustworthy Computing, East China Normal University, Shanghai, China, 200062. E-mail: {dongxiaolei, zfcao}@sei.ecnu.edu.cn.*
- *X. Lin is with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, Canada. E-mail: xiaodong.lin@uoit.ca.*

Manuscript received 1 Dec. 2013; revised 4 Mar. 2014; accepted 12 Mar. 2014. Date of publication 26 Mar. 2014; date of current version 8 May 2015.
Recommended for acceptance by X. Li.
For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TPDS.2014.2314119

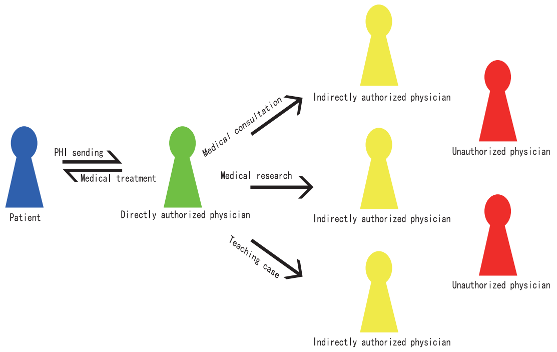


Fig. 1. Multiple security and privacy levels in m-Healthcare cloud computing system.

conclude that the patient is suffering from a specific disease with a high probability. Unfortunately, the problem of how to protect both the patients' data confidentiality and identity privacy in the distributed m-healthcare cloud computing scenario under the malicious model was left untouched.

In this paper, we consider simultaneously achieving data confidentiality and identity privacy with high efficiency. As is described in Fig. 1, in distributed m-healthcare cloud computing systems, all the members can be classified into three categories: the directly authorized physicians with green labels in the local healthcare provider who are authorized by the patients and can both access the patient's personal health information and verify the patient's identity and the indirectly authorized physicians with yellow labels in the remote healthcare providers who are authorized by the directly authorized physicians for medical consultant or some research purposes (i.e., since they are not authorized by the patients, we use the term 'indirectly authorized' instead). They can only access the personal health information, but not the patient's identity. For the unauthorized persons with red labels, nothing could be obtained. By extending the techniques of attribute based access control [22] and designated verifier signatures (DVS) [21] on de-identified health information [27], we realize three different levels of privacy-preserving requirement mentioned above. The main contributions of this paper are summarized as follows.

(1) A novel authorized accessible privacy model (AAPM) for the multi-level privacy-preserving cooperative authentication is established to allow the patients to authorize corresponding privileges to different kinds of physicians located in distributed healthcare providers by setting an access tree supporting flexible threshold predicates.

(2) Based on AAPM, a patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA) in the distributed m-healthcare cloud computing system is proposed, realizing three different levels of security and privacy requirement for the patients.

(3) The formal security proof and simulation results show that our scheme far outperforms the previous constructions in terms of privacy-preserving capability, computational, communication and storage overhead.

The rest of this paper is organized as follows. We discuss related work in the next section. In Section 3, the network model of a distributed m-healthcare cloud computing system is illustrated. We provide some background and preliminaries required throughout the paper in Section 4. Then, we establish a novel authorized accessible privacy model and propose a patient self-controllable multi-level privacy-preserving cooperative authentication scheme respectively in Section 5 and Section 6. In Section 7, we give the security proof and performance evaluations of the proposed scheme. Finally, Section 8 concludes the paper.

2 Related Work

There exist a series of constructions for authorized access control of patients' personal health information [8], [9], [10], [11], [15], [16], [18], [19], [31], [32]. As we discussed in the previous section, they mainly study the issue of data confidentiality in the central cloud computing architecture, while leaving the challenging problem of realizing different security and privacy-preserving levels with respect to (w.r.t.) kinds of physicians accessing distributed cloud servers unsolved. On the other hand, anonymous identification schemes are emerging by exploiting pseudonyms and other privacy-preserving techniques [4], [10], [11], [12], [13], [14], [17], [20], [23], [25]. Lin et. al. proposed SAGE achieving not only the content-oriented privacy but also the contextual privacy against a strong global adversary [12]. Sun et al. proposed a solution to privacy and emergency responses based on anonymous credential, pseudorandom number generator and proof of knowledge [11], [13]. Lu et al. proposed a privacy-preserving authentication scheme in anonymous P2P systems based on Zero-Knowledge Proof [14]. However, the heavy computational overhead of Zero-Knowledge Proof makes it impractical when directly applied to the distributed m-healthcare cloud computing systems where the computational resource for patients is constrained. Misic and Misic suggested patients have to consent to treatment and be alerted every time when associated physicians access their records [31], [32]. Riedl et al. presented a new architecture of pseudonymiaztion for protecting privacy in E-health (PIPE) [25]. Slamanig and Stingl integrated pseudonymization of medical data, identity management, obfuscation of metadata with anonymous authentication to prevent disclosure attacks and statistical analysis in [26] and suggested a secure mechanism guaranteeing anonymity and privacy in both the personal health information transferring and storage at a central m-healthcare cloud server [7]. Schechter et al. proposed an anonymous authentication of membership in dynamic groups [6]. However, since the anonymous authentication mentioned above [6], [7] are established based on public key infrastructure (PKI), the need of an online certificate authority (CA) and one unique public key encryption for each symmetric key k for data encryption at the portal of authorized physicians made the overhead of the construction grow linearly with size of the group. Furthermore, the anonymity level depends on the size of the anonymity set making the anonymous authentication impractical in specific surroundings where the patients are sparsely distributed.

In this paper, the security and anonymity level of our proposed construction is significantly enhanced by associating it to the underlying Gap Bilinear Diffie-Hellman (GBDH) problem and the number of patients' attributes to deal with the privacy leakage in patient sparsely distributed

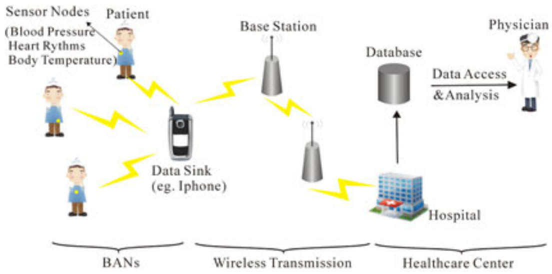


Fig. 2. An basic architecture of the e-health system.

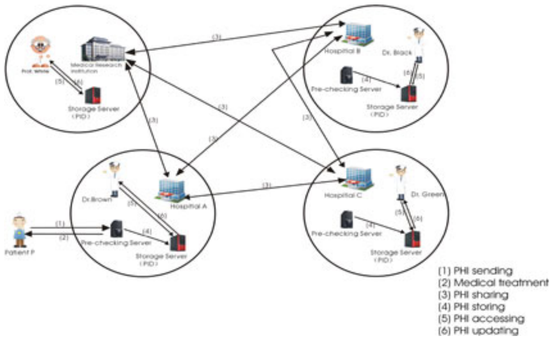


Fig. 3. An overview of our distributed m-healthcare cloud computing system.

scenarios in [6], [7]. More significantly, without the knowledge of which physician in the healthcare provider is professional in treating his illness, the best way for the patient is to encrypt his own PHI under a specified access policy rather than assign each physician a secret key. As a result, the authorized physicians whose attribute set satisfies the access policy can recover the PHI and the access control management also becomes more efficient.

Last but not least, it is noticed that our construction essentially differs from the trivial combination of attribute based encryption [22] and designated verifier signature [21]. As the simulation results illustrate, we simultaneously achieve the functionalities of both access control for personal health information and anonymous authentication for patients with significantly less overhead than the trivial combination of the two building blocks above. Therefore, our PSMPA far outperforms the previous schemes [21], [30] in efficiently realizing access control of patients' personal health information and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing systems.

3 Network Model

The basic e-healthcare system illustrated in Fig. 2 mainly consists of three components: body area networks (BANs), wireless transmission networks and the healthcare providers equipped with their own cloud servers [1], [2]. The patient's personal health information is securely transmitted to the healthcare provider for the authorized physicians to access and perform medical treatment.

We further illustrate the unique characteristics of distributed m-healthcare cloud computing systems where all the personal health information can be shared among patients suffering from the same disease for mutual support or among the authorized physicians in distributed healthcare providers and medical research institutions for medical consultation. A typical architecture of a distributed m-healthcare cloud computing system is shown in Fig. 3. There are three distributed healthcare providers A, B, C and the medical research institution D, where Dr. Brown, Dr. Black, Dr. Green and Prof. White are working respectively. Each of them possesses its own cloud server. It is assumed that patient P registers at hospital A, all her/his personal health information is stored in hospital A's cloud server, and Dr. Brown is one of his directly authorized physicians. For medical consultation or other research purposes in cooperation with hospitals B, C and medical research institution D, it is required for Dr. Brown to generate three indistinguishable transcript simulations of patient P's personal health information and share them among the distributed cloud servers of the hospitals B, C and medical research institution D.

