PEACE: An Efficient and Secure Patient-centric Access Control Scheme for eHealth Care System

Mrinmoy Barua, Xiaohui Liang, Rongxing Lu, and Xuemin (Sherman) Shen
Department of Electrical and Computer Engineering
University of Waterloo, Waterloo, Canada N2L 3G1
Email: mbarua@ecemail.uwaterloo.ca; {x27liang, rxlu, xshen}@bbcr.uwaterloo.ca

Abstract—**In this paper, we propose an efficient and secure patient-centric access control (PEACE) scheme for the emerging electronic health care (eHealth) system. In order to assure the privacy of patient personal health information (PHI), we define different access privileges to data requesters according to their roles, and then assign different attribute sets to the data requesters. By using these different sets of attribute, we construct the patient-centric access policies of patient PHI. The PEACE scheme can guarantee PHI integrity and confidentiality by adopting digital signature and pseudo-identity techniques. It encompasses identity based cryptography to aggregate remote patient PHI securely. Extensive security and performance analyses demonstrate that the PEACE scheme is able to achieve desired security requirements at the cost of an acceptable communication delay.**

Index Terms—**eHealth, security, privacy, attribute-based encryption, access control.**

I. Introduction

ELECTRONIC health (eHealth) care system is a promising technology that has drawn extensive attention from both academia and industry recently. It describes the application of information and communication technologies across the whole range of function that affect the PHI. The eHealth system shows a high potential to improve the quality of diagnosis, reduce medical costs and help address the reliable and on-demand health care challenges posed by the aging society. Recent advances in Wireless Body Area Networks (WBANs) have made it possible to deploy bio-sensors on, in, or around the patient body and allow to continuous monitoring of physiological parameters (e.g., electrocardiogram (ECG), blood oxygen levels) with physical activities. It has lent great forces to the migration of health care system from hospital or care unit to the patient's residence. Integrating this technology with the existing wireless technologies permits real-time mobile and permanent monitoring of patients, even during their daily normal activities. In such a heterogeneous wireless environment, secure communication of the patient PHI with integrity and confidentiality is an essential part of a reliable eHealth care system.

In addition, the eHealth care system needs to ensure the availability of PHI in electronic form adheres to the same levels of privacy and disclosure policy as applicable to present-day paper-based patient-records accessible only from the physician's office. Instead of storing the PHI locally, the recent advancement of cloud computing allows us to store all PHI centrally and ensures availability with reduces the capital and operational expenditures. Moving patients PHI into a cloud or in a central storage offers enormous conveniences to the eHealth care providers, since they don't have to care about the complexities of direct hardware management [1]. However, patient's privacy with proper access control of this available PHI is a growing concern in the eHealth care industry due to its direct involvement to human.

To address the patient privacy, we use attribute based ciphertext policy [2] to control the access to the patient private PHI and identity based encryption for secure communication between patient and eHealth care service provider. Our contributions are in three-fold: a) provide an architectural model of eHealth care system, b) show how PEACE provides a secure communication between remote patient and eHealth care provider, and c) present an patient-centric access control policy that helps PEACE to has more reliability. To construct this access control policy, we assign different attribute sets to data requesters based on their relation to the patient. For example, general users may know some common attributes of a patient, e.g., location, gender; patient's relatives or health care givers may know more private information of a patient, likely medication details, patient date of birth, patient phone number, etc.; health insurance providers may have more privileges and can know patient health card number, Social Identification number, etc.

The remainder of this paper is organized as follows. Section II contains a brief description of related work. System model and security requirements are presented in Section III. Preliminaries such as bilinear pairing, security definition are introduced in Section IV. The proposed scheme is presented in Section V. Section VI and Section VII provide security analysis and performance analysis of the proposed PEACE scheme respectively. The paper is concluded in Section VIII.

II. Related Work

Hybrid security policy for WBAN with Quality of Services (QoS) have recently been proposed for secure eHealth care system in [3]. R. Lu. et al. presented a mobile health care social network, where two patients can communicate each other if they have the same symptoms [4]. Liang et. al.[5] presented a patient self-controllable access policy so that patients would have the primary control of the access to their own personal health information. Xiaodong et al. [6] proposed a privacy preserving scheme for health care that can effectively works against global adversary. Health records

978-1-4244-9920-5/11/$26.00 ©2011 IEEE

sharing and integrating in health care cloud was discussed in [7]. In [1], Shucheng Yu et al. proposed a fine gained data access control in cloud computing based on key-policy based attribute based encryption (KP-ABE). Confidentiality of user access privilege and user secret key accountability can be achieved by their work. A mandatory access control model to protect patient's metadata with privacy was presented in [8]. It was shown that the use of fragmentation after encryption greatly improves overall security because potential attackers need to compromise more data file to gain access. An efficient cloud storage sharing scheme was presented in [9]. The scheme worked on hierarchical identity based encryption, where intended recipients can share the file by using their private keys.

