Attribute-Based Data Access Control for Multi-Authority System

Ahmad Salehi S.*, Carsten Rudolph* and Marthie Grobler†
*Department of Software Systems and Cybersecurity, Monash University, Melbourne, Australia
†Distributed Systems Security, CSIRO's Data61, Melbourne, Australia
* Email:{ahmad.salehishahraki and carsten.rudolph}@monash.edu
† Email:{marthie.grobler}@data61.csiro.au

***Abstract*—Access control and authorization in universal basic services is one of the main security issues in distributed systems. In particular, access control in distributed systems, such as in healthcare systems, are crucial to improve facility safety and security. This can lead to the provision of better quality of life and contribute to a healthier future. In order to provide better services, it is necessary to develop a suitable and acceptable authorization system to prevent unauthorized access to data shared in these highly dynamic distributed environments. In practice, several types of service providers, institutes, and authorities generate a variety of data in a shared environment via central authority for their entities. Generally, the use of a central authority introduces several security and privacy issues due to the increased risk if the central authority is compromised. To address this issue, several traditional access control models have been developed and introduced. These models, however, have raised several critical security issues, and there is often a need to combine it with a cryptographic approach to offer and create better access control service to users in multi-domains. To achieve this, we provide an appropriate solution to this issue. In this paper, we introduce an access control policy model for the multi-authority system, which enables attribute authorities to control the security setting. We present a new access control framework for a dynamic authorization model that uses Attribute-Based Access Control (ABAC) and digital signature. We first define and present our system and then formalize the construction of the proposed system. Our system provides flexible access control and enhanced privacy in applied and distributed environments.**

Keywords – Access control, policy, distributed systems, healthcare, security.

I. Introduction

Fast-developing emerging technologies, particularly in the healthcare domain, is creating a considerable amount of important and sensitive data. Due to the nature of this data, it may be necessary to share this at any time with different users in different locations, such as different health professionals in various healthcare domain settings [1], who aim to provide better healthcare services and improve patients' quality of life [2]. In our scenario, the healthcare data (or patient information), associated services (the various healthcare services) and technologies (such as the Internet of Things (IoT) and medical devices) need to be controlled over these different healthcare domains [3], [4], particularly considering the different local storage systems in the different hospitals [5]–[7].

Since healthcare data are often stored in multiple domains, it is necessary to protect the privacy of shared data using a proper access control policy system [8]. Systems are used to prevent unauthorized access to sensitive data. The majority of current access control approaches do not provide flexible access control due to several limitations, such as deciding on and enforcing policies in a multi-domain. Additionally, these domains generally do not willingly communicate with each other via a central authority, since the security compromise of a central authority can introduce a number of challenges.

In practice, healthcare data is generated and maintained by several users and objects from various domains (e.g., Hospital 1 and Hospital 2) with different levels of security and policies. To prevent unauthorized access to data in local and multi-domain databases, numerous access control techniques and approaches are proposed and used to support fine-grained data access control in distributed systems. Approaches and developments in healthcare to provide a wide range of access control mechanisms are based on centralized access control. However, centralized access control is limited to mechanisms for sharing particularly sensitive healthcare data, such as heart rate measurements and blood tests. A centralized system creates vast risks for privacy breaches or different type of attacks affecting the availability of healthcare data [9]. Moreover, users require the establishment of different types of trusted users to control access to a centralized system. For example, a third party, such as a cloud server, can decide what data should be accessible and what type of policy should be enforced. Furthermore, enforcing centralized management policies in distributed systems is insufficient and unacceptable in a real-world access control system because of the variety of security and privacy settings and risks.

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) [10] was introduced in the United States (US) to ensure the privacy of shared healthcare data in the local and international level. It was created primarily to modernize the flow of healthcare information, stipulate how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage [10]. Further, in 2014, the National Institute of Standards and Technology (NIST) introduced an extensive guide to Attribute-Based Access Control (ABAC) that can be used to implement HIPAA requirements from technical and organizational points of view [11]. However, ABAC is not suitable for multi-domain access control because of the

2324-9013/20/$31.00 ©2020 IEEE
DOI 10.1109/TrustCom50675.2020.00251

massive scale, and it is not easy to control and manage attributes in cross-domain [3], [4]. A suitable access control policy is therefore required to guarantee the privacy of shared data in multi-domains without relying on a central authority for authentication and authorization processes [12]. However, a natural progression of this work is to propose a detailed construction and security proof.

To date, several traditional access control models have been proposed (e.g., Access Control List (ACL), Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Lattice-Based Access Control (LBAC) and Attribute-Based Access Control (ABAC)) to provide better services [13]–[18]. Of these, ABAC is a promising traditional approach [11], [13], [17], [19]–[26], using various attributes to define the relationships between and within domains and entities (e.g., users and relevant data) [20]. For example, an access control policy in [19] presented a policy delegation with the aim to exchange generated policy between entities within and between domains. Although ABAC models provide a proper access control policy system, these policies are not easy to control and manage in multi-domains with different levels of security and privacy requirements.

