Secure and Privacy-Preserving Referral Framework for E-Health System

Oladayo Olakanmi*[‡], Ismaila Kamil*, Sunday Ogundoyin*

* Department of Electrical and Electronic Engineering, University of Ibadan, Nigeria

[‡] Oladayo Olakanmi; Tel: +234-8068730815, e-mail: olarad4u@yahoo.com

Abstract- Doctors have a crucial role in promoting the physical wellbeing of patients and ensuring that they are given the safest and effective treatments that meet their medical needs and preferences. Due to an extensive area of the field of medicine, doctors do not have complete knowledge about a patient diagnosis and the special tools required, hence there is need for referral. Referral requires the transfer of patients and their sensitive medical information to a specialist in order to develop a tailored treatment or suggestion for a better healthcare treatment. Therefore, it is imperative to search for a specialist in that area of specialization who will not only have access to the patient's relevant health information but also be able to proffer solutions to health challenges. However, if this is not done securely and anonymously, it would not only affect the confidentiality of the data but also exposes the privacy of patient and physicians to adversaries. Therefore, there is need for an efficient referral framework that is capable of securing patient's data, and protecting patient's and physician's identities during the referral.

In this paper, we proposed a referral framework with efficient security and privacy schemes for achieving anonymous authentication during the referral process and a trust model for efficient rating and selection of specialists. To preserve privacy of the physicians, we leverage pseudonyms for anonymous authentication. A time-bound group signature was proposed by modifying existing group signatures for a robust grouping of physicians based on their specialisations and a trust model for determining the competency of specialist.

Keywords - Time-bound; Group signature; Referral; Trust value; Specialist.

1. Introduction

Generally, there are two categories of medical practitioners: General practitioner or Primary Doctor **PD** and Specialist or Secondary Doctor **SD**. Under normal circumstances, PDs are the first practitioner to consult for medical treatments. Therefore, it is imperative for PDs to have broad knowledge in all areas of medicine, and be able to recognize common sickness and pathology. A PD is able to diagnose patient's problems, write prescriptions, and advise patients on their health status and requirements. However, PDs often do not have the in-depth knowledge required for a specific branch of medicine such as cardiology, surgery, oncology, etc. Therefore, referral of patients to an SD is inevitable. In medical field, referral is the transfer of patient's care from one clinician to another through a health care known as tertiary care. A clinician is a health care professional that offers primary health care, such as Optometrist, Podiatrist, Psychologist, Registered Nurse, Physician, etc., to patients. A doctor becomes a medical specialist in a particular area of medicine after acquiring special expertise or skills to tackle a diagnosis in greater in-depth. Most times, the patient does not have a pre-knowledge of which SD could be contacted for a certain ailment. This is usually achieved through the referral from the PD. However, the security of the communication link between PD and SD, determination of the competency of SD, and privacy of users are pertinent for an efficient referral system. In the context of health information, privacy is the right of a patient to keep his health information from being disclosed to an unauthorised person. It involves controlling who is authorised to access a patient's protected health information (PHI); under what conditions patient's PHI may be accessed, used or disclosed to a third party. This is usually achieved through an access control policy and procedure. On the other hand, security is a mechanism for protecting the privacy of a patient‘s health information. Security includes the ability to control access to PHI and protecting patient’s health information from unauthorised disclosure, modification, loss, or destruction.

During the specialist's selection process, it is important to ensure that a competent SD is selected or recommended to handle a patient's health problem. In the conventional paper-based health system, a SD is selected based on the past achievements or recorded successes and experience in such area of expertise. However, this may not be sufficient in determining a reliable and capable SD. For example, the past experience may not be enough to rate the level of competency or expertise of the SD. Also, the privacy of the physician, patient, and specialist cannot be preserved with this conventional method of health system [1].

Conventionally, referral of patients in eHealth is done using localised web-based electronic referral system whereby health care providers receive, process, and monitor referral requests from other hospitals. However, with the huge benefits of cloud computing, most health service providers are moving their resources into the cloud. Therefore, there is a need for an efficient referral framework that allows a PD to search for competent specialists in the cloud server to handle a patient's case without compromising both the patient's and physicians' privacies. The challenges are in two folds: how to determine the competency of a specialist based on trust level, and how to achieve a secure and robust referral framework that is capable of protecting the privacy of patients. To achieve these, we implemented a trust model to achieve effective and secure selection of specialists to handle patients’ health challenges; we leverage pseudonyms for physicians' privacy and anonymity; and a time-bound group signature for an anonymous authentication and grouping of specialists.

2. Literature Review

There have been different proposed schemes on protecting patients’ health records in eHealth systems. Li et al [22] proposed a novel framework for implementing fine-grained data access control to protect patient's health record (PHR) data under multi-owner settings. Their scheme enables patients to have full control over their PHR by using attribute-based encryption to encrypt all files. In [7], the authors proposed a fine-grained health information access control framework in the cloud for lightweight Internet of Things (IoT) devices with data dynamics auditing and attribute revocation functions. They employed ciphertext-policy attribute-based encryption (CP-ABE) to achieve security and privacy. Furthermore, Guo et al [1] designed a privacy-preserving attribute-based authentication system for eHealth networks. Their framework authenticates users using verifiable attributes while keeping their attributes and identities concealed.

A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency known as SPOC was proposed [28]. With SPOC, the resources available on other opportunistically contacted medical users' smartphones can be combined to address the computing-intensive personal health information (PHI) process in emergency situations. To minimise the PHI privacy disclosure, SPOC introduces a user-centric two-phase privacy access control to allow only those medical users who have similar symptoms to participate in opportunistic computing. Also, to achieve user-centric privacy access control, an efficient attribute-based access control and non-homomorphic encryption-based privacy-preserving scalar product computation (PPSPC) protocol was presented. In [29], the authors proposed a secure and privacy-preserving eHealth using Architecture for the Notification of Traffic Incidents and Congestion (NOTICE) called WEHealth. WEHealth is a service-oriented PHR system through which drivers can consult and edit the health information in traffic, especially under emergency situations. WEHealth also allows users in wireless vehicular network to have access to health record system. Authentication and authorization of users is achieved by using the belts of NOTICE as the infrastructure of PKI, and privacy preservation through the use of pseudonyms. However, the need for referral of patients to specialists was not addressed in [28] and [29].

There have been various proposed works on referral system and protection of patient's health information. For instance, Almanscori et al [16] proposed an electronic referral system based on decision support and recommendation techniques. Their scheme allows the use of previous referral transactions through decision making and recommendations. In [18], an Electronic Medical Referral System (EMRS) was proposed to reduce the patient's and specialist's referral wait times and resolve cost-cutting issues. Moreover, the multi-disciplinary team in Radiotherapy Department at St. James' Institute of Oncology in University of Leeds, United Kingdom also implemented an electronic referral system called ebooking [19]. The University of California San Francisco (UCSF) and San Francisco General Hospital (SFGH) also developed a HIPAA-compliant web-based e-Referral system that allows effective communication between General Practitioners (GP) and Specialists [20]. In the same way, the King Fahd Medical City (KFMC) hospital in Saudi Arabia developed a user-friendly patients' referral system known as Patient Referral System-version 2.0, which is a web-based application that helps the KFMC hospital to receive, process, control, and monitor referral requests from other hospitals [21]. However, all the above approaches are electronic web-based applications, and the security and the privacy of the entities involved were not considered. Thus, there is need to implement a flexible, secure, and privacy-preserving framework that could effectively handles patient referral issues and serves as basis for future work in referral systems.

3. Problem Standardization

In this section, we give succinct problem formulation, system model and adversary model for the referral framework.