4 Preliminaries

(1) *Bilinear Pairing*. Let $\mathbb{G}_0$, $\mathbb{G}_1$ be two cyclic multiplicative groups generated by g with the same prime order p. Let $e : \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$ be a bilinear mapping with the following properties.

(1) Bilinearity: for all $u, v \in \mathbb{G}_0$ and $a, b \in \mathbb{Z}_p$, we have $e(u^a, v^b) = e(u, v)^{ab}$.

(2) Non-degeneracy: $e(g, g) \neq 1$.

We say $\mathbb{G}_0$ is a bilinear group if the group operations in $\mathbb{G}_0$ and the bilinear map $e : \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$ are both efficiently computable. Notice that the map e is symmetric since $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$.

The related complexity assumptions are as follows.

(2) *Bilinear Diffie-Hellman Problem (BDHP)*. Given g as a generator of $\mathbb{G}_0$ as well as g^a, g^b, g^c for unknown randomly chosen $a, b, c \in \mathbb{Z}_p^*$, compute $e(g, g)^{abc}$.

(3) *Decisional Bilinear Diffie-Hellman Problem (DBDHP)*. Given g as a generator of $\mathbb{G}_0$ as well as g^a, g^b, g^c for unknown randomly chosen $a, b, c \in \mathbb{Z}_p^*$ and $h \in \mathbb{G}_1$, decide whether $h = e(g, g)^{abc}$.

(4) *Gap Bilinear Diffie-Hellman Problem (GBDHP)*. Given g as a generator of $\mathbb{G}_0$ as well as g^a, g^b, g^c for unknown randomly chosen $a, b, c \in \mathbb{Z}_p^*$, compute $e(g, g)^{abc}$ with the help of the DBDH oracle.

5 Authorized Accessible Privacy Model

In this section, we propose a novel authorized accessible privacy model for distributed m-healthcare cloud computing systems which consists of the following two components: an attribute based designated verifier signature scheme (ADVS) and the corresponding adversary model.

5.1 Attribute Based Designated Verifier Signature Scheme

We propose a patient self-controllable and multi-level privacy-preserving cooperative authentication scheme based on ADVS to realize three levels of security and privacy requirement in distributed m-healthcare cloud computing system which mainly consists of the following five algorithms: *Setup*, *Key Extraction*, *Sign*, *Verify* and *Transcript Simulation Generation*. Denote the universe of attributes as U.

We say an attribute set ω satisfies a specific access structure $\mathbb{A}$ if and only if $\mathbb{A}(\omega) = 1$ where ω is chosen from U. The algorithms are defined as follows.

Setup. On input 1^l, where l is the security parameter, this algorithm outputs public parameters and y as the master key for the central attribute authority.

Key Extract. Suppose that a physician requests an attribute set $\omega_D \in U$. The attribute authority computes sk_D for him if he is eligible to be issued with sk_D for these attributes.

Sign. A deterministic algorithm that uses the patient's private key sk_P, the uniform public key pk_D of the healthcare provider where the physicians work and a message m to generate a signature σ. That is, $\sigma \leftarrow Sign(sk_P, pk_D, m)$.

Verify. Assume a physician wants to verify a signature σ with an access structure $\mathbb{A}$ and possesses a subset of attributes $\omega_J \subseteq \omega_D$ satisfying $\mathbb{A}(\omega_J) = 1$, a deterministic verification algorithm can be operated. Upon obtaining a signature σ, he takes as input his attribute private key sk_D and the patient's public key pk_P, then returns the message m and $True$ if the signature is correct, or $\perp$ otherwise. That is, $\{True, \perp\} \leftarrow Verify(sk_D, pk_P, m, \sigma)$.

Transcript Simulation Generation. We require that the directly authorized physicians who hold the authorized private key sk_D can always produce identically distributed transcripts indistinguishable from the original protocol via the *Transcript Simulation* algorithm.

Due to the fact that the *Transcript Simulation* algorithm can generate identically distributed transcripts indistinguishable from the original signature σ, the patient's identity can be well protected from the indirectly authorized physicians for whom only the transcripts are delivered. In addition to the main algorithms described above, we also require the following properties.

Correctness. All signatures generated correctly by *Sign* would pass *verify* operated by the directly authorized physicians,

$$Pr[True \leftarrow Verify(sk_D, pk_P, m, Sign(sk_P, pk_D, m))] = 1. \quad (1)$$

5.2 Adversary Models

(1) *Unforgeability*. In an attribute based designated verifier signature scheme, as to unforgeability, we mean that the adversary wants to forge a signature w.r.t an unsatisfied verifier's specific access structure. The definition of unforgeability allows an adversary not to generate an effective signature with an access structure $\mathbb{A}^*$ for the verifiers if he has not queried the private key for ω^* or any superset of it such that $\mathbb{A}^*(\omega^*) = 1$, or he has not queried the signature on the forged message m^* with an access structure $\mathbb{A}^*$ such that $\mathbb{A}^*(\omega^*) = 1$. We provide a formal definition of existential unforgeability of PSMPA under a chosen message attack. It is defined using the following game between an adversary $\mathscr{A}$ and a simulator $\mathscr{B}$.

Initial Phase. $\mathscr{A}$ chooses and outputs a challenge access structure $\mathbb{A}^*$ that will be included in the forged signature.

Setup Phase. After receiving the challenge access structure $\mathbb{A}^*$, $\mathscr{B}$ selects a proper security parameter 1^l, runs the *Setup* algorithm to generate key pairs (sk, pk), sends pk and other public parameters to the adversary $\mathscr{A}$ and remains the private key sk secretly.

Query Phase. After receiving the public parameters, $\mathscr{A}$ can operate a polynomially bounded number of queries on ω_D and $(m, \mathbb{A}^*)$ to the key extraction oracle and the signing oracle between the patient and the corresponding physician at most q_k, q_s times respectively. $\mathscr{B}$ answers with sk_D and σ as the responses. As to the verifying queries, $\mathscr{A}$ can request a signature verification on a pair (m, σ) between the patient and the directly authorized physicians at most q_v times. In respond, $\mathscr{B}$ outputs $True$ if it is correct, or $\perp$ otherwise.

Forgery Phase. Finally, the adversary $\mathscr{A}$ outputs a signature σ^* on messages m^* with respect to $\mathbb{A}^*$ which is the challenge access structure sent to $\mathscr{B}$ during the initial phase. The forged signature must satisfy the following three properties.

(1) $\mathscr{A}$ did not send queries of the attribute set $\omega_D \subseteq \omega^*$ satisfying $\mathbb{A}^*(\omega_D) = 1$ to the key extraction oracle.

(2) $(m^*, \mathbb{A}^*)$ has not been queried to the signing oracle between the patient P and the corresponding physician D.

(3) σ^* is a valid signature of the message m^* between the patient P and the corresponding physician D.

Definition 1. *Assume the probability of an adversary $\mathscr{A}$ to win the game is $Succ^{EFCMA}_{PSMPA,\mathscr{A}(t,q_{H_0},q_{H_1},q_k,q_s,q_v)}(l)$. We say that PSMPA is existentially unforgeable under a chosen message attack if the probability of success of any polynomially bounded adversary $\mathscr{A}$ running in time at most t and making at most $q_{H_0}, q_{H_1}, q_k, q_s, q_v$ queries to the random oracle $\mathscr{H}_0$, $\mathscr{H}_1$, key extraction oracle, signing oracle and the verifying oracle in the game described above is negligible. Namely*

$$Succ^{EFCMA}_{PSMPA,\mathscr{A}(t,q_{H_0},q_{H_1},q_k,q_s,q_v)}(l) \leq \epsilon. \quad (2)$$

(2) *Anonymity for the Patient*. To guarantee a strong privacy for the patient, the signature reveals nothing about the identity of the patient except the information explicitly revealed. Its formal definition is described as follows.

Definition 2. *A PSMPA scheme satisfies the property of patient privacy if for any two attribute sets ω_0, ω_1 w.r.t. identities ID_0, ID_1, a message m and a signature σ on predicate $\mathbb{A}$ satisfying $\mathbb{A}(\omega_0) = \mathbb{A}(\omega_1) = 1$, any adversary $\mathscr{A}$, even with unbounded computational ability cannot identify which attribute set is utilized to generate the signature with the probability better than random guessing. Namely, $\mathscr{A}$ can only correctly output the identity generating the signature with probability no better than $\frac{1}{2}$ even the adversary $\mathscr{A}$ has access to the directly authorized physicians' private keys.*

6 PSMPA DESIGN

In this section, we give a design of the proposed PSMPA to implement AAPM introduced previously, realizing three different levels of security and privacy requirements. The notations used in our scheme are illustrated in Table 1.

