2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering

A Dynamic Access Control Policy Model for Sharing of Healthcare Data in Multiple Domains

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

***Abstract*—Authorization models have been developed to prevent unauthorized access to valuable resources such as electronic healthcare records (EHRs). In an applied environment, such as the healthcare domain, there are several types of authorities that generate EHRs and other security parameters via central authority for their users and the attribute authorities. The use of a central authority introduces several challenges in terms of security and privacy due to the increased risk if the central authority is compromised or corrupted. Observing that this research area has not been well addressed to date, we propose and present the first decentralized multi-authority attribute-based access control (DMA-ABAC) model based on the policy model, which enables authorities to independently control their security settings. We present an access control framework for a dynamic cross-domain authorization model that combines Attribute-Based Access Control (ABAC) and Attribute-Based Group Signature (ABGS). This combination aims at providing flexible access control with resistance against reply and third party storage attacks and attribute collusion, and enhanced access control, privacy and selective attributes.**

Keywords–anonymity, attribute-based access control, cross-domain, distributed, healthcare, security, privacy.

I. Introduction

An increasing global population combined with rapid development of technologies (e.g., Wireless Body Area Networks (WBANs) and Wireless Sensor Networks (WSNs)) generate enormous amounts of data in different forms [1]–[4]. This data may be shared with various users, located in the same or different domains, with a diverse range of settings [1]. In a group collaboration and data sharing application, it is very useful for users to exchange information amongst themselves and between their domains using unique attributes (such as specific properties for the subject, object, environment, and action) to determine any duty and responsibility. These properties are especially useful in distributed systems when a user is required to move within and between domains [5]. We propose and present a decentralized multi-authority attribute-based access control (DMA-ABAC) system that facilitates the easy sharing of data within and between multiple domains. To illustrate the application of our DMA-ABAC system, we will apply all scenarios and examples within the healthcare domain. This domain is sufficiently complex to enable the illustration of various scenarios to motivate the design and development of DMA-ABAC.

The current situation is that data is held by separate entities and that various policies and access control mechanisms are used to prevent malicious and unauthorized access to data by both insiders and outsiders. Cross-domain access is restricted to mechanisms for the explicit sharing of particular pieces of information. Approaches to provide wider access are either based on centralized storage or require synchronized cross-domain security and policies. Centralized data creates huge risks for privacy breaches or attacks affecting the complete set of available data. Furthermore, entities would need to give up data sovereignty and a highly trusted entity needs to be established to control access, i.e. decide on and enforce policies. However, these domains may not willingly communicate with each other via a central authority because a number of challenges can be introduced if the central authority is compromised. A compromised authority can enable an attacker to affect the entire of system.

Data generated, stored and shared must further comply with relevant standards and requirements [6] as introduced by the relevant domain authorities. Within the healthcare domain, consideration must be given to the Health Insurance Portability and Accountability Act (HIPAA) [7] to ensure the privacy of shared healthcare data and the confidentiality, integrity, and availability of data over different domains. To this extent, the National Institute of Standards and Technology (NIST) introduced a guide to Attribute-Based Access Control (ABAC) that can be used to implement HIPAA requirements from technical and organizational points of view [8], [9]. However, this is solely focused on single-domain access control and does not consider the control of data and their services and technologies shared over different domains and storage systems [10], [11]. A proper authorization model is therefore needed to ensure the privacy of shared data over different domains to support existing authorization models focused on preventing unauthorized access to valuable resources in cross-domain [12].

In order to provide and receive healthcare services, it is obligatory for users and patients to register with a local domain. Thus, a process is required to identify a person (regardless of the role that person plays as either health professional or patient). A distributed cross-domain access control model, such as the DMA-ABAC model that we developed, can rely on these existing identification processes to provide cross-domain identity information. The goal of developing such a cross-domain access control model is to restrict any central authority to this minimal role of identifying persons and then satisfying the requirements within the local domain.