Several cryptographic ABAC approaches and schemes have been proposed to permit a healthcare service provider access to specific data [27]. The Attribute-Based Encryption (ABE) models are a subset of cryptographic ABAC models, which mainly focus on access control based on access structure [27], [28]. In ABE, a user can gain access to data if, and only if, the user's attributes meet the policy and defined access structure. In the majority of ABE models, the access structure is publicly distributed along with generated ciphertext. Generally, this increases the vulnerability of the data access structure while a user is able to decrypt the ciphertext. Furthermore, ABE increases the decryption cost because the number of bi-linear operations increases along with the number of attributes used in the access structure. Similar to ABE, the Attribute-Based Signature (ABS) is a popular cryptographic primitive that enables a healthcare service provider to sign the message with their own attribute private key [29]. Although this is an interesting primitive and has great importance since the access control is based on entities attributes, existing ABS schemes still suffer from third party and key management complexity issues [30]. Besides, the size of the signature in ABS is linearly increased in a distributed system.

In this paper, we contribute an access control policy combination solution of ABAC and digital signatures. We address the problem of central access to decision systems by introducing a suitable multi-domain healthcare scenario based on current issues and interaction of relevant entities in distributed environments. This work has led us to propose a new access control system for a dynamic authorization model (DAM), which uses the advantages of traditional access control and cryptographic methods. In this policy system, the final access control decision and policy enforcement is based on ABAC, that relies on the user's attributes. The concept of a digital signature is further used to securely exchange the user's attributes between authorities and entities in multi-domains. In our proposed model, there is no requirement for any third party to manage and generate global parameters (e.g., key pairs and identity), except for generating initial parameters during a trusted setup. Our system meets multi-domain requirements and keeps the security settings of the distributed environment locally. This system offers more opportunities to prevent unauthorized access, protect the privacy of users, and to keep security settings in cross-domain environments. Moreover, we analyze the proposed model and prove that our scheme archives the following security properties: flexible access control with resistance against reply attack, attribute collusion, and access control and privacy.

The remainder of this paper is organized as follows. Section II discusses the ABAC general model. Section III discusses the overview of the system model and security requirements. Section IV introduces our proposed approach. Section V discusses the working example under our proposed model. Section VI concludes the paper.

II. ABAC General Model

ABAC is an emerging access control model that can control for the right access to shared data by evaluating policies and attributes of the subject, object, environment, and action. In ABAC, a user sends a query to gain access to specific data within and between different domains. The key components of ABAC are the policy decision point (PDP); policy administration point (PAP); policy information point (PIP); and 4) policy enforcement point (PEP)[1]. In practice, the ABAC model cannot successfully be applied in multi-domains with multiple security and privacy requirements and settings [11], [12], [32]. The general architecture of NIST's ABAC model is presented in Fig. 1.

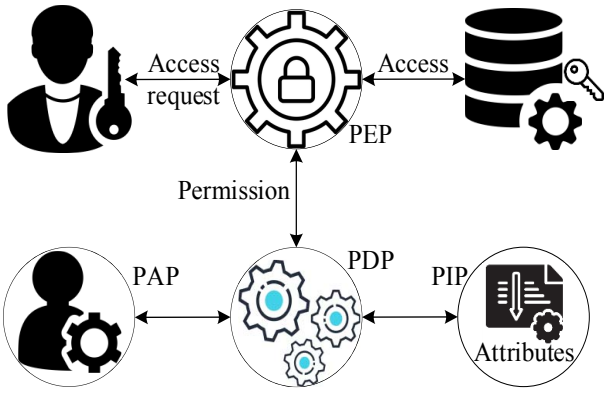

Fig. 1. ABAC Architecture.

[1]For additional information about the ABAC standard and components refer to [11], [12], [31].

The list of main abbreviations used in this paper is depicted in Table I.

TABLE I
LIST OF ABBREVIATIONS.

Abbreviation	Explanation
AA	Attribute Authority to which a patient or user belongs
EHR	Electronic healthcare record
EMR	Electronic medical record
EM	Emergency department
ABAC	Attribute-Based Access Control
HSP	Healthcare service providers
NIST	National Institute of Standards and Technology
HIPAA	Health Insurance Portability and Accountability Act
RBAC	Role-Based Access Control
ABE	Attribute-Based Encryption
IBE	Identity-Based Encryption
ABS	Attribute-Based Signature
PDP	Policy decision point
PIP	Policy information point
PEP	Policy enforcement point
O	Data owner (i.e. patient)
U	Data consumer (i.e. user)

III. ARCHITECTURE

In this section, we present our system model and apply it to a general healthcare scenario to illustrate its benefits.

A. Our System Model

In our system model, we consider several domains, with each domain including several entities (e.g., patients and professional staff as users). We assume that each patient and user belongs to one domain (for example, patient 1 belongs to Hospital 1). The healthcare data is stored at the hospital to which the patient belongs, and the data should be made accessible through sharing with other users in the multi-domain. The architecture of the system model is presented in Fig. 2. To overcome the security issues of a traditional ABAC model, the proposed model attempts to meet the following security requirements: replay attack, attribute collusion, access control and privacy. This paper focuses on a single domain and multi-domain healthcare scenario to provide an appropriate model for application in real worldd healthcare systems [12].

