TR-MABE: White-Box Traceable and Revocable Multi-authority Attribute-based Encryption and Its Applications to Multi-level Privacy-preserving e-Healthcare Cloud Computing Systems

Jun Zhou, Zhenfu Cao*, Xiaolei Dong*, Xiaodong Lin
Department of Computer Science and Engineering, Shanghai Jiao Tong University
Shanghai 200240, China
Email: zhoujun_tdt@sjtu.edu.cn
Shanghai Key Lab for Trustworthy Computing, East China Normal University
Shanghai 200062, China
Email: zfcao@sei.ecnu.edu.cn, dongxiaolei@sei.ecnu.edu.cn
Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, Canada
Email: xiaodong.lin@uoit.ca

***Abstract*—Cloud-assisted e-healthcare systems significantly facilitate the patients to outsource their personal health information (PHI) for medical treatment of high quality and efficiency. Unfortunately, a series of unaddressed security and privacy issues dramatically impede its practicability and popularity. In e-healthcare systems, it is expected that only the primary physicians responsible for the patients treatment can not only access the PHI content but verify the real identity of the patient. Secondary physicians participating in medical consultation and/or research tasks, however, are only permitted to view or use the content of the protected PHI, while unauthorized entities cannot obtain anything. Existing work mainly focuses on patients conditional identity privacy by exploiting group signatures, which are very computationally costly. In this paper, we propose a white-box traceable and revocable multi-authority attribute-based encryption named TR-MABE to efficiently achieve multilevel privacy preservation without introducing additional special signatures. It can efficiently prevent secondary physicians from knowing the patients identity. Also, it can efficiently track the physicians who leak secret keys used to protect patients identity and PHI. Finally, formal security proof and extensive simulations demonstrate the effectiveness and practicability of our proposed TR-MABE in e-healthcare cloud computing systems.**

***Index Terms*—Cloud computing system, attribute-based encryption, multi-authority, traceability and revocability**

I. Introduction

E-healthcare cloud computing systems profoundly benefit the patients to obtain medical treatment of high quality and efficiency, especially for the resource-asymmetric settings where the hand-held devices monitoring and collecting the real-time personal health information (PHI) are energy constrained, but e-healthcare cloud servers used by healthcare providers are generally assumed to possess substantial storage and computational ability [1,2]. The frequently collected PHI is required to be outsourced to the cloud for storage and preprocessing before given to corresponding physicians for medical diagnosis.

Nevertheless, in contrast to traditional access control scenarios where the user and the platform are suggested to be located in the same trust domain, the e-healthcare cloud server is universally assumed to be semi-trusted in the honest-but-curious model [2,7], which tries its best to retrieve private information of the patients from the interactions while precisely executing the protocol specifications. Therefore, the PHI must be stored in the e-healthcare cloud in its encrypted form to achieve data confidentiality. Additionally, the physicians in the healthcare provider can further be classified into three categories: the primary physicians taking responsibility of a patient's medical treatment can not only access her/his PHI content, but correctly verify her/his real identity; the secondary physicians participating in medical consultation when the patient's health condition is intractable or dedicating in the medical research where PHI is provided as clinical data, are not required (necessary) to know the patient's real identity but the PHI content itself; the unauthorized persons can obtain neither. Therefore, a promising solution is to have a patient self controllable fine-grained multiple level access control. Last but not least, a tricky physician or a single compromised central/attribute authority would illegally leak the secret keys for deciphering patient's private PHI or recovering patient's real identity to associated pharmaceutical companies or medical equipment companies to make targeted smartphone advertisement for specific group of patients suffering from certain types of disease. More seriously, if the private PHI containing serious health condition were abused by the insurance company or the human resource department, the patients would be denied for renewal of their insurances and labor contracts. Consequently, a multi-authority attribute-based encryption simultaneously possessing the prop-

* Corresponding authors at: Shanghai Key Lab for Trustworthy Computing, East China Normal University, Shanghai, China

erties of efficient traceability and revocability is required to prevent a single authority compromise and/or the authorized physicians from exposing secret keys to untrusted entities without accountability.

Unfortunately, existing work on secure and privacy preserving access control in e-heathcare systems can not achieve the security and privacy requirement mentioned above. M. Li et al. proposed a patient-centric and fine-grained data access control in multi-owner settings for personal health records in cloud computing [4] by exploiting the technique of multi-authority attribute-based encryption (MABE), however, the issues of patient identity privacy and malicious physician's traceability are left unaddressed. The technique of group signature [17][18] which is widely adopted to conditionally protect the sender's identity cannot well adapt to the e-healthcare systems since the optimally-designed group signature generation algorithm would still cost the patient's energy-constrained hand-held device huge volume of computational resources. Recently, Z. Liu et al. presented a white-box traceable ciphertext-policy attribute-based encryption supporting monotone access structures [14]. However, it cannot be straightforwardly applied to solve the problems presented above since the efficient attribute revocation in the multi-authority settings was not studied in [14]. Therefore, how to design a traceable and revocable multi-authority attribute-based encryption for fine-grained multiple level access control in the e-healthcare cloud computing systems still remains a challenging open problem.

In this paper, TR-MABE is proposed to realize all the aforementioned security and privacy requirements with significantly enhanced efficiency. The main contributions are outlined as follows.

(1) A white-box traceable and revocable multi-authority attribute-based encryption TR-MABE is proposed for fine-grained multiple level access control in e-healthcare cloud computing systems. Both the patient's private PHI and his identity are firstly encrypted under the access policy specified by the patient himself and outsourced to the e-healthcare cloud. Then, by exploiting our proposed attribute revocation, the secondary physicians are deprived of the privilege of knowing the patient's real identity. To the best of our knowledge, it is the first time to utilize attribute revocation to achieve the patient's multilevel (conditional) identity privacy.

(2) The property of traceability is realized to protect the patient's private PHI from being abused and exposed for target advertisement, since once the secret key is illegally leaked, the source of PHI will be precisely traced. The suggested multi-authority setting in e-healthcare cloud computing systems also significantly reduces the risk of a single central/attribute authority being compromised for potential privacy leakage.

(3) Without introducing extra special signatures, the multi-level privacy preservation is efficiently realized by outsourcing the storage revocation (i.e. ciphertext updating) to the e-healthcare cloud. Formal security proof and extensive simulation evaluations illustrate our proposed TR-MABE is secure against chosen plaintext attack in the standard model and outperforms the state-of-the-art in terms of storage, computational and communication overhead.

The remainder of this paper is organized as follows. Related work is introduced in Sec. II. The system architecture and the formal security models are presented in Sec. III. We propose TR-MABE for fine-grained multiple level access control in e-healthcare cloud computing systems in Sec. IV, followed by the formal security proof and performance evaluations respectively in Sec. V and Sec. VI. Finally, we draw the conclusion in Sec. VII.

II. Related Work

There exist a series of constructions for fine-grained access control of patient's PHI content [3-8,13,15,16,22], which mainly studied the issue of data confidentiality in a central cloud computing architecture, while leaving the challenging problem of realizing multilevel privacy preservation for kinds of physicians untouched. On the other hand, anonymous identification schemes are also profoundly focused on by exploiting the techniques of pseudonyms, group signatures and other privacy-preserving techniques [11,12,21,23-25].

To realize PHI fine-grained access control using attribute based cryptography techniques, Yu et al. proposed a fine-grained distributed data access control scheme in body area networks using attribute based encryption [5]. M. Li et al. proposed a patient-centric and fine-grained data access control in multi-owner settings for personal health records in cloud computing [4] by exploiting the technique of multi-authority attribute-based encryption (MABE). A rendezvous-based access control method providing access if and only if the patient and healthcare worker meet in the physical world was proposed by F. Dillema et al. [6]. However, these schemes placed importance elementally on the data confidentiality of the personal health information, leaving the patients' identity privacy issues unsolved.

To achieve patient's identity privacy protection exploiting anonymous identification, the technique of group signature [17][18] is widely adopted. X. Lin et al. proposed SAGE achieving not only the content-oriented privacy but also the contextual privacy against a strong global adversary [11]. J. Sun et al. proposed a solution to privacy and emergency responses based on anonymous credential, pseudorandom number generator and proof of knowledge [8]. L. Lu et al. proposed a privacy-preserving authentication scheme in anonymous P2P systems based on zero-knowledge proof [12]. J. Zhou et al. presented a multilevel privacy-preserving cooperative authentication in m-healthcare cloud computing systems [3]. However, the considerable amount of computational overhead in group signature and zero-knowledge proof makes it impractical for the resource-constrained hand-held mobile devices at the patient's end in e-healthcare systems.