Setup. Let $\mathbb{G}_0$ be a bilinear group of prime order p and g be a generator of $\mathbb{G}_0$. Construct a bilinear map $e : \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$, where $\mathbb{G}_1$ is a group of the same order p. Pick $g_1 \in \mathbb{G}_0$, $y \in \mathbb{Z}_p^*$ at random and compute $g_2 = g^y$.

TABLE 1
Notations in Our Scheme

Notation	Description
d_x	threshold for node x in access tree $\mathscr{T}$
k_x	number of attributes required to be owned by the patient w.r.t. node x
$q_x(\cdot)$	$D_x = d_x - 1$-degree polynomial assigned to node x
ψ_x	a default attribute set of size $d_x - 1$ for node x
sk^{HP}	uniform private key of the healthcare center
pk^{HP}	uniform public key of the healthcare center
ω_D	the set of attributes owned by the physician
sk_D	private key of the physician
ω_x^*	attributes in predicate of node x for physicians
$\psi_x^{'}$	a subset of default attribute set of size $d_x - k_x$ chosen by the patient
K_{Enc}/K_{Dec}	symmetric key for message encryption/decrption
K_{Sig}	signing key for ADVS
ω_J	the subset of physician's attribute set of size k_x chosen to satisfy the predicate
H_0, H_1, H_2	hash functions mapping $\{0,1\}^* \to \mathbb{G}_0$, $\{0,1\}^* \to \mathbb{Z}_p^*$ and $\mathbb{G}_1 \to \{0,1\}^{k_{Enc}}$

Three cryptographically collision-resistant hash functions are selected: $H_0 : \{0,1\}^* \to \mathbb{G}_0$, $H_1 : \{0,1\}^* \to \mathbb{Z}_p^*$ and $H_2 : \mathbb{G}_1 \to \{0,1\}^{k_{Enc}}$ where k_{Enc} is the length of symmetric key in the secure private key encryption construction chosen by the patient. Then, define the attributes in universe U as elements in $\mathbb{Z}_p$. If $q_x(\cdot)$ is a polynomial w.r.t. leaf nodes, a default attribute set from $\mathbb{Z}_p$ with the size of $d_x - 1$ is given as $\psi_x = \{\psi_1, \psi_2, \ldots, \psi_{d_x - 1}\}$ in the access tree. ω_D represents the set of attributes possessed by the physician.

Key Extract. The patient's private key is $b \in \mathbb{Z}_p^*$ and the corresponding public key is $B = g^b$. Assume that the patient's registered local healthcare provider holds a uniform private key $sk^{HP} = hc$ shared by each physician working in it and the corresponding public key is $pk^{HP} = g_1^{hc}$. Let the attribute private key of the physician be

$$sk_D = (\gamma_i, \delta_i) = \left((g_1 H_0(i))^{q_x(i)}, g^{q_x(i)}\right)_{i \in \omega_D \cup \psi_x}, \tag{3}$$

and the public parameters be

$$(p, g, e, \mathbb{G}_0, \mathbb{G}_1, H_0, H_1, H_2, g_1, g_2). \tag{4}$$

ω_x^* is a set of required attributes the patient chooses for the predicate which his expected directly authorized physicians must satisfy.

Sign. The signing algorithm outputs a signature of the patient's personal health information m which can only be recovered and verified by the directly authorized physicians whose sets of attributes satisfy the access tree $\mathscr{T}$. The patient first chooses a polynomial $q_x(\cdot)$ for each node x in $\mathscr{T}$ of the degree $D_x = d_x - 1$.

Starting with the root node R, the algorithm chooses a random $y \in \mathbb{Z}_p$ and sets $q_R(0) = y$. Then, it chooses $d_R - 1$ other points on the polynomial q_R randomly to define it completely. For any other node x, it sets $q_x(0) = q_{parent(x)}(index(x))$ and chooses $d_x - 1$ other points randomly to completely define $q_x(\cdot)$. Specifically in detail, the node predicate $\mathscr{I}_{\mathrm{k}_x, \omega_x^*}(\cdot) \to 0/1$ towards each node polynomial $q_x(\cdot)$ with threshold k_x from 1 to $d_x - 1$ is supposed as follows:

$$\mathscr{I}_{\mathrm{k}_x, \omega_x^*}(\omega_x) = \begin{cases} 1, & |\omega_x \cap \omega_x^*| \geq k_x, \\ 0, & otherwise. \end{cases} \tag{5}$$

To sign a message m with the verification predicate $\mathscr{T}$, for the leaf node x in the access tree $\mathscr{T}$, let the current threshold required for the physician be k_x. For the leaf node polynomial $q_x(\cdot)$, the patient randomly selects a default subset $\psi'_x \subseteq \psi_x$ with $|\psi'_x| = d_x - k_x$ and calculates $B_{P_i} = H_0(i)^b$ for $i \in \omega_x^* \cup \psi'_x$. Then, he can derive the corresponding keys for authentication

$$K_{Encp} = e(g_1, g_2)^b, K_{Enc} = H_2(K_{Encp}), \tag{6}$$

$$K_{Sig} = K_{Encp} e(pk^{HP}, g_2). \tag{7}$$

Finally, the patient randomly selects $r_i \in \mathbb{Z}_p^*$ for each $i \in \omega_x^* \cup \psi'_x$, makes g^{r_i} $(i \in \omega_x^* \cup \psi'_x)$ public and computes the signature as follows:

$$\sigma' = H_1(m \parallel K_{Sig}), C_0 = E_{pk^{HP}}(B \parallel B_{P_i}), \tag{8}$$

$$C = E_{K_{Enc}}(m), \sigma''_i = \left\{H_0(i)^{r_i}\right\}_{i \in \omega_x^* \cup \psi'_x}, \sigma''' = H_0(m)^b, \tag{9}$$

where $E_{pk^{HP}}(\cdot), E_{K_{Enc}}(\cdot)$ are secure public key and private key encryptions chosen by the patient. After that, he can output the signature $\sigma = (\omega_x^*, C_0, C, \sigma', \sigma''_i, \sigma''')$.

Verify. After receiving the signature σ, the physicians working in the patient's registered local healthcare provider can first decipher $B \parallel B_{P_i} = D_{sk^{HP}}(C_0)$, where $D_{sk^{HP}}(\cdot)$ is the decryption algorithm of the public key encryption. If the set of attributes possessed by the physician satisfies the access tree $\mathscr{T}$, he can further operate the verification by performing a recursive algorithm presented in the following.

For the leaf node x, to verify the signature with the node predicate $\mathscr{I}_{\mathrm{k}_x, \omega_x^*}(\cdot)$, namely to prove owning at least k_x attributes among an attribute set ω_x^* with the size of n_x, the physician first selects a subset $\omega_J \subseteq \omega_D \cap \omega_x^*$ of the size k_x, chooses $r'_i \in_R \mathbb{Z}_p^*$ for each $i \in \omega_x^* \cup \psi'_x$ and computes

$$V' = \prod_{i \in \omega_J \cup \psi'_x} \gamma_i^{\Delta_{i, \omega_J \cup \psi'_x}(0)}, V'' = \prod_{i \in \omega_x^* \cup \psi'_x} (\sigma''_i)^{r'_i}, \tag{10}$$

$$V''' = \prod_{i \in \omega_J \cup \psi'_x} e\left(B_{P_i}, \delta_i^{\Delta_{i, \omega_J \cup \psi'_x}(0)} g^{r_i r'_i}\right), \tag{11}$$

$$V'''' = \prod_{i \in \omega_x^* \setminus \omega_J} e\left(B_{P_i}, g^{r_i r'_i}\right), \tag{12}$$

$$\begin{aligned} K^x_{Decp} &= \frac{e(V'V'', B)}{V'''V''''} \\ &= \frac{e\big(g_1^{q_x(0)} \prod_{i\in\omega_J\cup\psi'_x} H_0(i)^{q_x(i)\Delta_{i,\omega_J\cup\psi'_x}(0)+r_i r'_i}, g^b\big)}{\prod_{i\in\omega_J\cup\psi'_x} e\big(H_0(i)^b, g^{q_x(i)\Delta_{i,\omega_J\cup\psi'_x}(0)+r_i r'_i}\big)} \cdot \\ &\quad \frac{e\big(\prod_{\omega^*_x\setminus\omega_J} H_0(i)^{r_i r'_i}, g^b\big)}{\prod_{i\in\omega^*_x\setminus\omega_J} e\big(H_0(i)^b, g^{r_i r'_i}\big)} \\ &= e\big(g_1^{q_x(0)}, g^b\big) = e(g_1, g_2)^b. \end{aligned}$$