Healthcare application example: As a use case, we consider the following scenario. Alice is a patient in Hospital 1 (AA_1) and Bob is a doctor in Hospital 2 (AA_2). Bob would like to access Alice's healthcare data to monitor her medical condition when required. Bob should not be required to register as a user for the Hospital 1 domain, and Alice's identity, attributes and private information should not be revealed to any other AA, including AA_2 where Bob works or another third party. Let us assume that Alice has attributes {"Hospital 1", "Healthcare Service Center", "Microbiology Department", "female", and "Name id = Alice"}. Based on this healthcare scenario, her data must be stored in a local database in AA_1 to be accessible to professional staff such as Bob. Alice does not want to reveal any additional information or attributes to either Bob or Bob's domain authority or any third party (e.g., the cloud). Bob has attributes {"Hospital 2", "Healthcare service center",

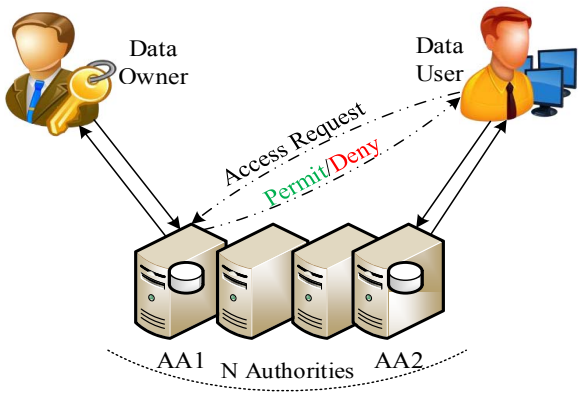

Fig. 2. Multi-Authority System Architecture.

"emergency department", "Doctor with Id = 10", and "2 pm to 4 pm on weekdays"}. Based on this, Bob can access Alice's data only if his attributes can satisfy the access structure (τ) for Alice as defined by Alice herself or AA_1 on behalf of Alice. In our scenarios, Alice may not want to delegate all her attributes to Bob but may delegate those attributes that are sufficient to satisfy the τ. Alice does not allow Bob to delegate the attributes further [12].

- Attribute Authority (AA): The AA acts as the manager of either an AA_1 (Hospital 1) or AA_2 (Hospital 2), working under the national and local laws and regulations of its domain. The AA_s is responsible for managing and generating the required parameters, such as attributes and keys.
- The data owner (patient) and consumer (user): A patient is a person in a healthcare system who may receive treatment. A user is a professional staff member (healthcare service provider) who would like to access the healthcare data if required. In our model, the patient's healthcare data are stored in AA_1 and the user located in AA_2.
- Access structure (τ): The access structure includes a set of the user's attributes that needs to meet the condition and target of an access request to permit the user access to the data. A simple access structure in our system model is as follows: Alice {Hospital A $\wedge$ Healthcare service centre $\wedge$ Emergency department $\wedge$ Doctor with Id = 10}. An example of an access structure based on those as mentioned above is depicted in Fig. 3.

B. General Healthcare Scenarios

The overall aim of access control is to manage access to healthcare information and to identify unauthorized users. To recognize and determine the security level and the variety of players in a domain, we describe a simple healthcare scenario. We consider a scenario where a university student faints while running on a treadmill at a gym. First, the alarm is sent onward to a medical server for further services. The specialist service

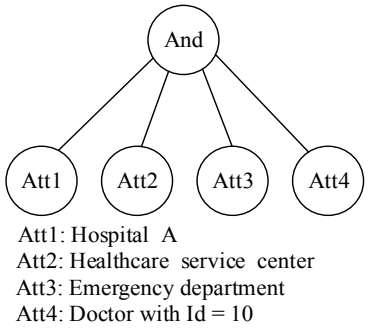

Fig. 3. An example of access control structure.

provider is required to access the patient profile remotely from a hospital in real-time. The professional staff in the emergency department also need to have access to the patient's history.

Several users may require access to the data, from different locations and multiple domains. In this scenario, it is important to know what information is required for different types of stakeholders [33]. Who can control and manage the users, as well as the shared information, over open networks? Who can have access to what, and how much data must be accessible? Who can access health records and from where? Why must specific users have access to healthcare information and how much access should they have? Thus, an appropriate mechanism is required to address the issues involved in granting the right permission to authorized users. Due to the variability of the healthcare scenarios, it suitable to use ABAC regarding the different factors such as duties, attributes, roles, policies, and security and privacy requirements in healthcare environments. These factors may also demand consideration of more conditions relevant to the scenarios.

IV. Our Proposed ABAC Approach

In this section, we present our proposed approach and include details of the proposed scheme.

A. Details of the Proposed Scheme

In our technique, the system initialization must first be set up with the necessary parameters, such as the attributes, public and private keys, signature and appropriate certificate within and between AA_s. An attribute key distribution based on the proposed system model is then required to permit the user and patient to receive an appropriate set of attributes from their AA. In our model, the attribute key distribution is divided into two phases. In the first phase, the attribute is assigned to the patient and user via their AA, and the attribute is delegated to the domain or the user via AA_2. For this to happen, a secure channel between AA_s (AA_1 and AA_2) is required before the exchange of any attributes. Additionally, in our proposed scheme, the access decision happens in AA_1, which requires the user from an AA_2 to communicate securely with the authorization system in the AA_1. This prevents unauthorized disclosure of the set of attributes between AA_s. The second phase is where the access decision is made in the AA_1, based on the current permission and patient's target, and condition after evaluating the access request. The system allows the user to access the particular data if, and only if, the attributes owned by the user can satisfy the τ defined by patient and system model called policy system model. The list of main notations used in this paper is depicted in Table II.