3.1 *Problem Formulation*

It is very important for any referral framework to be able to efficiently select the best SDs for a patient in a secure manner, and also thwarts any form of attack that is capable of compromising the efficiency of the framework. We formulated two problems so as to address the security and privacy issues in the referral system, as discussed below.

Problem 1: *(Efficient selection of specialists) Given a compromised primary doctor, $\mathcal{A}$, and a specialist, B. Assuming $\mathcal{A}$ is capable of either launching ballot-stuffing attack in favour of B by reporting an erroneous high competency score for B or bad-mouthing attack against B by reporting an erroneous low competency score about B during the rating of specialists in the referral framework. The problem is how to prevent $\mathcal{A}$ from launching these two forms of attacks on B so as not to influence the selection.*

Thwarting these attacks is requisite to determining the efficiency of the proposed novel trust model. Our decay trust model handles ballot-stuffing attack by increasing the rate of decay of the trust value of the SD if not selected for a certain period of time and bad-mouthing attack by using an average trust value of all the trust values reported by PDs who engaged the service of the SD for a particular period of time.

Problem 2: *(Anonymous Authentication and Escalation of privilege) Given an adversary $\mathcal{A}$ who wants to link set of medical data to a patient. Also, the possibility of a specialist using expired or compromised key to access patient's data.*

In our work, we use pseudo-identity to achieve strong anonymity, group signature to classify specialists, and a time-bound group secret key to prevent escalation of privilege.

3.2 *System Model*

The overview of our system model is as shown in Fig.1. The system model contains three entities: Primary Doctor (PD), Specialist (SD) or Consultant, and the Medical Practitioners' Agency (MPA).

a. **Primary Doctor (PD):** A PD is a physician that handles a patient's general health problems. The PD is responsible for handling patient's general health condition and initiates a referral process if needed.

b. **Specialist (SD):** A SD or consultant is one who is well versed in a given specialization of medicine. In other words, a SD has a deeper knowledge in a particular area of medical field. The SD is contacted by the PD to handle a patient's special health challenge through a referral process.

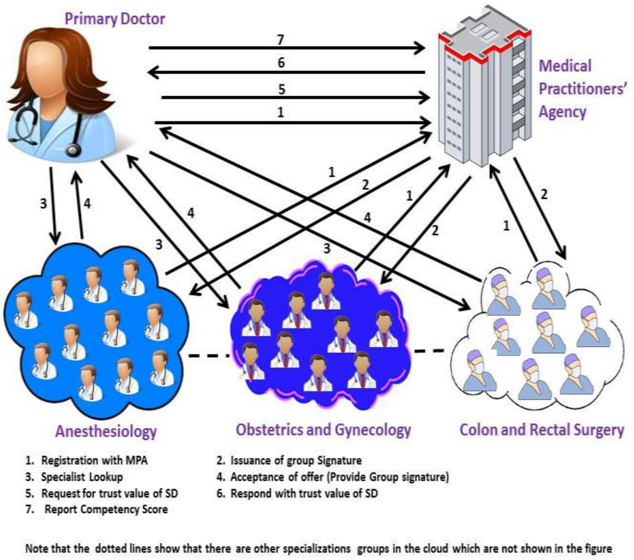

Primary Doctor
Medical Practitioners' Agency
7
6
5
1
3
4
1
2
1
4
2
3
3
2
1
Anesthesiology
Obstetrics and Gynecology
Colon and Rectal Surgery
1. Registration with MPA
3. Specialist Lookup
5. Request for trust value of SD
7. Report Competency Score
2. Issuance of group Signature
4. Acceptance of offer (Provide Group signature)
6. Respond with trust value of SD
Note that the dotted lines show that there are other specializations groups in the cloud which are not shown in the figure

Fig. 1. The System Model for the Referral Scheme

c. **Medical Practitioners' Agency (MPA):** The MPA is responsible for regulating, managing, and monitoring the activities of every physician. It is also responsible for determining the trust rating and competency level of physicians. All qualified physicians must register with the MPA.

3.3 *Adversary Model*

In our system, we considered various types of passive and active attacks that can be launched on the referral framework. Firstly, we consider Sybil attack where an attacker impersonates a registered physician in order to gain access to the patient's sensitive health information. This attack cannot be successful in our system since all communications are done using pseudonyms. Another possible attack is Sniffing attack, whereby an adversary eavesdrops on the wireless network and modifies or alters the data during transmission. This attack is also not feasible in our scheme because all data in transit is encrypted. Also, it is possible for a SD to repudiate the acceptance offer by denying that he did not signify interest in handling the patient's case. Our system is able to prevent non-repudiation because the MPA can link the pseudonym to the real identity of the physician.

Because of the insecure nature of wireless communication networks, attackers may stay on the communication link to capture transmitted messages and modify it. This attack is known as data modification attack. This type of attack cannot be successful because each physician can verify the correctness of the signature of the messages. Tracing attack is not possible in our framework. The use of pseudonym will ensure non-traceability of physician's real identity. Moreover, we also take into consideration collusion attack between the PD and SD, or between SD and malicious users. No entities can collude to obtain the secret key of a physician because different randomly generated numbers are used by the MPA to compute these secret keys. However, we assume the PD is trusted and does not disclose the secret health information of patients to any third party; otherwise this type of attack cannot be prevented.

4. Preliminaries

Here, we describe the background knowledge required for the referral framework.

4.1 *Bilinear Pairings*

Let $\mathbb{G}_1$, and $\mathbb{G}_2$ be two cyclic multiplicative groups of the same large prime order p, with generators g_1 and g_2 respectively, used by the MPA to generate the time-bound secret keys for every physician (SD and PD). ψ is an efficiently computable isomorphism from $\psi(g_2) = g_1$. e is an efficiently computable bilinear map with the following properties:

a. **Bilinearity**: A map $e: G_1 X G_2 \rightarrow G_T$ is bilinear if $e(aP, bQ) = e(P, Q)^{ab}$

b. **Non-degeneracy**: $\forall p \in G_1, e(P, P) \neq 1, p \neq 0$

c. **Computability**: e is efficiently computable. That is, there exists an efficient algorithm to compute $e(P,Q), \forall P,Q, \in G_1$.

4.2 *Computational Assumptions*

Our referral framework is based on the q-Strong Diffie-Hellman (q-SDH) assumption [23][24][25][26] in $(\mathbb{G}_1, \mathbb{G}_2)$, Discrete-Logarithm (DL) assumption in $\mathbb{G}_1$, and the Decision Diffie-Hellman (DDH) assumption in $\mathbb{G}_1$.

q-SDH Problem in $(\mathbb{G}_1, \mathbb{G}_2)$**:** Let g_2 be a generator of $\mathbb{G}_2$ and $g_1 \leftarrow \psi(g_2)$. Given the tuple $(g_1, g_2, {g_2}^{\gamma}, \cdots {g_2}^{\gamma^q})$, output a pair $(g_1^{\overline{\frac{1}{(\gamma+x)}}}, x)$, where $x \in \mathbb{Z}_p^*$.

We say that the $(\hat{t}, \varepsilon)$-q-SDH assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$ if no $\hat{t}$-time algorithm has the probability of at least ε in solving the q-SDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$.

DL Problem in $\mathbb{G}_1$**:** Let g be a generator of $\mathbb{G}_1$ and $a \in \mathbb{Z}_p^*$. Given $(g, g^a) \in {\mathbb{G}_1}^2$, output a.

We say that the $(\hat{t}, \varepsilon)$-DL assumption holds in $\mathbb{G}_1$ if no $\hat{t}$-time algorithm has the probability of at least ε in solving the DL problem in $\mathbb{G}_1$.