Significantly distinguishing from the existing work, a white-box traceable and revocable multi-authority ciphertext policy attribute-based encryption TR-MABE is proposed to address the issues of both PHI data confidentiality and patient identity privacy in the multilevel privacy preservation way that the primary physicians taking responsibility of a patient's medical treatment can not only access her/his PHI content, but correctly verify her/his real identity; the secondary physicians participating in medical consultation or dedicating in the medical research cannot know the patient's real identity but the PHI content; the unauthorized persons who cannot obtain anything. Without introducing extra special signatures, our TR-MABE is efficiently constructed by outsoucing the storage revocation (i.e. ciphertext updating) to the cloud and well adapts to the e-healthcare systems.

III. System Architecture and Security Model

In this section, we briefly present the architecture of the e-healthcare cloud computing system and the formal security model of our proposed TR-MABE.

A. System Architecture

The architecture of the e-healthcare cloud computing system mainly comprises the following components: the body area networks (BANs) that frequently monitor the realtime personal health information (PHI) and outsouce it in the encrypted form into the cloud by the patient's hand held devices; the e-healthcare cloud server that stores huge volumes of patients' PHI and performs the efficient attribute revocation mechanism to realize multilevel fine-grained access control for privacy preservation; and the healthcare provider that includes both the primary physicians taking responsibility of the specific patient's medical treatment and the secondary physicians co-operative to complete medical consultation and research tasks. Additionally in our e-healthcare cloud computing system, there also exist D central authorities (CAs) and K attribute authorities (AAs) respectively denoted as $CA_1, CA_2, \cdots, CA_D$ and $AA_1, AA_2, \cdots, AA_K$. Each physician has a global identifier $gid \in GID$ and obtains the keys w.r.t. his unique gid from $CA_i(i \in \{1, 2, \cdots, D\})$s where GID is the identity set of all physicians. Each attribute authority $AA_k(k \in \{1, 2, \cdots, K\})$ manages a set of attributes $U_k(U_i \cap U_j = \phi \ \wedge \ U = \cup_{k=1}^{K} U_k)(i, j \in \{1, 2, \cdots, K\} \wedge i \neq j)$ and the authorized physicians (i.e. both the primary and secondary physicians) with attribute set AS_{gid} can obtain their attribute secret keys from the corresponding AA_ks. With the list of secondary and unauthorized physicians rl, CAs, AAs and the cloud also perform secret key and ciphertext updating. It is also assumed that all the multiple central authorities are run by different organizations, all of which are governed under some ordinance by the government. This multiple authority setting significantly relieves the patient's trust on one single CA or AA, since it is unlikely for all the authorities CAs and AAs to collude (or be compromised) to derive the secret keys. Fig. 1 illustrates the architecture of the e-healthcare cloud computing system.

B. Definitions and Security Model

The proposed TR-MABE consists of the following algorithms: **GlobalInit**: This algorithm takes as input the security parameter λ and outputs the global public parameter $GPAR$ of the system.

CASetup: This algorithm is run by each CA_i with $GPAR$ and its index i as input, and outputs the master secret key $CAMSK_d$, the public parameters $CAPAR_i$ and the public key $CAPK_i$.

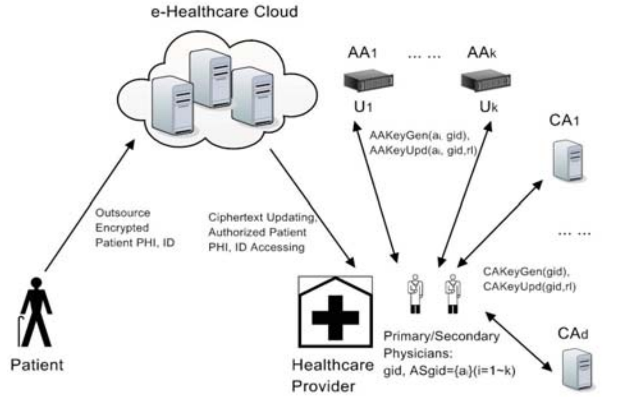

Fig. 1: Architecture of e-Healthcare Cloud Computing System

AASetup: This algorithm is run by each AA_k with $GPAR$, the index k and its attribute set U_k as input, and outputs the public parameter $AAPAR_k$, public key $AAPK_k$ and master secret key $AAMSK_k$.

Encrypt: This algorithm takes as input the PHI data m, the identity encryption key K_{id}, the data encryption key K_{data}, the access policy $\mathbb{P} = (A, \rho) \vee (B, \theta)$ defined on the attribute universe U, the global public parameter $GPAR$, CAs' public keys $CAPK_d(d \in \{1, 2, \cdots, D\})$ and AAs' public keys $AAPK_k$. Then, it outputs ciphertexts respectively associated to the patient identity encryption key, data encryption key, the PHI content together with the patient's real identity as $C_{K_{Data}}, C_{K_{id}}, CT_{PHI}, CT_{ID_{pat}}$ where ID_{pat} is the patient's real identity.

CAKeyGen: When an authorized physician (including both primary and secondary physicians) with global identifier gid registers to CA_i for obtaining a key, CA_i runs the algorithm with the input $gid, \tau = 0, GPAR, AAPK_k(k \in \{1, 2, \cdots, K\})$ and CA_i's master secret key $CAMSK_i$ where τ is the tag denoting key generation when $\tau = 0$ and key updating when $\tau = 1$. It outputs a pair of physician-central-keys $pcsk^0_{gid,i}, pcpk^0_{gid,i}$.

AAKeyGen: When an authorized physician requests a secret key for attribute att from AA_k, the latter runs the algorithm taking $att, AAMSK_k, pcpk^0_{gid,i}, GPAR, CAPK_i(i \in \{1, 2, \cdots, D\})$ as the input and outputs a physician-attr-key $pask^0_{att,gid,i}$ if all $pcpk^0_{gid,i}$s are valid; otherwise, it outputs $\perp$. For an authorized physician possessing the attribute set AS_{gid}, his decryption key is defined as $DeKey_{gid} = (pcsk^0_{gid,i}, pcpk_{gid,i}, pask^0_{att,gid,i})$ where $i \in \{1, 2, \cdots, D\}, att \in AS_{gid}$.

CAKeyUpd: This algorithm takes as input a revocation list rl including a set of global identifiers $gid_{rl}, \tau = 1, GPAR, AAPK_k$ and the master secret key $CAMSK_i$, then outputs the updated physician-central-secret-keys $pcsk^1_{gid,i}, pcpk^1_{gid,i}$.

AAKeyUpd: This algorithm takes as input $att, AAMSK_k, pcpk^1_{gid,i}, GPAR, CAPK_i (i \in \{1, 2, \cdots, D\})$, and outputs the updated physician-attr-key $pask^1_{att,gid,i}$.
CTUpd: This algorithm is performed by the e-healthcare cloud server. To revoke the secondary physician's ability to access the patient's real identity, it takes $GPAR, CAPK_i, AAPK_k$, the updated access policy $\mathbb{P}^{upd} = (A, \rho) \vee (B^{upd}, \theta^{upd})$ and the ciphertext $CT_{K_{id}}$, outputs the updated identity ciphertext $CT^{upd}_{K_{id}}$.
Decrypt: While receiving the ciphertexts $C^{upd}_{K_{id}}, C_{K_{data}}, CT_{ID_{pat}}, CT_{PHI}$, on input $pcpk^1_{gid,i}, pcsk^1_{gid,i}, pask^1_{att,gid,i}$, the authorized primary physician can recover both the identity encryption key K_{id} and data encryption key K_{data} to decipher the patient's real identity ID_{pat} and the original PHI data m_{pat}, but the secondary physician can only successfully recover the patient's PHI m_{pat} rather than the identity ID_{pat}.