TABLE II
LIST OF NOTATIONS.

Notation	Explanation
$U_{k,id}$	User belongs to the FHD_m
$O_{l,id}$	Patient where is belongs to the HHD_n
$\mathbb{G}_0$ and $\mathbb{G}_1$	Two multiplicative cyclic groups of prime number
$\mathcal{T}$	Access structure
MSK_m	Master key belongs to the m^{th} AA_m
PUB_m	Public key belongs to the m^{th} AA_m
P	Policy
$\mapsto$	Given permission to
EMR_{obj}	Electronic medical record
EMR_{id}	Electronic medical record request identification
RE	Read as a permission
WR	Write as a permission
Re, WR	Read or Write as a permission
EM	Emergency department
α_m	Secret key belong to the AA_m
X_m	Public key belong to the AA_m
$t_{m,i}$	Secret attribute belongs to the original attributes of AA_m
$T_{m,i}$	Public attribute belongs to the original attributes of AA_m
PKI_{AA_m}	Public key infrastructure (PKI) certificate belongs to the AA_m
PKI'_{U_k}	PKI certificate of the m^{th} belongs to the AA_m
$t_{m,\omega}$	Particular secret attribute belongs to the AA_m
ω	Set of attributes obtained by user from respective AA
ATA_k^m	Token assigned to the U_k by respectively AA
S_k^m	signature related to ATA_k^m
UAR'_k	Set of attributes belonging to the U_k where the attribute can reveal for AA_m via access request
A'_m	Set of attributes handled by AA_m on behalf of their entities

B. Preliminaries

In this subsection, we introduce the essential elements needed to understand our proposed model.

- *Attributes*

In our system model, we have two types of attributes where the called attribute is assigned to U (user) or O (patient) via their respective authority $AA_1 \mapsto O_1$ and the attributes delegate to another authority via user or attribute authority $AA_1 \mapsto AA_2$ (AA_1: $O_1 \mapsto AA_2$).

- *Bi-linear map*

In this paper, we use the concept of bi-linear group maps for user commitment generation and to verify the internal and external access request and the attribute issuer. For this, we used the bi-linear map defined in [30], but we consider $\mathbb{G}_0$ and $\mathbb{G}_1$ instead of $\mathbb{G}_1$ and $\mathbb{G}_2$. The bi-linear pairings of algebraic curves are defined as a map. Consider $\mathbb{G}_0$ and $\mathbb{G}_1$ by two multiplicative cyclic groups of prime number as denoting p

and the g be a generated of $\mathbb{G}_0$. A pairing map is e: $\mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$, where must satisfy the following properties [34].

- Bi-linear: for any $u, v \in \mathbb{G}_1$, and a, b $\in \mathbb{Z}_p$, it has $e(u^a,v^b) = e(u,v)^{ab}$;
- Non-degeneracy: e(g,g) $\neq$ 1, where 1 is the unit parameter in $\mathbb{G}_T$;
- Computability: there is an efficient algorithm to compute $\mathbb{G}_0$ and $e : \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$ for all $u, v \in \mathbb{G}_0$.

We assume that that the bi-linear group is symmetric if there exists an efficiently computable isomorphism ϕ from $\mathbb{G}_0$ to $\mathbb{G}_1$ and an efficiently computable isomorphism ϕ' from $\mathbb{G}_1$ to $\mathbb{G}_0$. Similarly, we say that the bi-linear group is asymmetric if such ϕ does not exist [30].

- *Patient's data anatomy*

The data owner, referred to as the patient, may receive a variety of medical treatments for any particular condition at AA_1. We assume that the patient has already registered with AA_1 and that he/she has identification $O_{1,id}$ that is belongs to AA_1. In our system model, the healthcare data is referred to as EMR_{OBJ}, and can be any patient's sensitive information such as personal information and healthcare conditions.

- *Patient's policy anatomy*

We define the patient's policy anatomy as an access policy called PP, where a patient uses the policy and security requirements associated with his/her sensitive data to grant particular permission to an internal or external user. This means, a user needs to satisfy the PP related to the access structure to get his/her permission to access specific data on a healthcare database in AA_1. The simple policy anatomy is presented in the following. Usually, a user is allowed to read (denoted as RE), write (denoted as WR) or perform both actions (RE and WR) on healthcare data while he/she grants the security requirement created by O_1. As a tangible example, a healthcare service provider (HSP) belonging to AA_2 and a healthcare service center are able to access (write and read) health data where denoted as EMR_{hc}, (PP_{hc}: ($HSP \wedge AA_2$) $\mapsto$ RE & WR). The doctor from the emergency department (EM) needs to have access (read) to the data (PP_{hc}: (*doctor* $\wedge$ $AA_2 \wedge EM$) $\mapsto$ RE and P: $\tau \rightarrow$ X).