DDH Problem in $\mathbb{G}_1$**:** Let g be a generator of $\mathbb{G}_1$ and $a, b, c \in \mathbb{Z}_p^*$. Given $(g, g^a, g^b, g^c) \in {\mathbb{G}_1}^4$, output 'yes' if $c = ab$ and 'no' otherwise.

We say that the $(\hat{t}, \varepsilon)$-DDH assumption holds in $\mathbb{G}_1$ if no $\hat{t}$-time algorithm has the probability of at least ε in solving the DDH problem in $\mathbb{G}_1$

4.3 *0-Encoding and 1-Encoding*

In [27], the authors develop an encoding scheme known as 0-Encoding and 1-Encoding that helps to convert *greater than* predicate to *set* intersection predicate. 0/1-Encoding allows the MPA to include the expiration date into the physician's secret key and the signer to append the expiration date on the signed message. Obviously, the verifier will accept the signature if there exist a common element between the signer's secret key expiration date and signature expiration date. 0/1-Encoding converts a date format in binary to a value in $\mathbb{Z}_p$ as follows:

a. Let $t = t_{[l]}t_{[l-1]} \cdots\cdots t_{[1]}$ be an l-bit encoded in binary string. The 0-encoding of a string, t, is represented by the set:

$$0 - ENC\colon {T_t}^0 = \{t_{[l]}t_{[l-1]} \cdots\cdot t_{[i+1]}1 \parallel t_{[i]} = 0, 1 \leq i \leq l\}$$

The 1-encoding of a string, t, is represented by the set:

1-ENC: ${T_t}^1 = \{t_{[l]}t_{[l-1]} \cdots\cdot t_{[i]}1 \parallel t_{[i]} = 1, 1 \leq i \leq l\}$

b. From the theorem in [27], if $x \geq y$ there exists a common element in ${T_x}^1$ and ${T_y}^0$. To ensure that the sets in ${T_t}^0$ and ${T_t}^1$ start with 1, we redefine the sets as the decimal number sets represented as:

$$\overline{{T_t}^0} = \{1 \cdot 10^{l-i+1} + t_{[l]} \cdot 10^{l-i} + \ldots\ldots + t_{[i+1]} \cdot 10^1 + 1 \parallel t_{[i]} = 0, 1 \leq i \leq l\},$$ and

$$\overline{{T_t}^1} = \{1 \cdot 10^{l-i+1} + t_{[l]} \cdot 10^{l-i} + \ldots\ldots + t_{[i+1]} \cdot 10^1 + t_{[i]} \parallel t_{[i]} = 1, 1 \leq i \leq l\}$$

3. To make sure that the number of elements in the two sets is equal, we apply padding with dummy elements to obtain the following two functions: $0 - ENC \leftarrow \{t_l, t_{[l-1]}, \ldots\ldots t_1\}$, where

$$t_{[i]} = \begin{cases} z, & z \in \overline{{T_t}^0}, \quad \lfloor log_{10} z \rfloor - 1 = i \\ 2\,.\,10^1 & otherwise \end{cases}$$

$1 - ENC \leftarrow \{t_l, t_{[l-1]}, \ldots\ldots t_1\}$, where

$$t_{[i]} = \begin{cases} z, & z \in \overline{{T_t}^1}, \quad \lfloor log_{10} z \rfloor - 1 = i \\ 3\,.\,10^1 & otherwise \end{cases}$$

Example Assuming two dates in the format '"YYMM'" as:
January, 2017 ('"1701'") and May, 2017 ('1705'").
Convert these dates to binary strings: x = 11010101001 ('"1705'"), y= 11010100101 ('"1701'").
Then,

$${T_x}^1 = \begin{Bmatrix} 11,1101,110101,11010101, \\ 11010101001 \end{Bmatrix}$$

${T_y}^0 = \{111,11011,1101011,11010101,$

$1101010011,11010100101\}$

$\overline{T_x}^1 = \{111,11101,1110101,111010101,$

$111010101001\}$

$\overline{T_y}^0 = \{1111,111011,11101011,111010101,$

$11101010011,111010100101\}$

After padding with dummy elements, we have $0 - ENC(y) \rightarrow \{20,200,1111,20000,111011,$

$2000000,11101011,\mathbf{111010101},2000000000,$

$11101010011,111010100101\}$

$1 - ENC(x) \rightarrow \{30,111,3000,11101,300000,$

$1110101,30000000,\mathbf{111010101},3000000000,$

$30000000000,111010101001\}$

Since $x > y$, 0-ENC(y) and 1-ENC(x) have a common element **111010101**. For detailed proof, the reader can refer to the theorem in [27].

5. Anonymous Referral Framework

Our referral scheme consists of three components: Key management architecture, time-bound group signature for classification of physician, and request and selection of SD. Firstly, all the physicians (PD and SD) register with the MPA which computes pseudo-identity for each physician. This pseudo-ID will be used for communication so that the true identities are concealed so as to ensure physicians privacy preservation. The MPA also performs grouping of physician based on their specialization. It generates the master secret key, public key, and secret key for every physician in each group. Then, it sends the group public and secret key to every physician and stores the group master secret key to ensure non-repudiation by physicians.

Every physician sending a message must sign it using their time-bound group signatures. This will enable the receiver to determine the group or specialization that a physician belongs to. On receiving a message, the receiver performs two levels of verification: verification check and revocation check. The verification check helps the verifier to determine the validity of the signature while the revocation check helps to know whether the sender has been revoked or not by the MPA.

As discussed earlier, a PD often need to refer a patient to a SD who can proffer better diagnosis to the patient's health challenges. To initiate a referral, the PD requests for a competent SD in the cloud who can handle the patient's case. The interested SDs respond with their acceptance messages and append their group signatures. The PD verifies the authenticity of the group signatures and then contacts the MPA for the trust values of the SDs. The MPA computes the trust values of the SDs and reports it to the PD. Consequently, the PD selects the best SD based on the trust values received from the MPA. After the selected SD has completed the diagnosis, the PD performs the rating of the SD and sends the competency score to the MPA. Nevertheless, if an SD is not selected to make diagnosis for a period of time, their trust level drops. This decay in trust value is achieved by our proposed trust model.

Our referral framework components are described as follows:

5.1 *Key Management Architecture*

The key management scheme for our referral scheme is described as follows:

a. During the registration, a physician, Doc_k, provides the identity and professional credentials, ID_k, to the MPA. The MPA randomly selects $\gamma_i \overset{R}{\leftarrow} \mathbb{Z}_p^*$ for each specialisation group and computes the pseudonym of Doc_k as: ${\digamma_i}^k \leftarrow ID_k \oplus H(\gamma_i) \in \mathbb{Z}_p^*$, where i is the specialisation group index, k is the physician index, and $H\colon \{0,1\}^* \leftarrow \mathbb{G}$ is a one-way collision-resistant hash function.

b. The MPA generates for each specialization group, i, a random $x_i', x_i'' \in \mathbb{Z}_p^*$ and then selects $\zeta_0 \overset{R}{\leftarrow} \in \mathbb{Z}_p^*$ and $\zeta_1,\ \zeta_2 \in \mathbb{G}_2$ such that $\zeta_1 = {\zeta_0}^{x_i'}$, $\zeta_2 = {\zeta_0}^{x_i''}$, then set $d_i = g_2^{{\digamma_i}^k}$, where $\digamma_i^k$ is the pseudo-identity of Doc_k . The group public key of Doc_k of specialisation group i is $gpk_i{}^k = (g_1, g_2, d_i)|i \in (1,2,\cdots n)$, where n is the total number of specialisation groups. The time-bound group master secret key, $gmsk_i{}^k$, of Doc_k of specialisation group i, is $(x_i{}', x_i{}'')$.