We now consider the recursive case when x is a non-leaf node. The verification algorithm will proceed as follows. For all nodes z that are children of x, it calls the same verification algorithm with respect to itself and stores the corresponding partial output as F_z. Let $\mathbb{S}_x$ be an arbitrary k_x-sized set of child nodes z such that $F_z \neq \perp$. If no such set exists, the node will not be satisfied and the function will return $\perp$. Then, the physicians can compute

$$\begin{aligned} K^x_{Decp} &= e\big(F_x, g^b\big) = e\bigg(\prod_{z\in\mathbb{S}_x} F_z^{\Delta_{i,\mathbb{S}'_x}(0)}, g^b\bigg) \\ &\qquad (i = index(x) \; and \;\; \mathbb{S}'_x = \{index(z) : z \in \mathbb{S}_x\}) \\ &= e\bigg(\prod_{z\in\mathbb{S}_x} g_1^{q_z(0)\Delta_{i,\mathbb{S}'_x}(0)}, g^b\bigg) \\ &= e\bigg(\prod_{z\in\mathbb{S}_x} g_1^{q_{parent(z)}(index(z))\Delta_{i,\mathbb{S}'_x}(0)}, g^b\bigg) \\ &= e\bigg(\prod_{z\in\mathbb{S}_x} g_1^{q_x(i)\Delta_{i,\mathbb{S}'_x}(0)}, g^b\bigg) \\ &= e\big(g_1^{q_x(0)}, g^b\big). \end{aligned}$$

Now, we have defined the verification function for each node in the access tree $\mathscr{T}$. By using the recursive algorithm defined above, the physicians can complete verification by simply calling the function on the root node R of the access tree $\mathscr{T}$. Finally, the directly-authorized physician computes

$$K_{Decp} = e(F_R, B) = e\big(g_1^{q_R(0)}, g^b\big) = e(g_1, g_2)^b, \qquad (13)$$

$$K_{Dec} = H_2(K_{Decp}), m = D_{K_{Dec}}(C), \qquad (14)$$

and verifies whether both

$$\begin{aligned} &e(g, \sigma''') = e(B, H_0(m)), \\ &H_1(m \parallel K_{Decp} e(g_1, g_2)^{hc}) = H_1(m \parallel K_{Sig}) = \sigma', \end{aligned} \qquad (15)$$

hold, where $D_{K_{Dec}}(\cdot)$ is the decryption algorithm for the private key encryption. If Equation (15) holds, the physician outputs *Ture*; otherwise, outputs $\perp$.

Transcript Simulation. When the medical consultation or research is required, the directly authorized physician generates a protected session secret SS_j which is unique to each consultation j made for each patient (i.e., it is noted that the protected session secrets are not frequently generated, since the number of medical consultations required for each patient is very limited at most two-three times for especially intractable cases). Then, he can generate the transcript simulations σ_T shared among indirectly-authorized physicians by performing the following operations. First, he computes $K^T_{Decp} = K_{Decp}^{H_1(SS_j)}, K^T_{Dec} = H_2(K^T_{Decp})$ to encrypt a specific message m to C_T and computes $\sigma'_T = H_1(m \parallel K^T_{Decp} e(pk^{HP'}, g_2)) = H_1(m \parallel K^T_{Sig})$, where $pk^{HP'}$ is the public key of the hospital where the indirectly authorized physician works. Then, he computes $B_T = B^{H_1(SS_j)}, B^T_{P_i} = B_{P_i}^{H_1(SS_j)}$ and encrypts them as $C^T_0 = E_{pk^{HP'}}(B_T \parallel B^T_{P_i})$. Finally, he computes $\sigma'''_T = (\sigma''')^{H_0(SS_j)}$ and completes the transcript simulation as $\sigma_T = (\omega^*_x, C^T_0, C_T, \sigma'_T, \sigma''_i, \sigma'''_T)$.

Remark: In our proposed PSMPA, for directly authorized physicians, performing the *Verify* algorithm allows them to both decipher the patient's identity $B \parallel B_{P_i}$ using the private key of the patient's registered local healthcare provider sk^{HP} and recover the patient's personal health information m using the authorized attribute private key sk_D. (i.e., Although other physicians working in the patient's registered HP can derive $B \parallel B_{P_i}$, they cannot decipher the personal health information. Therefore, the unlinkability between the patient identity and his personal health information can still be preserved). For indirectly authorized physicians working in other hospitals or institutions, only the identically distributed and indistinguishable transcript σ_T is delivered (i.e., from which only the blinded identity $B_T \parallel B^T_{P_i}$ randomized by the protected session secret SS_j can be derived) and they cannot get the patient's authentic identity since they fail in recovering $B \parallel B_{P_i}$ from σ without sk^{HP}. For unauthorized persons (adversaries), nothing could be obtained. It is also observed that for the latter two categories, different signatures generated by the same patient cannot even be linkable without knowing his real identity.

7 Analysis

7.1 Security Proof

Theorem 1 (Unforgeability). *Let $\mathscr{A}$ be a malicious adversary with existential forgeability under chosen message attack against our PSMPA scheme with a success probability defined as $Succ^{EFCMA}_{PSMPA,\mathscr{A}(t,q_{H_0},q_{H_1},q_k,q_s,q_v)}$. In time t, he can make at most q_{H_0}, q_{H_1} queries to the random oracle H_0, $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}^*_p$ ($p \geq 2^l$, l is the system's security parameter), q_k queries to the key extraction oracle, q_s queries to the signing oracle and q_v queries to the verification oracle. Then, provided that $E_{pk^{HP}}, E_{K_{Enc}}(\cdot)$ are secure public key and private key encryptions, there exists a simulator $\mathscr{B}$ who can use $\mathscr{A}$ to solve an instance of the GBDH Problem with the probability:*

$$\begin{aligned} &Succ^{GBDH}_{\mathscr{B}} \\ &\quad \geq \prod_{x\in|\mathbb{X}_{unsat}|} \frac{1}{C(d_x - 1, d_x - k_x)} Succ^{EFCMA}_{Sig,\mathscr{A}} - \frac{q_v}{2^l - q_{H_1} - q_s}. \end{aligned}$$

Proof. Provided that $E_{pk^{HP}}, E_{K_{Enc}}(\cdot)$ are secure public key and private key encryptions, it is necessary for us to prove the remaining part of the construction secure under the authorized accessible privacy model described in Section 5. The construction can be proven secure in the selective predicate model. Given a random instance $\{g, g^a, g^b, g^c\}$ of the Gap Bilinear Diffie-Hellman problem, we will show how the simulator $\mathscr{B}$ can use $\mathscr{A}$ to obtain the value $e(g,g)^{abc}$ with the help of DBDH oracle. Let the default attribute set be $\psi_x = \{\psi_1, \psi_2, \ldots, \psi_{d_x-1}\}$ for the predefined integer d_x. First, the adversary $\mathscr{A}$ outputs the challenge predicate $\mathscr{T}^*$ including a node challenge predicate, namely, a threshold function k_x $(k_x \leq d_x)$ out of n_x element attribute set ω_x^* for each polynomial $q_x(\cdot)$. Then $\mathscr{B}$ selects randomly a subset $\psi_x^* \subseteq \psi_x$ with $|\psi_x^*| = d_x - k_x$. In the proof we regard the hash functions as the random oracles $\mathscr{H}_0$ and $\mathscr{H}_1$. $\mathscr{B}$ simulates all the oracles to answer $\mathscr{A}$'s queries and maintains $\mathscr{H}_0$-list and $\mathscr{H}_1$-list to record all the hash queries and the corresponding responses. $\mathscr{H}_0$-list consists of the items (s, l, h), where s is the input of the hash and h is the output of the hash. $\mathscr{H}_1$-list consists of the items (m, r, σ', tag), where (m, r) is the input of the hash and σ' is the output of the hash function. $tag = 1$ if $t = \frac{r}{pk^{HP = e(g,g)^{abc}}}$, otherwise $tag = 0$, which is determined by DBDH oracle. We assume that $\mathscr{A}$ is well-behaved in the sense that $\mathscr{A}$ will never repeat the same queries in our simulation. $\mathscr{B}$ simulates the setup algorithm and sets $g_1 = g^a, g_2 = g^c, B = g^b$. □

$\mathscr{H}_0$ Queries. Upon receiving a query (s_i, m_i) $(i \in [1, q_{H_0}])$ to $\mathscr{H}_0$, $\mathscr{B}$ simulates $\mathscr{H}_0$ as follows.