$$EMR_{hc}(P_{hc} : (HSP \wedge AA_2) \rightarrow read\&write) \qquad (1)$$

C. Proposed model construction

In this section we present our proposed model with four phases:

i) Phase 1: Model initialization

- The first stage is dedicated to setup and to initiate the multi-authority model. Universal parameters are required for the authorities, to be shared within and between the attribute authorities. For this stage, the system takes the security parameters as an input and generates six tuples (p, H, $\mathbb{G}_1$, $\mathbb{G}_0$, e, g) as the bi-linear parameters for output with the secure hash function H: $(0,1)^* \rightarrow \mathbb{G}$ ($H \in \mathbb{Z}_P^*$). This also enables the new domain to join the multi-authority setting in anytime by giving the legal evidence.
- In the second stage and after the successful universal globalization setup, the respective parameters between the domains and respective users need to be initiated with the AA. For this, we denote A_m as a set of attribute generates by a respective authority such as AA_m as well as $U_{k,id}$ for each user belonging to the same domain. The details of this algorithm described in the following.
  1) Each authority selects a randomized system as a secret key called α_m, where it is a component of $\mathbb{Z}_P^*$. X_m = g^{α_m} broadcast as a public key of each AA.
  2) The public key calculates AA_m ($Y_m = e$(g,g)$^{\alpha_m}$) respectively, as well as each of the AA_m randomly selected $t_{m,i}$, which belongs to $\mathbb{Z}_P^*$. Hence, any attribute generated by an attribute authority along with their pubic key denotes as a $T_{m,i}$, equal to $g^{t_{m,i}}$.
  3) In the last step, the authorities like AA_m hold the generated public and private key as a master secret key where it denotes as a MSK_m and includes the secret key and the randomized selection key ($\alpha_m, t_{m,i}$). The corresponding public key broadcast by AA_m where called PUB_m. This includes the Y_m and $T_{m,i}$.

ii) Phase 2: Secure communication between Attribute Authorities (AA_m and AA_n)

As discussed in our system model, the healthcare service provider as a user can access the data if, and only if, the user attributes related to his/her request can be verified by the authorization system where this system is located in the AA_1. Regarding this, secure communication between AA_1 and AA_2 (AA_m and AA_n) is required to prevent the attributes of a user from being disclosed against any other AA_s. An external user belonging to AA_2 also requires a shared session to establish secure communication between him/herself and AA_2. To this end, we assume there is a current PKI model that generates certificates for each authority and respective user, such as PKI_{AA_m} and PKI'_{U_k}. $t_{m,\omega}$ is also the secret attribute belonging to the AA_m. Note that exploring security properties of PKI is out of scope in this work.

iii) Phase 3: Distribution of entities attributes

In our system model, the respective AA_s generate and assign the relevant and necessity attribute keys to their entities under the national and local laws and regulations of the domain while the entity provides evidence of his/her eligibility. Here, we assume that the user is eligible and a member of the domain ($U_{1,id} \in AA_m$). After user eligibility is satisfied, the user's attribute key is assigned and called the assigned token attribute ATA_k^m. The corresponding signature for the user, generated by AA_m, denotes the S_k^m. In addition, we denote ω as a set of attributes that $U_{k,id}$ is required to obtain from their respective AA.

In this stage, we assume that the $U_{k,id}$ proves that he/she is eligible to obtain the ω, so the respective authority generates the ATA_k^m associated with PKI_{AA_m} as well as PKI'_{U_k}

belonging to the receiver. The X_m as well as $t_{m,\omega}$ is used by the AA_m to generate the signature, S. Also, the S_k^m generated by the authority is equal to $X_m^{(H(ATA_k^m)+t_{m,\omega})^{-1}}$, and then this calculates as a $g^{\alpha_m(H(ATA_k^m)+t_{m,\omega})^{-1}}$. Hence, the signed token related to eligible user for an access request is $\{ATA_k^m, S_k^m\}$.

iv) Phase 4: Access decision

As we discussed above, the access decision is determined in AA_1, to which the patient belongs, and the healthcare data is stored for further services. The access decision is made in AA_1 after evaluating the access request and corresponding attributes from the user. Hence, the user allows access to the health records if, and only if, the attributes owned by the user can satisfy the access structure defined by the AA_1 on behalf of the patient.

Based on the PKI assumption discussed earlier, we assume the authentication session completed using the PKI_{AA_m} and PKI'_{U_k}. Then, the user requests access to particular data, including access request identification (EMR_{id}), health data (EMR_{obj}) and a particular action required for this access request. In the first step, the request will be evaluated by the PEP while the access request is received by the authorization system. The particular access requirements are based on the user's access request. The data owner access structure generates and then forwards this to the user, which this denotes as a τ. For this, the user selects the particular attributes to belong to his/herself called UAR'_k, where the selected attributes can satisfy the access requirements, define on τ. The selected attributes UAR'_k must be a subset of attributes assigned by the attribute authority A'_m to the user. After this, the subset of the user's attribute singed and the relative token is transferred to PEP in AA_1. The token need to be validated, and then the UAR'_k evaluated by the PDP. In the end, the user allows access to a particular resource after giving permission; otherwise, the access is denied. The process of validation and commitments is explained below in detail.