Attribute based encryption, a novel extension from identity based encryption by enabling expressive access policy to control the decryption process was presented in [2][10][11], where the encrypter encrypted the data by using some attributes. The attribute set was used to describe a user's credentials.

III. System Model and Security Requirements

In this section, we define the system model and then describe the security requirements of the proposed PEACE scheme.

A. System Model

In our system model, the eHealth care service provider works as a trusted party, where a patient is registered. The encrypted data is stored in a centralize storage, health-cloud, for future access. Based on the major operations, the proposed scheme can be classified into four major steps, as shown in Fig 1.

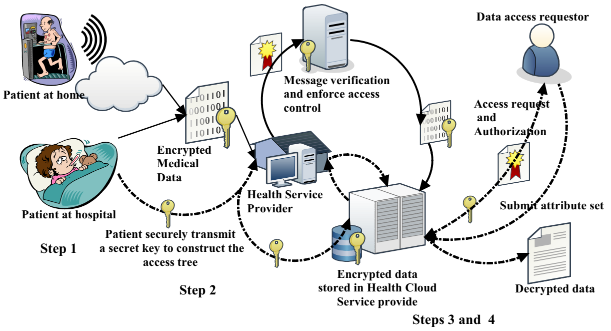

Patient at home
Data access requestor
Message verification and enforce access control
Access request and Authorization
Encrypted Medical Data
Patient at hospital
Health Service Provider
Submit attribute set
Step 1
Patient securely transmit a secret key to construct the access tree
Step 2
Encrypted data stored in Health Cloud Service provide
Decrypted data
Steps 3 and 4

Fig. 1. Secure data storage at Health-Cloud and secure data outsourcing

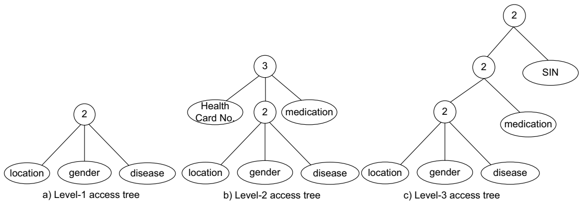
Step 1 (PHI collection): In this initial step, using different body sensors, PHI is sensed and ready to be transmitted to the trusted eHealth care service provider.

Step 2 (Secure data communication): In this step, public key cryptography is used to securely transfer collected PHI to the eHealth care service provider. Patient securely transfer a secret key to the trusted eHealth care provider, if he authorized the service provider to build-up the access tree.

Step 3 (PHI processing at eHealth care provider): After receiving the PHI securely, eHealth care service provider classifies the PHI based on the attributes set chosen by the patient. It then makes different privacy levels of data requesters based on their roles (e.g., level-1: general users, level-2: pharmacist, level-3: doctors, etc.) and assigns different set of attributes to these different levels.

Step 4 (Transfer PHI to the cloud storage and control access): After the data classification, encrypted data securely transfer to the cloud storage, shows as 'Health Cloud' in the Fig. 1. eHealth care service providers may operate either real-time or periodically based on the existing infrastructures. Data access requester sends their request to the cloud storage with a data block identity. They may also request for the corresponding attribute sets. In this case, the cloud storage provider communicates with the eHealth care service provider and verifies the authentication of the requesters. The data requester, as a node in the access tree ($\mathbb{T}$), can decrypt a ciphertext if and only if other corresponding nodes (users) also cooperate with him, or he has all the attribute sets to complete the $\mathbb{T}$.

In our system model, we classify the data requester as health worker, physicians, researchers, insurance companies, and agencies, etc. Some of them only need the accumulated number of patients in a specific area, some need disease related syndromes, age and gender specific characteristics, while others may need medication details. Fig. 2 shows possible access structures based on different privacy levels, where intermediate nodes work as a logic gates. For example, "2 of (location, gender, disease)" in the fig. 2(a) can be converted to "(location AND gender) OR (gender AND disease) OR (disease AND location)".



a) Level-1 access tree b) Level-2 access tree c) Level-3 access tree

Fig. 2. Access trees based on different data privacy level

B. Security Requirements

We aim at achieving the following security objectives.