The formal security model of our proposed TR-MABE is defined by the following game run between a challenger $\mathcal{B}$ and an adversary $\mathcal{A}$. Given the public parameters, $\mathcal{A}$ can corrupt CAs and AAs by identifying $\mathbb{D}_c \subset \mathbb{D}, \mathbb{K}_c \subset \mathbb{K}$ where $\mathbb{D}\backslash\mathbb{D}_c \neq \phi, \mathbb{K}\backslash\mathbb{K}_c \neq \phi$. W.l.o.g, it is assumed that $|\mathbb{D}\backslash\mathbb{D}_c| = 1$.
Setup: The challenger $\mathcal{B}$ runs algorithms **GlobalInit**(λ), **CASetup**$(GPAR, i)$, **AASetup**$(GPAR, k, U_k)$ and gives $GPAR, CAPAR_i, CAPK_i, AAPAR_k, AAPK_k$ to the adversary $\mathcal{A}$. Then, $\mathcal{A}$ specifies the target uncorrupted CA with index $i^* \in \mathbb{D}$ and a set of corrupted AAs $\mathbb{K}_c \subset \mathbb{K}$. $CAMSK_i (i \in \mathbb{D}\backslash\{i^*\}), AAMSK_k (k \in \mathbb{K}_c)$ are given to $\mathcal{A}$.
Key query phase I: The adversary $\mathcal{A}$ queries the following oracles.
$O^{CAKGen}(gid, i)$: $\mathcal{A}$ queries with gid, i^* where gid is the global identity. $\mathcal{B}$ sets the tag $\tau = 0$ and returns the corresponding physician-central-key $(pcsk^0_{gid,i}, pcpk_{gid,i})$. $O^{AAKGen}(att, pcpk_{gid,i}, k)$: $\mathcal{A}$ queries with $(att, pcpk_{gid,i}, k)$ where $i \in \mathbb{D}, k \in \mathbb{K}\backslash\mathbb{K}_c$. $pcpk_{gid,i}$ is the physician-central-public-key and att is the attribute in U_k. This oracle returns $pask^0_{gid}$ if the submitted $pcpk_{gid,i}$ are valid; otherwise, it returns $\perp$. $O^{KeyUpd}(rl)$: $\mathcal{A}$ queries with a revocation list rl including the identities of secondary physicians gid_{rl}. $\mathcal{B}$ sets the tag $\tau = 1$ and returns the updated physician-central-secret-key $pcsk^1_{gid,i}$.
Challenge phase: The adversary $\mathcal{A}$ submits two messages m_0, m_1 of equal length and an access policy $\mathbb{P}^*$. The challenger $\mathcal{B}$ flips a random coin $\beta \in \{0, 1\}$ and sends $\mathcal{A}$ the associated ciphertext of m_β under $\mathbb{P}^*$ to $\mathcal{A}$.
Key query phase II: The adversary $\mathcal{A}$ is once again given the access to three oracles in **Key query phase I**.
Guess: The adversary $\mathcal{A}$ outputs a bit β'. The experiment outputs 1 if and only if $\beta' = \beta$ and the following condition holds: (1) The access policy P^* cannot be satisfied by $AS_{gid_\mathcal{A}}$, where $AS_{gid_\mathcal{A}}$ is the attribute set w.r.t. the physician's global identity $gid_\mathcal{A}$ queried to O^{AAKGen} by $\mathcal{A}$; (2) For each key query to O^{CAKGen} and O^{AAKGen} such that $P^*(AS_{gid_\mathcal{A}} \cup (\cup_{k_c \in \mathbb{K}_c} U_{k_c})) = 1$, $gid_\mathcal{A} \in rl$ for each query to O^{KeyUpd}.

Definition 1: A TR-MABE scheme is secure if for any polynomial time adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ in the security game $Adv^{TR-MABE}(\lambda) = |Pr[\beta = \beta'] - 1/2|$ is negligible in λ.

The traceability of our proposed TR-MABE is also formally defined by describing a security game between a challenger $\mathcal{B}$ and an adversary $\mathcal{A}$ as follows.
Setup: The challenger $\mathcal{B}$ runs algorithms **GlobalInit**(λ), **CASetup**$(GPAR, i)$, **AASetup**$(GPAR, k, U_k)$ and gives $GPAR, CAPAR_i, CAPK_i, AAPAR_k, AAPK_k$ to the adversary $\mathcal{A}$.
Key query: $\mathcal{A}$ queries the challenger by accessing the oracles $O^{CAKGen}(gid, i), O^{AAKGen}$ and O^{KeyUpd} with the constrained condition the same as the security game of TR-MABE defined above.
Key forgery: $\mathcal{A}$ outputs a decryption key $DeKey^*_{gid}$. $\mathcal{A}$ wins the traceability game if $Trace(GPAR, CAPAR_i, CAPK_i, AAPAR_k, AAPK_k, T, DeKey^*_{gid}) \neq \perp$ namely $DeKey^*_{gid}$ is well-formed, and $Trace(GPAR, CAPAR_i, CAPK_i, AAPAR_k, AAPK_k, T, DeKey^*_{gid}) \notin \{gid_\mathcal{A}\}$.

Definition 2: A TR-MABE scheme is fully traceable if for any polynomial time adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ in the traceability game $Adv^{Trace}(\lambda) = Pr[Trace(GPAR, CAPAR_i, CAPK_i, AAPAR_k, AAPK_k, T, DeKey^*_{gid}) \notin \{\perp\} \cup \{gid_\mathcal{A}\}]$ is negligible in λ.

IV. Proposed TR-MABE Construction

In this section, we firstly propose a piecewise ciphertext policy multi-authority attribute-based encryption PT-MABE with white-box traceability. Then, by exploiting the technique of revocable storage [10], we further give our white-box traceable and revocable multi-authority attribute-based encryption named TR-MABE construction for fine-grained multiple level access control in e-healthcare cloud computing systems.

A. Proposed PT-MABE

The proposed PT-MABE serves the basis of our final TR-MABE construction and mainly comprises of the algorithms **GlobalInit**,**CASetup**,**AASetup**,**Encrypt**,**CAKeyGen**,**AAKeyGen**,**Decrypt** and **Trace** that are detailed as follows.
GlobalInit: On input 1^λ where λ is the security parameter, this algorithm outputs the global public parameters $GPAR$. Let $\mathbb{G}$ be a bilinear group of order $N = p_1p_2p_3$ and G_{p_i} be the subgroup of order p_i in $\mathbb{G}$, where p_1, p_2, p_3 are distinct big primes. Let $g \in \mathbb{G}_{p_1}$ as the generator of $\mathbb{G}_{p_1}$ and it randomly selects $h \in_R \mathbb{G}_{p_1}$. Let X_3 be generator of $\mathbb{G}_{p_3}$. The global public parameter is published as $GPAR = (N, g, h, X_3, \Sigma_{Sig})$, where $\Sigma_{Sig} = (KeyGen, Sign, Verify)$ is the description of a secure signature scheme unforgeable against chosen-message attack.
CASetup: On input $GPAR$, this algorithm outputs CA's public parameter $CAPAR$, public key $CAPK$ and master

secret key $CAMSK$. Firstly, each $CA_i(i = 1, 2, \cdots, D)$ runs the **KeyGen** algorithm of Σ_{Sig} to generate a pair of secret key and public key (sk_i, pk_i) respectively for sign and verification. Then, it randomly selects $\alpha_i, a_i \in_R \mathbb{Z}_N$. Finally, CA_i publishes its public parameter $CAPAR_i = (e(g,g)^{\alpha_i}, g^{a_i})$, $CAPK_i = pk_i$ and set its master secret key $CAMSK_i = (\alpha_i, a_i, sk_i)$. The table T_i is initialized to be empty.

AASetup: On input $GPAR$, the attribute universe U_k belonging to AA_k and the AA's index k, this algorithm outputs AA_k's public parameter $AAPAR_k$, public key $AAPK_k$ and master secret key $AAMSK_k$. For each $att \in U_k$, AA_k randomly selects $s_{att} \in_R \mathbb{Z}_N$ and sets $T_{att} = g^{s_{att}}$. It also randomly selects $v_{k,i} \in_R \mathbb{Z}_N(i = 1, 2, \cdots, D)$ and computes $V_{k,i} = g^{v_{k,i}}$.

