Collaborative and Secure Sharing of Healthcare Records Using Attribute-Based Authenticated Access

Mohamed Abomhara

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

Huihui Yang

NISlab and CCIS
Norwegian University of Science and Technology
Gjøvik, Norway
Email: huihui.yang@ccis.no

***Abstract*—The electronic health records are a widely utilized system in electronic health. It offers an efficient way to share patient health records among those in the medical industry, such as physicians and nurses. The barrier that currently overshadows the effective use of electronic health records is the lack of security control over information flow where sensitive health information is shared among a group of people within or across organizations. This study highlights authorization matters in cooperative engagements with complex scenarios in the collaborative healthcare domain. The 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, we first investigate and gain a deep understanding of insider threat problems in the collaborative healthcare domain. Second, 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, which, is a way to authenticate users by attributes or their properties. Finally, we evaluate the security of the proposed scheme to ensure our proposed scheme is unforgeable, coalition resistant, and traceable as well as it providers confidentiality and anonymity.**

Keywords–Healthcare; Access control; Authorization; Collaboration environments; Attribute based authentication.

I. INTRODUCTION

The electronic health records (EHRs) [1], [2], [3] is a widely utilized application in healthcare sector. It offers an efficient way to share patient health records among those in the medical industry, such as physicians and nurses. Here, patient data is captured over time and electronically stored in databases to enable secure and reliable access. EHRs are highly beneficial to end users and health providers alike. Advances in EHRs systems will likely reduce the cost of care by facilitating easy collaborative support from multiple parties to fulfill the information requirements of daily clinical care [4], [3], [5]. Patient and healthcare providers can cooperate continuously with one another to attain health services at lower prices [6], [7]. In addition, enhancing the quality and delivery of health services by giving healthcare providers access to information they require to provide rapid patient care [1], [3]. 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 [1], [8], [9]. Moreover, collaboration among healthcare organizations is required for patients being transferred from one healthcare provider to another for specialized treatment [10], [11].

Although EHRs systems may improve the quality of healthcare, the digitalization of health records, the collection, evaluation and provisioning of patient data, and the transmission of health data over public networks (the Internet) pose new privacy and security threats [5], [12], [13] such as data breaches and healthcare data misuse, leaving patients and healthcare providers vulnerable to these threats. 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.

The patient health record is a sensitive collection of information that calls for appropriate security mechanisms to ensure confidentiality and protect integrity of data as well as filter out irrelevant information to reduce information overload [14], [15]. According to the Health Information Portability and Accountability Act (HIPAA) [16], [17], the keepers of health records are required to take the necessary steps needed to protect the confidentiality, integrity and privacy, among others, of the patient health records [18]. As a result, ensuring confidentiality and protect integrity of data in EHR systems with proper authorization control has always been viewed as a growing concern in the healthcare industry.

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. 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.

A. Access Control Mechanism

Access control enables determining if the person or object, once identified, is permitted to access the resource. As shown in Figure 1, access control is a combination of authentication and authorization processes aimed at managing and securing access to system resources while also protecting resources' confidentiality and integrity, among others.

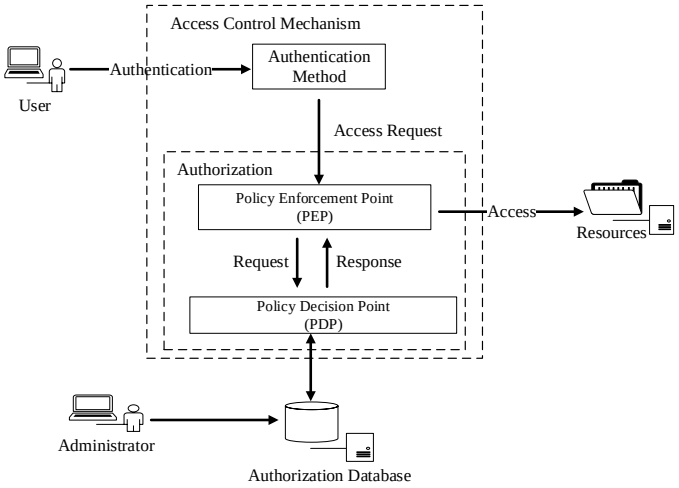


Figure 1. Authorization mechanism

Authentication entails validating the identity establishment between two communicating parties, showing what or who the user is? Authorization checks if the user can access the resources he/she has requested or not. When a user requests an access to resource on the system, first, the user has to authenticate himself/herself to the system, then the authorization process decides on the access request to be permitted or denied based on the authorization policies. The policy enforcement point (PEP) (Figure 1) intercepts a user's request to access a resource. The PEP forwards the request to the policy decision point (PDP) to obtain the access decision (permit or deny). PEP then acts on the received decision. The PDP is used to evaluate access requests against authorization policies and makes decisions according to the information contained in the request before issuing access decisions [19].