1) *Patient-centric access control:* The system should provide patient-centric access control, where a patient can decides who can get the access to his/her stored PHI.
2) *Message integrity, source authentication and non-repudiation:* All accepted messages should be delivered unaltered, and the origin of the messages should be authenticated by the eHealth care service provider. To ensure the non-repudiation, the patient can not refute the validity of a PHI afterward.
3) *Prevention of Ciphertext-only attack:* The system should be secured enough to prevent recover of the plaintext from a set of stored ciphertexts.
4) *Provide patient privacy:* Privacy is one of the important concerns from a patient perspective. Illegal disclosure and improper use of patient PHI can cause legal disputes and undesirable damaging in patient's personal life.
5) *Resistant to collusion attack:* Users can not get any access to the encrypted data even by sharing information in a group.
6) *Resistant to Denial-of-Service (DoS) attack:* The DoS attack may be caused due to the large groups of legitimate users access the eHealth care service provider at

the same time, or the attacker continuously launch false traffic with a high data rate. The system should ensure acceptable QoS level to resist the DoS attack.

IV. Preliminaries

Since the bilinear pairing and the attribute based ciphertext policy work as the basis of our proposed scheme, we briefly review some related definitions and problem hardness, which closely follow those in [12].

Basic of Bilinear Pairing Consider two groups $\mathbb{G}_1$ an additive, and $\mathbb{G}_2$ a multiplicative group of the same prime order q. Let P and Q be the two generators of $\mathbb{G}_1$, and aP is the a times addition of P. We can write the mapping e as $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ which has the following properties:

1) Bilinear: $\forall P, Q \in \mathbb{G}_1, \forall a, b \in Z_q^*$ $e(aP, bQ) = e(P, Q)^{ab}$
2) Non-Degeneracy: $P \neq 0 \Rightarrow e(P, P) \neq 1$
3) Symmetric:$\forall P, Q \in G_1, e(P, Q) = e(Q, P)$.
4) Computability: e is efficiently computable.

Definition (BDH Parameter Generator): An algorithm Gen is called a BDH (Bilinear Diffe-Hellman) parameter generator if Gen takes a sufficient large security parameter $K > 0$ as input, runs in polynomial time in K, outputs a prime number q, the description of two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of order q, and the description of a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$.

Definition (BDH Problem hardness): Given a random element $P \in \mathbb{G}_1$, as well as aP,bP,cP, for some random $a, b, c \in \mathbb{Z}_q^*$; there is no efficient algorithm to compute $e(P, P)^{abc} \in \mathbb{G}_2$ from $P, aP, bP, cP \in \mathbb{G}_1$. This implies the hardness of the BDH in the group $\mathbb{G}_1$ [12].

Definition (Access Structure [2]): Let $\{a_1, a_2, ..., a_n\}$ be a set of health attributes. The sets $\mathbb{A}$ ($\mathbb{A} \subset 2^{\{a_1,a_2,...,a_n\}}$) are called the authorized attributes set, and the sets not in $\mathbb{A}$ are called the unauthorized sets. $\mathbb{A}$ is monotone if $\forall B, C : if B \subseteq \mathbb{A}$ and $B \subseteq C$ then $C \subseteq \mathbb{A}$.

In the access-tree construction, ciphertexts are labeled with a set of descriptive authorized attributes. Secret keys are identified by an access tree in which each interior node of the tree is a threshold gate and the leaves are associated with attributes.

Setup(1^t): The probabilistic polynomial time (PPT) setup algorithm takes as input a security parameter 1^t. It outputs the public parameters PK and a master key MK which is known only to the private key generator.

$\mathbf{Encrypt_1(PKs, m, PKr)}$: The encryption algorithm takes the public parameters of the sender and receiver and encrypt the message 'm' by doing mapping and XOR operations. We use $Encrypt_2(PK, M, A)$ function to encrypt the message M and store in the health cloud. This encryption algorithm takes the system public parameters PK, a message M, and an access structure $\mathbb{A}$ over the universe of health attributes. The encrypted ciphertext CT can only be decrypted if and only if the user possesses the set of health attributes that satisfy the access tree structure.

