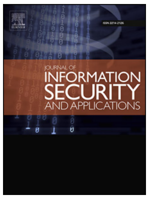
Journal of Information Security and Applications 37 (2017) 50–64

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa



# Attribute based access control scheme with controlled access delegation for collaborative E-health environments

Harsha S. Gardiyawasam Pussewalage*, Vladimir A. Oleshchuk

*Department of Information and Communication Technology, University of Agder, N-4898 Grimstad, Norway*

ARTICLE INFO

*Article history:*

*Keywords:*
Attribute based access control
Access delegation
Security
Electronic health records

ABSTRACT

Modern electronic healthcare (e-health) settings constitute collaborative environments with complex access requirements. Thus, there is a need for sophisticated fine-grained access control mechanisms to cater these access demands and thereby experience the full potential of e-health systems. In order to realize a flexible access control scheme, integrating access delegation is of paramount importance. However, access delegation has to be enforced in a controlled manner so that it will not jeopardize the security of the system. In this paper, we addressed this issue through proposing an attribute based access control scheme integrated with controlled access delegation capabilities. We demonstrate how the proposed scheme could function by considering a health information sharing scenario which constitutes a collaborative environment. The proposed scheme capable of provisioning multi-level access delegation with each delegating user having the capability of controlling further delegations by the delegatee. In addition, the scheme is also integrated with a mechanism to limit the total number of delegations allowable for a given attribute to accommodate for inappropriate user behaviors. Thus, users can claim access to resources by providing a proof that they possess attribute sets (attributes may or may not be delegated) that satisfy the relevant attribute based access policies which govern the access to the shared resources. The proposed scheme is also equipped with on-demand attribute revocation mechanism along with preventing attacks via attribute collusion. Furthermore, we have shown that the proposed access control scheme is secure and also exhibits superior delegation capabilities compared to the existing attribute based schemes coupled with access delegation capabilities.

## 1. Introduction

The healthcare industry has been experiencing a significant boost in the recent years due to the integration of sophisticated information and communication technologies (ICT). Advancement of technologies such as telecommunication, wearable computing, cloud computing, Internet of Things (IoT) allowed the possibility of providing healthcare services at an affordable price to its consumers with enhanced flexibility and patient outreach as well as improved care [1,2]. Along with this transition, more and more care deliverers upgraded the traditional paper based patient health records to electronic versions, in general denoted as electronic health records (EHR). Such records provide the platform for efficient sharing of patient health information among different healthcare settings and different care deliverers enabling wider reach and better service for the consumers. However, given that every EHR accumulates significant amount of private information over time it is evident that any sort of illegitimate disclosure may threaten one's life, social status as well as social stability [3]. According to the findings in [4,5], such security and privacy breaches have been escalating in an alarming rate, which is mainly caused by not paying enough attention to associated security and privacy issues when integrating technological innovation. Thus, it is of paramount importance to develop e-health systems with flexible information sharing while ensuring security and privacy of associated parties.

Access requirements in e-health environments are complex and diverse in nature. Typically, treatment process of a patient may require collaborative efforts of multiple parties including general practitioners, emergency staff members, specialists in the patient's home care provider as well as professionals from foreign care providers in certain situations [6,7]. Thus, such environments induce challenges with respect to access such as provisioning varying levels of authorization for different recipients, flexible inter-organizational health data sharing as well as controlled delegation of access for users who may or may not be known to the data owner.

[*] Corresponding author.
*E-mail address:* harsha.sandaruwan@uia.no (H.S. Gardiyawasam Pussewalage).

https://doi.org/10.1016/j.jisa.2017.10.004
2214-2126/© 2017 Elsevier Ltd. All rights reserved.

Access control mechanisms have been widely utilized for ensuring secure and restricted access for computer resources, especially in multi-user data sharing settings [8]. However, existing solutions developed based on the traditional access control schemes do not address all the aforementioned challenges sufficiently [9]. Among the traditional access control schemes, access control lists (ACL) [10] suffer significantly from the inability to scale when considering the requirements of multi-user healthcare systems. Role based access control (RBAC) schemes facilitate much more stronger access flexibility through incorporating contextual information along with user roles for access decision making [11–14]. One of the main issues with aforementioned RBAC solutions is that every user must be a registered entity in the system. Thus, it is infeasible to achieve seamless inter-organizational data sharing which is important in e-health settings. More recently, attributes driven methods received significant attention as a means of overcoming the associated bottlenecks in RBAC solutions. Existing attribute based solutions can be divided into two classes of solutions - attribute based encryption (ABE) driven schemes and attribute based access control (ABAC) driven schemes. ABE based schemes provide an elegant way of encrypting data according to an attribute set chosen by the encryptor which should be satisfied by the decryptor in order to have a successful decryption [15]. ABE based health information management schemes are presented in [7,16–18]. In general, solutions belonging to this class suffer from the inability to withstand for the access dynamism associated with e-health applications, especially considering the fact that such solutions need to modify the ciphertext when associated access structure is modified. This incurs a significant additional overhead to the system. In addition, the complex key management associated with ABE schemes makes integrating delegation capabilities hard to achieve in practice. ABAC, on the other hand is similar to RBAC in the sense that it is also a policy driven access control mechanism but it uses attributes of subject, object as well as the environmental attributes instead of organizational roles to make access decisions. Thus, ABAC facilitates inter-organizational data access forming the platform for realizing fine-grained, flexible access control mechanism [19]. However, ABAC is not yet formally standardized while a general guideline for ABAC implementations is published by National Institute of Standards and Technology (NIST) recently [20]. Given the versatility of ABAC, it has the potential to support flexible access control with controlled access delegation for dynamic e-health systems, but no notable efforts in this context are yet available.

