Attribute-Based Authenticated Access for Secure Sharing of Healthcare Records in Collaborative Environments

Mohamed Abomhara and Huihui Yang

Department of Information and Communication Technology
University of Agder, Grimsatd, Norway
Email: {mohamed.abomhara, huihui.yang }@uia.no

***Abstract*—This study highlights authorization matters in cooperative engagements with complex scenarios in the collaborative healthcare domain. Focus is mainly on collaborative activities that are best accomplished by organized groups of healthcare practitioners within or among healthcare organizations with the objective of accomplishing a specific task (a case of patient treatment). In this study, an authorization schema is proposed that is suitable for collaborative healthcare systems to address the issue of information sharing and information security. The proposed scheme is based on attribute-based authentication (ABA), which is a way to authenticate users by attributes or their properties. The main goal is to provide an authorization model that strikes a balance between collaboration, flexible access to patient information and safeguarding sensitive patient information.**

Keywords–Electronic health records; Authorization; Authentication; Data security and privacy; Attribute-based authentication; Collaboration.

I. Introduction and Motivation

Electronic health records (EHRs) are widely adopted by healthcare providers and patients to efficiently and effectively create, manage and access patient healthcare information [1], [2], [3]. Integrated use of EHRs seem promising in enhancing healthcare services due to a number of attractive features, such as improving the quality and delivery of health services by giving healthcare providers access to information they require to provide rapid patient care [1]. In addition, reducing the cost of care by facilitating easy collaborative support from multiple parties to fulfill the information requirements of daily clinical care [4], [5].

Typically, rapid patient care requires the collaborative support of different parties including primary care physicians, specialists, medical laboratory technicians, radiology technicians and many other medical practitioners [6], [7]. Moreover, collaboration among healthcare organizations is required for patients being transferred from one healthcare provider to another for specialized treatment [8]. However, security control over information flow is a key aspect of such collaboration where sensitive information is shared among a group of people within or across organizations. In this study, focus is mainly on authorization issues when EHRs are shared among healthcare providers in collaborative environments with the objective of accomplishing a specific task.

A. Problem Definition

EHRs system is considered in this study. Multiple owners (referring to patients who have full control of their EHRs) and healthcare providers, such as physicians, nurses, family, and relatives, among others, who require access to these EHRs to perform a task. Healthcare providers can only access and perform actions (e.g., read and/or write) to patients' EHRs, for which they are responsible. For example, doctors have access to their own patients' data, but not the data of another doctor's patients, while nurses or personal assistants have access to the information of the patients for whom they are responsible [9]. On the one hand, healthcare services need the collaborative support of multiple healthcare professionals and administrators in order to deliver rapid patient care. Therefore, multiple healthcare providers (e.g., doctors and nurses) may require access to patient information to perform tasks. On the other hand, EHRs contain sensitive information about patients, including demographic information, medical history, laboratory tests and radiologic images that call for appropriate authorization mechanisms in place to ensure that information is accessible only to those authorized to have access [10].

The main concern with EHRs sharing during collaborative support is having an authorization mechanism with flexibility to allow access to a wide variety of authorized healthcare providers while preventing unauthorized access. Since healthcare services necessitate collaborative support from multiple parties and healthcare teamwork occurs within a dynamic group, dynamic authorization is required to allow team members to access classified EHRs.

B. Study Objective

The main objectives of this work is to design an attribute-based group authorization model that is suitable for collaborative healthcare systems to address the concern with information sharing and information access. The proposed model ensures that access rights are dynamically adapted to the actual needs of healthcare providers. Healthcare providers can access the resources associated with a work task, but only while the work task is active. Once the task is completed, access rights should be invalidated.

C. Structure of the Study

The remaining parts of this study are organized as follows. In Section II, a brief description of the EHRs system, the usage scenario and security requirements are provided. Proposed scheme and security analysis are presented in Section III. Finally, conclusions and aspects for future work are given in Section IV.