AA_k publishes its public parameter $AAPAR_k = (\{T_{att}|att \in U_k\})$, $AAPK_k = V_{k,i}$ and sets its master secret key $AAMSK_k = (v_{k,i}, \{s_{att}|att \in U_k\})$.

Encrypt: On input the patient's real identity ID_{pat}, the PHI message m_{pat}, the symmetric identity encryption key K_{id}, data encryption key K_{data}, the access policy $\mathbb{A} = (A, \rho)$, $GPAR, CAPAR, AAPAR_k$, the patient's hand-held device performs the encryption and outputs the ciphertext CT. The access policy is represented by an LSSS matrix (A, ρ), where A is an $l \times n$ matrix and ρ maps each row A_x to an attribute $\rho(x)$. ρ is required not to map different rows to the same attribute. Then, it randomly selects a vector $\vec{v} = (s, v_2, \cdots, v_n) \in \mathbb{Z}_N^n$. For each $x \in \{1, 2, \cdots, l\}$, it randomly selects $r_x \in \mathbb{Z}_N$. Let $\lambda_x = A_x \cdot v$, the ciphertext is

$$\begin{aligned} &CT_{K_{cgy}} = K_{cgy} \prod_{i=1}^{d} e(g,g)^{\alpha_i s}, C^{'} = g^s, C_i^{''} = g^{a_i s}, \\ &\{C_x = h^{A_x \cdot \vec{v}} T_{\rho(x)}^{-r_x}, C_x^{'} = g^{r_x}\}(x \in \{1, 2, \cdots, l\}) \end{aligned} \quad (1)$$

together with the access policy $\mathbb{A} = (A, \rho)$, where $cgy \in \{id, data\}$. It is observed that $C_{A,\rho}^{cgy} = (CT_{K_{cgy}}, C^{'}, C_i^{''}, \{C_x, C_x^{'}(x \in \{1, 2, \cdots, l\})\})$. Finally, it encrypts the patient's real identity ID_{pat} and her/his PHI m_{pat} as $CT_{ID_{pat}} = E_{K_{id}}(ID_{pat}), CT_{PHI} = E_{K_{data}}(m_{pat})$ where $E_{K_{id}/K_{data}}(\cdot)$ is a secure symmetric key encryptions under K_{id}/K_{data}.

CAKeyGen: When an authorized physician registers his gid to $CA_i(i = 1, 2, \cdots, D)$ for requesting the physician-central-keys, the latter randomly selects $c_i \in \mathbb{Z}_N^*$. Let $\mu_i = \alpha_{u,i}$ if $\tau = 0$ and $\mu_i = \alpha_i - \alpha_{u,i}$ if $\tau = 1$. Then, CA_i randomly chooses $r_{gid,i} \in \mathbb{Z}_N, R_{gid,i}, R_{gid,i}^{'}, R_{gid,i}^{''} \in \mathbb{G}_{p_3}$, computes

$$\begin{aligned} &pcsk_{gid,i} = g^{\frac{\mu_i}{a_i + c_i}} h_{gid,i}^{r_{gid,i}} R_{gid,i}, pcsk_{gid,i}^{'} = c_i, \\ &L_{gid,i} = g_{gid,i}^{r_{gid,i}} R_{gid,i}^{'}, L_{gid,i}^{'} = (g^{a_i})^{r_{gid,i}} R_{gid,i}^{''}. \end{aligned} \quad (2)$$

It is noted that $\frac{\mu_i}{a_i+c_i}$ is computed modulo N. In the unlikely events that $gcd(a_i + c_i, N) \neq 1$ or c_i has been in T_i, CA_i repeats the above again using another randomly selected value $c_i \in \mathbb{Z}_N^*$. Finally, it puts the tuple (c_i, gid) into the table T_i.

For $k = 1$ to K, CA_i randomly selects $R_{gid,k,i} \in \mathbb{G}_{p_3}$ and computes

$$\Gamma_{gid,k,i} = V_{k,i}^{(a_i+c_i)r_{gid,i}} R_{gid,k,i}. \quad (3)$$

Finally, CA_i generates the signature $\sigma_{gid,i} = Sig_{sk_i}(gid \parallel L_{gid,i} \parallel L_{gid,i}^{'} \parallel \cup_{k=1}^{K} \Gamma_{gid,k,i})$ and publishes $pcpk_{gid,i} = (gid, L_{gid,i}, L_{gid,i}^{'}, \{\Gamma_{gid,k,i}\}, \sigma_{gid,i})$ where $k \in \{1, 2, \cdots, K\}$.

AAKeyGen: When an authorized physician submits her/his $pcpk_{gid,i}$ to the attribute authority AA_k for requesting the secret key for some attribute $att \in U_k$ in her/his attribute set AS_{gid}, the latter firstly checks whether the following equations hold,

$$\begin{aligned} &VALID \leftarrow \\ &Verify_{pk_i}(gid \parallel L_{gid,i} \parallel L_{gid,i}^{'} \parallel \cup_{k=1}^{K} \Gamma_{gid,k,i}, \sigma_{gid,i}), \\ &e(g, \Gamma_{gid,k,i}) = e(V_{k,i}, L_{gid,i}^{'} L_{gid,i}^{pcsk_{gid,i}^{'}}). \end{aligned} \quad (4)$$

If either fails to pass the verification, AA_k outputs $\perp$ which indicates the submitted $pcpk_{gid,i}$ are invalid.

Then, AA_k randomly selects $R_{att,gid}^{'} \in \mathbb{G}_{p_3}$ and computes

$$\begin{aligned} pask_{att,gid,i} &= (\Gamma_{gid,k,i})^{s_{att}/v_{k,i}} R_{att,gid}^{'} \\ &= (V_{k,i}^{(a_i+c_i)r_{gid,i}} R_{gid,k,i})^{s_{att}/v_{k,i}} R_{att,gid}^{'} \\ &= T_{att}^{(a_i+c_i)r_{gid,i}} R_{gid,k,i}^{s_{att,i}/v_{k,i}} R_{att,gid}^{'} \\ &= T_{att}^{(a_i+c_i)r_{gid,i}} R_{att,gid,i}, \end{aligned} \quad (5)$$

if we let $R_{att,gid,i} = R_{gid,k,i}^{s_{att}/v_{k,i}} R_{att,gid}^{'}$. Therefore, we have $pask_{gid,i} = \{pask_{att,gid,i}|att \in AS_{gid}\}$ where AS_{gid} is the attribute set held by the physician with global identity gid.

Decrypt: The authorized physician can successfully decipher the message by utilizing both $pcsk_{gid,i}$s respectively with $\mu_i = \alpha_{u,i}(\tau = 0)$ and $\mu_i = \alpha_i - \alpha_{u,i}(\tau = 1)$. We take $\mu_i = \alpha_{u,i}$ for example to explain the following steps. Firstly, if the physician's attribute set AS_{gid} satisfies the access policy $\mathbb{A} = (A, \rho)$, he computes constants $\omega_x \in \mathbb{Z}_N$ such that $\sum_{\rho(x) \in AS_{gid}} \omega_x A_x = (1, 0, \cdots, 0)$. Then, he computes

$$\begin{aligned} &\frac{e((C^{'})^{pcsk_{gid,i}^{'}} C_i^{''}, pcsk_{gid,i})}{\prod_{\rho(x) \in AS_{gid}} (e(C_x, L_{gid,i}^{pcsk_{gid,i}^{'}} L_{gid,i}^{'}) e(C_x^{'}, pask_{\rho(x),gid,i}))^{\omega_x}} \\ &= e(g,g)^{\alpha_{u,i} s}. \end{aligned} \quad (6)$$

Similarly, the primary physicians can recover $e(g,g)^{(\alpha_i - \alpha_{u,i})s}$. Finally, the data encryption key K_{data} can be recovered by

$$K_{cgy} = \frac{CT_{K_{cgy}}}{\prod_{i=1}^{D} (e(g,g)^{\alpha_{u,i} s} e(g,g)^{(\alpha_i - \alpha_{u,i})s})}, \quad (7)$$

where $cgy \in \{id, data\}$. Therefore, the patient's real identity and PHI can be deciphered as $ID_{pat} = D_{K_{id}}(CT_{ID_{pat}}), m_{pat} = D_{K_{data}}(CT_{m_{pat}})$ where $D_{K_{id}/K_{data}}(\cdot)$ is the corresponding decryption algorithms of $E_{K_{id}/K_{data}}(\cdot)$.