$\mathbf{Decrypt_1(PK, C, d)}$: The decryption algorithm takses as input the public parameter PK, ciphertext C, and the product of the receiver's secret key and sender PK's hash value. The health care provider uses this function to decrypt the encrypt message sent by the user for further processing. Another decryption function $Decrypt_2(PK, CT, SK)$ takes as input the public parameters PK, a ciphertext CT, which contains the access policy $\mathbb{A}$, and a secret key SK, which is a private key for a set S of health attributes. If the set S of attributes satisfies the access structure $\mathbb{A}$, the algorithm will decrypt the ciphertext and return the message M.

The set of algorithms must satisfy the standard consistency requirements: For $(PK, MK) \leftarrow Setup(1^t)$, $(k, E) \leftarrow Encryption(PK, \gamma)$, $D_{\mathbb{A}} \leftarrow KeyGen(PM, MK, \mathbb{A})$ and $\mathbb{A}(\gamma) = 1$ (i.e. the attribute set γ satisfies the access structure $\mathbb{A}$), then we have $Pr[Decryption(PK, E(M), D_{\mathbb{A}}) = k] = 1$.

V. Proposed PEACE Scheme

The four major categories describe in the system model can be integrated into two major phases, as shown in Fig 3.

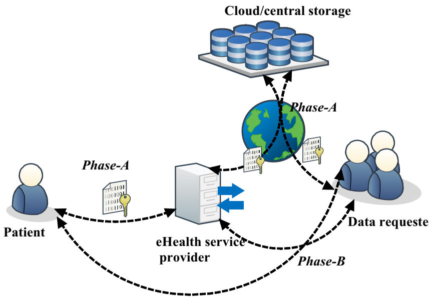


Fig. 3. Integrated two major phases of the proposed scheme

A. Phase-A: secure data communication:

In the phase-A, the scheme defines the secure and privacy preserving communication between different eHealth users. Here, we describe the secure communication steps between a remote user and an eHealth service provider; communication among others e.g., eHelath service provider and the cloud storage or data requesters will follow the same steps.

Step 1 (System initialization): Given the security parameter S', the bilinear parameters (q, G_1, G_2, e, P) are generated by the function $setup(S')$. It is assumed that a unique ID is given to the health care provider (hcp) by a trusted authority and the health service providers will do the following initializations:

1) Select a random number $\alpha \in_R Z_q^*$ and compute the public key $PK_{hcp} = \alpha.P$;
2) Generate the hash function $H_1 : \{0, 1\} \to \mathbb{G}_1^*$ and compute the key $K_{hcp} = H_1(ID)$ for message encryption and decryption;
3) Generate the secure hash function $H_2 : \{0, 1\}^* \to \{0, 1\}^n$, $H_3 : \{0, 1\}^* \to G_1^*$ and $H_4 : G_2 \to \{0, 1\}^*$.
4) Compute the remote user's pseudo-identity $(U_{PID}) = H_2(U_{ID})$, and store a copy of it for future verification;
5) Securely distribute U_{PID}, H_2, H_3, and H_4 to its subscribers.

An individual user (U) will do the following steps:

1) User Chooses a random number $r \in_R Z_q^*$ and computes the public key $PK_U = r.P$

2) User selects a random number $\beta \in_R Z_q^*$, to calculate the session key $P_\beta = \beta.P$
3) User computes the message token $T = H_2(m|U_{PID}|session\_id)$ and sends it to the receiver along with encrypted data and session key.

Step 2 (Secure message communication): After the system initialization, both parties use the data encryption and decryption algorithms to securely transmit their data. Here, we show how an user will encrypt the message 'm' ($Equ.1$) and decrypt the encrypted message by the corresponding eHealth care service provider. The user encrypts the message, m, based on the public key of the corresponding receiver using the identity based encryption [12].

$$v = Encrypt_1(PK_{hcp}, m, PK_U) = m \oplus H_4(g_U^r) \quad (1)$$

Here, $Q_U = H_3(U_{PID})$; $H_3 : \{0,1\}^* \rightarrow G_1^*$, a random oracle; $g_u = e(Q_U, PK_{hcp})$, and $H_4 : G_2 \rightarrow \{0,1\}^*$, a random oracle.