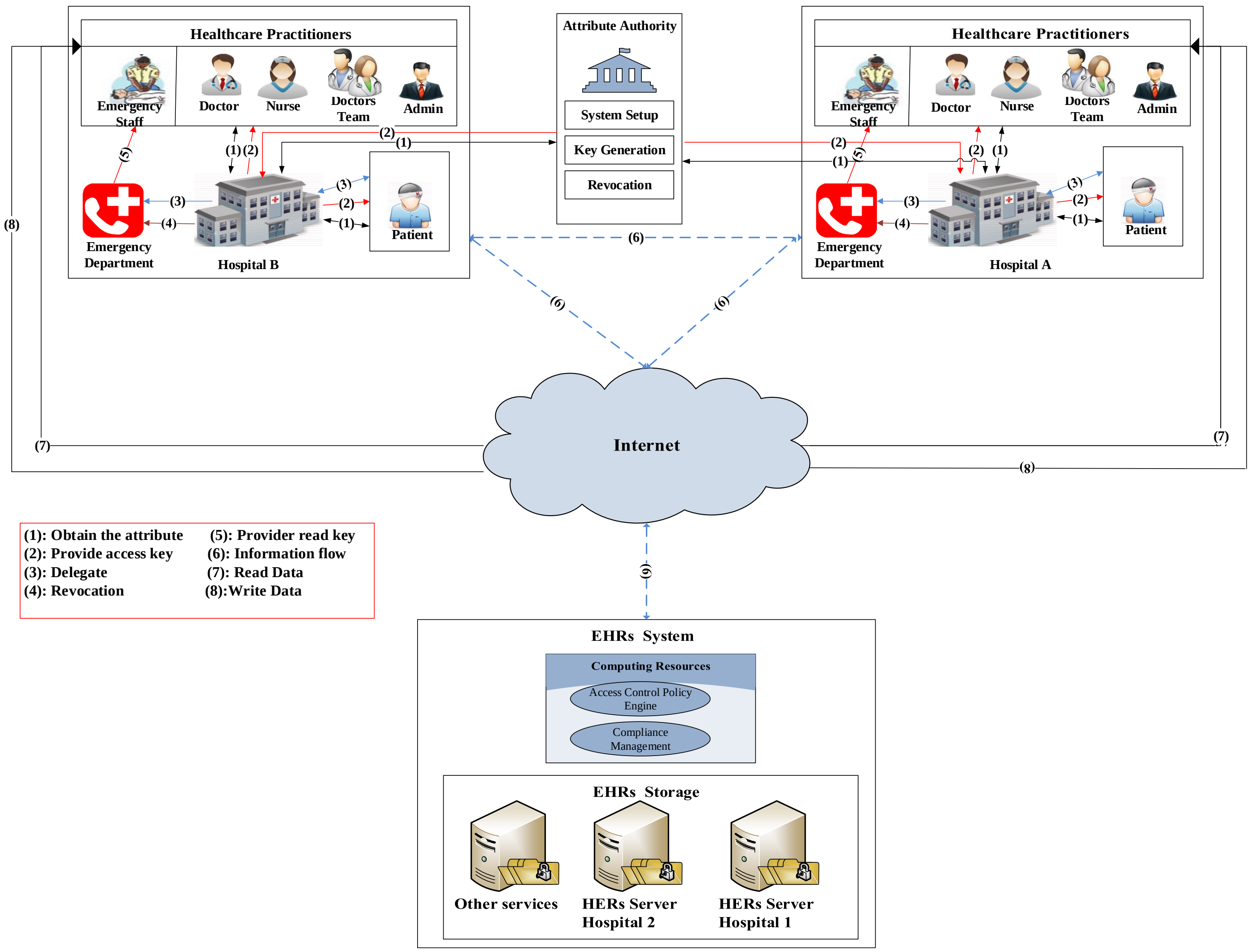

Figure 1. Reference system architecture overview

II. EHR SYSTEM

In this section, relevant work underlying the current study is discussed. First, the system architecture is briefly introduced, followed by the usage scenario and an overview of security requirements.

A. Systems architecture

In Figure. 1, the architecture of the reference system is illustrated. The reference system includes the following main domains:

1) **EHRs**: The medical records are collected, stored and provisioned by the electronic health records system to achieve the features of low cost operation, collaborative support and ubiquitous services. The EHRs can reside in a centralized or distributed systems depending on the deployment needs [11]. Authorized healthcare providers, including hospitals and healthcare practitioners can access EHRs through different services such as web portals and health apps [12]. The access to medical files is controlled via the requirements of attributes. For each medical file, the access policy is represented by a combination of attributes. When a user (patients and healthcare providers) requires to access (read, write, etc) the file, it should show an evidence that it satisfies the required attributes. Only if the evidence is valid that the user's access requirement can be granted. This process will be implemented by an attribute-based authentication (ABA) scheme presented in Section III-A.

2) **Trusted authority**: A fully trusted authority such as the Ministry of Health is responsible for key generation, distribution and management of users' keys. The main responsibilities of the trusted authority include the following:

a) Generate the main system public and private keys.

b) Generate user keys for each user.

c) Generate public and attribute keys for each attribute in the system.

d) Generate attribute keys for attributes possessed by each user.

As for implementation, it is possible to have different authorities perform these responsibilities separately, such that the compromise of one authority will not lead to the compromise of the whole system. More specifically, healthcare delivery organizations (e.g., hospitals) perform as a registration center with a certain qualification certified by the trusted authority. Healthcare delivery organizations are responsible for checking their healthcare practitioners' professional expertise and send their attributes to the trusted authority to issue the corresponding attribute-based credentials.