c. The MPA randomly selects $t_k{}' \overset{R}{\leftarrow} \mathbb{Z}_p^*$, and also obtains generators $(\hat{u}, \hat{v})$ in G_2 from H, where $(\hat{u}, \hat{v}) \leftarrow H(gpk_i{}^k, M, t_k{}') \in G_2{}^2$, then images in G_1 as $u \leftarrow \psi(\hat{u})$ and $v \leftarrow \psi(\hat{v})$ such that $u^{x_i'} = v^{x_i''} = \omega \in G_1$.

d. The MPA decides the expiration date, τ_i^k, for a physician's time-bound group secret key, $gsk_i{}^k$. She encodes the expiration date using the l-Encoding:
$\tau_{ij}{}^k, j \in [1, l] \leftarrow 1 - Enc(\tau_i{}^k)$ Where l is the length of the date format used and τ_{ij}^k is the encoded expiration date. 0/1-encoding converts a date format in binary to a value in $\mathbb{Z}_p^*$. Then, the MPA sets:

$$A_i{}^k \leftarrow g_1^{\frac{1}{\tau_{ij}^k \cdot \digamma_i{}^k + \gamma_i}}$$

The physician's time-bound secret key is $gsk_i{}^k = A_i{}^k$

e. The MPA securely sends $\{gsk_i{}^k, gpk_i{}^k, \digamma_i{}^k\}$ to Doc_k and stores $\{(ID_k, A_i{}^k), \tau_i{}^k, \gamma_i, gmsk_i{}^k\}$. Then it publishes the public parameter: param = $\{G_1, G_2, g_1, g_2, \psi, e, u, v, w\}$

5.2 *Time-bound Group Signature*

Time-bound group signature phase involves two stages: generation and verification.

5.2.1 Generation

Any physician sending a message must sign it using their own time-bound group signature parameters. We modified the group signature proposed in [3] and [15] to evolve a time-bound group signature described as follows:

a. Doc_k selects a random exponent $\alpha, \beta, \xi \in \mathbb{Z}_p{}^*$ and computes pseudonyms as:

$T_1 \leftarrow u^\alpha$, $T_2 \leftarrow v^\beta$, $T_3 \leftarrow A_i{}^k \omega^{\alpha+\beta}$, $T_4 \leftarrow \omega^{\alpha+\beta}$

b. Doc_k sets $\delta_1 \leftarrow \alpha\xi, \delta_2 \leftarrow \beta\xi$ and randomly selects $b_\alpha, b_\beta, b_\xi, b_{\delta_1}$,and $b_{\delta_2} \in \mathbb{Z}_p^*$

c. Doc_k computes helper values $R_1, R_2, R_3, R_4, R_5, R_6$, and R_7 as:

$R_1 \leftarrow u^{b_\alpha}$

$R_2 \leftarrow v^{b_\beta}$

$R_3 \leftarrow e(T_3, g_2)^{b_\xi}. e(\omega, d_i)^{-t_k'(b_\alpha + b_\xi)}$

$. e(\omega, g_2)^{-b_{\delta_1} - b_{\delta_2}}$

$R_4 \leftarrow \omega^{b_\alpha + b_\beta}$

$R_5 \leftarrow T_1^{b_\xi}. u^{-b_{\delta_1}}$

$R_6 \leftarrow T_2^{b_\xi}. v^{-b_{\delta_2}}$

$R_7 \leftarrow T_4^{b_\xi}. \omega^{-b_{\delta_1} - b_{\delta_2}}$

d. Doc_k computes a challenge $c \in \mathbb{Z}_p^*$ as:
$c \leftarrow H(gpk_i, M, t_k{}', T_1, T_2, T_3, T_4, R_1, R_2,$

$R_3, R_4, R_5, R_6, R_7)$

e. Doc_k computes response values as : $r_\alpha = b_\alpha - c\alpha, r_\beta = b_\beta - c\beta, r_\xi = b_\xi - c\xi, r_{\delta_1} = b_{\delta_1} - c\delta_1, r_{\delta_2} = b_{\delta_2} - c\delta_2$

f. Doc_k generates the signature for its group as:
$\sigma_i{}^k \leftarrow (t_k{}', T_1, T_2, T_3, T_4, c, r_\alpha, r_\beta, r_\xi, r_{\delta_1}, r_{\delta_2})$

g. Doc_k sends the message, M, with the signature, $\sigma_i{}^k$, that could be verified.

5.2.2 Verification

Every physician and the MPA can verify a time-bound group signature by using the sender's public key. The following operation is performed:

Verification Check: The time validity of the signature is checked to ascertain the signature is valid. The time measured by the verifier must be equal to or newer than the current date. If $t_k{}^m \geq t_k{}'$, the algorithm runs, otherwise it is aborted, where $t_k{}^m$ is the date measured by the verifier and $t_k{}'$ is the current date.

The verifier computes $(\hat{u},\hat{v}) \leftarrow H_0(gpk_i{}^k, M, t_k')$ and their images u and v in $G_1: u \leftarrow \psi(\hat{u}), v \leftarrow \psi(\hat{v})$, and recomputes $\dot{R}_1, \dot{R}_2, \dot{R}_3, \dot{R}_4, \dot{R}_5, \dot{R}_6$, and $\dot{R}_7$ as:

$$\dot{R}_1 \leftarrow T_1{}^c u^{r_\alpha}$$

$$\dot{R}_2 \leftarrow T_2{}^c v^{r_\beta}$$

$$\dot{R}_3 \leftarrow e(T_3, g_2)^{r_\xi}. e(\omega, d_i)^{-t_k'(r_\alpha + r_\xi)}$$

$$. e(\omega, g_2)^{-r_{\delta_1} - r_{\delta_2}}. e\left(T_4, d_i{}^{t_k'}\right)^c . e(g_1, g_2)^{-c}$$

$$\dot{R}_4 \leftarrow T_4{}^c \omega^{r_\alpha + r_\beta}$$

$$\dot{R}_5 \leftarrow T_1{}^{r_\xi} u^{-r_{\delta_1}}$$

$$\dot{R}_6 \leftarrow T_2{}^{r_\xi} v^{-r_{\delta_2}}$$

$$\dot{R}_7 \leftarrow T_4{}^{r_\xi} \omega^{-r_{\delta_1} - r_{\delta_2}}$$

The verifier checks that the challenge c is correct:

$$c \overset{?}{=} H(gpk_i{}^k, M, t_k', T_1, T_2, T_3, T_4, \dot{R}_1, \dot{R}_2, \dot{R}_3, \dot{R}_4, \dot{R}_5, \dot{R}_6, \dot{R}_7) \dots\dots\dots\dots\dots\dots (1)$$

The signature is valid if equation (1) holds. If it does, the message is accepted, else it is rejected.

Revocation Check: The MPA creates the revocation list, RL. For a given $A_i{}^k \in RL$, the verifier checks if $A_i{}^k$ is encoded in (T_1, T_2, T_3) by checking:

$$e(T_3/A_i{}^k, \zeta_0) \overset{?}{=} e(T_1, \zeta_1). e(T_2, \zeta_2) \cdots\cdots\cdots (2)$$

If equation (2) holds, the signed message is discarded because the k^{th} physician with $A_i{}^k$ has been revoked by the MPA.