As we mentioned, there is a token from the user that matches with his/her access request and a token set from the authority to which the user belongs. The authorization engine checks whether the tokens are received from the same request and the system will reject the access if, and only if, both of the tokens belong to the same authority. This can prevent an attribute collision. The system then checks the certificate belonging to the user and his/her domain to validate the eligibility of the user. In this stage, access to the healthcare resource is immediately rejected if, and only if, the certificate does not match the original certificate. Not only does this enable the system to prevent an attribute collision, but also enables the system to find the impersonating user. The authorization system continues if, and only if, both of the requirements described above are fulfilled.

In this step, we assume that the generated assigned token has not expired. Here, the access request automatically will be rejected if, and only if, the token has expired; otherwise, the system continues to verify that the S belongs to the user. We denote $PUT_{m,\omega} = g^{t_{m,\omega}}$ for the public attribute related to respective AA of the user U_m. The authorization system calculates a helper string (denoted as ST), which is equal to $g^{H(ATA_k^m)}PUT_{m,\omega}$ and then calculates as a $g^{H(ATA_k^m)} + t_{m,\omega}$. In the following step, the system uses the signature and string to compute: $e(S_k^m, ST) = e(g^{\alpha_m(H(ATA_k^m)+t_{m,\omega})^{-1}}, g^{H(ATA_k^m)} + t_{m,\omega})$. The corresponding attributes associated with the assigned token is valid, verify and satisfy the access structure if, and only if, the computation answer is similar the Y_m (public attributes of the respective authority belonging to the user). As a result, the system grants the user access to the specific healthcare data when it is required.

D. Security analysis

We now give a specific security evaluation and analysis of the presented model to demonstrate and highlight the strengths of the proposed scheme in terms of known security attacks.

i) *Replay attack:*

We assume that there is an adversary who intercepted ATA_k^m where the token belongs to U_k. Let us say the adversary sends a request to access to EMR with the amount of attribute, which can satisfy the access structure. To do this, the adversary needs to authenticate him/herself with the authorization system located in AA_1. The authentication will be rejected while the system recognizes that the secret keys of the adversary are not matching the secret key of the user belonging to AA_2. This is checked by using the attribute own by the user and the shared PKI certificate between domains.

ii) *Attribute collusion:*

In ABAC, the attribute collusion requires to increases the privacy of the system and prevents illegal access to healthcare data because it generates attribute keys for two different users. The resistance to attribute collusion also prevents the authorities from revealing the attributes. Let us say AA_1 handles the ω_3, ω_4, and the healthcare data in the respective authority. We assume that there are two users (U_3 and U_4) from different domains and tokens, such as ATA_3 and ATA_4. The ω_3 and ω_4 are also denoted as a set of an attribute for each authority. For this, we assume that U_3 is interested in accessing the healthcare resource using both ATA_3 and ATA_4. In this step, both the public and private key of U_3 are evaluated to validate the eligibility of the user using corresponding certificates. The system recognizes the user is not valid as his/her attributes do not match with ATA_4. Hence, this attack will not happen, and this demonstrates the proposed model is collusion resistant to the attribute.

iii) *Access control and privacy:*

A suitable access control framework is proposed based on the use of multi-domains presented with the following feature to meet the requirements presented model. Our model supports the use of a multi-domain, which can provide both a centralized and decentralized access control model without relying on third party control over data. As stated earlier, a user needs to prove their eligibility and evidence to get access to healthcare

resources. Here, we assume that the adversary is not able to forge the signature S. Hence, critical information such as attributes will include disclosure to a corresponding authority or user. Therefore, this increase the privacy of sensitive data in multi-domain.

iv) *Resistance to third party storage attacker:*

As we mentioned earlier in our system model, AA_1 is a domain where the patient is located and the data is stored. AA_2 is a foreign domain where the user is located and his or her data stored. In this paper, we assume there is no malicious actor inside the domain in this step. Both domains are responsible for generating attributes and relative security parameters (e.g., key pairs and certificates) for their users. Also, we assume that there is a malicious actor inside the cloud storage. In this case, the malicious actor in the cloud or third party storage will not be able to access the healthcare resources stored in the local domain because all the entities key attributes and security parameters are generated and controlled in AA_s.

V. An application scenario

The following example model has been selected to demonstrate how our system works in reality. We assume that there is a hospital in Melbourne, Australia, that has established a single-domain access control system. Practically, developing a secure healthcare system is the main goal to achieve a high level of security, to keep the privacy of sensitive data and to provide decentralized access control.

We assumed that there is an access control system (NIST's ABAC) developed and working well based on what we presented in this research project (refer to Section II). In practice, each hospital may deploy a different access control system based on its security setting and local rules and regulations. Although this can differ between hospitals, the main concept of access control systems is based on a general ABAC. It can enable each system to independently make changes at any time if required through the local authority. This can increase the performance of the access control system, and small changes in the policy system do not require multi-domain approval. The policies are frequently updated according to the local standard and security setting to permit or deny access to sensitive data. Hence, the final decision will take less time rather than in a multi-domain policy system.