The encrypted message is decrypted using the $Dec(PK_U, v, d)$ function, where $d = \alpha H_3(U_{PID})$ and α is the secret key of the corresponding agent.

$$Decrypt_1(PK_U, v, d) = m \quad (2)$$

$Decrypt_1(PK_U, v, d) = v \oplus H_4(e(d, PK_U)$
$= v \oplus H_4(e(\alpha H_3(U_{PID})), rP) = v \oplus H_4(e(H_3(U_{PID}), P)^{r\alpha})$
$= v \oplus H_4(e(H_3(U_{PID}), \alpha P)^r) = (m \oplus H_4(g_u^r) \oplus H_4(g_u^r))$
$= m$

Step 3 (Message Signature and Verification): To ensure data integrity, the receiver will verify the message signature after receiving it. By doing it, the eHealth service provider can verifies the data originated from the specific patient and can not be altered after signing it. We use the cryptographic digital signature ($Equ.(3)$), based on the bilinear pairing to provide data integrity. The patient first creates a session key $P_\beta = \beta P$, here $\beta \in_R Z_q^*$, and computes the message token T. He then computes the signature using the equation (3).

$$S = \frac{1}{v + \beta + r + T} P \quad (3)$$

The eHealth service provider verifies the signature by using the equation (4).

$$e(vP + P_\beta + PK_{U_{PDA}} + TP, S) = e(P, P) \quad (4)$$

$e(vP + P_\beta + PK_{U_{PDA}} + TP, S) = e((v + \beta + r + T)P, (v + \beta + r + T)^{-1}P) = e(P, P)^{(v+\beta+r+T)(v+\beta+r+T)^{-1}} = e(P, P)$

B. Phase B: Control of data requesters access

In a traditional public key cryptography system, the receiver and sender need each other public parameters to encrypt a message. But in the eHealth care system, the patient does not have any knowledge about the data requester or does not know who is going to access his PHI. Therefore, the security scheme by itself has to be capable to grant access control remotely. We use attribute based ciphertext policy with privacy leveling to solve this challenge. Based on the different roles of the data requesters, an access tree is created and the requester needs to provide corresponding attributes (nodes of the tree) to have the secret key and thereafter he can use the secret key to decrypt the encrypted data (PHI). Providing falls attributes will stop the decryption processes immediately and the data requester learns nothing more than the attributes he/she is entitled. Details construction of the access tree with related key-generation, encryption, and decryption algorithms are described below.

Access Tree ($\mathbb{T}$): Let $\mathbb{T}$ represent an access structure. Each non-leaf node of the tree represents a threshold gate. If num_x is the number of children of a node x and k_x is the threshold value, then $0 \leq k_x \leq num_x$. When $k_x = 1$, the threshold gate is an OR gate, when $k_x = num_x$, it is an AND gate, finally when $1 \leq k_x \leq num_x$, it is a combination of AND and OR gates (Fig. 2). The function $parent(x)$ returns the parent of node x. The function $att(x)$ is defined only if x is a leaf node and denotes the attribute associated with the leaf node x. The function $index(x)$ returns an ordering number associated with node x.

Let $\mathbb{T}$ be an access tree with root 'r'. Denote by $\mathbb{T}_x$ the subtree of $\mathbb{T}$ rooted at the node 'x'. Hence $\mathbb{T}$ is the same as $\mathbb{T}_r$. If a set of health attributes ω satisfies the access tree $\mathbb{T}_x$, we denote it as $\mathbb{T}_x(\omega) = 1$. We compute $\mathbb{T}_x(\omega)$ recursively as follows:

If 'x' is a non-leaf node, evaluate $\mathbb{T}_z(\omega)$ for all children z of node 'x'. $\mathbb{T}_x(\omega)$ returns 1 if and only if at least k_x children return 1. If 'x' is a leaf node, then $\mathbb{T}_x(\omega)$ returns 1 if and only if $att(x) \in \omega$.

Data formation and authentication: Before encrypting the data packets, the trusted eHealth care provider classifies the data set based on some privacy levels and assign some attributes on that message block (M). It then concatenates the message block (M), user pseudo identity U_{PID}, and the $session\_id$. After that the trusted eHealth care provider computes the token value $T = H_2(M|U_{PID}|session\_id)$. It then computes the signature using the equation 3. Local health care provider will store the block sequence and patient pseudo identity for future verification. Fig. 4 shows the data packet structure. The health cloud service provider will check the message authenticity by verify the signature using the equation 4.