5.3 Request and Selection of SD

Our system model in Fig. 1 describes the selection process. The cloud server consists of SDs grouped using their specialization such as anesthesiology, obstetrics and gynecology, colon and rectal surgery, etc. Firstly, the PD and SD register with the MPA by providing their personal details and professional credentials. The MPA generates the pseudo-identity and the group key for each physician. During referral, the PD searches in the cloud for qualified and capable specialists for a patient. The interested SDs respond with their group signatures and pseudo-identities. The PD contacts the MPA for the trust values of the interested SDs and the MPA responds with their computed trust values. The trust value determines the competency or level of expertise of an SD. The PD selects the best SD based on the trust values received from the MPA. After the SD has finished the consultation or treatment, PD sends a competency score or rating back to the MPA stating the pass rate of the selected SD. This competency score is later used by the MPA to update the trust value of the SD.

A simplified selection procedure is shown in Fig. 2, where only a specialty group is considered. The PD performs a lookup in the cloud server for a competent and capable SD. The interested SD responds with her group signature and pseudo-identity. Moreover, the PD contacts the MPA for the trust value of the SD, while the MPA responds with the requested trust value after a successful verification of the group signatures of the PD and SD, and a check against Sybil attack. The selection of suitable and competent SD involves request initiation by the PD, determination of trust value of the SD, and recommendation of SD by the PD as follows:

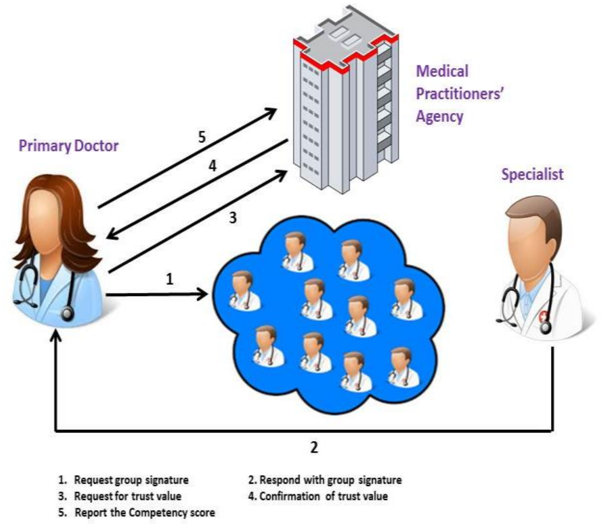

Medical
Practitioners'
Agency
Primary Doctor
Specialist
5
4
3
1
2
1. Request group signature
2. Respond with group signature
3. Request for trust value
4. Confirmation of trust value
5. Report the Competency score

Fig. 2. Simplified System Model for the Referral Scheme

5.3.1 *Request Initiation*

When the need for referral arises, the PD searches for a competent SD in the cloud based on their trust values. One or more interested SDs respond to the request. The PD contacts the MPA for the trust values of the interested SDs, and then selects the best SD using the trust values as the competency metrics. The request for SD involves the following steps:

Step 1: Because the secret key ${gsk_i}^k$ is time-bound, the PD verifies its validity by checking:

$$e({A_i}^k, {d_i}^{{\tau_{ij}}^k}.g_2^{\gamma_i}) \overset{?}{=} e(g_1, g_2)$$

If it has expires, she needs to contact the MPA for renewal. After a successful validation of the secret key, the PD proceeds to step 2.

Step 2: The PD, k, computes a request for specialist packet, m_R, as: $m_R := (\digamma_{k(PD)} \parallel {M_R}^k \parallel {\sigma_i}_{(PD)}^k)$, where ${M_R}^k$ is the request for specialist message, ${\sigma_i}_{(PD)}^k$ is the time-bound group signature of PD, k, on ${M_R}^k$ for group i, and $\digamma_{k(PD)}$ is the pseudo-identity of PD. The request packet, m_R, is encrypted as : $C_R \leftarrow Enc(m_R)$. The PD sends this encrypted request message to the cloud server consisting of several SDs.

Step 3: The interested SD decrypts the received C_R and verifies the time-bound group signature, ${\sigma_i}_{(PD)}^k$, by checking if equations (1) and (2) hold. If they are true, she decides whether to accept or reject the offer.

Step 4: After the SD has accepted the referral request, then she computes the acceptance packet, m_A as: $m_A := (\digamma_{k(SD)} \parallel {M_A}^k \parallel {\sigma_i}_{(SD)}^k)$, where ${M_A}^k$ is the acceptance message, ${\sigma_i}_{(SD)}^k$ is the time-bound group signature of SD, k, for group i, and $\digamma_{k(SD)}$ is the pseudo-identity of k. The acceptance packet is encrypted as: $C_A \leftarrow Enc(m_A)$.

The SD sends the encrypted acceptance packet to the PD. Other interested SDs do the same by computing C_A and send it to the PD.

Step 5: Upon receiving C_A from all the interested SDs, the PD decrypts it and then verifies the time-bound group signature, ${\sigma_i}_{(SD)}^k$, by checking if equations (1) and (2) hold. If they do, she accepts the acceptance message, ${M_A}^k$, else she rejects it. If verification succeeds, the PD proceeds to step 6, else the process is halted.

Step 6: The PD computes the request for trust value packet for SD, k as: $m_{RTV} := (\digamma_{k(SD)} \parallel M_{RTV}^k \parallel \digamma_{k(PD)} \parallel {\sigma_i}_{(PD)}^k)$, where M_{RTV}^k is the request for trust value message, ${\sigma_i}_{(PD)}^k$ is the time-bound group signature of PD, k, for group i, $\digamma_{k(PD)}$ is the pseudo-identity of PD, and $\digamma_{k(SD)}$ is the pseudo-identity of SD. The request for trust value message is encrypted as: $C_{RTV} \leftarrow Enc(m_{RTV})$. The PD repeats the same for all SDs and then sends the encrypted request for trust value messages to the MPA.

Step 7: The MPA decrypts the received C_{RTV} and verifies the time-bound group signature, ${\sigma_i}_{(PD)}^k$, by checking if equations (1) and (2) are true. If so, she accepts the message, otherwise she discards it.

Step 8: The MPA verifies the pseudo-identity, $\digamma_{k(PD)}$ and $\digamma_{k(SD)}$ by checking:

$$ID_{k_{(SD)}} \overset{?}{=} \digamma_{k(SD)} \oplus H(\gamma_i)$$

$$ID_{k_{(PD)}} \overset{?}{=} \digamma_{k(PD)} \oplus H(\gamma_i)$$

The MPA repeats the same procedure for all other SDs.

Step 9: The MPA computes the trust values of the SDs, as shown in the next section, if equations (3) and (4) hold. Otherwise, Sybil attack is detected and she discards the request for trust value packet.

Step 10: The MPA sends the trust values of the SDs back to the PD, who then selects the SD with highest trust value as the most competent one to handle the patient's diagnosis.

5.3.2 *Rating of SD*

After the consultation, the PD performs the following:

Step 1: The PD computes the competency packet of the SD as: $c := \Big(\digamma_{k(SD)} \parallel C \parallel t_k'' \parallel \digamma_{k(PD)} \parallel$

$\sigma^{k}_{i(PD)}\big)$, where C is the competency score or rating, $\digamma_{k(SD)}$ is the pseudo-identity of the SD, $\digamma_{k(PD)}$ is the pseudo-identity of the PD, $\sigma^{k}_{i(PD)}$ is the time-bound group signature of the PD, and t''_k is the current date.

Step 2: The PD encrypts the competency score as: $C_C \leftarrow Enc(C)$. She then sends the message, C_C, to the MPA.

Step 3: The MPA decrypts the message, C_C, and checks whether equations (1), (2), (3), and (4) are true. If valid, she stores (C, t''_k) and uses it to build up the trust level for the SD with pseudonym, $\digamma_k(SD)$ as shown in the next section.