Trace: The tricky physicians leaking the secret key used to protect patient's identity and PHI would be successfully traced. If the decryption key is of the form $SK_{gid}^{Dec} = \{SK_{gid,i}|i \in \{1, 2, \cdots, D\}\} = \{pcsk_{gid,i}, pcsk_{gid,i}^{'}, L_{gid,i}, L_{gid,i}^{'}, pask_{att,gid,i}|i \in \{1, 2, \cdots,$

$D\}\}$ and satisfies all of the following five checks, it is a well formed decryption key whose decryption privilege is represented by the attribute set

$$AS_{gid} = \{att | att \in \cup_{k=1}^{K} U_k \\ \wedge e(V_{k,i}, L_{gid,i}^{pcsk'_{gid,i}} L'_{gid,i}) = e(g, \Gamma_{gid,k,i}) \neq 1\};$$

otherwise, it is not well-formed and the algorithm outputs $\perp$. If SK_{gid}^{Dec} is well-formed, the algorithm will search $pcsk'_{gid,i}(i = 1, 2, \cdots, D)$ in table T_i maintained by CA_i. If it is found in T_i, the associated identity gid will be output; otherwise, a special identity gid_ϕ that never appears in T_i will be output. The key sanity checks are performed as follows,

$$\begin{aligned} &(1)\ pcsk'_{gid,i} \in \mathbb{Z}_N, \\ &\quad pcsk_{gid,i}, L_{gid,i}, L'_{gid,i}, pask_{att,gid,i} \in \mathbb{G}, \\ &(2)\ e(g, L'_{gid,i}) = e(g^{a_i}, L_{gid,i}) \neq 1, \\ &(3)\ e(g^{a_i} g^{pcsk'_{gid,i}}, pcsk_{gid,i}) \\ &\quad = e(g,g)^\alpha e(L_{gid,i}^{pcsk'_{gid,i}} L'_{gid,i}, h) \neq 1, \\ &(4)\ \exists att \in AS_{gid}, s.t. \\ &\quad e(V_{k,i}, L_{gid,i}^{pcsk'_{gid,i}} L'_{gid,i}) = e(g, pask_{att,gid,i}) \neq 1. \end{aligned}$$

B. Proposed TR-MABE

In this subsection, we propose the white-box traceable and revocable multi-authority attribute-based encryption TR-MABE for fine-grained multiple level access control in e-healthcare cloud computing system based on PT-MABE presented in the previous section by exploiting the technique suggested by Sahai et al. [10]. Our intuitions can be outlined as follows: first of all, the patient's private PHI together with her/his real identity is encrypted under the unique access policy specified by the patient himself and outsourced into the e-heathcare cloud. Then, since the patient has no knowledge of physician status (i.e. which set of physicians are available and professional in treating her/his disease), the cloud serving the function as preliminary examination will help to select a group of primary physicians taking responsibility of the patient's treatment according to the access policy specified by the patient, and update the identity key ciphertext component which can be deciphered by the primary physicians using their updated keys. Additionally, the tricky physicians leaking the secret key used to protect patient's identity and PHI would be successfully traced. The details of our proposed TR-MABE are described in the following where the algorithms of **AASetup** and **AAKeyGen** are the same as PT-MABE.

GlobalInit: On input 1^λ where λ is the security parameter, this algorithm calls $PT - MABE.GlobalInit$ to output the corresponding $GPAR$.

CASetup: On input $GPAR$, this algorithm calls $PT - MABE.CASetup$ to generate $CAPAR, CAPK$ and $CAMSK$.

Encrypt: Without loss of generality, it is assumed that the patient's real identity ID_{pat} and his PHI m_{pat} are encrypted at time t. For each $y \in \mathcal{T}_t$, the patient computes

$$C_y^{(A,\rho),cgy} = PT - MABE.Encrypt(GPAR, CAPAR_i, \\ AAPAR_k, K_{cgy}, (A,\rho) \vee (B_y, \theta_y)), \tag{8}$$

where $cgy \in \{id, data\}$ and returns $C_t^{(A,\rho),cgy} = \{C_y^{(A,\rho),cgy} : y \in \mathcal{T}_t\}$. It is noted that by calling the algorithm $PT - MABE.Encrypt$, the patient also generates $CT_{ID_{pat}}, CT_{PHI}$ and outsources $C_t^{(A,\rho),cgy}, CT_{ID_{pat}}, CT_{PHI}$ into the e-healthcare cloud.

CAKeyGen: For all $u \in Path(gid)$ where gid is the global identity of the physician, CA_i performs

$$(pcsk_{u,i}^0, pcpk_{u,i}^0) = PT - MABE. \\ CAKeyGen(u, GPAR, AAPK_k, CAMSK, \tau = 0) \tag{9}$$

and returns $(pcsk_{gid,i}^0, pcpk_{gid,i}^0) = \{(pcsk_{u,i}^0, pcpk_{u,i}^0) : u \in Path(gid)\}$.

CAKeyUpd: For all $u \in \mathcal{U}(rl)$, CA_i computes

$$(pcsk_{u,s_t,i}^1, pcpk_{u,s_t,i}^1) = PT - MABE. \\ CAKeyGen(u, GPAR, AAPK_k, CAMSK, \tau = 1), \tag{10}$$

where $s_t = \{w_{i,t[i]} : i \in \{1, 2, \cdots, r\}\}$, and returns $(pcsk_{t,i}^1, pcpk_{t,i}^1) = \{(pcsk_{u,s_t,i}^1, pcpk_{u,s_t,i}^1) : u \in \mathcal{U}(rl)\}$ where rl is the list of secondary physicians who are not permitted to know the patient's real identity ID_{pat}.

AAKeyUpd: This algorithm calls $PT - MABE.AAKeyGen$ on the inputs $(pcsk_{t,i}^1, pcpk_{t,i}^1)$ output by **CAKeyUpd** and the physician's attributes $att \in AS_{gid}$ belonging to the management of AA_k, and outputs $pask_{t,i}^1 = \{pask_{u,s_t,i}^1 : u \in \mathcal{U}(rl)\}$.

Decrypt: For each primary physician whose identity $gid \notin rl$ when $(pcsk_{t',i}^1, pcpk_{t',i}^1)$ is created, there exists some node of $u \in \mathcal{U}(rl) \cap Path(gid)$. For this u, there exists

$$(pcsk_{u,i}^0, pcpk_{u,i}^0) \in (pcsk_{gid,i}^0, pcpk_{gid,i}^0), \\ (pcsk_{u,s_{t'},i}^1, pcpk_{u,s_{t'},i}^1) \in (pcsk_{t',i}^1, pcpk_{t',i}^1). \tag{11}$$

Additionally, if $t' \geq t$, this implies that there exists some $y \in \mathcal{T}_t$ such that y is an ancestor of t' and consequently $(B_y, \theta_y)(s_{t'}) = 1$. For this y, the physicians take $C_y^{A,\rho} \in C_t^{A,\rho}$ and perform

$$PT - MABE.Decrypt(pcsk_{u,i}^0, pcpk_{u,i}^0, pask_{u,i}^0, \\ pcsk_{u,s_{t'},i}^1, pcpk_{u,s_{t'},i}^1, pask_{u,s_{t'},i}^1, C_y^{A,\rho}). \tag{12}$$

It is observed that if $(A,\rho)(AS_{gid}) = 1$, then $(A,\rho) \vee (B_y, \beta_y)(AS_{gid}) = (A,\rho) \vee (B_y, \beta_y)(s_{t'}) = 1$, which means the symmetric encryption keys $K_{cgy}(cgy \in \{id, data\})$ can be successfully recovered. Then, it is noted that by calling the algorithm $PT - MABE.Decrypt$, the authorized physician can obtain the patient's real identity $ID_{pat} = D_{K_{id}}(CT_{ID_{pat}})$ and her/his PHI content $m_{pat} = D_{K_{data}}(CT_{m_{pat}})$.