In the literature, two main access control models have been developed: role-based access control (RBAC) [20] and attribute-based access control (ABAC) [21]. RBAC allows organizations to enforce access policies based on user' roles (job functions) rather than users or groups [10]. RBAC promotes the management of related permissions instead of individual ones. The sets of permissions are compiled under a particular role. Consequently, all permissions are managed based on the role itself. Any changes in the permission within the role will impact the subjects who are assigned the corresponding role. In ABAC [21], permissions to access the objects are not directly given to the subject. It uses attributes of the subject (e.g., name, age or role in organization) and attributes of object (e.g., metadata properties) to provide authorizations as shown in Figure 2. The permissions in ABAC depend on a combination of a set of attributes and their relative values [22]. When a user wants to access an object, it sends an access request to the system with its attributes. PDP receives the request from PEP and combines the user's attributes, the object's attributes and environmental conditions (e.g., time and location), then check if they satisfy the authorization policies (Figure 2). If so, the subject's access request will be allowed and it will be enforced by the PEP [23]. During the process described above, PDP's decision making part can be considered as a part of authentication, while the authorization policy enforcing part by PEP be can considered as authorization.

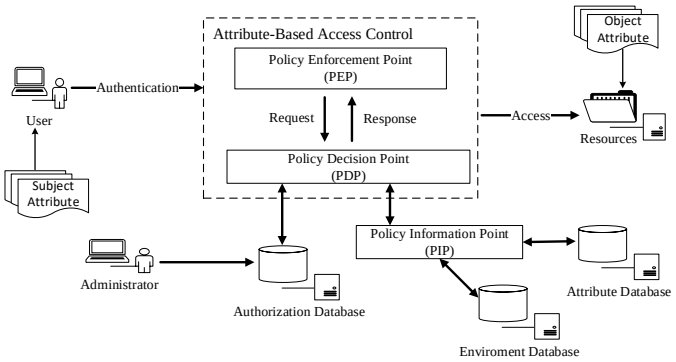


Figure 2. Access control mechanism for ABAC

To combine the strengths of both approaches without being hindered by their limitations, we proposed the work-based access control (WBAC) model [10], [24], [25], [26]. WBAC model is proposed by introducing the team role concept and modifying the user-role assignment model from RBAC and ABAC. The main goals of WBAC are flexibility, easy manageability, security, as well as suitability to support cooperative work of dynamic teams in healthcare environments [25]. In the proposed model, a secondary RBAC layer, with extra roles extracted from team work requirements, is added to RBAC and ABAC Layers to manage the complexity of cooperative engagements in the healthcare domain. Policies related to collaboration and team work are encapsulated within this coordinating layer to ensure that the attribute layer is not overly burdened. In this study, focus is mainly on authentication using attribute-based authentication (ABA) [27], [23], [28], [29]. We propose an authentication scheme using ABA to authenticate users by attributes or their properties.

ABA is part of ABAC and the authentication result of ABA is an important factor to decide whether a user's access request can be enforced or not. ABA is used as an approach to authenticate users by their attributes, so that users can get authenticated anonymously and their privacy can be protected [28]. Since there have already been lots of research on the cryptographic construction of attribute-based signatures (ABS) [30], [31] and attribute-based encryption (ABE) [32], it must be a good choice to utilize these results to construct ABA schemes for for collaborative healthcare systems.

B. Study Contribution

The main contribution of this work are as follows:

1) Investigate and gain a deep understanding of collaborative healthcare environment and insider security threats associated with it.
2) 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.
3) Evaluate and analysis the security of the proposed model.

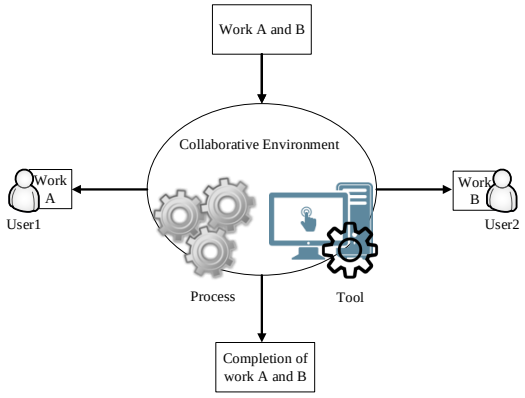


Figure 3. Collaborative environment and work sharing

C. Structure of the Study

The remaining parts of this study are organized as follows. In Section II, a brief description of the collaboration environment and insider threats in healthcare is presented. An overview of the EHRs systems architecture and usage scenario are provided in Section III. Security assumption and requirements are given in Section IV. Section V presents the proposed scheme. Security analysis is provided in Section VI. Finally, conclusions and aspects for future work are given in Section VII.

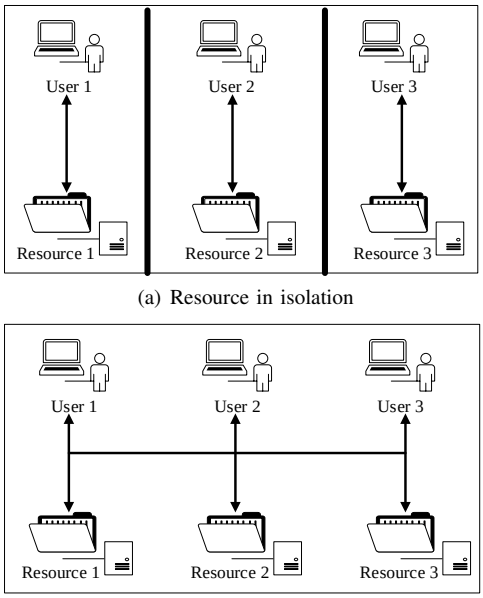
II. Background Knowledge

In this section, relevant work related to the study is reviewed. An overview of healthcare collaboration environment is presented, followed by a brief summary of the insider threat problem in the healthcare domain is highlighted. The main aim of this section is to understand the security requirements and propose an attribute-based group authorization model that ensures sufficient security, which strikes a balance between collaboration and safeguarding sensitive patient information.