Combining traditional [8] and cryptographic [13] schemes

2324-9013/19/$31.00 ©2019 IEEE
DOI 10.1109/TrustCom/BigDataSE.2019.00088

offers a proper solution to design and propose an ABAC model. In this type of model, there are multiple domains with different settings, with each domain responsible for generating attributes and secret keys for their users. With this model, several attributes and secret keys are assigned to users through a variety of authorities. The policies determine which users are able to access specific data, specifying which attributes are required to satisfy the data policy for data access. Although a possible method is to build a central authority system to manage all authorities and user parameters, it introduces a number of challenges if the central authority is compromised.

A. Related Work

Several traditional access control models are proposed and applied in a variety of scenarios [5], [14]–[22]. One of the most important traditional access control models is ABAC [8], [15], [22]–[30], where users' attributes are formulated and common attributes defined to provide trust between domains [24], [25]. Based on the traditional model, a hierarchical group ABAC framework was proposed to assign the attributes based on each group [15]. To reduce the number of rules and permissions in the system, a multi-domain approach using the notion of ABAC associated with the attribute's value was further proposed and a policy delegation was extended with the aim of transferring parts of a policy between users [15], [21], [26]. This model was revised to an administrative authorization model using the hierarchical group ABAC concept called group user role administrator [27].

Similarly, in 2015 Xiong [23] proposed a policy delegation with the aim of transferring parts of or the entire policy between users and domains. However, these models were found too complex for large environments. Although traditional approaches provide a better access control model with greater flexibility, these policies are not easy to manage and cannot be applied in cross-domains with multiple security and privacy requirements. This lessens the usability of traditional access control models in cross-domain. The focus is therefore on improving efficiency, scalabililty, and ease of configuration, but no unique architecture of these can be applied in both single and multi-domain scenarios.

Additionally, several attribute-based cryptographic approaches (such as Attribute-Based Encryption (ABE) and Attribute-Based Signature (ABS)) have been proposed to grant users access to particular resources in single and multi-domains [31]. The ABE models are mainly focused on the access structure [31] and associates with ciphertext. The user is able to access the data if, and only if the user's attributes can satisfy the access structure, which make ABE models closer to traditional access control. To address the issues relating to traditional and ABE models, the ABS is an interesting and versatile primitive cryptography approach that enables users to sign the message with his or her private key with fine-grained access control, where the private key associates with the user attributes [32]. This enables user anonymity because the verifier only need to check the user attributes. This is of great significance since the access control in cross-domain is based on attributes. However, most current ABS models are still suffering from central authority issues and therefore the ABS models are problematic since both authorities in cross-domain need to generate key parameters for both users and domain authority [33]. These proposed schemes introduce issues such as key management complexity, high communication and computation cost, key size, signature size and also most of proposed models suffering from central authority issues.

Attribute-Based Group Signature (ABGS) is another interesting and useful paradigm of cryptography primitive. This type of model is a generation of focused ABS and group signature [34] to allow users to anonymously sign messages on behalf of another member who processes the attributes [35]. The ABGS was introduced to maintain the signer's anonymity while the user signs the message on behalf of another group member. The signer can sign the message using certain attributes and then the verifier as the manager of the attribute authority accepts the message if, and only if the associated signature demonstrates that this message is signed by a user who possesses adequate attributes to satisfy the given access structure defined in the access policy. The ABGS permits the authority to specify the role of a user who signed the message within the group. Although a generic framework based on the ABGS have been proposed and formulated [13], the proposed model is based on a single authority. This provides further motivation to propose a new approach to address traditional and cryptography access control based on policies for distributed system with an original contribution to eliminate and minimize control of a third party on sensitive data.

B. Our Contribution

In this paper, we look briefly at the history and background of access control models and their limitations. We next discuss access control concepts and existing studies and investigate the interactions and cooperation between different entities in cross-domains. We then focus on two aspects of a network model that result from centralized and decentralized scenarios to identify the effects of these relationships on access control models. For the first time, we propose a new access control model called DMA-ABAC. In our proposed model, there is no requirement for any third party or central authority to generate global parameters, with the exception of generating initial parameters during trusted setup. This makes the DMA-ABAC scheme more scalable, with each attribute authority allowed to independently control their entities. This enables the entire system model to work even in the event that one of the attribute authorities is compromised or corrupted. Hence, we present the first contraction of DMA-ABAC using the generic framework of the ABAC [8], [9] and ABGS [13] standards.