CTUpdate: After the patient's ciphertexts

$C_t^{(A,\rho),cgy}, CT_{ID_{pat}}, CT_{PHI}$ are outsourced into the e-healthcare cloud, the latter would update $C_t^{(A,\rho),id}$ to guarantee that only the primacy physicians who are responsible of the medical treatment for patient ID_{pat} can know her/his real identity. Without loss of generality, this update is operated at time $t' = t+1$. For all $u \in \mathcal{T}_{t+1}$, the e-healthcare cloud searches $y \in \mathcal{T}_t$ such that y is an ancestor of u and there exists a $C_y^{(A,\rho),id}$ component in $C_t^{(A,\rho),id}$. For all such u, the cloud computes

$$C_u^{(A,\rho),id} = PT-MABE.Delegate(GPAR, CAPAR_i, AAPAR_k, C_y^{(A,\rho),id}, (A,\rho) \vee (B_u, \beta_u)), \tag{13}$$

and returns $C_{t+1}^{(A,\rho),id} = \{C_u^{(A,\rho),id} : u \in \mathcal{T}_{t+1}\}$ to the physicians.

V. Security Analysis

In this section, we give the formal security proof of our proposed TR-MABE to achieve multi-level privacy-preserving e-healthcare cloud computing systems. Though we can prove the security of our proposed TR-MABE from scratch under the three assumptions presented in Sec. IV, for brief presentation, we reduce the security to the existing work [9,14].

Theorem 1: If the fully secure multi-authority CP-ABE is secure in the security game of [9], then our proposed TR-MABE scheme is secure in the security game given in Sec. III-B.

Proof: Suppose there exists a PPT adversary $\mathcal{A}$ that can break our proposed PT-MABE scheme with advantage Adv_{ptmabe}, we construct a PPT algorithm $\mathcal{B}$ to break the underlying multi-authority CP-ABE scheme with the advantage Adv_{mabe} that equals to Adv_{ptmabe}.

Setup. Multi-authority CP-ABE gives $\mathcal{B}$ the public parameters $GPK = (N, g, h, X_3, \sum_{sign}), CPK_d = e(g,g)^{\alpha_i} (i = 1, 2, \cdots, D), CAPK_i = VerifyKey_i, APK_k = \{T_{att} = g^{s_{att}} | att \in U_k\}, ACPK_k = \{V_{k,i} = g^{v_{k,i}} | (i = 1, 2, \cdots, D)\}$. $\mathcal{B}$ randomly selects $a_i \in \mathbb{Z}_N (i = 1, 2, \cdots, D)$, then gives the adversary $\mathcal{A}$ the following public parameters $GPAR = (N, g, h, X_3, \sum_{sign}), CAPAR_i = (e(g,g)^{\alpha_i}, g^{a_i}) (i = 1, 2, \cdots, D), CAPK_i = VerifyKey_i, AAPAR_k = \{T_{att} = g^{s_{att}} | att \in U_k\}, AAPK_k = \{V_{k,i} = g^{v_{k,i}} | (i = 1, 2, \cdots, D)\}$ and initializes table $T_i = \phi$. Then, the adversary $\mathcal{A}$ specifies the target uncorrupted CA with index $i^* \in \mathbb{D}$ and a set of corrupted AAs $\mathbb{K}_c \in \mathbb{K}$. Then, $\mathcal{B}$ submits $i^*, \mathbb{K}_c$ to multi-authority CP-ABE and obtains $CMSK_i = (\alpha_i, SignKey_i) (i \in \mathbb{D} \backslash i^*), AMSK_k = (\{s_{att} | att \in U_k\} (k \in \mathbb{K}_c), \{v_{k,i} | i \in \mathbb{D} \backslash i^*, k \in \mathbb{K}_c\})$. Then, $\mathcal{B}$ gives back the adversary $\mathcal{A}$ with $CAMSK_i = (\alpha_i, a_i, SignKey_i) (i \in \mathbb{D} \backslash i^*), AAMSK_k = AMSK_k$.

Key query Phase 1. (1) When the adversary $\mathcal{A}$ submits gid, i^* to the oracle O^{CAKGen}, the simulator $\mathcal{B}$ sets $\tau = 0$, submits (gid, i^*) to multi-authority CP-ABE and obtains $ucsk_{gid,i^*}^{MA} = g^{\alpha_{u,i^*}} h^{r_{gid,i^*}^{MA}} R_{gid,i^*}$, $L_{gid,i^*}^{MA} = g^{r_{gid,i^*}^{MA}} R'_{gid,i^*}$ and $\Gamma_{gid,i^*,k}^{MA} = V_{k,i^*}^{r_{gid,i^*}^{MA}} R_{gid,i^*,k} (k \notin \mathbb{K}_c)$. (i.e. it is assumed that digital signature $Sign$ is secure against message forgery attack, therefore we briefly omit it in the proof.) Then, the simulator $\mathcal{B}$ randomly selects $c_{i^*} \in \mathbb{Z}_N^*$ and computes $1/(a_{i^*} + c_{i^*}) \ mod \ N$. In the unlikely events that $gcd(a_{i^*} + c_{i^*}, N) \neq 1$ or c_{i^*} has been in T_{i^*}, $\mathcal{B}$ repeats it again using another randomly selected value $c_{i^*} \in \mathbb{Z}_N^*$. By implicitly setting $r_{gid,i^*} = r_{gid,i^*}^{MA} / (a_{i^*} + c_{i^*})$ and $pcsk'_{gid,i^*} = c_{i^*}$, $\mathcal{B}$ randomly selects $R'' \in \mathbb{G}_{p_3}$ by using X_3 and $t_{gid,i^*} \in \mathbb{Z}_N$, then computes

$$\begin{aligned}
&pcsk_{gid,i^*} = (ucsk_{gid,i^*}^{MA})^{\frac{1}{a_{i^*}+c_{i^*}}} \\
&= (g^{\alpha_{u,i^*}} h_{gid,i^*}^{r_{gid,i^*}^{MA}} R_{gid,i^*})^{\frac{1}{a_{i^*}+c_{i^*}}} = g^{\frac{\alpha_{u,i^*}}{a_{i^*}+c_{i^*}}} h^{r_{gid,i^*}} R_{gid,i^*}^{\frac{1}{a_{i^*}+c_{i^*}}} \\
&L_{gid,i^*} = (L_{gid,i^*}^{MA})^{\frac{1}{a_{i^*}+c_{i^*}}} = g^{r_{gid,i^*}} (R'_{gid,i^*})^{\frac{1}{a_{i^*}+c_{i^*}}} \\
&L'_{gid,i^*} = (L_{gid,i^*}^{MA})^{\frac{a_{i^*}}{a_{i^*}+c_{i^*}}} R'' \\
&= g^{a_{i^*} r_{gid,i^*}} (R'_{gid,i^*})^{\frac{a_{i^*}}{a_{i^*}+c_{i^*}}} R'' \\
&\Gamma_{gid,i^*,k} = \Gamma_{gid,i^*,k}^{MA} \\
&= V_{k,i^*}^{r_{gid,i^*}^{MA}} R_{gid,i^*,k} = V_{k,i^*}^{a_{i^*}+c_{i^*} r_{gid,i^*}} R_{gid,i^*,k}.
\end{aligned} \tag{14}$$

Then, for all $u \in Path(gid)$, do the same as the query operations described above. Finally, $\mathcal{B}$ gives $pcsk_{u,i^*}, pcsk'_{u,i^*}, L_{u,i^*}, L'_{u,i^*}, \Gamma_{u,i^*,k} (k \notin \mathbb{K}_c)$ to the adversary $\mathcal{A}$ and puts the tuple (c_{i^*}, gid) into table T_i.
(2) When the adversary $\mathcal{A}$ submits $(att, pcpk_{gid,d}, k)$ to O^{AAKGen} for querying the attribute decryption key, $\mathcal{B}$ firstly verifies whether the following equations hold

$$\begin{aligned}
&VALID \leftarrow \\
&Verify_{pk_{i^*}}(gid \parallel L_{gid,i^*} \parallel L'_{gid,i^*} \parallel \cup_{k \notin \mathbb{K}_c} \Gamma_{gid,k,i^*}, \sigma_{gid,i^*}), \\
&e(g, \Gamma_{gid,k,i^*}) = e(V_{k,i^*}, L'_{gid,i^*} L_{gid,i^*}^{pcsk'_{gid,i^*}}).
\end{aligned} \tag{15}$$