Access delegation is a vital property for realizing flexible access control in collaborative e-health environments. For instance, consider a scenario where a cardiologist, Alice of hospital A wants to acquire some expert views from a cardiac surgeon, Bob who is residing in a different country regarding one of his patient's current condition. Further assume that the corresponding patient's EHR is associated with an attribute access structure $\mathcal{T} = (Cardiologist \wedge Hospital\_A)$ giving permission to cardiologists in hospital A to access the relevant EHR. With the presence of delegation capability, it is possible to temporarily delegate attributes *Cardiologist, Hospital_A* to Bob and grant him the access for the required EHR. Incorporating such delegating capability induces the following challenges which need to be taken into consideration. Suppose Alice possesses the attribute set $\omega_{Alice} = \{Director, Hospital\_A, Cardiologist\}$. During delegation, Alice may not want to delegate all her attributes to Bob while delegating the attributes *Cardiologist, Hospital_A* which are sufficient to satisfy $\mathcal{T}$. Another consideration would be Alice may or may not be interested in allowing Bob to further delegate the attributes. Suppose that Alice wants to delegate the attribute *Director* to Charlie for one week while she is on leave. However, she does not want Bob and Charlie to collude their delegated attributes to ascertain access to resources which are not possible on their own. We call the access delegation capability adhering to the aforementioned challenges as controlled access delegation. Revocation of attributes is also quite crucial for any ABAC system and even more vital when the system is integrated with access delegation capabilities. Revoking of attributes is required in situations where assigned/delegated attributes are expired as well as when the attributes of a user are updated. For instance, in the example that we have given previously, Alice may only interested in delegating the attribute, *Director* to Charlie while she is away. When she resumes duty, the attribute delegated to Charlie should be revoked to prevent illegitimate access as well as preventing Charlie from further delegations.

### 1.1. Our contributions

Although many access control schemes have been proposed to this date, access control schemes integrated with access delegation capabilities are few. We have only come across two such solutions [17,21], in which delegation capabilities are integrated to ABE models to achieve flexible access control. Despite the fact that the scheme in [21] capable of allowing a user to delegate access to another user (via delegating attributes), there is no mechanism to control the subsequent access delegations. The scheme in [17] provides a solution to the aforementioned issue by using a trusted third party (TTP). However, given that the TTP has a complete view of who delegates which attribute to whom might affect the privacy of users. In addition, both schemes in [17,21] do not possess a mechanism to control the maximum number of delegations permitted for a given attribute. Hence, the existing solutions lack the control over access delegation. Therefore, the main contribution of this paper is an ABAC scheme integrated with controlled access delegation which can ensure flexible and secure sharing of EHRs in a collaborative e-health environment. The novelty of the proposed access control scheme is two fold:

- The scheme is capable of providing multi-level controlled access delegation. Each attribute delegating user has the capability to allow or deny any further delegations by the delegatee while the maximum number of delegations permitted for a given attribute is also controlled by the attribute issuing authority which handles the delegating attribute.
- The scheme is coupled with on-demand attribute revocation where users and attribute issuing authorities have the capability of revoking the attributes of its descendants, if required.

In addition, the proposed scheme also ensures that attributes (may or may not be delegated) cannot be colluded by two or more users to gain access to a resource which is not feasible on their own. We also show that the proposed scheme satisfies the intended security requirements while providing evidence for its feasibility in terms of associated computational cost based on simulation results.

### 1.2. Organization

The remainder of this paper is organized as follows. In Section 2, we introduce the case description for which the access control scheme is proposed, along with the security model and associated security requirements. Preliminary knowledge corresponding to the proposed scheme is given in Section 3. In Section 4, we provide a general overview of the proposed scheme before the phases of the proposed scheme are presented in-detail in Section 5. In Section 6, we analyze the security of the proposed scheme while we evaluate the performance in terms of computational cost in Section 7. We present relevant related works in Section 8 along with a comparison of them with the proposed access control scheme before the paper is concluded in Section 9.