A. Collaborative Environment

A collaborative environment is a virtual infrastructure that allows individuals to cooperate with greater ease to perform their duties. It provides the necessary processes and tools to promote teamwork among individuals with similar goals [33]. For example, work can be divided amongst the team and performed separately (Figure 3). Afterwards, the outcome of each individual is assembled into a cohesive whole.

Collaboration at a medical facility is an integral part of the work process, whereby experts with different specializations and backgrounds must contribute together as a group in order to ensure treatment success. This necessity is further amplified with the increasing complexity of the medical domain. Healthcare services necessitate collaborative support from multiple parties to fulfill the information requirements of daily clinical care and provide rapid patient care. Collaborative support is required within healthcare organizations such as hospitals, where patient records must be moved among healthcare professionals, laboratories and wards, to name a few [10]. Collaboration among healthcare organizations is also essential for patients being transferred from one healthcare provider to another for specialized treatment. Such collaboration within or among



(a) Resource in isolation

(b) Resource sharing in collaborative environment

Figure 4. Resource in isolation and resource sharing

healthcare organizations has been shown to provide cost-effective healthcare services [10]. EHRs improve how people work and enables more fluent cooperation between personnel at a medical facility. To cite an example, collaborative medical imaging [34] demonstrates the importance of sharing between medical practitioners. It utilizes cloud computing to provide a repository of medical imaging for physicians to discuss, diagnose and treat a particular disease effectively as a team.

One of the key aspects of a collaborative environment is the sharing of resources. To cooperate, each team member must be prepared to gather and share their findings with the rest of the team members. In Figure 4, initially each individual is accessing their own resource in isolation (Figure 4(a)). However, once collaboration is established, the process of sharing transpires (Figure 4(b)). Resource sharing is vital in collaboration. In order to analyze, decide and solve a certain problem collaboratively, team members must have similar knowledge of the defining situation. This way, cooperation can be achieved without the aggravating friction. However, balancing between collaboration and security of shared information is difficult. On the one hand, collaborative systems are targeted towards making all system elements (i.e., hardware, software, data, humans, processes) available to all who need it. On the other hand, security seeks to ensure the availability, confidentiality, and integrity of these elements while providing them only to those with proper authorization. Therefore, avoiding security and privacy violation are very important while sharing resources with others [10], [35].

B. Insider Threats

Although a collaborative environment can help enhance healthcare quality, it may also render the shared resources more vulnerable to insider threats [36], [37], [38]. This happens when someone within the collaborative team accesses shared resources for unethical reasons, for instance accessing a patient's private information for personal gain. In Figure 5,

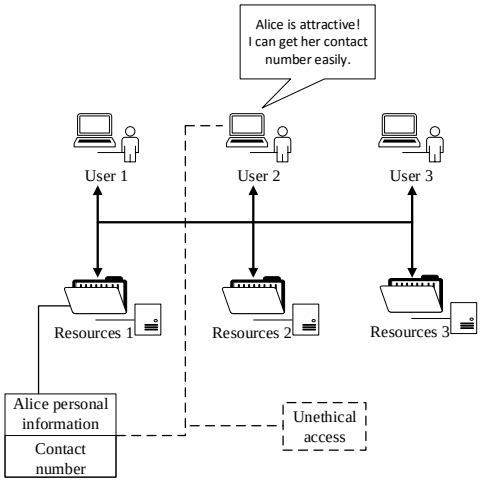


Figure 5. Insider Threat during collaboration

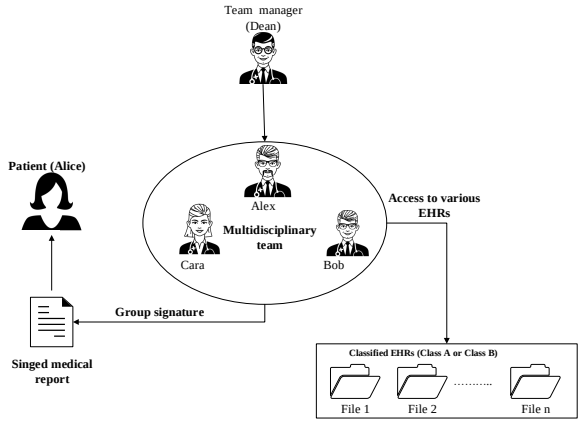


Figure 6. An example scenario of collaboration and sharing of healthcare data

it is assumed that three physicians are working collaboratively on a case at the hospital. They are discussing the possible treatment for a patient named *Alice*. To do so, they must analyze her medical file, but not her personal information. However, the 2^{nd} physician is attracted to the patient. He exploits the collaborative environment to obtain her contact number without permission.

Insider threats pose a serious concern in the healthcare industry. In 2015, it was reported [39] that 35.5% of documented breaches involved medical counterparts. It is the second highest category in comparison. Breaches include stealing protected health information for later use to launch numerous fraud attacks on related medical parties. The danger with insider threats that occur due to the collaborative effort in healthcare is their low detectability. In other words, an incident could happen repeatedly over an extended period of time without being discovered by authorities. Actual attacks on victims can therefore be attempted at any time, which makes the threat harder to combat. Given the severity of insider threats within the healthcare sector, a number of countermeasures have been developed. These measures can be divided into two main categories: passive and active [36], [40], [41]. Passive measures are more geared toward detecting the perpetrators while active measures protect targeted assets from being compromised altogether.