Given this scenario, the admin of the domain uses our system to experiment with the following:

- Local (Single) domain.

In a real system, the access control system is set up and configured for the first time, and it requires light updates and modifications based on new user and patient information. The admin of the domain can use any local ABAC system such as our local ABAC (Similar to NIST's ABAC) to introduce new attributes and the relationship between attributes and the stored data in the local database. Additionally, it requires introducing rules and mapping them to the attributes to represent access control. According to this, the size of the domain and the number of users cannot affect the access control service time for each local request. Hence, there are no critical issues for a local user such as doctor Bob while he is able to gain access to local data. The reason is that Bob also uses the local system and does not require an extra process for validation of identity and verification.

- Multi-domain

Here, we have two scenarios to demonstrate how our access control policy system works in a multi-domain.

1) The first case scenario, a user like a doctor Bob (belonging to AA_2 in Melbourne) may be invited to AA_1 in Brisbane, Australia for collaboration purposes. He is aware that there are multi-domain solutions and requirements to access his patient information, but is not sure about the quality of remote access in the multi-domain. Bob may instruct his device (e.g., laptop or smartphone) to collect local information from AA_1 to facilitate the collaboration. Whilst at AA_1, Bob has patients in AA_2 whose activity he needs to monitor. In this step, he will send a request to get access to sensitive data located in AA_1 where he originally belongs. Based on our system, he will use the public certificate from AA_1 and not AA_2. Although a public certificate is required to verify the place where Bob travelled for his new business, Bob can gain access to his patient data without any issues, as his own attributes are originally from AA_1.
2) The second case scenario, a user like Bob, wants to gain access to Alice's data from AA_2 in Brisbane. Note that Bob in the second case scenario originally belongs to AA_2 and Alice is located in AA_1 in Melbourne. In the first step and sequence, he will get his own attributes and key pairs from AA_2. To do his duty, he will follow the process of DAM (refer to Section IV). He can gain access to data if, and only if, his attributes can satisfy the policy requirements specified by AA_1 and not his local authority (AA_2).

A few main advantages of our system model are as follows: The authorization process will stop in the first step, if, and only if, the user is unable to satisfy the access requirements. This is because of the authorization request is blocked once Bob's protocol is unable to provide the necessary attributes based on the access structure. Although communication and computation overheads are not in our scope, our system also reduces communication and computation overheads in a multi-domain. Furthermore, by using our protocol, cross-authority is not able to learn anything from the user while he is requesting access to data. Additionally, we can achieve attribute anonymity, user anonymity, and attribute privacy by using the concept of a digital signature. Our system also enables us to achieve selective attribute, dynamic change, flexible access control and resistance to attribute collusion as we state above. Furthermore, we propose the first access control policy system that achieves attribute exchange property in multi-domain, where this enables us to distribute attributes in a multi-domain.

VI. Conclusion and Future Work

Access to sensitive data and associated services and technologies in multi-domains poses several security and privacy concerns. To overcome these concerns, we introduce a dynamic access control policy model called DAM. DAM permits a healthcare service provider (e.g., a doctor) access to patient data at any time and from any location. Our model provides a solution for a distributed healthcare system to decide whether a user is eligible for access based on their attributes. We have achieved a DAM scheme which provides flexible access control while ensuring privacy and security in multi-domains. Our solution and security analysis demonstrates that DAM is beneficial to preserving the privacy of users and ensuring data security. Furthermore, we plan to develop and implement our proposed model to show the feasibility of our model in practice.

References

[1] M. Beltrán, "Identifying, authenticating and authorizing smart objects and end users to cloud services in internet of things," *Computers & Security*, 2018.

[2] A. Anjum, K.-K. R. Choo, A. Khan, A. Haroon, S. Khan, S. U. Khan, N. Ahmad, B. Raza *et al.*, "An efficient privacy mechanism for electronic health records," *computers & security*, vol. 72, pp. 196–211, 2018.

[3] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wireless Networks*, vol. 17, no. 1, pp. 1–18, 2011.

[4] J. Stevovic, F. Casati, B. Farraj, J. Li, H. R. Motahari-Nezhad, and G. Armellin, "Compliance aware cross-organization medical record sharing," in *Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on*. IEEE, 2013, pp. 772–775.

[5] S. A. Salehi, M. Razzaque, I. Tomeo-Reyes, N. Hussain, and V. Kaviani, "Efficient high-rate key management technique for wireless body area networks," in *2016 22nd Asia-Pacific Conference on Communications (APCC)*. IEEE, 2016, pp. 529–534.

[6] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the internet of things: Big challenges and new opportunities," *Computer Networks*, vol. 112, pp. 237–262, 2017.

[7] A. Salehi, C. Rudolph, and M. Grobler, "A dynamic cross-domain access control model for collaborative healthcare application," in *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. IEEE, 2019, pp. 643–648.

[8] S. A. Salehi, M. A. Razzaque, I. Tomeo-Reyes, and N. Hussain, "Ieee 802.15. 6 standard in wireless body area networks from a healthcare point of view," in *2016 22nd Asia-Pacific Conference on Communications (APCC)*. IEEE, 2016, pp. 523–528.