Moreover, we analyse the proposed model and prove that our model able to archives the following security properties: flexible access control with resistance against replay attack, attribute collusion, access control, privacy and selective attribute. To our knowledge, this is the first study to propose a DMA-ABAC using the advantages of classic [8], [9] and

cryptographic [13] ABAC. Within the healthcare area the application of this model is useful to prevent unauthorized user access in the cross-domain, based on the policy system to meet the requirements of HIPAA and NIST and prevent unauthorized user access in cross-domains.

This paper is organized as follows. Section I discusses the background and related work. Section II presents the system model and security requirements. Section III presents an overview of our proposed approach. Section IV gives a specific security evaluation of the proposed model. Section V discusses the significance of our proposed model. Section VI makes some conclusions and mentions future work.

II. System Model And Security Requirements

In this section, we define and present the overview of the ABAC structure as well as the system model based on the ABAC approach for healthcare application and HIPAA rules and regulations. This forms the basis of our proposed DMA-ABAC model. We also describe a security model and the requirements of the proposed model to fulfil the security and privacy requirements. The list of main abbreviations used in this paper are depicted in Table I.

TABLE I
LIST OF ABBREVIATIONS.

Abbreviation	Explanation
AA	Attribute authority to which a patient or user belongs
HHD	The AA where healthcare data are placed
FHD	The AA where the foreign user is placed
EHR	Electronic healthcare 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
ABGS	Attribute-based group signature
PDP	Policy decision point
PIP	Policy information point
PEP	Policy enforcement point
PAP	Policy administration point
O	Data owner where called patient
U	Data consumer where called user
$\mathcal{T}$	Access structure
$\mapsto$	Given permission to
ω	User's attributes obtained from respective AA
CAO	Certificate authority organization

A. ABAC System Model

ABAC is an emerging authorization model that is of interest to industry, academia, and businesses. In ABAC, access to the resources is granted by evaluation of policies and attributes of the subject, object, environment, and action. The subject sends the request to access particular resources in a single domain. The correct access is granted based on policies defined by the system and entity attributes. The main components of the ABAC standard include: 1) policy decision point (PDP); 2) policy administration point (PAP); 3) policy information point (PIP); and 4) policy enforcement point (PEP). This provides a better access control model with greater flexibility. For additional information about the ABAC standard and components refer to [8], [9]. Despite NIST publishing extensive guidelines related to the use of ABAC [8], [9], there is no unique solution or accepted model for multi-domain, and a structure has not been formalized or implemented for cross-domains in practice [12]. Generally, the current ABAC model cannot successfully be applied in cross-domains with multiple security and privacy requirements and setting [8], [9].

B. System Model

The model of healthcare systems that we introduce relates mainly to hospital environments, where each hospital is assumed to constitute one domain with their own security and privacy requirements.

For this, we consider a number of domains including patients and users. These domains are responsible for providing a variety of healthcare services. We assume that each patient and user belongs to one domain. The related patient data are stored in the local healthcare database (HD) in the hospital and should be made accessible through sharing with other users. The users in the same or a different domain may access classified information according to their responsibility. The architecture of the system model is presented in Fig. 1.

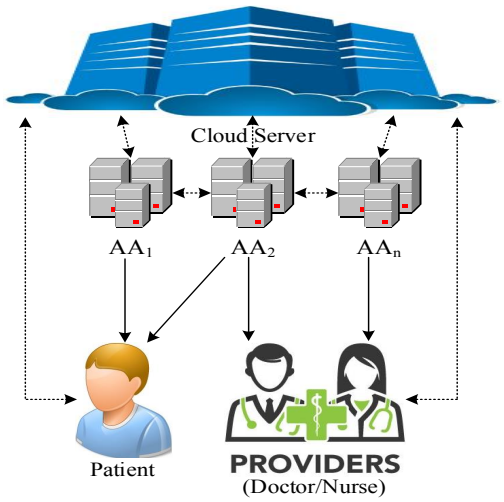

Fig. 1. Cross-Domain System Architecture.