To begin insider threat analysis, applying a framework can be quite useful [42], [43]. Insider threats are analyzed from four main aspects: the catalyst that can lead to an attack, the actor, the attack and the organization characteristic. These aspects can provide authorities with a method of formalizing the dominant patterns in an attack. Authorization and access control are the most popular approaches for developing an active form of mitigating insider threats [44], [10], [45], [46]. For instance, in order to secure a shared repository on epidemics, the group-based discretionary access control [47] is employed. It allows certain individuals to access the data and prohibits others based on their group membership.

III. Electronic Health Records

Healthcare providers deal with large number of sensitive healthcare records, which are shared and collaboratively used among different healthcare practitioners [8]. Collaboration occurs when a healthcare provider such as primary care doctor requests help from another healthcare provider to treat a case. To better understand collaborations in the healthcare domain, in this section, we present a usage scenarios provide examples of collaboration and healthcare data sharing, followed by the EHRs system architecture.

A. Usage Scenario: Multiple Healthcare Practitioners Cooperation Among Multiple Healthcare Organizations

As shown in Figure 6, a typical use case scenario adopted from [4] is presented. 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 8). *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 8), 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) [16] minimal disclosure principle.

In such group consultation, also so-called multidisciplinary team consultation [48], [49], [50], it is noticeable that, several healthcare professionals are involved in various roles to provide patient care. That includes primary care doctors, general physicians and specialists. Every participant needs to obtain the medical records they request based on HIPAA [16] minimal disclosure principle [4], [8]. In this case, the act of managing the collaborative work must be clearly defined. By default, only the main practitioner should be aware of the patient's personal information. The other medical practitioners with supporting roles are given information based on their

contributing roles (need-to-know principle) [51]. 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.

Hospital personnel roles are often simplistically split into medical practitioners, nurses and administrators [52], [53]. However, in [10], we further categorized personnel roles into a total of nine roles per group, which are classified into main, action, thought and management roles, as shown in Figure 7.

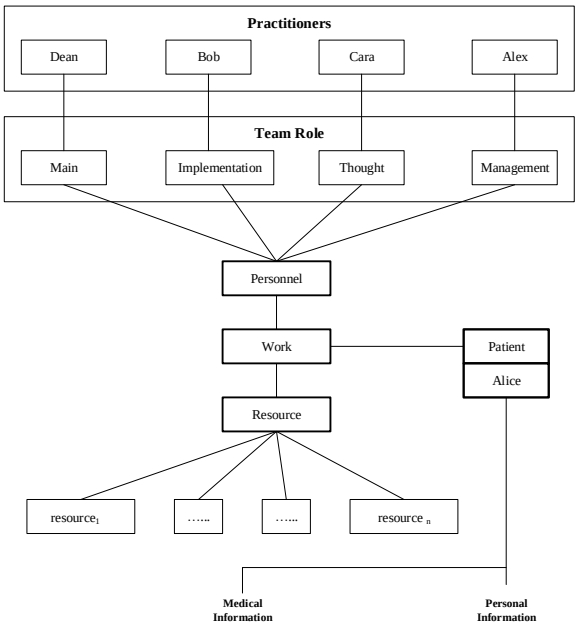


Figure 7. EHRs usage scenario

The workflow of every healthcare practitioner is as follows:

1) The general practitioner (*Dean*) could not solve *Alice*'s case. He invites multidisciplinary team including *Bob*, *Cara* and *Alex* to help. In this team consideration, *Dean* is the core physician of the collaborative work. He 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. This implies that his possesses the main team role (Figure 7). In other words, he owns the collaborative work initiated. Therefore, full access is given to *Dean* with regard to the information related to the patient. He can access the personal information of the patient as well as the medical records. Moreover, the general practitioner must revoke the team 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. It must be reminded however, that access to a collaborative resource can be tailored more specifically by harnessing the stipulated team roles. *Bob* is involved in the action part of the collaboration. Therefore, his team provider falls under the category of action.
3) *Cara* has more of a thought 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 team) of specialists and practitioners do not have to have access. In WBAC, we assume that each resource (EHR files) in the system are divided into two types, mainly *private* and *protected* during the collaborative work. The collaborative resources required for work are enumerated in Table form as proposed by Abomhara and Køien in [10]. Each 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.

B. EHRs Systems Architecture

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 and nurses, among others, who require access to these EHRs to perform a task. In Figure 8, 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 [54]. Authorized healthcare providers, including hospitals and healthcare practitioners can access EHRs through different services such as web portals and health apps [55]. In WBAC, we assumed that all the medical records covered by WBAC are classified into two sets of objects (*private* and *protected*) listed in the permissions that are assigned to roles and team roles, which will be accessed by a users.