(1) If there exists $(s_i, l_i, l_i', h_i, h_i')$ in $\mathscr{H}_0$-list, return h_i to the adversary $\mathscr{A}$.

(2) Otherwise, if $s_i \in \omega_x^* \cup \psi_x^*$, $\mathscr{B}$ chooses $l_i \in \mathbb{Z}_p^*$ at random and computes $h_i = g^{l_i}$. Else, $\mathscr{B}$ chooses $l_i \in \mathbb{Z}_p^*$ at random and computes $h_i = g^{l_i}/g_1$. Then, $\mathscr{B}$ randomly selects $l_i' \in \mathbb{Z}_p^*$, computes $h_i' = g^{l_i'}$ and adds $(s_i, l_i, l_i', h_i, h_i')$ into $\mathscr{H}_0$-list and returns h_i, h_i' as the answer.

$\mathscr{H}_1$ Queries. $\mathscr{B}$ simulates $\mathscr{H}_1$ as follows. For any query $(m_i, r_i)(i \in [1, q_{H_1}])$ to $\mathscr{H}_1$, $\mathscr{B}$ submits (g^a, g^b, g^c, t_i) to the DBDH oracle and it will tell $\mathscr{B}$ whether $t_i = e(g,g)^{abc}$. Then, there are following two cases for $\mathscr{B}$ to simulate $\mathscr{H}_1$ oracle.

(1) If $t_i = e(g,g)^{abc}$, $\mathscr{B}$ checks $\mathscr{H}_1$-list

(1.1) If there exists an item $(m_i, \perp, \sigma_i', 1)$ in $\mathscr{H}_1$-list, $\mathscr{B}$ returns σ_i' as the answer. The items of this form in $\mathscr{H}_1$-list can be added during the signing queries.

(1.2) Otherwise, $\mathscr{B}$ chooses $\sigma_i' \in_R \mathbb{Z}_p^*$ such that there is no item $(\cdot, \cdot, \sigma_i', \cdot)$ in $\mathscr{H}_1$-list. $\mathscr{B}$ then adds $(m_i, t_i, \sigma_i', 1)$ into $\mathscr{H}_1$-list and returns σ_i' as the answer.

(2) Else if $t_i \neq e(g,g)^{abc}$, $\mathscr{B}$ chooses $\sigma_i' \in_R \mathbb{Z}_p^*$ such that there is no item $(\cdot, \cdot, \sigma_i', \cdot)$ in $\mathscr{H}_1$-list. $\mathscr{B}$ then adds $(m_i, t_i, \sigma_i', 0)$ into $\mathscr{H}_1$-list and returns σ_i' as the answer.

Key extraction queries. Suppose $\mathscr{A}$ adaptively makes a request for the private key towards the challenge predicate $\mathscr{T}^*$ where $\mathscr{T}^*(\omega) = \mathscr{O}$. To simulate the private key, $\mathscr{B}$ needs to assign a polynomial $q_x(\cdot)$ of degree d_x for each node x in the access tree $\mathscr{T}^*$. Assume that the adversary $\mathscr{A}$ makes at most q_k private key extraction queries and the requesting set of attributes ω satisfies $|\omega \cap \omega_x^*| < k_x$ for some polynomial $q_x(\cdot)$. Simulator $\mathscr{B}$ first defines three sets Γ, Γ', $\mathbb{S}$ in the following manner: $\Gamma = (\omega \cap \omega_x^*) \cup \psi_x^*$ and Γ' such that $\Gamma \subseteq \Gamma' \subseteq \mathbb{S}$ and $|\,\Gamma'\,| = d_x - 1$. Let $\mathbb{S} = \Gamma' \cup \{0\}$.

For every $s_i \in \Gamma'$, simulator $\mathscr{B}$ runs $\mathscr{H}_0$ oracle to get $(s_i, l_i, \cdot, h_i, \cdot)$ in the $\mathscr{H}_0$-list, picks $\lambda_i \in \mathbb{Z}_p^*$ at random, computes $sk_{D_i} = ((g_1 h_i)^{\lambda_i}, g^{\lambda_i})$ and let $\lambda_i = q_x(s_i)$.

For the $s_i \in \mathbb{S}\backslash\Gamma'$, the simulator $\mathscr{B}$ runs $\mathscr{H}_0$ oracle to get $(s_i, l_i, \cdot, h_i, \cdot)$ in the $\mathscr{H}_0$-list, computes

$$sk_{D_i} = \left(\left(\prod_{s_j \in \Gamma'} (g_1 h_i)^{\Delta_{s_j,\mathbb{S}}(s_i)\lambda_j} \right) g_2^{\Delta_{0,\mathbb{S}}(s_i) l_i}, \right. \\ \left. \left(\prod_{s_j \in \Gamma'} g^{\Delta_{s_j,\mathbb{S}}(s_i)\lambda_j} \right) g_2^{\Delta_{0,\mathbb{S}}(s_i)} \right), \tag{16}$$

and returns $\{sk_{D_i}\}_{i \in \omega}$ to the adversary $\mathscr{A}$.

Now the simulator $\mathscr{B}$ defines $\lambda_i = q_x(s_i)$ for a random polynomial $q_x(\cdot)$ of degree $d_x - 1$ over $\mathbb{Z}_p^*$ such that $q_x(0) = c$. In this way, from the view of adversary $\mathscr{A}$, when $s_i \in \Gamma'$ the simulated sk_{D_i} and those sk_{D_i} in the real attack are identically distributed. Even when $s_i \notin \Gamma'$, the above simulation is also correctly distributed. Since $s_i \notin \Gamma'$ means $s_i \notin \Gamma$, we have $g_1 h_i = g^{l_i}$. Noting $g_2 = g^c$, we have

$$\begin{aligned} sk_{D_i} &= \left(\left(g^{l_i(\sum_{s_j \in \Gamma'} \Delta_{s_j,\mathbb{S}}(s_i) q_x(s_j))} \right) g^{\Delta_{0,\mathbb{S}}(s_i) l_i c}, \right. \\ &\quad \left. \left(g^{\sum_{s_j \in \Gamma'} \Delta_{s_j,\mathbb{S}}(s_i) q_x(s_j)} \right) g^{\Delta_{0,\mathbb{S}}(s_i) c} \right) \\ &= \left(g^{l_i(\sum_{s_j \in \Gamma'} \Delta_{s_j,\mathbb{S}}(s_i) q_x(s_j) + \Delta_{0,\mathbb{S}}(s_i) q_x(0))}, \right. \\ &\quad \left. g^{\sum_{s_j \in \Gamma'} \Delta_{s_j,\mathbb{S}}(s_i) q_x(s_j) + \Delta_{0,\mathbb{S}}(s_i) q_x(0)} \right) \\ &= \left(g^{l_i q_x(s_i)}, g^{q_x(s_i)} \right) \\ &= \left((g_1 h_i)^{q_x(s_i)}, g^{q_x(s_i)} \right) \\ &= \left((g_1 H_0(s_i))^{q_x(s_i)}, g^{q_x(s_i)} \right). \end{aligned}$$

Therefore, all the private keys $\{sk_{D_i}\}_{i \in \omega \cup \psi_x^*}$ simulated by $\mathscr{B}$ are distributed identically to the ones in the real attack. Finally, the simulator $\mathscr{B}$ can construct the private keys for the access tree $\mathscr{T}^*$ and the distribution of the private keys for $\mathscr{T}^*$ is identical to that in the original scheme.

Signing queries. $\mathscr{B}$ simulates the signing oracle as follows. After receiving $\mathscr{A}$'s choice of the message m_i, $\mathscr{B}$ checks the $\mathscr{H}_1$-list.

(1) If there is an item $(m_i, t_i, \sigma_i', 1)$ in $\mathscr{H}_1$-list where $t_i = e(g,g)^{abc}$, $\mathscr{B}$ outputs $(\omega_x^*, \sigma_i', \sigma_{i_j}'', \sigma_i''')$ as the signature, where $\sigma_{i_j}'', \sigma_i'''$ can be generated according to the answers from running $\mathscr{H}_0$ oracle for queries $(s_j \in \omega_x^* \cup \psi_x^*, m_i)$.