5.3.3 *Determination of decay-trust value*

We developed a trust model that the MPA uses to compute the trust value of a specialist. The trust value is determined as follows:

At the point of registration with the MPA, an initial decay-trust value, η_0, is assigned to every specialist. As a specialist is being selected to make diagnosis of a patient's health issues, her trust value builds up. The MPA computes the trust value of a specialist, SD_k for a given consultation as:

$$\eta_{SD_k} \quad = \frac{\alpha_{PD\rightarrow SD}}{\alpha_{PD\rightarrow SD} + \beta_{PD\rightarrow SD}}$$

where $\alpha_{PD\rightarrow SD}$ is the number of success recorded by SD_k as reported by PD_k and $\beta_{PD\rightarrow SD}$ is the number of failure recorded by SD_k as reported by PD_k.

The average trust value of SD_k over a period of time, t, is given as:

$$\eta_t = \frac{\Sigma \eta_{SD_k}}{N},$$

where N is the total number of PD who selected the SD_k within the period t. Therefore, the total trust value of SD_k is:

$$\Upsilon_t = \eta_0 + \eta_t$$

where η_0 is the initial trust assigned to a specialist at the time of registration with the MPA.

However, in case the specialist, SD_k, is not selected for a period of time,t, using the decay trust model, her trust value decays as:

$$\Upsilon_t = \Upsilon_{t-1} - [1 - e^{-(t+C)/t^2}],\ 1 \leq C \leq 100$$

where C is the competency score or rating of SD_k by the PD.

6. Data Access Control for Referral of Patient

The overview of the data access control for the referral framework is shown in Fig. 3. It consists of four entities: Patient, PD, SD, PHR, and Medical Emergency Services (MES). The Patient's body comprises of several wearable or implantable wireless body sensor (WBS) that continuously monitor the health status and transmit - through a WBAN gateway- the aggregated perturbed data to a PHR cloud server. That is, the WBS generates a set of perturb for every instance of measurement.

The patient has full control over her PHR and can only be accessed by authorised users. The patient generates a token for authentication to

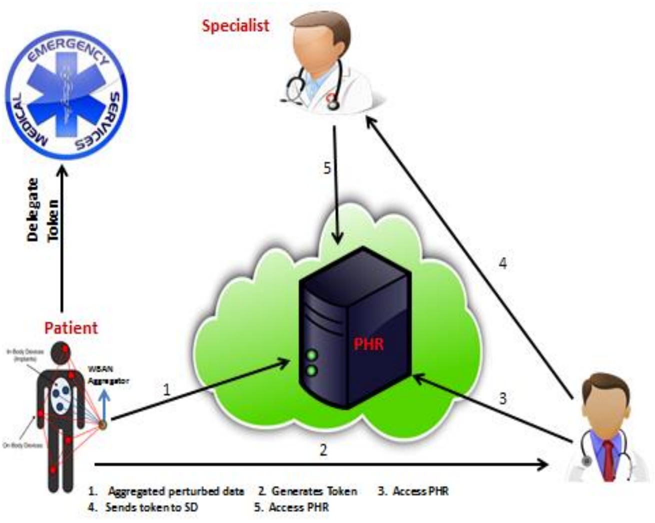

EMERGENCY MEDICAL SERVICES
Specialist
Delegate Token
5
4
PHR
Patient
In-Body Devices (Implants)
WBAN Aggregator
On-Body Devices
1
3
2
1. Aggregated perturbed data 2. Generates Token 3. Access PHR
4. Sends token to SD 5. Access PHR

Fig. 3 Data Access Control for Referral framework

the PHR, asymmetrically encrypts it, and sends it to the PD and PS. The PD uses this token for authentication to the PHR. In an emergency situation, the patient can delegate a medical emergency service (MES) to generate the token for authentication to the PHR cloud server. During the referral, the PD asymmetrically encrypts the token, and sends it to the selected specialist. The specialist presents this token to the PHR cloud server for authentication. The cloud server and SD authenticate each other. Consequently, if the authentication succeeds, the SD can access the PHR by reconstructing the original data from the perturbed data.

7. Anonymous Authentication Protocol for Referral of Patient

For PHR access, the SD must be authenticated by the PHR server (PS) while the SD must be certain that the PS is a legitimate cloud server. For authentication, the PD asymmetrically encrypts the perturbation parameter and sends it to the SD. The authentication and key agreement procedure between the SD and PS is shown in Fig. 4, and described as follow:

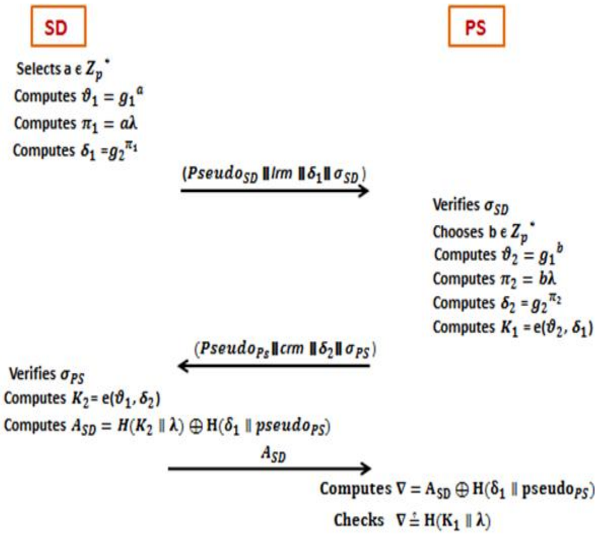

SD
PS
Selects a ϵ Z_p^*
Computes $\vartheta_1 = g_1^a$
Computes $\pi_1 = a\lambda$
Computes $\delta_1 = g_2^{\pi_1}$
$(Pseudo_{SD} \| lrm \| \delta_1 \| \sigma_{SD})$
Verifies σ_{SD}
Chooses b ϵ Z_p^*
Computes $\vartheta_2 = g_1^b$
Computes $\pi_2 = b\lambda$
Computes $\delta_2 = g_2^{\pi_2}$
Computes $K_1 = e(\vartheta_2, \delta_1)$
$(Pseudo_{PS} \| crm \| \delta_2 \| \sigma_{PS})$
Verifies σ_{PS}
Computes $K_2 = e(\vartheta_1, \delta_2)$
Computes $A_{SD} = H(K_2 \| \lambda) \oplus H(\delta_1 \| pseudo_{PS})$
A_{SD}
Computes $\nabla = A_{SD} \oplus H(\delta_1 \| pseudo_{PS})$
Checks $\nabla \overset{?}{=} H(K_1 \| \lambda)$

Fig. 4 Anonymous Authentication Protocol for Referral of Patient

a. A patient generates a master secret key, msk, by randomly selecting $\lambda \in \mathbb{Z}_p^*$ and sends it to the PD and PS.

b. SD randomly selects $a \in \mathbb{Z}_p^*$ and computes $\vartheta_1 = g_1^a$, $\pi_1 = a\lambda$ and $\delta_1 = g_2^{\pi_1}$. Then, SD securely sends $(pseudo_{SD} \| lrm \| \delta_1 \| \sigma_{SD})$ to PS, where lrm is the login request message, $pseudo_{SD}$ is the pseudonym of

c. SD, and σ_{SD} is the time-bound group signature of SD.