3) **Healthcare providers**: Healthcare providers from various domains, such as doctors, nurses, radiology technicians and pharmacists, to name a few, require access to patients' records to perform a task. Once a new healthcare practitioner join a system, the healthcare delivery organization must send healthcare practitioner' attributes to the trusted authority to obtain attributes based credentials. Healthcare practitioners apply their authentication credentials obtained from the trusted authority to access classified EHRs through authorization mechanisms in the EHR aggregator. In case of group collaboration, multiple EHRs have to be shared with various healthcare providers and practitioners. A group manager is responsible for registering healthcare practitioners to form a group. The hospital's (registration center) responsibility is to verify the authenticity of each healthcare practitioners in the group based on the professional expertise and required access, and send it to the trusted authority to issue the corresponding group credentials for the group.

B. *Usage scenario of work-based authentication*

In this Section, a typical use case scenario adopted from [4] is presented. As shown in Figure. 2 , a patient named Alice is recently diagnosed with gastric cancer. Surgical removal of the stomach (gastrectomy) is the only curative treatment. For many patients, chemotherapy and radiation therapy are given after surgery to improve the chances of curing. Alice entered a cancer-treatment center at her chosen hospital (e.g., hospital A in Figure.1). Alice has a general practitioner (Dean) who she regularly visits. Upon entering the hospital, Alice also sees an attending doctor (Bob) from the hospital. Alice's health condition has caused some complications, so her attending doctor would like to seek expert opinions and consultation regarding Alice's treatment from different hospitals (e.g., hospital B in Figure.1), including Alice's specific general practitioner who is fully informed about Alice's medical history. Note that the invited practitioners are specialized in different areas, where some are specialists and others are general practitioners. In such group consultation, every participant needs to obtain the medical records they request based on the health insurance portability and accountability act (HIPAA) [13] minimal disclosure principle.

Furthermore, the consultation results, such as diagnosis and treatment suggestions, should be signed and certified by this group of specialists and practitioners. The medical certificate with their signatures is sent to Alice.

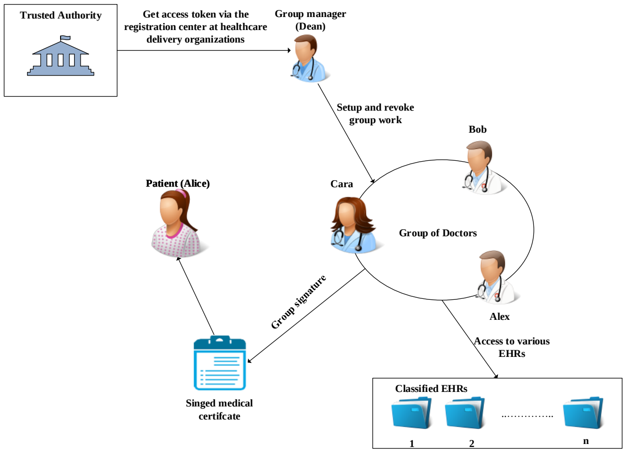

Figure 2. An EHRs usage scenario

In this case, the act of managing the collaborative work must be clearly defined. By default, only the main practitioner (Dean) should be aware of the patient's personal information. The three other medical practitioners with supporting roles are given information based on their contributing roles (need-to-know principle) [14]. For instance, if the supporting party is included solely for consultation purposes concerning the disease, only information essential for diagnosis is provided. It is not necessary to allow perusal of personal information related to the patient. In this way, improper access to the patient's sensitive information can be prevented.

Hospital personnel roles are often simplistically split into medical practitioners, nurses and administrators [15], [16]. However, in [17] (paper by one of us), we further categorized personnel roles into a total of nine roles per group, which are classified into main, action, strategic and management roles, as shown in Figure. 3.

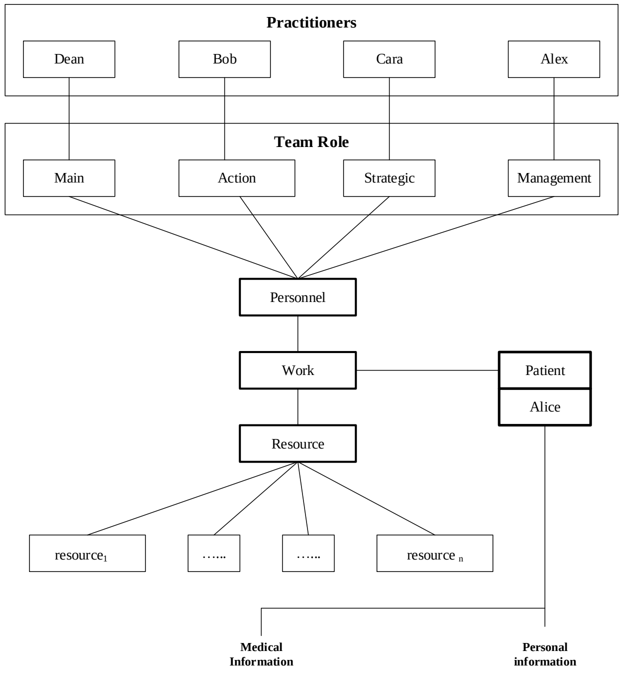

Figure 3. EHRs usage scenario

The workflow of every healthcare practitioner is as follows:

1) The general practitioner (Dean) serves as the group manager. He is responsible for initiating the work (treatment of Alice's case) and choosing the practitioners (group of doctors) who may be required to attend Alice's consultation and treatment. Moreover, the general practitioner must revoke the group upon completion of the patient's diagnosis consultation.
2) Bob helps Dean with the operational part of the case. Operation refers to a series of responsibilities that entail interaction with the patient. Bob needs to see Alice on a face-to-face basis to perform various tasks that are related to her recovery. In this respect, there is a need for Bob to know personal and medical information about Alice to perform his duty effectively.
3) Cara has more of a strategy role. She is responsible for helping Dean solve the medical case. There is no need for Cara to meet Alice personally on a day-to-day basis. In fact, Cara is only required to analyze the medical situation and suggest a possible solution. Cara's strategic role within the team implies a rather clear indication of the access that she needs. Since Cara is predominantly preoccupied with diagnosing the disease, there is no urgent need for her to know the patient's personal information. As such, she is only given access to the patient's medical information as per her strategic team role.
4) With the increasing number of physicians working on Alice's case, their interaction can become more complex. For instance, if there exists a competition between conflicting diagnoses given by Bob and Cara, which would gain priority? This is where Alex comes in. He contributes to the team by coordinating the interaction of the other members by taking on the team management role. To work effectively, Alex does not really need to know the patient's personal information. However, he must be aware of the patient's medical information to enable coordination.

In addition, Alice may have some historical health information (e.g., mental illness or sexual issues, etc.), to which the group (or some of the group) of specialists and practitioners do not have to have access. We assume that each resource (EHR files) in the system are divided into type, mainly shareable and non-shareable during the collaborative work. The collaborative resources required for work are enumerated in table form as proposed by Abomhara in [17]. Each shared resource is tied to the set of collaborative roles or team roles that can access it. In effect, the selected roles will determine the extent of collaborative access.

C. Security requirements

Some of the requirements of a well-designed attribute-based authentication system were presented by Yang [18], [19]. According to our usage scenario, the system should fulfill the following requirements:

- **Confidentiality**: Unauthorized users who do not possess enough attribute satisfying the authorization policy should be prevented from reading EHR documents.
- **Minimum attributes leakage**: To be authenticated, healthcare provider only need to provide required attributes rather than the whole package of attributes it possesses.
- **Signature**: The final medical report of Alice's treatment should be signed by appropriate practitioners using digital signatures.
  Alice should be able to verify the authenticity of the consultation results through the practitioner's digital signature. Note that the practitioner's digital signature can be opened (reveal the practitioner's identity) depending on the requirements. In some cases, practitioners do not want to reveal their identities when participating in group treatment.
- **Unforgeability**: An adversary who does not belong to the group should not be able to impersonate a group member and forge a valid signature to get authenticated.
- **Coalition resistance**: Group members should not be able to pile up their attributes to forge a signature to help a member to get authenticated.

III. Proposed scheme

In this section, the system setup and security analysis are presented.

A. System setup

System setup, including key generation, distribution and revocation are explained in this subsection. As mentioned before (Section II-A), the trusted authority is responsible for users' key and attribute key generation. For each user in the system, the trusted authority will generate a unique user key that represents the user's identity information and will be used to trace users' identities if necessary. The proposed scheme is based on bilinear mapping [20], [21].

Definition 1: **[Bilinear Mapping]** [22] Let G_1, G_2 and G_3 be cyclic groups of prime order p, with $g_1 \in G_1$ and $g_2 \in G_2$ as the generators. e is an efficient bilinear map if the following two properties hold.

1) Bi-linearity: equation $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ holds for any $a, b \in \mathbb{Z}_p^*$.
2) Non-degenerate: $e(g_1, g_2) \neq 1_{G_3}$, where 1_{G_3} is the unit of G_3.

Firstly, the proposed ABA scheme needs to set up the system, which is considered as a preparation for the phase of signature generation, verification and opening. During system setup, the system main parameters, such as main public and private keys set will be generated by the trusted authority. Based on the main private and public keys set, the trust authority will generate system attribute keys and users' keys. More importantly, the trusted authority will authorize Dean the power to generate attribute keys for group members. This is how Dean gains the control over the group.

Assume k_0 is the system security parameter. G_1, G_2 are two multiplicative groups of prime order p with $g_1 \in G_1$ and $g_2 \in G_2$ as their generators. Let $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear mapping. Select $h \in G_1$, $\xi_1, \xi_2 \in \mathbb{Z}_p^*$, where $\mathbb{Z}_p^* = \{a \in \mathbb{Z}_p | gcd(a, p) = 1\}$ is a multiplicative group modulo a big prime number p. Set $u, v \in G_1$ such that $u^{\xi_1} = v^{\xi_2} = h$. Select $x_0, \beta_0 \in \mathbb{Z}_p^*$ as the top secret and compute $w_0 = g_1^{x_0}$, $f_0 = g_1^{1/\beta_0}$ and $h_0 = g_1^{\beta_0}$. The public key set of the trusted authority is denoted by $MPK =< G_1, G_2, g_1, g_2, h, u, v, f_0, h_0, w_0 >$ and the private key set is $MSK =< x_0, \beta_0, \xi_1, \xi_2 >$, where the pair $< \xi_1, \xi_2 >$ is handed to the opener as its tracing key tk.