(2) Else, $\mathscr{B}$ chooses $\sigma_i' \in_R \mathbb{Z}_p^*$ such that there is no item $(\cdot, \cdot, \sigma_i', \cdot)$ in $\mathscr{H}_1$-list. $\mathscr{B}$ then adds $(m_i, \perp, \sigma_i', 1)$ into $\mathscr{H}_1$-list and returns $(\omega_x^*, \sigma_i', \sigma_{i_j}'', \sigma_i''')$ as the signature, where $\sigma_{i_j}'', \sigma_i'''$ can be generated the same as what is operated in the first case.

Verifying Queries. After receiving $\mathscr{A}$'s request (m_i, σ_i), $\mathscr{B}$ simulates the verifying oracle as follows.

(1) If there is no item $(\cdot, \cdot, \sigma_i', \cdot)$ in $\mathscr{H}_1$-list, $\mathscr{B}$ simulates the verification and rejects (m_i, σ_i') as an invalid signature.

(2) Else if there is an item $(\cdot, \cdot, \sigma_i', \cdot)$ in $\mathscr{H}_1$-list, and

(2.1) If this item has the form of $(m_i, \perp, \sigma_i', 1)$ or $(m_i, t_i, \sigma_i', 1)$, $\mathscr{B}$ will accept it as a valid signature.

(2.2) Otherwise, $\mathscr{B}$ will reject it as an invalid signature.

This makes a difference only if $(m_i, \sigma_i^{'})$ is a valid signature and $\sigma_i^{'}$ is not queried from $\mathscr{H}_1$. Since $\mathscr{H}_1$ is uniformly distributed, for all verifying queries this case happens with the probability less than $\frac{q_v}{2^l - q_{H_1} - q_s}$.

Now, if the adversary $\mathscr{A}$ outputs a valid signature (m^*, σ^*) such that $Verify(m^*, \sigma^*, sk_D, B) = 1$, it means that there is an item $(\cdot, \cdot, \sigma^{'*}, \cdot)$ in $\mathscr{H}_1$-list. By the definition of the EFCMA adversary model, m^* cannot be queried in the signing oracle, therefore $\sigma^{'*}$ must be returned as the hash value of $\mathscr{A}$'s query (m^*, r^*). That is to say there is an item $(m^*, t^*, \sigma^{'*}, 1)$ in $\mathscr{H}_1$-list and $t^* = e(g, g)^{abc}$. Besides, for the success of $\mathscr{B}$, it is required for the correct guess of $d_x - k_x$ element subset ψ_x^* from a $d_x - 1$ element set ψ_x, the probability is $\frac{1}{C(d_x - 1, d_x - k_x)}$. Since the simulator $\mathscr{B}$ has the knowledge of the challenge predicate $\mathscr{T}^*$, he can compute the number of unsatisfied leaf node polynomials $q_x(\cdot)$ corresponding to the challenged set of attributes selected by the adversary $\mathscr{A}$, namely there are the corresponding number of polynomials whose default sets of attributes are required for the adversary's guessing. We denote this number as $|\mathbb{X}_{unsat}|$. Therefore, $\mathscr{B}$ successfully solves the GBDH problem with the probability:

$$Succ_{\mathscr{B}}^{GBDH} \geq \prod_{x \in |\mathbb{X}_{unsat}|} \frac{1}{C(d_x - 1, d_x - k_x)} Succ_{Sig, \mathscr{A}}^{EFCMA} - \frac{q_v}{2^l - q_{H_1} - q_s}.$$

Theorem 2 (Privacy of Patient's Identity). *Our proposed PSMPA achieves signer-attribute privacy, namely both the indirectly authorized physicians and unauthorized persons cannot correctly distinguish the identities of the patients from each other.*

Proof. In our scheme, without loss of generality, for a (k_x, n_x) threshold attribute based verification with respect to one specific node x in the access tree $\mathscr{T}$, it is impossible for the indirectly authorized physicians playing the role of medical consultation or research staff to distinguish which k_x attributes are really used in leaf node x for verification (i.e., the directly authorized physicians from whom the transcript simulation is delivered). The reason is that any attribute subset of the size k_x can satisfy the predicate. In this way can the unconditional signer-attribute privacy of PSMPA be achieved. The details of the proof are described as follows.

First, the attribute authority runs the setup algorithm to get the master key y, the public parameters and gives them to the adversary. Then, the adversary $\mathscr{A}$ outputs two attribute set ω_0^* and ω_1^* where $\omega^{*'} = \omega_0^* \cap \omega_1^*$. Let $\omega_b^{''} = \omega_b^* \cup \psi_x$ for $b \in \{0, 1\}$. Assume simulator $\mathscr{B}$ has generated the private keys $sk_{\omega_0^{*''}} = (\gamma_i^0, \delta_i^0)$ and $sk_{\omega_1^{*''}} = (\gamma_i^1, \delta_i^1)$ for ω_0^* and ω_1^* respectively, where $\gamma_i^b = (g_1 H_0(i))^{q_x(i)}$ and $\delta_i^b = g^{q_x(i)}$ for each $i \in \omega_b^{*''}(b \in \{0, 1\})$. $q_x(\cdot)$ is a $d_x - 1$ polynomial with $q_x(0) = q_{parent(x)}(index(x))$ and $q_r(0) = y$.

Next, the adversary $\mathscr{A}$ outputs a subset with the size of k_x-element $\omega^* = \{i_1, i_2, \cdots, i_{k_x}\} \subseteq \omega^{*'}$, where $|\omega^*| \leq d_x$. Upon receiving a specific signature, it asks the simulator $\mathscr{B}$ to verify it with respect to ω_b^* using either $sk_{\omega_0^{*''}}$ or $sk_{\omega_1^{*''}}$ and generate the corresponding two transcript simulations for the adversary $\mathscr{A}$. The simulator chooses a random bit $b \in \{0, 1\}$, a $d_x - k_x$ element subset $\psi_x^{'} = \{\psi_{k_x+1}, \psi_{k_x+2}, \ldots, \psi_{d_x}\} \subseteq \psi_x$ and outputs the verification $.H_1(m \parallel K_{Decp} e(g_1, g_2)^{hc})$

$$\Bigg(K_{Decp} = \left\{ e\left(g_1^{q_x(0)} \prod_{i \in \omega_J \cup \psi_x^{'}} H_0(i)^{q_x(i) \Delta_{i, \omega_J \cup \psi_x^{'}}(0) + r_i r_i^{'}} \prod_{\omega_x^* \backslash \omega_J} H_0(i)^{r_i r_i^{'}}, g^b \right) \right\} \Bigg/ \left\{ \prod_{i \in \omega_J \cup \psi_x^{'}} e\left(H_0(i)^b, g^{q_x(i) \Delta_{i, \omega_J \cup \psi_x^{'}}(0) + r_i r_i^{'}}\right) \prod_{i \in \omega_x^* \backslash \omega_J} e\left(H_0(i)^b, g^{r_i r_i^{'}}\right) \right\} \Bigg)$$

by running the verification algorithm with the private keys $sk_{\omega_b^{*''}}$. Based on the Lagrange interpolation, it is obviously seen that the signature can be verified by using $sk_{\omega_0^{*''}}$ or $sk_{\omega_1^{*''}}$ since the negotiated signature key K_{Sig}^* can be generated by either private key possessed by each of the two physicians who has at least k_x common attributes in the intersection of ω_x^* and $\omega_b^*(b \in \{0, 1\})$. Therefore, we have proved that the transcript simulation of a specific signature can be generated by the directly authorized physicians with either private key of $sk_{\omega_0^{*''}}$ and $sk_{\omega_1^{*''}}$ or the patient himself, namely our patient self-controllable authentication scheme (PSMPA) satisfies unconditional signer-attribute privacy. □

7.2 Performance Analysis

(1) *Numerical analysis*. We now consider the efficiency of PSMPA in terms of storage overhead, computational complexity and communication cost.