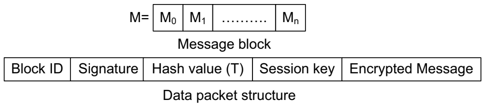

M= | M_0 | M_1 | .... | M_n
Message block
Block ID | Signature | Hash value (T) | Session key | Encrypted Message
Data packet structure

Fig. 4. Data packet architecture

The health cloud service provider will generate the signature in the same way and store along with the encrypted messages for the data requester verification purposes.

$\mathbf{Encrypt_2(PK, M, T)}$: The algorithm first chooses a polynomial q_x for each node x in the tree T. These polynomials are chosen in a top-down manner, starting from the root node. For each node x in the tree, set the degree d_x of the polynomial q_x to be one less than the threshold value of k_x. Starting with the root node 'R', the algorithm chooses a random $s \in \mathbb{Z}_p$ and sets $q_R(0) = s$. Then it chooses d_R other points of the polynomial q_R randomly to define it completely. For any other node x, it sets $q_x(0) = q_{parent(x)}(index(x))$ and chooses d_x other points randomly to completely define q_x.Finally, the ciphertext is then constructed by giving the access tree structure $\mathbb{T}$ and compute

$$CT = \Big(\mathbb{T}, C^{‘} = Me(g,g)^{\alpha s}, C = h^{s}, \\ \forall y \in Y : C_y = g^{q_y(0)}, C^{‘}_y = H(att(y))^{q_y(0)}\Big) \tag{5}$$

KeyGen(MK,S): The key generation algorithm takes as input a set of attributes S and outputs a key that identifies with the set. The algorithm first chooses a random $r \in \mathbb{Z}_p$, and then random $r_j \in \mathbb{Z}_p$ for each attribute $j \in S$, and outputs the key as

$$SK = \Big(D = g^{\alpha + r)/\beta}, \\ \forall j \in S : D_j = g^{r}.H(j)^{r_j}, D^{‘}_j = g^{r_j}\Big) \tag{6}$$

$\mathbf{Decrypt_2(CT, SK)}:$ The decryption procedure works as recursively and is defined by the function $DecryptNode(CT, Sk, x)$ that takes as input a ciphertext CT and a private key SK. If the node x is a leaf node, then the function works as follows:

$DecryptNode(CT, SK, x) = \frac{e(D_i, C_x)}{e(D^{‘}_i, C^{‘}_x)}$
$= \frac{e(g^{r}.H(i)^{r_i}, h^{q_x(0)})}{e(g^{r_i}, H(i)^{q_x(0)})} = e(g,g)^{rq_x(0)}$

Here $i \in S$. If $i \notin S$, we define $DecryptNode(CT, Sk, x) = \perp$. When x is a non-leaf node, the algorithm is called by its all child nodes z. It then stores the output of $DecryptNode(CT, Sk, z)$ as F_z. Detail is shown in [2]. If the data requester can submit all the attributes correctly, the algorithm then executes on the root node 'R'. If the tree is satisfied by S, we set $A = DecryptNode(CT, SK, r) = e(g,g)^{rq_R(0)} = e(g,g)^{rs}$. The message 'M' can be decrypted by computing

$$C^{‘}/(e(C,D)/A) = C^{‘}/(e(h^{s}, g^{(\alpha + r)/\beta})/e(g,g)^{rs}) = M$$

VI. Security Analysis

In this section, we evaluate the security and privacy issues of the proposed scheme.

The PEACE scheme ensures user and eHealth agent's identity privacy: User and health agent use pseudo identity instead of their unique identity, and these pseudo identities are generated by a strong one-way hash function. The construction of the hash function is easy to sample and compute but hard to invert. Therefore, the privacy is ensured by the proposed scheme.

The scheme is secure to chosen ciphertext-only attack: Data transmissions from user to health agent, as well as from health agent to health cloud service provider are done with proper encryption schemes ($Encryption_1$ and $Encryption_2$). The processes are indistinguishable under chosen ciphertext attack based on the BDH problem hardness and this hardness ensures there is no probabilistic polynomial time algorithm that can decrypt the message from a set of chosen ciphertext.