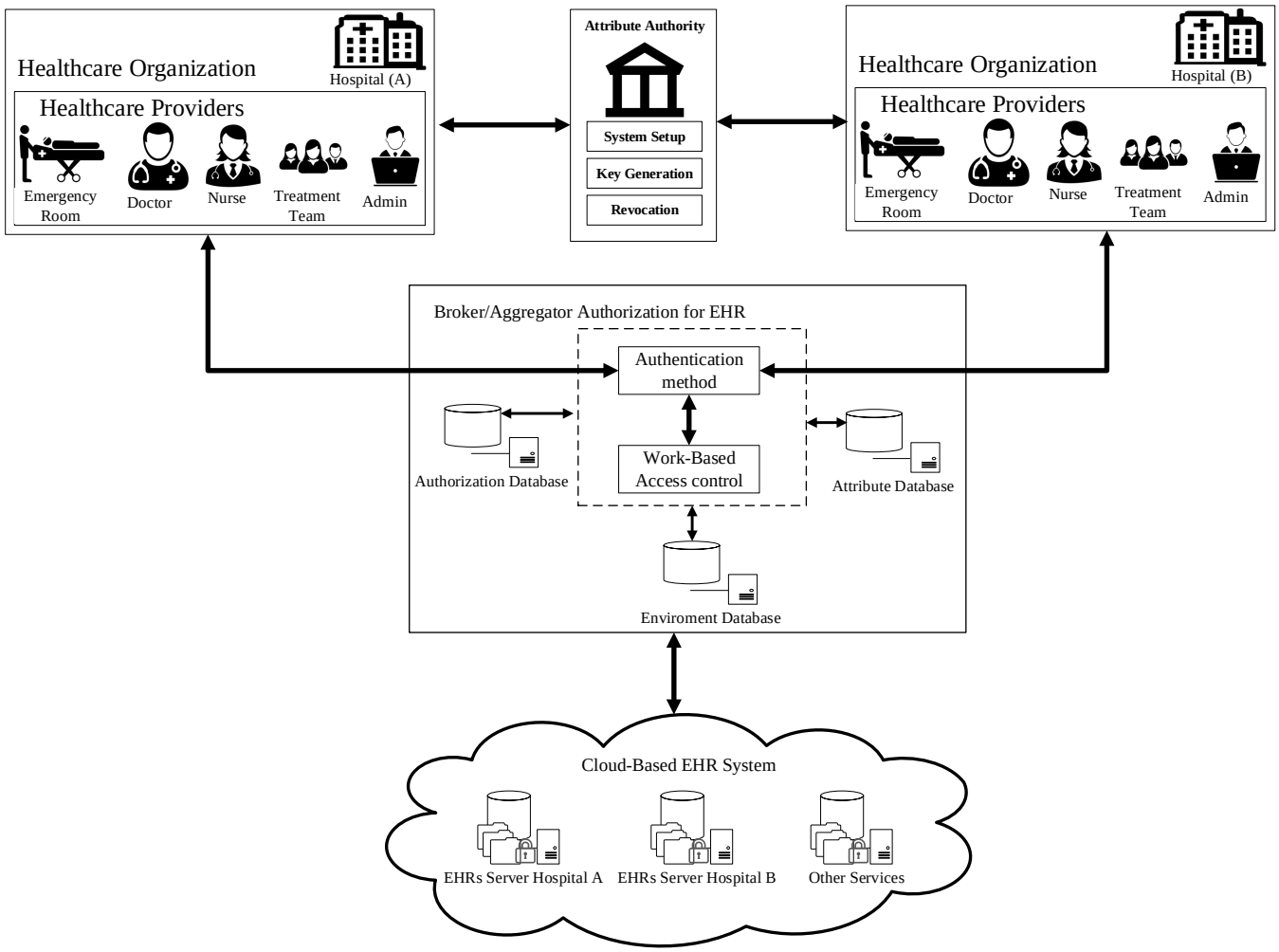


Figure 8. Reference system architecture overview

a) $Private$ object contains medical records related to personal information such as names and addresses as well as resources that are not related to the current patient case such as family medical history and sexual health, among others.
b) $Protected$ object contains resources related to current patient case. For example, consider *Alice*'s case (Section III-A), we could say that protected objects contains resources related to *Alice*'s current case such as past surgical history, data related to abdominal CT scan (computed tomography scan) and gastroscopy data, to name a few.

The access to medical records is controlled via the team roles and the requirements of attributes. For each medical records, the access policy is represented by a combination of attributes. When a user (healthcare providers who have already joined a team and assigned to team role) requires to access (read, write, etc) the file on EHRs, it should show an evidence that it satisfies the required attributes. Only if the evidence is valid, the user's access can be granted. This process will be implemented by an ABA scheme presented in Section V-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 to 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. As for implementation, it is possible to have different authorities to 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.

3) **Healthcare providers**: Healthcare providers from various domains, such as doctors, nurses, radiology technicians and pharmacists, among others, require access to patients' records to perform a task. Once a new healthcare practitioner joins 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.

IV. Security Assumption and Requirements

In this study, we consider the healthcare providers are honest and trusted but curious. That means, they will try to find as much as confidential and private information just for curiosity. Therefore, healthcare providers will try to access files on EHRs, which are beyond their privileges (i.g, healthcare providers intend to access the medical records that needed to fulfill their tasks but sometimes they intentionally or unintentionally access patients' medical records that are irrelevant to their task [56]). For example, as shown in Figure 5, a healthcare provider may want to obtain information about the patient for his/her own interest. To do so, healthcare provider may impersonate other healthcare provider. Also, healthcare provider may collude with other healthcare providers to gain an access to information. Thus to achieve a secure sharing of EHRs, a core requirements of a well-designed ABA system were presented by Yang [28], [29]. According to our assumption and usage scenarioa, the system should fulfill the following requirements:

- **Confidentiality**: Unauthorized users who do not possess enough attributes satisfying the authorization policy should be prevented from reading EHR documents.
- **Minimum attributes leakage**: To be authenticated, a 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.