Then the system setup proceeds as follows.

1) **Dean authorization**: Dean described in our usage scenario can be considered as an attribute domain authority in the scheme proposed in [23]. To authorize Dean, first, the trusted authority selects a secret $x_d \in \mathbb{Z}_p^*$ and computes $A_d = g_1^{(x_0+x_d)/\beta_0}$ and $w_d = g^{x_d}$. The pair $DSK =< A_d, x_d >$ is the Dean's private key and A_d should be registered in the opener's database for identity tracing. $DPK =< w_d >$ as the Dean's public key.
2) **User key generation**: All users in the system should register themselves and obtain their users' key from the trusted authority. Assume there are N users in the EHRs usage case. To generate the secret key of user U_i $(1 \leq i \leq N)$, the trusted authority randomly selects $x_i \in \mathbb{Z}_p^*$ and computes $A_i = g_1^{(x_0+x_i)/\beta_0}$. $bsk_i =< A_i, x_i >$ is U_i's secret key base and A_i should be handed to the opener.
3) **Attribute key generation**: Assume the attribute set owned by all members in the EHRs usage case is denoted by $\Psi = \{att_1, \cdots, att_{N_a}\}$ $(N_a = |\Psi|)$. To generate a pair of private and public attribute key for an attribute $att_j \in \Psi$ $(1 \leq j \leq N_a)$, the trusted randomly selects $t_j \in \mathbb{Z}_p^*$ as its private attribute key and computes $apk_j = {g_1}^{t_j}$ as its public attribute key.
4) **Attribute key authorization**: The trusted authority authorize attribute keys to Dean. For attribute att_j, the trusted authority selects $r_j \in \mathbb{Z}_p^*$ and computes $T_{d,j} = g_1^{(x_0+x_d)/\beta_0} H(att_j)^{t_j+r_j}$ and $apk_{dj} = g_1^{r_j}$ as Dean's private and public attribute keys for attribute att_j respectively.
5) **User attribute key generation**: To be active in the EHRs usage case described above, each member should gain their attribute keys from Dean. Assume the attribute set possessed by user U_i is denoted by $\Psi_i = \{att_{i1}, \cdots, att_{iN_i}\}$. Assume attribute att_{ik} $(1 \leq k \leq N_i)$ corresponds to $att_j \in \Psi$. For simplicity, we will use att_j to represent att_{ik} instead. To generate a private attribute key of att_j $(1 \leq k \leq N_i)$ for U_i, Dean interacts with U_i and computes $T_{i,k} = f_0^{x_i} T_{d,j} = g_1^{(x_0+x_d+x_i)/\beta_0} H(att_j)^{t_j+r_j}$ as U_i's private attribute key for attribute att_j.

All these attribute keys are only active during the period of a specific workload. When this workload is finished, all attribute keys of users in this group should be revoked. This requirement can be realized by combining these attribute keys with a timing token. Thus, these attribute keys are only valid during this fixed time period.

B. Signature generation, verification and opening

After the system setup, all entities in the group of the EHRs usage case have obtained their users' keys and attribute keys for authentication. As described before, each medical file is bound with access policies represented by a combination of attributes. More specially, this combination of attributes is represented by an attribute tree [18]. An attribute tree is a tree structure that represents the logical relations among required attributes, based on which a user generates a signature as a proof of possessing the required attributes.

The user can only be authenticated when the signature is valid. However, it is also possible that the user's access request is reject even though the signature is valid because of other factors, such as system time, locations and so on.

Assume that U_i is a user to the authenticated, V is the verifier and f is the file that U_i wants to access. The verifier here can be the access system or another entity that is responsible for users' authentication. It depends on the specific enforcement of the system. The authentication phase proceeds as follows:

1) (U_i) **access request sending**: U_i sends a request to the verifier V wants to access file f.
2) (V) **attribute requirement embedding**: In this step, the verifier embeds a secret key K_s and the attribute requirements in an attribute tree and sends related parameters to U_i. The details are as follows:
   Once V receives the access request, it retrieves the access policy related to the requested access and file f. Next, V will generate an attribute tree Γ with root value $\alpha_r \in \mathbb{Z}_p^*$ for root r to represent the access requirement as described in [18]. The same as in [23], we use $q_{Node}()$ to denote the polynomial bound to an interior node $Node$. For a leaf node y whose parent is interior node $Node$, $q_y(0)$ is computed by $q_{Node}(0)$. Thereafter, the verifier computes
   $$\begin{aligned} K_s &= (e(f_0, w_0)e(g_1, w_d))^{\alpha_r} \\ &= e(g_1, g_1)^{(x_0+x_d)\alpha_r/\beta_0}. \end{aligned}$$
   Let $L(\Gamma)$ be the leaf node set of the attribute tree Γ. V computes $\forall y \in L(\Gamma), C_y = g_1^{q_y(0)}$ and $C'_y = H(y)^{q_y(0)}$ and sends $\{\Gamma, g_1^{\alpha_r}, \forall y \in Leaf(\Gamma) : C_y, C'_y\}$ to U_i.
3) (U_i) **signature generation**: In this step, U_i recovers the embedded secret key K_s as K_v first if it owns all the required attributes. Next it generates a signature as a proof that it possesses the required attributes and to provide traceability, which means that an opener can trace the identity information of U_i given this signature.
   The details are as follows. Assume U_i possesses all the required attributes represented by attribute tree Γ and att_{ik} owned by U_i is the attribute related to leaf node y in attribute tree Γ. After U_i receives the message from V, it computes
   $$\begin{aligned} &DecryptNode(T_{i,k}, C_y, C'_y, y) \\ &= \frac{e(T_{i,k}, C_y)}{e(apk_j apk_{dj}, C'_y)} \\ &= e(g_1, g_1)^{(x_0+x_d+u_k)q_y(0)/\beta_0}. \end{aligned}$$
   If x is an interior node, $DecryptNode(T_{k,j}, C_y, C'_y,$ $y)$ proceeds as follows: for all x' children z, $DecryptNode(T_{k,j}, C_y, C'_y, y)$ is called and the output is stored as F_z. Assume S_x is the subset of all x's children z and $ind(x)$ is the index of node x. We

define

$$\Delta_{S_x,ind(z)} = \prod_{l \in \{S_x - ind(x)\}} \frac{l}{ind(z) - l}.$$

Then we have

$$\begin{aligned}F_x = &\prod_{z \in S_x} F_z^{q_z(0)\Delta_{S_x,ind(z)}} \\ = &\prod_{z \in S_x} (e(g_1, g_1)^{(x_0+x_d+x_i)q_z(0)/\beta_0})^{\Delta_{S_x,ind(z)}} \\ = &\prod_{z \in S_x} (e(g_1, g_1)^{(x_0+x_d+x_i)q_{par(z)}(ind(z))/\beta_0})^{\Delta_{S_x,ind(z)}} \\ =&e(g_1, g_1)^{(x_0+x_d+x_i)q_x(0)/\beta_0}.\end{aligned}$$

U_i calls $DecryptNode(T_{i,k}, C_y, C'_y, y)$ for the root and gets the result

$$F_r = e(g_1, g_1)^{(x_0+x_d+x_i)\alpha_r/\beta_0}.$$

Next U_i computes

$$K_s = F_r/e(g_1^{x_i}, g_1^{\alpha_r}) = e(g_1, g_1)^{(x_0+x_d)\alpha_r/\beta_0} = K_v.$$

Until here, U_i has successfully recovered the embedded secret key K_s as K_v. In the following, U_i generate a signature to provide traceability.
The signer randomly selects ζ, α, β, r_ζ, r_α, r_β, r_x, r_{δ_1}, $r_{\delta_2} \in \mathbb{Z}_p^*$ and calculates

$$\begin{aligned}&C_1 = u^\zeta, C_2 = v^\beta, C_3 = A_i h^{\zeta+\beta}, \\ &\delta_1 = x_i\zeta, \delta_2 = x_i\beta, \\ &R_1 = u^{r_\zeta}, R_2 = v^{r_\beta}, R_4 = C_1^{r_x} u^{-r_{\delta_1}}, R_5 = C_2^{r_x} v^{-r_{\delta_2}}, \\ &R_3 = e(C_3, g_1)^{r_x} e(h, w_d)^{-r_\zeta - r_\beta} e(h, g_1)^{-r_{\delta_1} - r_{\delta_2}}, \\ &c = H_{K_s}(M, C_1, C_2, C_3, R_1, R_2, R_3, R_4, R_5) \in \mathbb{Z}_p^* \\ &s_\zeta = r_\zeta + c\zeta, s_\beta = r_\beta + c\beta, s_\alpha = r_\alpha + c\alpha, \\ &s_x = r_x + cx_i, s_{\delta_1} = r_{\delta_1} + c\delta_1, s_{\delta_2} = r_{\delta_2} + c\delta_2.\end{aligned}$$

Finally, the signer sends the signature $\sigma =< M, C_1, C_2, C_3, c, s_\zeta, s_\beta, s_\alpha, s_{\delta_1}, s_{\delta_2} >$ to the verifier.