The scheme is resistant to the eavesdropping and collusion attacks: An eavesdropping attacker aims at accessing the private and sensitive patient's medical data. This attack may be happened during the patient to eHealth care provider or eHealth care provider to the health cloud data communication. The BDH hardness ensures that the proposed scheme is resistant to this eavesdropping attack. To access the data at the health cloud server, an attacker needs to has sufficient attributes to complete the access tree. Here the random number 's' is divide into multiple shares based on the attributes set. For the non-privacy data set, he may get access and its allowed in our scheme. But he can't modified the data due to the verification bindings. However, for the patient sensitive data, a unique random number is embedded into both 'C' and 'D' of the equation shown in the $Decrypt_2(CT, SK)$ function. Without knowing that secret number, it is impossible to access the data in a probabilistic polynomial time. This hardness also demonstrates our scheme as a resistant to the collusion attack. Therefore, any attacker cannot successfully launch the eavesdropping or collusion attack to our proposed scheme.

The scheme ensures message integrity, non-repudiation, and source authentication: We use the patient's secret key and the session identity to generate the signature 'S' ($Equ.3$). The data receiver can verifies the signature by using the public parameters of the sender, shown in the Equ. 4. This verification ensures the corresponding source authentication. The scheme generates the message token value 'T' by computing the hash value of the concatenated message, patient's identity (P_{ID}), and a session sequence number. Only the patient and the eHealth care provider know the patient's original identity and the session sequence number. This token value is also used to generate the signature 'S'. Therefore the message integrity with non-repudiation can be provided by our proposed scheme.

VII. Performance Analysis

In this section, we first show the timing cost of operations used in PEACE. We then analyze the performance of PEACE to resist DoS attack, and conduct a simulation using NS 2.33.

Time cost: We consider 20ms and 550ms as the computation time for the pairing using a personal computer and PDA respectively [13]. Time cost of PEACE operations is given in table I.

TABLE I
Time cost for PEACE operations

Operation	Time	Operation	Time
Encryption1	C_e	Signature	C_m
Verification	C_e	Decryption1	C_e
Encryption2	$C_e + 2C_m$	Decryption2	$2C_e + C_m$

We denote by C_e a computation of the pairing, and C_m a scalar multiplication in G_1. Usually, pairing operations cost is much more than other computations. A single pairing C_e needs about 10 times more time to compute than a scalar multiplication C_m [14].

Analysis: The system blocking probability can be increased by high data rate traffic, or accessing the system by a large number of misbehaving users at a time. This increased rate of blocking probability is considered as a cause of DoS attack. In our analysis, we aim to minimize the blocking probability by restricting data rate and using multiple servers. We assume that the service provider serves multiple users. Users demand services according to a Poisson process and request independent and identical distributed exponential service time. We use M/M/1/K and M/M/m/K queuing model for analysis and assume that the blocking probability should be less than 30% to provide adequate Quality of Service (QoS) to the users. Blocking probability $P_1(K)$ and $P_m(K)$ of the M/M/1/K and M/M/m/K queue respectively can be written as follow:

$P_1(K) = \frac{1-\rho}{1-\rho^{K+1}}\rho^i$ and $P_m(K) = \frac{\rho^m/m!}{\sum_{i=0}^{K}\frac{\rho^i}{i!}}$; for $\rho = \frac{\lambda}{\mu} \neq 1$ and $0 \leq i \leq K$.

Derivation of above equations can be found in [15]. We consider the arrival rates λ for the normal and high data rate traffic are 3 and 6 per unit of time, respectively, while the service rate $\mu = 10$ is fixed. The number of users, K, varies from 0 to 50. For the M/M/m/K queue, the number of servers $m = 2$.

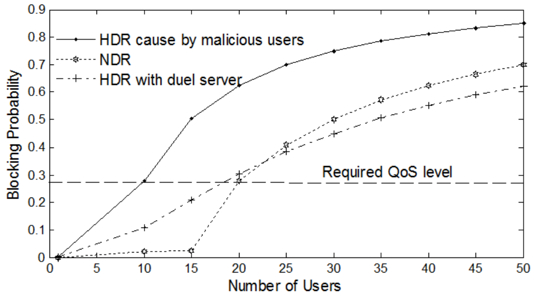


Fig. 5. Queuing comparisons for the QoS requirements

Fig. 5 shows that high data rate (HDR) created by malicious users causes high blocking probability compared to normal data rate (NDR), and ineffective to maintain QoS level for more than 10 users. We can use multiple server with fixed upper bound of the data rate to resist the DoS attack, and to ensure the required QoS with an acceptable number of users.

eHealth care scenario: We consider two types of users, wired and wireless, are connected to the eHealth care service provider. The eHealth care provider is linked to the cloud server through a wired connection. We define two types of scenarios, normal scenario (NrS) and high-dense scenario (HdS), in our model. NrS consists of 5 mobile users and 3 users with wired connection. For the HdS, we just double the respective numbers.