V. 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 III-B), 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 [57], [58].

Definition 1: **[Bilinear Mapping]** [59] 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 key sets will be generated by the trusted authority. Based on the main private and public key sets, 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 [60]. 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 $\Psi_i = \{att_{i1}, \cdots, att_{iN_i}\}$ and 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 [28]. 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 [28]. The same as in [60], 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

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

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

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

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

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

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 III-A, *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 signatures are 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 after the workload is finished. 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 issues. The second solution is to 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.

VI. Security analysis

In this section, we analyze the security requirements of the proposed model based on the security analysis described in Section IV, including confidentiality, minimum attributes leakage, signature, unforgeability and coalition resistance.

Confidentiality: When a user U_i wants to read EHR documents, he should successfully be authenticated by the ABA scheme proposed in Subsection V-B. From [60], we know that our ABA scheme satisfies the security requirement traceability, which means that a user without the required attributes cannot generate a valid signature to successfully authenticated. As a result, as long as user U_i is required to pass the authentication described in Subsection V-B before he accesses EHR documents, the confidentiality can be satisfied.

Unforgeability: requires that a user outside the group (an outsider) cannot generate a valid signature in the ABA scheme proposed in Subsection V-B. We assume that an outsider does not possess any valid required attributes. From the analysis of confidentiality, we know that a valid user who does not possess all required attribute cannot generate a valid signature, so an outsider without any valid required attributes cannot generated a valid signature.

Coalition resistance: This security requirement is weaker than traceability, because it is one way to try to forge a valid signature that the opener cannot trace its identity. Assume that the ABA scheme proposed in Subsection V-B is not coalition resistant, it means that a couple of users can pile up their attributes and generate a valid signature. Since these attributes do not belong to the same user in the group and it is valid, the identity retrieved from the signature does not belong to any user in the group. It contracts with the security requirement traceability. Therefore, the ABA scheme proposed in Subsection V-B is coalition resistant.

Minimum attributes leakage: This security requirement is straight forward. To generate a valid signature, a user only needs to use the required attributes other than the whole package of attributes he possesses.

Signature: This property can be satisfied by requiring *Alice*'s practitioner to generate a signature using its attribute keys based on the ABA scheme proposed in Subsection V-B, where as the verifier, *Alice* can define the required attributes and therefore can check the validity of the signature. When necessary, the signature can also be identified by the opener in the system.

VII. Discussion and Conclusions

A. Discussion

The central trusted authority within the healthcare system sustains an EHRs data source of aggregated to ensure availability and to provide an easy access to the health professionals. However, accessing patient's health records raises patient concerns about the security of their data. This is because patients generally want to make sure that their sensitive information is accessed by authorized and trusted healthcare providers. As such, a health supplier needs to be sure that actual legal entity is the only party to grant access to the EHRs. Furthermore, patient permission must also be considered to create a EHRs accessibility role.

The goal of this study is to have attribute verification within a group of healthcare providers. The main purpose of our scheme is authenticating users by attributes or their properties to achieve security requirement (Section IV) including confidentiality, anonymity, traceability, unforgeability, coalition resistance and signature.

Confidentiality protects system resources and information from unauthorized disclosure. In our study, healthcare providers who join a team of treatment (e.g., *Cara* and *Alex*) should register themselves to obtain their authorization key from the trusted authority (Section V-A). Therefore, all the healthcare providers who join *Alice*'s treatment will be identified by the team manager (*Dean*) and authorized to access *Alice*'s EHRs once they obtain their authorization keys. An important concerns about user' identity are anonymity and traceability of healthcare provider's identity. In other words, the verifier cannot get any identifying information related to the user during the authentication process [23]. On the one hand, anonymity is important to keep a patient' privacy. For example, in our scenario (Figure 6), assume that *Alice* dose not need anyone to know that she was treated by a gastroenterologist (*Cara*). Therefore, keeping the identity of *Cara* anonymized is a very impotent aspect. On the other hand, tracing of healthcare providers' identities is of great importance. When disputes happen and the identify of the healthcare provider are treated as legitimate evidence, tracing of the identity is useful. The main purpose of our scheme is to achieve anonymity and allow tractability. Since our scheme is based on group signatures, it is traceable. In our ABA scheme the system tracing the signers' identity is done by the attribute authority (opener). The identity revealing can only be performed when a disputes happens and a legal authority should authorize it. There are two requirements for identity reveal [60], [23]. First, given a valid signature, the opener should be able to trace the signature and reveal the identity information. Second, the revealed identity should belong to real signer rather than a forged one.

Digital signature forgery is another concern when designing of ABA schemes. Forgeability is the ability to create a signature by illegitimate signer such as an adversary. Our proposed scheme ensures that, a user (healthcare provider or adversary) who does not possess all required attribute cannot generate a valid signature. It is said the scheme is strongly unforgeable if the signature is existentially unforgeable under chosen-message attack [61], [62] and, given signatures on some messages, the adversary cannot produce a new signature. In this study, we have not analyze our scheme against chosen-message attack. But we assume that it is unforgeable since the adversary need a number of required attributes to generate a valid signature.

Coalition attack is one of the most difficult tasks in developing a group signature, It occurs when a malicious collisions of group members that produce untraceable signatures [63]. Considering the coalition resistance, in our scheme the user can only generate the signature if he or she has all the required attributes. As we showed in security analysis (Section VI) it is not possible for different users to collude and generate a valid signature together if they as a whole have all the required attributes.