d. Upon receiving $(pseudo_{SD} \| lrm \| \delta_1 \| \sigma_{SD})$, PS verifies σ_{SD} using the time-bound group signature verification scheme discussed earlier. If σ_{SD} is valid, PS selects a random $b \in \mathbb{Z}_p^*$ and computes, $\vartheta_2 = g_1^b$ $\pi_2 = b\lambda$, $\delta_2 = g_2^{\pi_2}$ and $K_1 = e(\vartheta_2, \delta_1)$. Then, PS securely sends $(pseudo_{PS} \| crm \| \delta_2 \| \sigma_{PS})$ to SD, where σ_{PS} is the signature of PS, crm the connection response message, $pseudo_{PS}$ is the pseudonym of PS and K_1 the session key. Otherwise, PS rejects the connection.

e. On receiving $(pseudo_{PS} \| crm \| \delta_2 \| \sigma_{PS})$, SD verifies σ_{PS}. If valid, SD computes $K_2 = e(\vartheta_1, \delta_2)$ as the session key and accepts the connection. Otherwise, SD rejects the connection. Then, SD computes $A_{SD} = H(K_2 \| \lambda) \oplus \mathrm{H}(\delta_1 \| pseudo_{PS})$ and securely sends it to PS.

f. Upon receiving A_{SD}, PS computes $\nabla = A_{SD} \oplus \mathrm{H}(\delta_1 \| pseudo_{PS})$, and checks if $\nabla \overset{?}{=} H(K_1 \| \lambda)$. If it holds, PS assumes that the SD has completed the authentication process and has successfully computed the session key.

g. It is easy to visualize that $K_1 = K_2$. After successful authentication, all communications between the SD and PS are done using the symmetric session key $K = K_1 = K_2$.

h. After five unsuccessful authentication attempts, the connection is closed for time, t, so as to prevent flooding the SD or PS with connection requests.

i. Then, the SD can proceed with reconstruction of the perturbed PHR using the perturbation parameter received from the PD.

8. Security Analysis

a. **Sybil attack resistance:** In our scheme, impersonation attack on the PD and SD is not possible. Suppose an adversary, $\mathcal{A}$ wants to impersonate a physician (PD or SD), Doc_k, she cannot obtain the secret key, ${A_i}^k$. Moreover, the group master secret key,(x', x''), and $(\gamma_i, {t_i}^k)$ are known to and kept by the MPA, hence it is impossible for $\mathcal{A}$ to produce a valid signature of PD or SD. Thus, Sybil attack is not possible in the scheme, except in a situation when ${gsk_i}^k$ is compromised. However, since ${gsk_i}^k$ is time-bound, even if it is compromised the adversary can only use it for a short period of time before expires.

b. **Resistant to Collusion Attack:** It is impossible for a SD to collude with a PD to report a malicious high competency score for the SD. In our framework authentication is done through pseudonyms, therefore no SD has the knowledge of who the PD is. Apart from this, our decay trust model takes care of malicious rating if the SD is not selected over certain period of time by increasing the rate of decay of his trust value. Moreover, it is quite impossible for an adversary, $\mathcal{A}$, to collude with an SD or a PD to obtain the secret key, ${A_i}^k$, of another physician. To obtain ${A_i}^k$, $\mathcal{A}$ must know the group master secret key,(x', x''), or $(\gamma_i, {t_i}^k)$, which is not possible because it was generated and possessed by the MPA. Hence, collusion attack is curtailed.

c. **Strong User Anonymity:** To ensure anonymity of physicians during the referral, authentication is done using pseudo-identities. The real identity of a physician, Doc_k is derived as follows;

$$ID_k \overset{?}{=} \digamma_k \oplus H(\gamma_i)$$

$$ID_k \overset{?}{=} \digamma_k \oplus H(\gamma_i) \oplus H(\gamma_i)$$
$$= ID_k$$

However, since γ_i is kept by the MPA, no entity can determine the real identity of any physician except the MPA. Hence, our scheme achieves strong user anonymity.

d. **Traceability:** Repudiation involves an entity denying being responsible for an action that was actually carried out by it. In our scheme, it is impossible for a PD or SD to repudiate signing a message. The MPA is able to open the signer of a message by re-computing the time-bound secret key of the signer using the group master secret key, ${gmsk_i}^k$, as follows:

$$A_i^k \overset{?}{\leftarrow} \frac{T_3}{{T_1}^{x_i'} . {T_2}^{x_i''}}$$

$$A_i^k \overset{?}{\leftarrow} \frac{{A_i}^k \omega^{\alpha+\beta}}{(u^\alpha)^{x_i'} . (v^\beta)^{x_i''}}$$

$$A_i^k \overset{?}{\leftarrow} \frac{{A_i}^k \omega^{\alpha+\beta}}{(u^{x_i'})^\alpha . (v^{x_i''})^\beta}$$

$$A_i^k \overset{?}{\leftarrow} \frac{{A_i}^k \omega^{\alpha+\beta}}{\omega^\alpha . \omega^\beta}$$

$$A_i^k \overset{?}{\leftarrow} \frac{{A_i}^k \omega^{\alpha+\beta}}{\omega^{\alpha+\beta}}$$

$$A_i^k \leftarrow {A_i}^k$$

Because the MPA stored $(ID_k, {A_i}^k)$ pair during the registration of the physician, it is able to determine the real identity of the signer. Nevertheless, no one else can perform this operation because (x_i', x_i'') is only known to and possess by the MPA.

e. **Provision of Countermeasure against Privilege Escalation**: We implemented an efficient revocation mechanism to thwart privilege escalation by revoked physicians. The expiration date has been encoded in the secret key, ${A_i}^k$, as ${\tau_{ij}}^k$. The revocation of a physician is in two forms: registration expires, and physician misbehaves and his license is revoked. If the registration expires, the secret key will not be valid again and the revoked physician's secret key is added to the revocation list, RL. On the other hand, if the physician's license is revoked due to misconduct, the MPA immediately blacklisted the secret key of the SD and updates its RL. To authenticate a physician, the verifier first check if the ${A_i}^k$ of the physician is encoded in (T_1, T_2, T_3) by checking the validity of

$$e(T_3/{A_i}^k, \zeta_0) \overset{?}{=} e(T_1, \zeta_1). e(T_2, \zeta_2)$$

If valid, the physician has been revoked by the MPA and the connection is closed. Thus, privilege escalation by physicians is thwarted.

9. Performance Evaluation

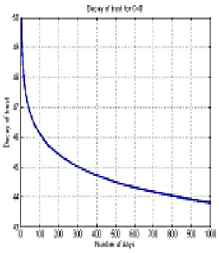
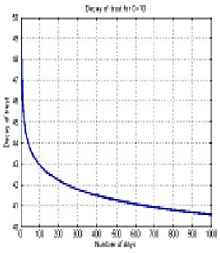
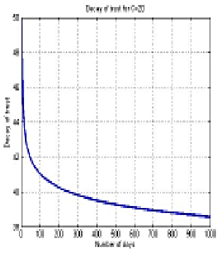
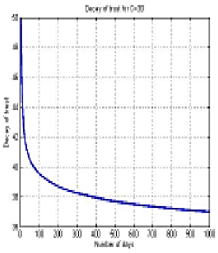
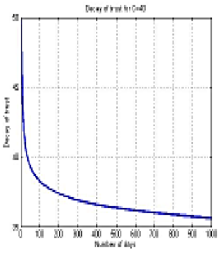
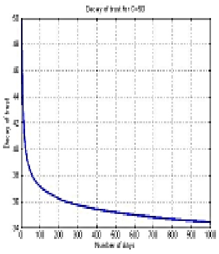
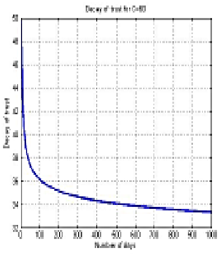
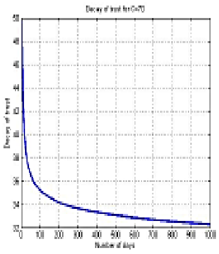
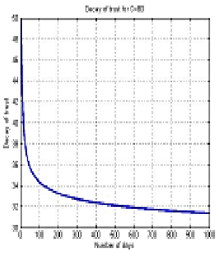
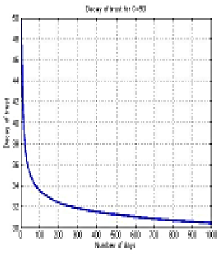
The proposed framework presents an efficient way of determining the trust value and selection of specialists. The decay of trust we employed is more efficient compared to the trust model proposed by [9] because our proposed trust model not only computes trust values but also introduces decay of trust value of an SD who is not engaged or selected over a certain period of time. We evaluated the performance of the proposed trust model by simulating the decay of trust values over a period of 1000 days for 10 different specialists with different competency rating, C, but the same initial trust value as shown in Table 1 . The results show that the competency rating influences the rate of decay of trust value. That is, the higher the earlier competency rating, the higher the rate of decay. For example, after 500 days, the decay of trust for the 10 different competency score of 0, 10, 20, 30, 40, 50, 60, 70, 80, and 90 are 44.5, 41.27, 39.28, 37.7, 36.35, 35.06, 34.07, 33.06, 32.12, and 31.23 respectively. It could be observed that the higher the earlier competency score, the higher the decay of trust. Also, the decay of trust plummets for the first 100 days that the SD was not engaged. These take care of any form of mistake or malicious high rating from PD.