4) (V) **signature verification**: V computes

$$\begin{aligned}R'_1 =&u^{s_\zeta} C_1^{-c}, R'_2 = v^{s_\beta} C_2^{-c}, R'_4 = u^{-s_{\delta_1}} C_1^{s_x}, R'_5 = v^{-s_{\delta_2}} C_2^{s_x}, \\ R'_3 =&e(C_3, g_1)^{s_x} e(h, w_d)^{-s_\zeta - s_\beta} e(h, g_1)^{-s_{\delta_1} - s_{\delta_2}} (\frac{e(C_3, w_d)}{e(g_1, g_1)})^c\end{aligned}$$

and $c' = H_{K_v}(M, C_1, C_2, C_3, R'_1, R'_2, R'_3, R'_4, R'_5)$. If c' equals to c that V has received from U_i, V believes that U_i owns the required attributes and the authentication succeeds.

5) **(The opener) signature opening**: The opener computes $A_i = C_3/(C_1^{\varepsilon_1} C_2^{\varepsilon_2})$, where A_i was registered in the opener's database as U_i's identity information during system setup.

C. Group operations

As described in Section II-B, Bob needs to read patients' personal and medical information, but Cara only needs to have access to patients' medical records. To achieve this goal, we first express these access policies based on attributes. When group members want to access the documents, they generate a signature based on the required attributes defined in the access policies. If their signature is valid, we believe that they satisfy the access policies and will be granted with the required access.

In addition, Dean needs to revoke this temporary group and the privileges granted to group members during this workload. There are two possible solutions. The first solution is to combine all keys generated for this temporary workload with a time token, but it requires a precise estimation about the time period how long this task will last. If the time period is too short, all keys will be revoked before the task is finished and the system has to be set up again. To the contrary, if the time period is too long, group members will still be able to access to patients' documents after the task is completed, which may cause security and privacy problems. The second solution is too add the temporary attribute public keys in a revocation list. Before signature verification, the verifier firsts check whether the related attribute public keys are valid. If not, the verifier will abort the signature verification, and group members will not gain additional access privileges when the temporary task finishes.

D. Security requirement analysis

Since our proposed model is a specific application of the general attribute-based HABA scheme from [23], it follows the same correctness and security requirements of the attribute-based HABA scheme. Hence we can draw the conclusion that the ABGA scheme proposed in this paper is correct. Meanwhile, it also provides anonymity and traceability. From the description from [23], we know that once an ABA scheme is fully anonymous and traceable, it also provides the security requirement of unlinkability, unforgeability and coalition resistance. These three security requirements are provided by the ABA scheme proposed in Section III.

- **Unlinkability**: Only the group manager (Dean) has the capability of revoking and discover the signers identity. This ensures that an adversary can not trace any member of the team because he or she unable to establish linkage between identities and attribute sets.
- **Unforgeability**: To get an access to EHRs, any member of the team must gain an attribute key from the team manger. Without this key, he or she will not be able to access EHRs. Therefore, an adversary cannot impersonate a group member unless he or she was assigned by the group manager.
- **Coalition resistance**: As mentioned earlier, users in the group cannot pile up their attributes to generate a signature. Therefore, they cannot conclude and cheat the system to get authenticated if a single user does not possess the required attributes.

IV. Conclusions and further work

In this work, an authorization scheme was proposed for collaborative healthcare system to address the problem of information sharing and information security. The proposed scheme provides an efficient solution to security challenges related to authorization. The security analysis has showed that our proposed scheme is unforgeable, coalition resistant, and traceable.

In the future, the plan is to develop and prototype the functionality to be implemented as well as evaluate the validity of the scheme based on its efficiency and practicality. Efficiency is the scheme's performance in terms of resource consumption, e.g., time and computational capability. Practicality denotes the possible difficulties in managing the model during actual implementation. The motivation behind studying the issue of efficiency and practicality is to simplify decentralized administrative tasks, and enhance the practicability of authorization in dynamic collaboration environments. It is very important to design system to not only ensure shared information confidentiality but also to avoid administration and management complexity.

EU countries are seeking new ways to modernize and transform their healthcare systems using information and communications technology in order to provide EU citizens (patients) with safe and high quality treatment in any European Union country [24], [25] (EU directive 2011/24/EU framework on cross-border health care collaboration in the EU [26], [27], [28]). The proposed scheme will be further investigated towards cross-border healthcare collaboration. The plan is to evaluate the validity of the scheme to provide solutions to improve healthcare quality, provide access to a high-quality healthcare system to all EU citizens around Europe, and support close cooperation between healthcare professionals and care providers from different organization.

ACKNOWLEDGMENT

The authors would like to thank Geir M. Køien for the support in investigating and writing this work.

REFERENCES

[1] N. Menachemi and T. H. Collum, "Benefits and drawbacks of electronic health record systems," Risk management and healthcare policy, vol. 4, 2011, p. 47.

[2] M.-H. Kuo, "Opportunities and challenges of cloud computing to improve health care services," Journal of medical Internet research, vol. 13, no. 3, 2011, p. e67.

[3] R. Wu, G.-J. Ahn, and H. Hu, "Secure sharing of electronic health records in clouds," in Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2012 8th International Conference on. IEEE, 2012, pp. 711–718.