If they do, $\mathcal{B}$ randomly selects $R'_{att,gid} \in \mathbb{G}_{p_3}$ and computes $pask_{att,gid,i^*} = (\Gamma_{gid,k,i^*})^{s_{att}/v_{k,i^*}} R'_{att,gid} = T_{att}^{a_{i^*}+c_{i^*}} r_{gid,i^*} R_{att,gid,i^*}$ where $R_{att,gid,i^*} = R_{gid,k,i^*}^{s_{att}/v_{k,i^*}} R'_{att,gid}$. Then, for all $u \in Path(gid)$, do the same as the query operations described above. Finally, $\mathcal{B}$ gives $pask_{att,u,i^*}$ back to $\mathcal{A}$.
(3) When the adversary $\mathcal{A}$ submits the revocation list rl to O^{KeyUpd}, $\mathcal{B}$ sets $\tau = 1$, performs the same operations as answering O^{CAKGen} and O^{AAKGen} with the exception that $u \in \mathcal{U}(rl)$ and returns $(pcsk_{t,i^*}^1, pcpk_{t,i^*}^1) = \{(pcsk_{u,s_t,i^*}^1, pcpk_{u,s_t,i^*}^1) : u \in \mathcal{U}(rl)\}$ and $pask_{t,i^*}^1 = \{pask_{u,s_t,i^*}^1 : u \in \mathcal{U}(rl)\}$ where $s_t = \{w_{i,t[i]} : i \in \{1, 2, \cdots, r\}\}$ by replacing α_{u,i^*} with $\alpha_i - \alpha_{u,i^*}$. This can be achieved as follows. $\mathcal{B}$ randomly selects $\alpha_i \in \mathbb{Z}_N$, computes g^{α}, $pcsk_{gid,i^*}^1 = g^{\alpha_i} (ucsk_{gid,i^*}^{MA})^{-\frac{1}{a_{i^*}+c_{i^*}}} = g^{\alpha_i} (g^{\alpha_{u,i^*}} h_{gid,i^*}^{r_{gid,i^*}^{MA}} R_{gid,i^*})^{-\frac{1}{a_{i^*}+c_{i^*}}} = g^{\frac{\alpha_i}{a_{i^*}+c_{i^*}} - \frac{\alpha_{u,i^*}}{a_{i^*}+c_{i^*}}} h^{r_{gid,i^*}} R_{gid,i^*}^{-\frac{1}{a_{i^*}+c_{i^*}}}$. It is noted that here we implicitly let $r_{gid,i^*} = -r_{gid,i^*}^{MA} / (a_{i^*} + c_{i^*})$ and the corresponding $pcpk_{t,i^*}^1, pask_{t,i^*}^1$ would not be changed when querying O^{KeyUpd}.

Challenge phase. The adversary $\mathcal{A}$ submits to $\mathcal{B}$ an LSSS matrix $P^* = (A^*, \rho) \vee (B_y^*, \theta_y)$ and two messages m_0, m_1 of the same length for each $y \in \mathcal{T}_t$ (i.e. m_0, m_1 refer to

K^0_{cgy}, K^1_{cgy} in our construction where $cgy \in \{id, data\}$ and the underlying $E_{K_{cgy}}(\cdot)$ is assumed to be a secure symmetric encryption). Then, $\mathcal{B}$ submits (P^*, m_0, m_1) to multi-authority CP-ABE, and obtains the challenge ciphertext in the form of

$$C^{MA} = m_b \prod_{i=1}^{d} e(g,g)^{\alpha_i s}, C^{',MA} = g^s,$$
$$\{C^{MA}_x = h^{(A^* \cup B^*_y)_x \cdot \vec{v}} T^{-r_x}_{\rho(x)},$$
$$C^{',MA}_x = g^{r_x}\}(x \in \{1, 2, \cdots, l\}) \tag{16}$$

along with the access policy $P^* = (A^*, \rho) \vee (B^*_y, \theta_y)$. Then, $\mathcal{B}$ gives the adversary $\mathcal{A}$ the challenge ciphertext as

$$CT_{K_{cgy}} = C^{MA} = m_b \prod_{i=1}^{d} e(g,g)^{\alpha_i s},$$
$$C^{'} = C^{',MA} = g^s, C^{''}_i = (C^{',MA})^{a_i} = g^{a_i s},$$
$$\{C_x = C^{MA}_x = h^{(A^* \cup B^*_y)_x \cdot \vec{v}} T^{-r_x}_{\rho(x)},$$
$$C^{'}_x = C^{',MA}_x = g^{r_x}\}(x \in \{1, 2, \cdots, l\}) \tag{17}$$

along with the access policy $P^* = (A^*, \rho) \vee (B^*_y, \theta_y)$. It is noted that the simulation operates with the restrictions that (1) The access policy P^* cannot be satisfied by $AS_{gid_{\mathcal{A}}}$, where $AS_{gid_{\mathcal{A}}}$ is the attribute set w.r.t. the physician's global identity $gid_{\mathcal{A}}$ queried to O^{AAKGen} by $\mathcal{A}$; (2) For each key query to O^{CAKGen} and O^{AAKGen} such that $P^*(AS_{gid_{\mathcal{A}}} \cup (\cup_{k_c \in \mathbb{K}_c} U_{k_c})) = 1$, $gid_{\mathcal{A}} \in rl$ for each query to O^{KeyUpd}.

Key query phase II. Same as **Key query phase I**.

Guess. The adversary $\mathcal{A}$ gives $\mathcal{B}$ a $\beta^{'}$ and $\mathcal{B}$ gives $\beta^{'}$ to multi-authority CP-ABE.

It is observed that the distributions of the public parameters, decryption keys and challenge ciphertexts are the same as the real scheme, therefore we have $Adv_{mabe} = Adv_{ptmabe}$. ■

Theorem 2: If the white-box traceable CP-ABE [14] is fully traceable, then our proposed TR-MABE is also fully traceable in the security game defined in Sec. III-B.

The formal security proof of reducing the property of fully traceability of our proposed TR-MABE can be reduced to the same property possessed by white-box traceable CP-ABE [14] and the reduction process resembles the proof we have given in deriving Theorem 1.

VI. Performance Evaluation

In this section, we study the performance evaluation of our proposed TR-MABE in e-healthcare cloud computing systems. Since the cloud is generally assumed to be resource abundant, we mainly focus on the computational and communication overhead loaded on both the patient and physician's ends. In the existing work, group signature has been profoundly studied and widely adopted to achieve conditional identity privacy, that is only the trusted authority (TA) possessing the trapdoor is allowed to trace the patient's real identity in the e-healthcare scenario. Therefore, TA is required to be online to recover the patient's real identity for her/his primary physicians, which is unrealistic and would bring about considerable complexity in practice. However, in our proposed TR-MABE, multilevel privacy preservation is achieved by exploiting the technique of revocable storage in the multi-authority setting. Without an online TA, our proposed construction can simultaneously trace the physicians who have leaked the secret key to unauthorized entities for potential patient's PHI and identity exposure. This functionality can also not be achieved by group signatures. In the following, we perform the efficiency simulation and comparisons between the state-of-the-art [17][18] and our proposed TR-MABE.

We conduct the experiments by exploiting PBC [19] and MIRACLE [20] libraries running on Linux platform with 2.93GHz processor to study the operation costs. The experimental results show a single pairing, exponentiation, multiplicative operation in $\mathbb{Z}_N$ with $|N| = 1536$-bits almost respectively cost 36.8 ms, 10.7 ms and 8.6 ms. The same operations in $\mathbb{Z}_p$ where $|p| = 512$-bits almost respectively cost 27.2 ms, 7.6 ms and 5.4 ms. Fig. 2 and Fig. 3 illustrate the computational cost comparison among Boyen's scheme [17], Liang's scheme [18] and our proposed TR-MABE respectively on the patient's and physician's ends. It is observed that the computational cost increases as the size of physician's attribute set N_{att} grows. However, by exploiting the technique of group signatures [17][18] widely adopted to achieve conditional identity privacy, the computational cost increase as the number of physicians grows since it is required for the patient to generate one group signature for each physician in the PKI setting. On the other hand, to achieve fine-grained PHI content access control, the computational overhead of PHI encryption in the underlying ciphertext policy attribute-based encryption (CP-ABE) [18] is also loaded on the patient's end. Therefore, the straightforward combination of the techniques of group signature and CP-ABE would bring about an intolerable computational complexity on the resource-constrained patient's end (i.e the hand-held mobile devices such as PDAs takes on the associated operations). Significantly from the existing techniques [17][18], our proposed TR-MABE requires no extra special kind of signature to achieve multilevel patient identity privacy and naturally embraces this functionality by designing the technique of traceable and revocable multi-authority CP-ABE. Therefore, the computational cost is independent of the number of physicians, dramatically lower than the state-of-the-art [17][18] and well adapts to the e-healthcare system.