The security requirement "signature" is very important because it provides three properties. First of all, the signature should be able to be verified by *Alice* that it is generated by a legal practitioner according to *Alice*'s treatment requirements. This property can prevent the case that the signature was forged by an illegal practitioner or an adversary. Secondly, the practitioner can keep itself anonymous if he wants, and this property is provided by the security requirement anonymity of the ABA scheme proposed in Section V. Finally, the practitioner cannot deny that the signature was actually generated by him since there is an opener who can "open" the signature and retrieves the practitioner's identity, and this property is provided by the security requirement traceability of the proposed ABA scheme.

B. 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 as well as it providers confidentiality and anonymity.

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 a system to not only ensure shared information confidentiality but also to avoid administration and management complexity.

Furthermore, in recent years, cloud computing and information technology adaptation to healthcare has become increasingly important in many countries [7], [64]. 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 [65], [66] (EU directive 2011/24/EU framework on cross-border health care collaboration in the EU [67], [68], [69]). Access to cross-border healthcare in the EU has undergone many developments in both academia and industries in order to meet EU healthcare domain needs. The eHealth Action Plan 2012-2020 [70] and the EU-funded project UNIversal solutions in TELemedicine deployment for European HEALTH care (United4health) [71] are among such developments. The aim

of these projects is 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.

Therefore, in future, 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 typesetting this work.

REFERENCES

[1] M. Abomhara and H. Yang, "Attribute-based authenticated access for secure sharing of healthcare records in collaborative environments," in the Eighth International Conference on eHealth, Telemedicine, and Social Medicine (eTELEMED 2016), 2016, pp. 138–144, ISBN:978-1-61208-470-1.

[2] C. Bain, "The implementation of the electronic medical records system in health care facilities," Procedia Manufacturing, vol. 3, 2015, pp. 4629–4634.

[3] 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.

[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] 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.

[6] U. D. of Health, H. Services et al., "Expanding the reach and impact of consumer e-health tools," Washington, DC: US Department of Health and Human Services, Office of Disease Prevention and Health Promotion, 2006.

[7] 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.

[8] 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.

[9] 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," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, 2013, pp. 131–143.

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

[11] 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.

[12] M. Meingast, T. Roosta, and S. Sastry, "Security and privacy issues with health care information technology," in 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2006. EMBS'06. IEEE, 2006, pp. 5453–5458.

[13] A. Appari and M. E. Johnson, "Information security and privacy in healthcare: current state of research," International journal of Internet and enterprise management, vol. 6, no. 4, 2010, pp. 279–314.

[14] R. Gajanayake, R. Iannella, and T. Sahama, "Privacy oriented access control for electronic health records," electronic Journal of Health Informatics, vol. 8, no. 2, 2014, p. 15.

[15] B. Alhaqbani and C. Fidge, "Access control requirements for processing electronic health records," in Business Process Management Workshops. Springer, 2008, pp. 371–382.

[16] 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.

[17] K. E. Artnak and M. Benson, "Evaluating hipaa compliance: A guide for researchers, privacy boards, and irbs," Nursing outlook, vol. 53, no. 2, 2005, pp. 79–87.

[18] H. Bidgoli, Handbook of Information Security, Information Warfare, Social, Legal, and International Issues and Security Foundations. John Wiley & Sons, 2006, vol. 2.

[19] N. Li, Q. Wang, W. Qardaji, E. Bertino, P. Rao, J. Lobo, and D. Lin, "Access control policy combining: theory meets practice," in the 14th ACM symposium on Access control models and technologies. ACM, 2009, pp. 135–144.

[20] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed nist standard for role-based access control," ACM Transactions on Information and System Security (TISSEC), vol. 4, no. 3, 2001, pp. 224–274.

[21] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to attribute based access control (abac) definition and considerations," NIST Special Publication, vol. 800, 2014, p. 162.

[22] A. Ubale Swapnaja, G. Modani Dattatray, and S. Apte Sulabha, "Analysis of dac mac rbac access control based models for security," International Journal of Computer Applications, vol. 104, no. 5, 2014.

[23] H. Yang, "Cryptographic enforcement of attribute-based authentication," doctoral Dissertations at the University of Agder, 2016, ISBN: 978-82-7117-826-0.

[24] M. Abomhara, H. Yang, and G. M. Køien, "Access control model for cooperative healthcare environments: Modeling and verification," in IEEE International Conference on Healthcare Informatics 2016 (ICHI 2016), 2016.

[25] M. Abomhara and M. Ben Lazrag, "Uml/ocl-based modeling of work-based access control policies for collaborative healthcare systems," in IEEE 18th International Conference on E-health, Networking, Applications, and Services (IEEE Healthcom 2016), 2016, doi: 978-1-5090-3370-6/16.

[26] M. Abomhara and H. Nergaard, "Modeling of work-based access control for cooperative healthcare systems with xacml," in the Fifth International Conference on Global Health Challenges (GLOBAL HEALTH 2016), 2016, pp. 14–21, ISBN: 978-1-61208-511-1.

[27] D. Khader, "Attribute based authentication schemes," Ph.D. dissertation, University of Bath, 2009.

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

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

[30] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures," in cryptographers Track at the RSA Conference. Springer, 2011, pp. 376–392.