Real life 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 AA such as AA_2 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 HD_1 to be accessible to Bob. Alice does not want to reveal any additional attributes to either Bob or Bob's domain authority or any third party. Bob has attributes {"Hospital 2", "Healthcare service center", "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 further delegate the attributes.

Another specialist, Carol, is registered as U_2 at AA_2 (Carol has attributes {"Hospital 2", "Healthcare service center", "emergency department", and "Doctor with Id = 11"}). She needs to access other data that belong to Alice that should not be accessible by Bob. In our model, both the stakeholders (Bob and Carol) are not interested in delegating their attributes to other stakeholder for further access. The presented model is demonstrated in Fig. 1, including five entities.

- Home healthcare domain (HHD): A hospital can be regarded as a healthcare domain. Each hospital comprises a patient, healthcare service provider and attribute authority component. In our model, the HHD is a trusted domain by itself, where the patient's sensitive data are stored for further services.
- Foreign healthcare domain (FHD): The FHD is a second healthcare domain, such as AA_2. The FHD's actions, regulations, and functionality are the same as for HHD but are located at a different location. The FHD is a foreign domain for the HHD, which means that the FHD can also act as an HHD.
- Attribute authority (AA): The AA acts as the manager of either an HHD or FHD, working under the national and local laws and regulations of its domain. The AA is responsible for managing and generating the required parameters, such as attributes and keys. The AA is trusted for the local domain but not as a foreign AA.
- The data owner (patient) and consumer (user): A patient is a person in a healthcare system who may receive a variety of medical treatments for any particular condition. A user is a healthcare service provider who would like to access patient data. In our model, the patient's healthcare data are stored in a HHD. A patient and user can belong to either an HHD or FHD but must be registered and listed in at least one AA.
- Access structure (τ): The τ includes a group of attributes and policies that need to be satisfied by the access request to grant the user access to particular resources.

C. Threat Model

Here, we introduce the threat model used in this research study to test our system model. The AA is assumed to be trusted by their local domain and is responsible for generating the necessary domain parameters and for verifying and validating the identity of legitimate users in the cross-domain. However, the AA may collapse as a result of an attack. An adversary may try to obtain particular parameters such as attributes and key parameters; this is called a collusion attack. For example, in our model, AA_1 is assumed to be a home server HHD because it stores patient data. An adversary may try to compromise the AA_1 to obtain secret information from the AA_s. The compromised AA will try to verify the user as a legal or illegal user, but the illegal user may obtain access to resources without real authorization. This is called a collusion user attack. As an example, a nurse from AA_2 may try to access patient data in AA_1 which must be accessible to U_1 from AA_2. In addition, a user can forge the attribute, which may allow access to any particular data.

D. Security Requirements

To overcome the problem explained above, the proposed model attempts to meet the following security requirements.

- Collusion resistance: The attacker should not be allowed to use the attributes or any critical domain parameters to decrypt messages, transfer data to illegal users, or delegate to illegal domain authorities.
- Attribute anonymity: The verifier must be able to corroborate a user's signature in an authentication process without revealing any attributes. This property is helpful for tracing the real identity of users while they are in the same group and each user is associated with a huge number of attributes from different domains.
- Dynamic change: This requirement is needed when a user dynamically joins or leaves a domain. The user must be able to obtain access to particular data whilst a user's attributes and permission must be revocable via different techniques and in different scenarios. In addition, it must be possible to revoke a user if his/her attributes are no longer valid in the system.
- Attribute collusion: Users in the same and different domains should be prevented from using the same attributes for their access model.
- Flexible access control: The access control model should be flexible enough to enable any user from visitor authorities to obtain access to particular health data without any registration on a local authority.
- User anonymity: This security requirements is required to secure the privacy of users' identification and attributes while sending requests to access health data in the home authority. This means that the user is not willing to reveal his/her real identity to another AA_s or to any third party.
- Selective attribute: The least number of attributes should be used in access control models, while satisfying the τ defined by the patient.