Fig. 4 illustrates communication overhead comparison among Boyen's scheme [17], Liang's scheme [18] and our proposed TR-MABE. It is obviously observed that the communication cost of Boyen's scheme [17] and Liang's scheme [18] sharply grows as the number of physicians increases from 50 to 500 in the healthcare provider and the size of physician's attribute set N_{att} increases from 10 to 30. However, the communication cost of our proposed TR-MABE is significantly lower than [17][18] and independent of the physician number.

VII. Conclusion

In this paper, a white-box traceable and revocable multi-authority attribute-based encryption named TR-MABE is pro-

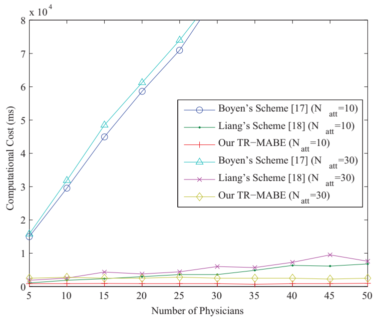

Fig. 2: Computational Cost Comparison on Patient End

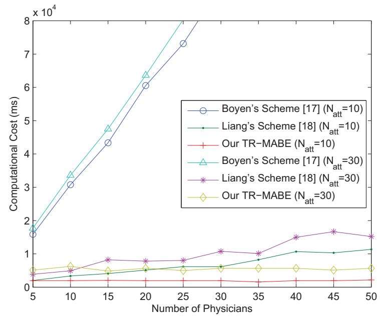

Fig. 3: Computational Cost Comparison on Physician End

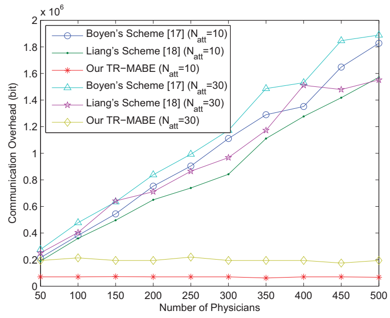

Fig. 4: Communication Overhead Comparison

posed to efficiently achieve multilevel privacy preservation. With the proposed TR-MABE, the primary physicians taking responsibility of a patient's medical treatment can not only access her/his PHI content, but correctly verify her/his real identity; the secondary physicians participating in medical consultation or dedicating in the medical research are not permitted to know the patient's real identity but the PHI content; the unauthorized persons cannot obtain anything. Additionally, it can efficiently track the physicians leaking secret keys used to protect patient's identity and PHI. Finally, formal security proof and extensive simulations illustrate our proposed TR-MABE is IND-CPA secure in the standard model and far outperforms the state-of-the-art in terms of storage, computational and communication overhead.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (Grant No. 61411146001, 61033014, 61373154 and 61371083) and the Prioritized Development Projects of the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20130073130004).

References

[1] I. Iakovidis, *Towards Personal Health Record: Current Situation, Obstacles and Trends in Inplementation of Electronic Healthcare Records in Europe*, International Journal of Medical Informatics, 52(1):105-115, 1998.

[2] 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 International Workshop on Wearable and Implantable Body Sensor Networks 2006-BSN 2006, April, 2006.

[3] J. Zhou, X. Lin, X. Dong and Z. Cao, *PSMPA: Patient Self-controllable and Multi-level Privacy-preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System*, IEEE Transactions on Parallel and Distributed Systems, to appear.

[4] 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*, SecureComm 2010, LNICST 50, pp.89-106, 2010.

[5] S. Yu, K. Ren and W. Lou, *FDAC: Toward Fine-grained Distributed Data Access Control in Wireless Sensor Networks*, In IEEE Infocom 2009.

[6] F.W. Dillema and S. Lupetti, *Rendezvous-based Access Control for Medical Records in the Pre-hospital Environment*, In HealthNet 2007.

[7] J. Zhou, Z. Cao, X. Dong, X. Lin and A. V. Vasilakos, *Securing m-Healthcare Social Networks: Challenges, Countermeasures and Future Directions*, IEEE Wireless Communications, vol. 20, No. 4, pp. 12-21, 2013.

[8] J. Sun, X. Zhu, C. Zhang and Y. Fang, *HCPP: Cryptography Based Secure EHR System for Patient Privacy and Emergency Healthcare*, ICDCS 2011.

[9] Z. Liu, Z. Cao, Q. Huang, D.S. Wong and T.H. Yuen, *Fully Secure Multi-authority Ciphertext-policy Attribute-based Encryption without Random Oracles*, ESORICS 2011, pp. 278-297.

[10] A. Sahai, H. Seyalioglu and B. Waters, *Dynamic Credentials and Ciphertext Delegation for Attribute-Based Encryption*, CRYPTO 2012, pp. 199-217.

[11] 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 Journal on Selected Areas in Communications, 27(4):365-378, May, 2009.

[12] 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 Transactions on Parallel and Distributed Systems, Vol. 19, No. 10, October, 2008.

[13] R. Lu, X. Lin, X. Liang and X. Shen, *A Secure Handshake Scheme with Symptoms-Matching for mHealthcare Social Network*, IEEE Journal on Selected Areas in Communications, Vol.27, No.4, pp.387-399, 2009.

[14] Z. Liu, Z. Cao and D.S. Wong, *White-box Traceable Ciphertext-policy Attribute-based Encryption Supporting Any Monotone Access Structures*, IEEE Transactions on Information Forensics and Security, vol. 8, No. 1, pp. 76-88, 2013.

[15] N. Cao, Z. Yang, C. Wang, K. Ren and W. Lou, *Privacy-preserving Query over Encrypted Graph-structured Data in Cloud Computing*, ICDCS 2011.

[16] V. Goyal, O. Pandey, A. Sahai and B. Waters, *Attribute-based Encryption for Fine-grained Access Control of Encrypted Data*, In ACM CCS'06, 2006.

[17] X. Boyen and B. Waters, *Full-domain Subgroup Hiding and Constant-size Group Signatures*, In: PKC 2007. LNCS, vol. 4450, pp. 1C15. Springer, Heidelberg, 2007.

[18] X. Liang, Z. Cao, J. Shao and H. Lin, *Short Group Signature without Random Oracles*, ICICS 2007, LNCS 4861, pp. 69C82, 2007.

[19] PBC Library, *http://crypto.stanford.edu/pbc/times.html*.

[20] *Multiprecision integer and rational arithmetic c/c++ library*, http://www.shamus.ie/.

[21] B. Riedl, V. Grascher and T. Neubauer, *A Secure E-health Architecture based on the Appliance of Pseudonymization*, Journal of Software, 3(2):23-32, February, 2008.

[22] J. Sun and Y. Fang, *Cross-domain Data Sharing in Distributed Electronic Health Record System*, IEEE Transactions on Parallel and Distributed Systems, vol. 21, No. 6, 2010.

[23] J. Misic and V. B. Misic, *Implementation of security policy for clinical information systems over wireless sensor networks*, Ad Hoc Networks, vol.5, no.1, pp.134-144, Jan 2007.

[24] S. Schechter, T. Parnell and A. Hartemink, *Anonymous Authentication of Membership in Dynamic Groups*, in Proceedings of the Third International Conference on Financial Cryptography, 1999.

[25] D. Slamanig, C. Stingl, C. Menard, M. Heiligenbrunner and J. Thierry, *Anonymity and Application Privacy in Context of Mobile Computing in eHealth*, Mobile Response, LNCS 5424, pp. 148-157, 2009.