[31] J. Li, M. H. Au, W. Susilo, D. Xie, and K. Ren, "Attribute-based signature and its applications," in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM, 2010, pp. 60–69.

[32] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in the 5th ACM Symposium on Information, Computer and Communications Security. ACM, 2010, pp. 261–270.

[33] C. Shah, "A framework for supporting user-centric collaborative information seeking," in PhD Thesis. University of North Carolina, 2010, pp. 1–268. [Online]. Available: http://comminfo.rutgers.edu/~chirags/papers/Shah_Dissertation.pdf

[34] I. H. Arka and K. Chellappan, "Collaborative compressed i-cloud medical image storage with decompress viewer," Procedia Computer Science, vol. 42, 2014, pp. 114–121.

[35] K. Asif, S. I. Ahamed, and N. Talukder, "Avoiding privacy violation for resource sharing in ad hoc networks of pervasive computing environment," in Proceedings of the 31st Annual International Computer

Software and Applications Conference-Volume 02. IEEE Computer Society, 2007, pp. 269–274.

[36] C. W. Probst, J. Hunker, D. Gollmann, and M. Bishop, Insider Threats in Cyber Security. Springer Science & Business Media, 2010, vol. 49.

[37] Y. Chen, S. Nyemba, and B. Malin, "Detecting anomalous insiders in collaborative information systems," Dependable and Secure Computing, IEEE Transactions on, vol. 9, no. 3, 2012, pp. 332–344.

[38] Y. Chen, S. Nyemba, W. Zhang, and B. Malin, "Leveraging social networks to detect anomalous insider actions in collaborative environments," in Intelligence and Security Informatics (ISI), 2011 IEEE International Conference on. IEEE, 2011, pp. 119–124.

[39] ITRC, "Identity theft rsesource centre (itrc) data breach reports," 2015. [Online]. Available: http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf

[40] N. T. Nguyen, P. L. Reiher, and G. H. Kuenning, "Detecting insider threats by monitoring system call activity." in IAW. Citeseer, 2003, pp. 45–52.

[41] M. Kandias, N. Virvilis, and D. Gritzalis, "The insider threat in cloud computing," in Critical Information Infrastructure Security. Springer, 2011, pp. 93–103.

[42] J. R. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. Wright, and M. Whitty, "Understanding insider threat: A framework for characterising attacks," in Security and Privacy Workshops (SPW), 2014 IEEE. IEEE, 2014, pp. 214–228.

[43] M. B. Salem, S. Hershkop, and S. J. Stolfo, "A survey of insider attack detection research," in Insider Attack and Cyber Security. Springer, 2008, pp. 69–90.

[44] W. Tolone, G.-J. Ahn, T. Pai, and S.-P. Hong, "Access control in collaborative systems," ACM Computing Surveys (CSUR), vol. 37, no. 1, 2005, pp. 29–41.

[45] S. Alshehri, S. Mishra, and R. Raj, "Insider threat mitigation and access control in healthcare systems," 2013.

[46] C. E. Rubio-Medrano, C. D'Souza, and G.-J. Ahn, "Supporting secure collaborations with attribute-based access control," in Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on. IEEE, 2013, pp. 525–530.

[47] J. , D. Domingos, M. J. Silva, and C. Santos, "Group-based discretionary access control for epidemiological resources," Procedia Technology, vol. 9, 2013, pp. 1149–1158.

[48] C. Borrill, M. West, D. Shapiro, and A. Rees, "Team working and effectiveness in health care," British Journal of Healthcare Management, vol. 6, no. 8, 2000, pp. 364–371.

[49] C. Taylor, A. J. Munro, R. Glynne-Jones, C. Griffith, P. Trevatt, M. Richards, and A. J. Ramirez, "Multidisciplinary team working in cancer: what is the evidence?" BMJ, vol. 340, 2010, p. c951.

[50] P. Mitchell, M. Wynia, R. Golden, B. McNellis, S. Okun, C. E. Webb, V. Rohrbach, and I. Von Kohorn, "Core principles & values of effective team-based health care," Washington, DC: Institute of Medicine, 2012.

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

[52] 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.

[53] 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.

[54] 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.

[55] 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.

[56] Q. Wang and H. Jin, "Quantified risk-adaptive access control for patient privacy protection in health information systems," in Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. ACM, 2011, pp. 406–410.

[57] 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.

[58] 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.

[59] 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.

[60] 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.

[61] D. Boneh, E. Shen, and B. Waters, "Strongly unforgeable signatures based on computational diffie-hellman," in International Workshop on Public Key Cryptography. Springer, 2006, pp. 229–240.

[62] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," SIAM Journal on Computing, vol. 17, no. 2, 1988, pp. 281–308.

[63] G. Ateniese, M. Joye, and G. Tsudik, On the difficulty of coalition-resistance in group signature schemes. IBM Thomas J. Watson Research Division, 1999.

[64] M. Dekker, "Critical cloud computing-a ciip perspective on cloud computing services," Report of the European Network and Information Security Agency, 2012.

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

[66] 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.

[67] 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

[68] ——, "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

[69] 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

[70] E. Commission, "ehealth action plan 2012-2020 innovative healthcare for the 21st century," European Commission staff working document for informative purposes, 2012. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2012:0413:FIN:EN:PDF

[71] United4Health, "P7 eu project united4health 2013." [Online]. Available: Umbrellaproject:http://www.united4health.eu/;Norwegianproject:http://www.united4health.no/.