Network simulation: Based on the theoretical analysis, we consider NrS, and HdS with single and duel server in our simulation. The performance metric used in our simulation is end-to-end delay, and all the wireless users are assumed to be in the access-point communication range. Table. II gives the different parameters used in our simulation.

TABLE II
SIMULATION PARAMETERS

Simulation time	150 sec
Number of nodes	NrS [wireless 5, wired 3]; HdS [wireless 10, wired 6]
Packet type	wireless-CBR, Wired-TCP
Packet size	512 bytes
Mobility	2-5 Km/hr [for wireless users]

Fig. 6 shows the average end-to-end delay of the different scenarios using the PEACE scheme.

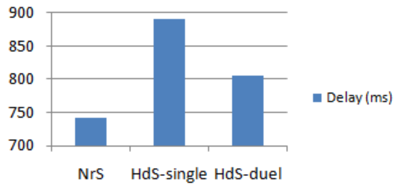


Fig. 6. Comparison of average end-to-end delay

Simulation results show that the average end-to-end delay of the proposed scheme is around 750 ms in a normal scenario and increases to 900 ms in a high-dense scenario, which is minimized to 800 ms by using the duel server. Based on the performance analyses, we can apply PEACE scheme in a duel server mode to resist DOS attack and provide a high QoS level for users.

VIII. CONCLUSION

In this paper, we have proposed a scheme, PEACE, to achieve patient-centric access control with security and privacy by exploiting attribute based encryption. Moreover PEACE enables the eHealth care service provider to reduce the overall maintaining cost by moving data to a centralized storage or cloud storage for further processing and long-term storage. The proposed scheme also preserves user privacy with data integrity. Through detailed security and performance analyses, it has been demonstrated that the proposed scheme is highly efficient to resist various possible attacks and malicious behavior.

REFERENCES

[1] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *INFOCOM, 2010 Proceedings IEEE*, 2010, pp. 1 –9.

[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Security and Privacy, 2007. SP '07. IEEE Symposium on*, May 2007, pp. 321 –334.

[3] M. Barua, M. S. Alam, X. Liang, and X. Shen, "Secure and quality of service assurance scheduling scheme for wban with application to ehealth," in *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*, Cancun, Quintana-Roo, Mexico, 2011, pp. 1 –5.

[4] R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social network," *Mobile Networks and Applications*, pp. 1–12, 2010.

[5] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on phi in ehealthcare systems," in *AHIC 2010*, Kitchener, Ontario, Canada, 2010, pp. 1–5.

[6] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: a strong privacy-preserving scheme against global eavesdropping for ehealth systems," *Selected Areas in Communications, IEEE Journal on*, vol. 27, no. 4, pp. 365 –378, May 2009.

[7] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, 2010, pp. 268 –275.

[8] J. Luna, M. Dikaiakos, M. Marazakis, and T. Kyprianou, "Data-centric privacy protocol for intensive care grids," *Information Technology in Biomedicine, IEEE Transactions on*, vol. 14, no. 6, pp. 1327 –1337, 2010.

[9] Q. Liu, G. Wang, and J. Wu, "Efficient sharing of secure cloud storage services," in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, 29 2010.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*, ser. CCS '06. New York, NY, USA: ACM, 2006, pp. 89–98.

[11] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption," in *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, ser. ASIACCS '09. New York, NY, USA: ACM, 2009, pp. 343–352.

[12] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*. London, UK: Springer-Verlag, 2001, pp. 213–229.

[13] A. Ramachandran, Z. Zhou, and D. Huang, "Computing cryptographic algorithms in portable and embedded devices," in *Portable Information Devices, 2007. PORTABLE07. IEEE International Conference on*, May 2007, pp. 1 –7.

[14] R. Zhu, G. Yang, and D. Wong, "An efficient identity-based key exchange protocol with kgs forward secrecy for low-power devices," *Internet and Network Economics*, vol. 3828, pp. 500–509, 2005.

[15] C. G. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*. Springer, 2010.