III. Our Proposed ABAC Approach

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

A. Summary of the Approach

As discussed above, a suitable system architecture is based on the concept of cross-domain. In our system model, the AA_1 is called the home domain and is where patient O is located and where his/her data are stored. The AA_2 is a foreign domain, such as the location of a user U. It is mandatory for both O and U to register with their respective AA. Each AA is responsible for generating the necessary parameters such as the attributes and either private or public keys for their entities. This occurs independently in our system model without relying on a third party. Therefore, a direct connection between O and U with their respective AA is required when U from AA_2 requests access to the data for O in AA_1. Different models, including signature schemes such as group signatures, are feasible solutions because the AA acts as the manager of the domain in our proposed model and can generate, manage, and control either O or U in their AA.

In the second stage, the user (in AA_2) sends a request to access healthcare data in AA_1. For this, first, we assume that access policies are mainly based on the standard published by the NIST [8], [9] with a potential extension of attribute types. The actual request of the user is forwarded to the PEP to check the request and to invoke a policy decision via the PDP. Thus, the request is forwarded to the PDP. The PDP evaluates the access request and monitors if suitable policies can be applied or not. The PDP generates the attribute query, based on the access structure τ and defined by the policy for the requested healthcare data. τ includes particular attributes such as object, subject, action, and environments. The user can access the data if, and only if the users attributes satisfy τ as checked by the authorization engine; otherwise, additional attributes might be requested by the system for new evaluation based on the access request. In this phase, a suitable protocol for the exchange of attributes is required. Attribute-based group signatures, such as [13], are one option to confirm attributes without revealing too much information about the identity of the user. After the PDP in AA_1 receives and checks the attributes, the authorization system permits or denies the access request if, and only if these particular attribute satisfy the policy requirements.

B. Preliminaries

In this section, we introduce the access structure components needed to understand our proposed model. The access structure τ is where a patient uses the policy and security requirements associated with his/her sensitive data to grant a particular permission to an internal or external user. This means that a user needs to satisfy the τ to obtain permission to access specific data from a healthcare database in AA_1. Usually a user is granted access to monitor (read), modify (write) or both on healthcare data while he/she assures the security requirement created by O_1. As a tangible example, a healthcare service provider belonging to AA_2 and a healthcare service center are able to access (write and read) to health data, (τ: (HSP $\wedge$ AA_2) $\mapsto$ read & write).

C. Proposed model construction

In this section we present our proposed model with four phases: multi-authority domain, domain localization, access request, and access decision. The main components of the DMA-ABAC framework is depicted in Fig. 2.

i) Phase 1: Multi-authority domain:

The first stage is dedicated to setup and initiate the multi-authority model. For this stage, the system applies for an attribute authority certificate from the certificate authority organization (CAO). This attribute certificate is only generated for the AA_s if, and only if the AA is legitimate; otherwise, the CAO declines to generate the corresponding certificate. This algorithm uses its secret key and authority's attributes as an input where the public certificate and corresponding group public certificate is generated, which enables the authority's administration for opening the signature.

ii) Phase 2: Domain localization:

In our system model, the respective AA_s generate and distribute the attributes and necessary security parameters to their members under the national and local laws and regulations of the domain while the members provide evidence of their eligibility. Here, we assume that the user is eligible and a member of the domain. After user eligibility is satisfied, the user's attributes are assigned.

iii) Phase 3: Access request:

In this phase and for the first step, the user requests access to particular data at AA_1; the request includes what type data is required to be accessed. In our model, the access request is received by PEP at AA_1, which then calls the PDP for access validation service. Permission is granted by PDP only when the permission is existing and not expired; otherwise, the PDP respond to the user with a request to provide additional attributes that can match and satisfy the τ.