As to the storage overhead, the size of public parameters in our scheme is linear to the number of attributes in ω_x^* and ψ_x'. The private key consists of two group elements in $\mathbb{G}_0$ for every leaf node in the key's corresponding access tree $\mathscr{T}$. That is the number of group elements in private keys equals to the number of attributes in the union of ω_D and a default set of attributes ψ_x. Assuming ω_x^* is one of the public parameters, the signature almost consists of one group element in $\mathbb{G}_0$ corresponding to each attribute in ω_x^* and ψ_x'. Therefore, the communication cost is independent of the number of attributes in ω_D possessed by each physician. As to the computational overhead, compared to the hash functions (e.g., SHA-1) and private key encryption (e.g., AES), the most resource-consuming operations in PSMPA are parings and exponentiations which we will focus on for evaluating the computational complexity. In the signing procedure, the number of modular exponentiations is almost linear to the number of attributes in the union of the requiring attribute set ω_x^* and a default subset of attributes ψ_x'. The verification procedure is by far the hardest to define performance for. In our verification algorithm described in Section 5, the number of parings and exponentiations might always be linear to the number of nodes in the access tree. However, it can be reduced to $O(|\mathbb{S}_R|(n + d - k))$ [22] where $\mathbb{S}_R$ denotes the first k_R sets of the smallest size corresponding to the leaf nodes. To

TABLE 2
Storage Overhead of PSMPA

Items	Storage Overhead
Public Key	$O(n+d-k)$
Private Key	$O(n_D+d)$
Signature	$O(n+d-k)$

TABLE 3
Computational Overhead of PSMPA

Items	Computational Overhead
Sign	$O(n+d-k)E$
Verify	$O(\lvert\mathbb{S}_r\rvert\,(n+d-k))(P+E)$

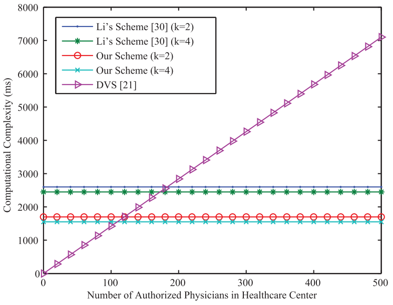


Fig. 4. Comparison of computational overhead among DVS, Li's scheme and PSMPA towards N.

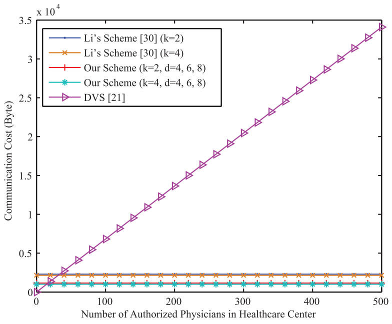


Fig. 5. Comparison of communication overhead among DVS, Li's scheme and PSMPA towards N.

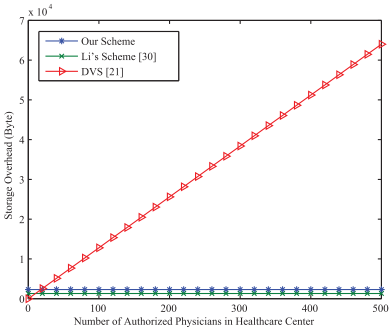


Fig. 6. Comparison of storage overhead among DVS, Li's Scheme and PSMPA towards N.

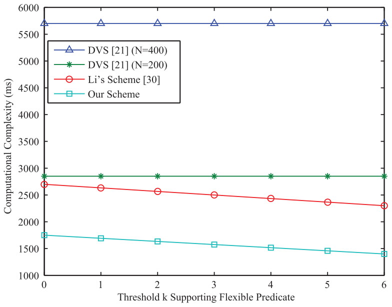


Fig. 7. Comparison of computational overhead among DVS, Li's scheme and PSMPA towards k.

achieve the same security, our construction performs more efficiently than the traditional designated verifier signature [21] for all the directly authorized physicians, where the overheads are linear to the number of directly authorized physicians. On the other hand, our construction also essentially distinguishes from the combination of a fine-grained attribute based encryption [22] and a traditional DVS [21] supporting flexible predicates, since in our construction the partial verifying key $e(g_1, g_2)^b$ is utilized for the secret key for encrypting m. It prevents the patient and the physicians from negotiating another symmetric encryption key in advance and saves almost half of the computational complexity, the signature size as well as the communication cost. Assume that n, n_D, d, k represent the size of the required set of attributes ω_x^*, the physician's attribute set ω_D, the default attribute set ψ_x and the flexible threshold respectively. P and E represent pairing and modular exponentiation operations. The storage and computational overhead of our construction PSMPA are illustrated in Tables 2 and 3 respectively.

(2) *Implementation*. In our implementation, we choose MIRACLE Library for simulating cryptographic operations using Microsoft C/C++ compilers. To achieve a comparable security of 1,024-bit RSA, According to the standards of Paring-based Crypto Library [24], our test is made on Linux platform with an Intel Core2 Duo 2.53 GHz CPU, which takes about 7 and 27 ms to perform a a scalar multiplication and pairing respectively. Consider a large quantity of pairing operations in our construction, it is reasonable to choose 512-bit SS curve $y^2 = x^3 + x$ for simulation. Assume that N represents the number of directly authorized physicians and we set $n = n_D = 10,\ d = 6,\ k \in \mathbb{Z} \wedge k \in [0, 6],\ N \in \mathbb{Z} \wedge N \in [0, 500]$, the efficiency comparisons between DVS [21], Li's scheme [30] and our construction are evaluated. Li et al. proposed a patient-centric and fine-grained data access control using ABE to secure personal health records in cloud computing [30] without privacy-preserving authentication. For comparison, to achieve the same functions of PSMPA, it could be considered as the combination of ABE [22] and DVS [21]. Fig. 4 shows that the computational complexity of PSMPA remains constant regardless of the number of directly authorized physicians and nearly half of the combination construction of ABE [22] and DVS [21] supporting flexible predicate. Fig. 5 illustrates the communication cost of PSMPA also remains constant, almost half of the combination construction and independent of the number of attributes d in ω_D. Fig. 6 shows that though the storage overhead of PSMPA is slightly more than the combination construction, it is independent of the number of directly authorized physicians and performs significantly better than traditional DVS [21], all of whose computational, communication and storage overhead increase linearly to the number of directly authorized physicians.

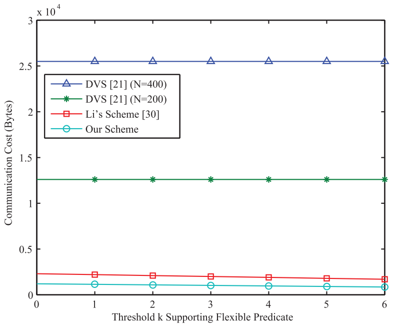


Fig. 8. Comparison of communication overhead among DVS, Li's scheme and PSCMA towards k.

Figs. 7 and 8 show that the computational and communication overhead of the combination construction decrease slightly faster than PSMPA as the threshold k increases, however, even when k reaches the maximum value equaling to d, the overheads are still much more than PSMPA. The comparison between our scheme and the anonymous authentication based on PKI [6], [7] w.r.t. the storage, communication and computational overhead towards N and k is identical to DVS [21], since to realize the same identity privacy, in all the constructions [6], [7], [21], a pair of public key and private key would be assigned to each directly authorized physician and the number of signature operations is also linear to the number of physicians, independent of the threshold k. The simulation results show our PSMPA better adapts to the distributed m-healthcare cloud computing system than previous schemes, especially for enhancing the energy-constrained mobile device's (the data sink's) efficiency.

8 Conclusions

In this paper, a novel authorized accessible privacy model and a patient self-controllable multi-level privacy-preserving cooperative authentication scheme realizing three different levels of security and privacy requirement in the distributed m-healthcare cloud computing system are proposed, followed by the formal security proof and efficiency evaluations which illustrate our PSMPA can resist various kinds of malicious attacks and far outperforms previous schemes in terms of storage, computational and communication overhead.

Acknowledgments

This work was supported by the National Program on Key Basic Research Project (973 Program) and National Natural Science Foundation of China under grant 2012CB723401, 61161140320, 61033014, 61373154 and 61371083. X. Dong and Z. Cao are the corresponding author.

References

[1] L. Gatzoulis and I. Iakovidis, "Wearable and portable E-health systems," *IEEE Eng. Med. Biol. Mag.*, vol. 26, no. 5, pp. 51–56, Sep.-Oct. 2007.

[2] I. Iakovidis, "Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare records in europe," *Int. J. Med. Inf.*, vol. 52, no. 1, pp. 105–115, 1998.

[3] E. Villalba, M. T. Arredondo, S. Guillen, and E. Hoyo-Barbolla, "A new solution for a heart failure monitoring system based on wearable and information technologies in," in *Proc. Int. Workshop Wearable Implantable Body Sens. Netw.*, Apr. 2006, pp. 150–153.

[4] R. Lu and Z. Cao, "Efficient remote user authentication scheme using smart card," *Comput. Netw.*, vol. 49, no. 4, pp. 535–540, 2005.

[5] M. D. N. Huda, N. Sonehara, and S. Yamada, "A privacy management architecture for patient-controlled personal health record system," *J. Eng. Sci. Technol.*, vol. 4, no. 2, pp. 154–170, 2009.

[6] S. Schechter, T. Parnell, and A. Hartemink, "Anonymous authentication of membership in dynamic groups in," in *Proc. 3rd Int. Conf. Financial Cryptography*, 1999, pp. 184–195.