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

[5] S. Silow-Carroll, J. N. Edwards, and D. Rodin, "Using electronic health records to improve quality and efficiency: the experiences of leading hospitals," Issue Brief (Commonw Fund), vol. 17, 2012, pp. 1–40.

[6] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," Information Systems, vol. 48, 2015, pp. 132–150.

[7] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 1, 2013, pp. 131–143.

[8] O. Moonian, S. Cheerkoot-Jalim, S. D. Nagowah, K. K. Khedo, R. Doomun, and Z. Cadersaib, "Hcrbac–an access control system for collaborative context-aware healthcare services in mauritius," Journal of Health Informatics in Developing Countries, vol. 2, no. 2, 2008.

[9] M. Abomhara, M. Gerdes, and G. M. Køien, "A stride-based threat model for telehealth systems," Norsk informasjonssikkerhetskonferanse (NISK), vol. 8, no. 1, 2015, pp. 82–96.

[10] K. T. Win, "A review of security of electronic health records," Health Information Management, vol. 34, no. 1, 2005, pp. 13–18.

[11] D. Patra, S. Ray, J. Mukhopadhyay, B. Majumdar, and A. Majumdar, "Achieving e-health care in a distributed ehr system," in e-Health Networking, Applications and Services, 2009. Healthcom 2009. 11th International Conference on. IEEE, 2009, pp. 101–107.

[12] S. de Lusignan, F. Mold, A. Sheikh, A. Majeed, J. C. Wyatt, T. Quinn, M. Cavill, T. A. Gronlund, C. Franco, U. Chauhan et al., "Patients online access to their electronic health records and linked online services: a systematic interpretative review," BMJ open, vol. 4, no. 9, 2014, p. e006021.

[13] S. J. Dwyer III, A. C. Weaver, and K. K. Hughes, "Health insurance portability and accountability act," Security Issues in the Digital Medical Enterprise, vol. 72, no. 2, 2004, pp. 9–18.

[14] R. S. Sandhu and P. Samarati, "Access control: principle and practice," Communications Magazine, IEEE, vol. 32, no. 9, 1994, pp. 40–48.

[15] M. A. Valentine and A. C. Edmondson, "Team scaffolds: How mesolevel structures enable role-based coordination in temporary groups," Organization Science, vol. 26, no. 2, 2015, pp. 405–422.

[16] N. Meslec and P. L. Curşeu, "Are balanced groups better? belbin roles in collaborative learning groups," Learning and Individual Differences, vol. 39, 2015, pp. 81–88.

[17] M. Abomhara and G. M. Køien, "Towards an access control model for collaborative healthcare systems," in proceedings of the 9th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2016), vol. 5, 2016, pp. 213–222.

[18] H. Yang and V. A. Oleshchuk, "A dynamic attribute-based authentication scheme," in Codes, Cryptology, and Information Security. Springer, 2015, pp. 106–118.

[19] ——, "An efficient traceable attribute-based authentication scheme with one-time attribute trees," in Secure IT Systems. Springer, 2015, pp. 123–135.

[20] T. Okamoto, "Cryptography based on bilinear maps," in Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2006, vol. 3857, pp. 35–50.

[21] R. Sahu and S. Padhye, "Efficient ID-based signature scheme from bilinear map," in Advances in Parallel Distributed Computing, ser. Communications in Computer and Information Science. Springer Berlin Heidelberg, 2011, vol. 203, pp. 301–306.

[22] Y. Qin, D. Feng, and X. Zhen, "An anonymous property-based attestation protocol from bilinear maps," in 2009 International Conference on Computational Science and Engineering (CSE '09), vol. 2, Aug 2009, pp. 732–738.

[23] H. Yang and V. A. Oleshchuk, "Traceable hierarchical attribute-based authentication for the cloud," in Communications and Network Security (CNS), 2015 IEEE Conference on. IEEE, 2015, pp. 685–689.

[24] D. Byrne, Enabling Good Health for All : A Reflection Process for a New EU Health Strategy. Commission of the European Communities, 2004.

[25] M. Wismar, W. Palm, J. Figueras, K. Ernst, E. Van Ginneken et al., "Cross-border health care in the european union: mapping and analysing practices and policies." Cross-border health care in the European Union: mapping and analysing practices and policies, 2011.

[26] E. Commission, "Expert panel on effective ways of investing in health: Cross-border cooperation," 2015. [Online]. Available: http://ec.europa.eu/health/expert_panel/opinions/docs/009_crossborder_cooperation_en.pdf

[27] ——, "Overview of the national laws on electronic health records in the eu member states and their interaction with the provision of cross-border ehealth services," EU Health Programme (2008-2013), 2013. [Online]. Available: http://ec.europa.eu/health/ehealth/docs/laws_report_recommendations_en.pdf

[28] I. Passarani, "Patient access to electronic health records," Report of the eHealth Stakeholder Group, 2013. [Online]. Available: http://ec.europa.eu/health/expert_panel/opinions/docs/009_crossborder_cooperation_en.pdf