[9] S. A. Salehi, M. Razzaque, P. Naraei, and A. Farrokhtala, "Detection of sinkhole attack in wireless sensor networks," in *2013 IEEE international conference on space science and communication (IconSpace)*. IEEE, 2013, pp. 361–365.

[10] "Guide to hipaa privacy rule and compliance," 2015. [Online]. Available: http://www.hipaa-101.com/

[11] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone *et al.*, "Guide to attribute based access control (abac) definition and considerations (draft)," *NIST special publication*, vol. 800, no. 162, 2013.

[12] A. S. Shahraki, C. Rudolph, and M. Grobler, "A dynamic access control policy model for sharing of healthcare data in multiple domains," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2019, pp. 618–625.

[13] D. Servos and S. L. Osborn, "Hgabac: Towards a formal model of hierarchical attribute-based access control," in *International Symposium on Foundations and Practice of Security*. Springer, 2014, pp. 187–204.

[14] M. Sookhak, F. R. Yu, M. K. Khan, Y. Xiang, and R. Buyya, "Attribute-based data access control in mobile cloud computing: Taxonomy and open issues," *Future Generation Computer Systems*, vol. 72, pp. 273–287, 2017.

[15] R. Ahuja and S. K. Mohanty, "A scalable attribute-based access control scheme with flexible delegation cum sharing of access privileges for cloud storage," *IEEE Transactions on Cloud Computing*, 2017.

[16] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog computing: A taxonomy, survey and future directions," in *Internet of everything*. Springer, 2018, pp. 103–130.

[17] P. Biswas, R. Sandhu, and R. Krishnan, "Attribute transformation for attribute-based access control," in *Proceedings of the 2nd ACM Workshop on Attribute-Based Access Control*. ACM, 2017, pp. 1–8.

[18] M. Tolba, S. Benferhat, K. Tabia, and A. Belkhir, "Handling capabilities in security policies," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2018, pp. 1922–1927.

[19] D. Xiong, P. Zou, J. Cai, and J. He, "A dynamic multi-domain access control model in cloud computing," in *International Symposium on Security in Computing and Communication*. Springer, 2015, pp. 3–12.

[20] W. W. Smari, P. Clemente, and J.-F. Lalande, "An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system," *Future Generation Computer Systems*, vol. 31, pp. 147–168, 2014.

[21] J. C. John, S. Sural, and A. Gupta, "Authorization management in multi-cloud collaboration using attribute-based access control," in *Parallel and Distributed Computing (ISPDC), 2016 15th International Symposium on*. IEEE, 2016, pp. 190–195.

[22] T. Faber, S. Schwab, and J. Wroclawski, "Authorization and access control: Abac," in *The GENI Book*. Springer, 2016, pp. 203–234.

[23] M. Gupta and R. Sandhu, "The gurag administrative model for user and group attribute assignment," in *International Conference on Network and System Security*. Springer, 2016, pp. 318–332.

[24] C. Ngo, Y. Demchenko, and C. de Laat, "Multi-tenant attribute-based access control for cloud infrastructure services," *Journal of Information Security and Applications*, vol. 27, pp. 65–84, 2016.

[25] Y. Benkaouz, M. Erradi, and B. Freisleben, "Work in progress: K-nearest neighbors techniques for abac policies clustering," in *Proceedings of the 2016 ACM International Workshop on Attribute Based Access Control*. ACM, 2016, pp. 72–75.

[26] A. J. Rashidi and A. Rezakhani, "A new approach to ranking attributes in attribute based access control using decision fusion," *Neural Computing and Applications*, vol. 28, no. 1, pp. 803–812, 2017.

[27] P. Zhang, Z. Chen, J. K. Liu, K. Liang, and H. Liu, "An efficient access control scheme with outsourcing capability and attribute update for fog computing," *Future Generation Computer Systems*, vol. 78, pp. 753–762, 2018.

[28] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "Dac-macs: Effective data access control for multiauthority cloud storage systems," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1790–1801, 2013.

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

[30] J. Sun, J. Qin, and J. Ma, "Securely outsourcing decentralized multi-authority attribute based signature," in *International Symposium on Cyberspace Safety and Security*. Springer, 2017, pp. 86–102.

[31] C. T. Hu, D. F. Ferraiolo, D. R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to attribute based access control (abac) definition and considerations," Tech. Rep., 2019.

[32] F. Rezaeibagha and Y. Mu, "Access control policy combination from similarity analysis for secure privacy-preserved ehr systems," in *2017 IEEE Trustcom/BigDataSE/ICESS*. IEEE, 2017, pp. 386–393.

[33] S. S. Ahmad, S. Camtepe, and D. Jayalath, "Understanding data flow and security requirements in wireless body area networks for healthcare," in *2015 17th International Conference on E-health Networking, Application & Services (HealthCom)*. IEEE, 2015, pp. 621–626.

[34] T. Yamakawa, S. Yamada, G. Hanaoka, and N. Kunihiro, "Self-bilinear map on unknown order groups from indistinguishability obfuscation and its applications," *Algorithmica*, vol. 79, no. 4, pp. 1286–1317, 2017.