[7] D. Slamanig, C. Stingl, C. Menard, M. Heiligenbrunner, and J. Thierry, "Anonymity and application privacy in context of mobile computing in eHealth," in *Mobile Response*, New York, NY, USA: Springer, 2009 pp. 148–157.

[8] J. Zhou and Z. Cao, "TIS: A threshold incentive scheme for secure and reliable data forwarding in vehicular delay tolerant networks," in *Proc. IEEE Global Commun. Conf.*, 2012, pp. 985–990.

[9] S. Yu, K. Ren, and W. Lou, "FDAC: Toward fine-grained distributed data access control in wireless sensor networks," in *Proc. IEEE Conf. Comput. Commun.*, 2009, pp. 963–971.

[10] F. W. Dillema and S. Lupetti, "Rendezvous-based access control for medical records in the pre-hospital environment," in *Proc. 1st ACM SIGMOBILE Int. Workshop Syst. Netw. Support Healthcare Assisted Living*, 2007, pp. 1–6.

[11] J. Sun, Y. Fang, and X. Zhu, "Privacy and emergency response in e-healthcare leveraging wireless body sensor networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 66–73, Feb. 2010.

[12] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "SAGE: A strong privacy-preserving scheme against global eavesdropping for E-health systems," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 365–378, May 2009.

[13] J. Sun, X. Zhu, C. Zhang, and Y. Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," in *Proc. 31st Int. Conf. Distrib. Comput. Syst.*, 2011, pp. 373–382.

[14] L. Lu, J. Han, Y. Liu, L. Hu, J. Huai, L. M. Ni, and J. Ma, "Pseudo trust: Zero-knowledge authentication in anonymous P2Ps," *IEEE Trans. Parallel Distrib. Syst.*, vol. 19, no. 10, pp. 1325–1337, Oct. 2008.

[15] J. Zhou and M. He, "An improved distributed key management scheme in wireless sensor networks," in *Proc. 9th Int. Workshop Inf. Security Appl.*, 2008, pp. 305–319.

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

[17] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *Proc. 16th ACM Conf. Comput. Commun. Security*, 2009, pp. 121–130.

[18] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.

[19] N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou, "Privacy-preserving query over encrypted graph-structured data in cloud computing," in *Proc. 31st Int. Conf. Distrib. Comput. Syst.*, 2011, pp. 393–402.

[20] F. Cao and Z. Cao, "A secure identity-based multi-proxy signature scheme," *Comput. Electr. Eng.*, vol. 35, pp. 86–95, 2009.

[21] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "Short designated verifier signature scheme and its identity-based variant," *Int. J. Netw. Security*, vol. 6, no. 1, pp. 82–93, Jan. 2008.

[22] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc ACM Conf. Comput. Commun. Security*, 2006, pp. 89–98.

[23] J. Li, M. H. Au, W. Susilo, D. Xie, and K. Ren, "Attribute-based signature and its applications," in *Proc. 5th ACM Symp. Inf., Comput. Commun. Security*, 2010, pp. 60–69.

[24] PBC Library, [online] http://crypto.stanford.edu/pbc/times.html, 2006.

[25] B. Riedl, V. Grascher, and T. Neubauer, "A secure e-health architecture based on the appliance of pseudonymization," *J. Softw.*, vol. 3, no. 2, pp. 23–32, Feb. 2008.

[26] D. Slamanig and C. Stingl, "Privacy aspects of E-health," in *Proc. 3rd. Int. Conf. Availab., Rel. Security*, 2008, pp. 1226–1233.

[27] *De-identified Health Inf.*, [online] http://aspe.hhs.gov/admnsimp/bannerps.htm, 2007.

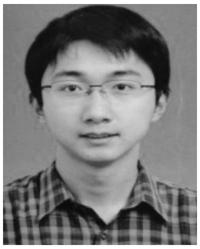
[28] R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social network," *J. Mobile Netw. Applications,* vol. 16, no. 6, pp. 683–694, Dec. 2011.

[29] J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic health record system," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 6, pp. 754–764, Jun. 2010.

[30] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in *Proc. 6th Int. ICST Conf. Security Privacy Comm. Netw.*, 2010, pp. 89–106.

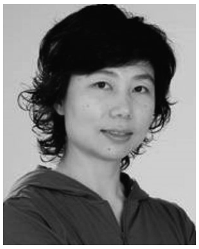
[31] J. Misic and V. Misic, "Enforcing patient privacy in healthcare WSNs through key distribution algorithms," *Security Commun. Netw. J.*, vol. 1, no. 5, pp. 417–429, 2008.

[32] J. Misic and V. B. Misic, "Implementation of security policy for clinical information systems over wireless sensor network," *Ad Hoc Netw.*, vol. 5, no. 1, pp. 134–144, Jan. 2007.



Jun Zhou is currently working toward the PhD degree in computer science with Trusted Digital Technology (TDT) Laboratory, Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. His research interests mainly include secure e-healthcare systems, privacy preserving outsourcing computation in cryptography, and information security. He is also enrolled in the Chen-hui Scholars Program of East China Normal University.

Xiaodong Lin (S'07-M'09-SM'12) received the PhD degree in information engineering from Beijing University of Posts and Telecommunications, China, and the PhD degree (with Outstanding Achievement in Graduate Studies Award) in electrical and computer engineering from the University of Waterloo, ON, Canada. He is currently an associate professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology (UOIT), Oshawa, ON, Canada. His research interests include wireless network security, applied cryptography, computer forensics, software security, and wireless networking and mobile computing. He won the Best Paper Awards at several conferences, including the 18th International Conference on Computer Communications and Networks (ICCCN 2009), the 5th International Conference on Body Area Networks (BodyNets 2010), and the IEEE International Conference on Communications (ICC 2007). He received the prestigious NSERC Canada Graduate Scholarships (CGS) Doctoral, and selected as university nominee for NSERC Doctoral Prize (Engineering and Computer Sciences category). He is a senior member of the IEEE.



Xiaolei Dong is a Distinguished Professor in East China Normal University. After her graduation with a doctorate degree from Harbin Institute of Technology, she pursued her post-doctoral study in SJTU from September 2001 to July 2003. Then, in August 2003, she joined the Department of Computer Science and Engineering of SJTU. Her primary research interests include Number Theory, Cryptography, Trusted Computing, etc. Since 1998, she has published more than 80 academic papers. As the first author, Dr. Dong has two textbooks published by Science Press and China Machine Press respectively. Her "Number Theory and Modern Cryptographic Algorithms" project won the first prize of China University Science and Technology Award in 2002. Her "New Theory of Cryptography and Some Basic Problems" project won the second prize of Shanghai Nature Science Award in 2007. Her "Formal Security Theory of Complex Cryptographic System and Applications" won the second prize of Ministry of Education Natural Science Progress Award in 2008. Currently, she hosts a number of research projects supported by the National Basic Research Program of China (973 Program), the special funds on information security of the National Development and Reform Commission and National Natural Science Foundation of China, etc. She is an associate editor of Security and Communication Networks (John Wiley).

Zhenfu Cao (SM'10) received the B.Sc. degree in computer science and technology and the Ph. D. degree in mathematics from Harbin Institute of Technology, Harbin, China, in 1983 and 1999, respectively. His research interests mainly include Number Theory, Cryptography and Information Security. Up to now (since 1981), more than 400 academic papers have been published in Journals or conferences. He was exceptionally promoted to Associate Professor in 1987, became a Professor in 1991 and is currently a Distinguished Professor in East China Normal University, China. He also serves as a member of the expert panel of the National Nature Science Fund of China. Prof. Cao is actively involved in the academic community, serving as Committee/Co-Chair and program committee member for several international conference committees, as follows: the IEEE Global Communications Conference (since 2008), the IEEE International Conference on Communications (since 2008), etc. He is the Associate Editor of Computers and Security (Elsevier) and Security and Communication Networks (John Wiley), an Editorial Board member of Fundamenta Informaticae (IOS) and Peer-to-Peer Networking and Applications (Springer-Verlag), and Guest Editor of Wireless Communications and Mobile Computing (Wiley), and IEEE Transactions on Parallel and Distributed Systems etc. He has received a number of awards, including the Youth Research Fund Award of the Chinese Academy of Science in 1986, the Ying-Tung Fok Young Teacher Award in 1989, the National Outstanding Youth Fund of China in 2002, the Special Allowance by the State Council in 2005, and a corecipient of the 2007 IEEE International Conference on Communications-Computer and Communications Security Symposium Best Paper Award in 2007. Prof. Cao is also the leaders of Asia 3 Foresight Program (61161140320) and the key project (61033014) of National Natural Science Foundation of China. He is a senior member of the IEEE.