10. Conclusion

The proposed secure and privacy-preserving framework provides an efficient patient's referral system through an effective and dynamic specialist selection procedure. The security analysis shows that the framework is secure against various forms of attacks like collusion attack, sybil attack, tracing attack, and provides high level of privacy. Our novel trust model employs trust decay which helps to ensure efficient specialist selection and rating.

Therefore, the framework is very efficient in selecting and rating competent specialists during referral in eHealth system.

Table 1. Decay of Trust value for Different Values of rating

C = 0	C = 10	C = 20	C = 30	C = 40
				
C = 50	**C = 60**	**C = 70**	**C = 80**	**C = 90**
				

References

[1] L. Guo, C. Zhang, J. Sun and Y. Fang, "PAAS: A privacy-preserving attribute-based authentication system for eHealth networks" *32nd IEEE international conference on distributed computing systems*, pp. 224-232, 2012.

[2] Y. Lee, S. Han, B. Chung, and D. Gyu Lee, "Anonymous authentication system using group signature", *IEEE proceedings of international conference on complex, intelligent, and software*, pp. 1235-1239, 2009.

[3] L. Malina, J Hajny, and Z. Martinasek. "Efficient group signatures with verifier-local revocation employing a natural expiration", *In proceedings of the 10th international conference on security and cryptography (SECRYPT-2013)*, pp.555-560, 2013.

[4] S. Mohanty, B. Majhi, and V. Iyern, "A strong designated verifiable group signature", *IEEE Journal*, pp. 518-523.

[5] Z. Xia, L. Zhang and D. Liu, "Attribute-based access control scheme with efficient revocation in cloud computing", *Journal in cloud computing and data mining, China Communications*, pp. 92-99, 2016.

[6] M. Chase, and S. Chow, "Improving privacy and security in multi-authority attribute-based encryption", *ACM* , pp. 121-129, 2009.

[7] L. Yeh, P. Chiang, Y. Tsai and J. Huang, "Cloud-based fine-grained health information access control framework for lightwieght IoT devices with dynamic auditing and attribute revocation", *IEEE transactions on cloud computing*, 2015.

[8] D. Ramesh and R. Priya, "Multi-authority scheme based CP-ABE with attribute revocation for cloud data storage", *IEEE*, 2016.

[9] A. Shabut, K. Dahal and I. Awan, "Enhancing dynamic recommender selection using multiple rules for trust and reputation models in MANETs", *IEEE 25th international conference on tools with artificial intelligence*, pp. 654-660, 2013.

[10] F. Femilshini, V. Ganeshkarthikeyan and S. Janani, "Privacy preserving revocation update protocol for group signature in cloud", IEEE international conference on Enigineering and Technology (ICETECH)‘", 2015.

[11] D. Yao and R. tamassia, "Anonymous role-based delegation with group signaures".

[12] C. Fan, J. Hsu, C. Wu, Y. Tseng, and W. Chen, "Anonymous credential scheme supporting active revocation", *Ninth asia joint conference on information security*, pp. 127-132, 2014.

[13] J. Li, X. Tan, X. Chen, D.S. Wong, and F. Xhafa, "OPoR: Enabling proof of retrievability in cloud computing with resource-constrained devices", *IEEE transaction on cloud computing*, vol. 3 no. 2, pp. 195-205, 2015.

[14] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing", *Advances in cryptology-CRYPTO 2001*, pp. 213-229, 2001.

[15] D. Boneh and H. Shacham, "Group Signatures with Verifier-Local Verification".

[16] W. Almanscori, A. Murshid, K. Xylogiannopoulos, R. Alhajj, and J. Rokne, "Electronic medical referral system:Decision support and recommendation approach".

[17] W. Dunning, A.Lewis, S.Malhotra, T.Nicholson, A. Wiygal, B. Tawney, and R. Bennet, "Design and development of a medical specialist referral system for the indigent population of Richmond". *In the proceedings of the 2005 systems and information engineering design symposium, Ellen .J. Bass, ed*, pp. 205-214, 2005.

[18] I. Reinhart, K. Dawoud, O. Shafiq, R. Alhajj, J. Rokne, S. Edworthy, "Electronic medical referral system: A forum-based approach". *In IEEE 13th international conference on e-health networking, applications, and services*, pp. 185-188, 2011.

[19] $Connect.qualitycare.org/oncology/$. Accessed 24th July, 2016.

[20]$www.ncbi.nlm.nih.gov/pmc/articules/PMC3243286/$. Latest Access Time for the Website is 1st October, 2016.

[21]$www.kfmc.med.sa/EN/E-Referral/Documents/Referral$. Latest Access Time for the Website is 26th July, 2016.

[22] 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", *Institute for computer sciences, social informatics and telecommunications engineering*, pp. 89-106, 2010.

[23] D. Boneh and X. Boyen. "Short signatures without random oracles". *In proceedings of advances in cryprtology - CRYPTO '04*, vol. 3027 of LNCS, pp. 56-73, 2004.

[24] D. Boneh, X. Boyen, and H. Shacham. "Short group signatures". *In the proceedings of advances in cryptology - CRYPTO '04*, Vol. 3152 of LNCS. pp. 41-55, 2004.

[25] D. Boneh and H. Shacham. "Group signatures with verifier-local revocation". *In proceedings of ACM conference on computer and communications security (CCS '04)*, pp. 168-177, 2004.

[26] T. Nakanishi and N. Funabiki. "Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps". *In proceedings of advances on cryptology - ASIACRYPT '05*, vol. 3788 of LNCS, pp. 533-548, 2005.

[27] H-Y. Lin and W-G. Tzeng. "An efficient solution to the millionaires' problem based on homomorphic encryption". *In proceedings of applied cryptography and network security (ACNS '05)*, vol. 3531 of LNCS, pp. 456-466, 2005.

[28] R. Lu, X. Lin, and X. Shen. "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-Healthcare emergency", *IEEE transactions on parallel and distributed systems*, vol. 24 No. 3, pp. 614-624, 2013.

[29] G. Yan, Y. Wang, M.C. Weigle, S. Olariu, and K. Ibrahim. "WEHealth: A secure and privacy preserving eHealth using NOTICE".