In the second step, the user sends a query to his/her authority to obtain a set of attributes according to the data access structure, which would allow the user to satisfy the policy requirements. The access structure includes particular attributes such as object, subject, action, and environments. For this, AA_2 selects a subset of attributes of all the users attributes that can satisfy the access structure. Based on this subset of the user's attributes, AA_2 generates the user's secret key corresponding to the user's attribute set and public key.

In the third step, the ABGS protocol receives the user's secret key, the access structure τ, the AA_2 public certificate generated by CAO and a message called m that it returns to the user, which includes the formal signature called σ. The user then signs the new access request by running a signature algorithm. The ABGS protocol enables the user to sign the message with fine-grained access control to process the specific user's attributes required for the policy system. At the end, the PEP makes another access request.

iv) Phase 4: Access decision:

As we discussed above, the access determination is determined in AA_1 where the healthcare data is stored for further services.

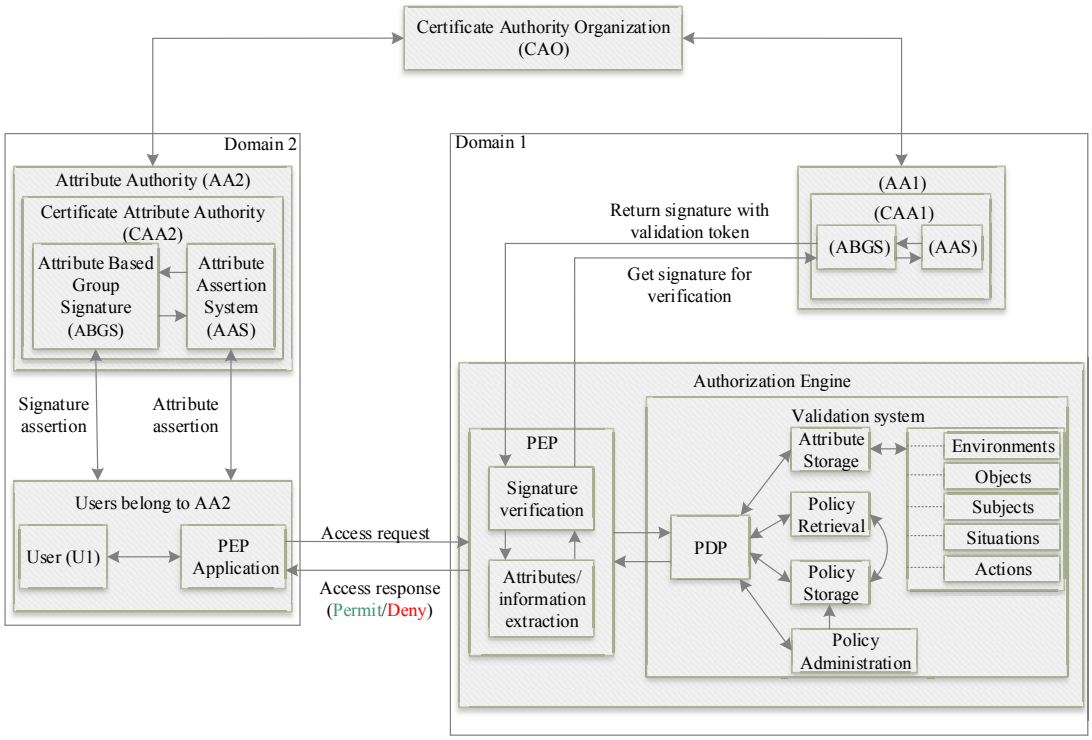

Fig. 2. Framework of the proposed model.

The access decision is made in the PDP, based on the current permission and the patient's access structure after evaluating the access request and corresponding user's attributes. Hence, the user allows access to the health records if, and only if the attributes owned by the user can satisfy the structure define by the patient or the AA_1 on behalf of the patient.

Here and in the first step, the access request is received and evaluated by the PEP whether the access requests comply with the access requirements or not. For this, the signature requires to verify underline ABGS protocol. The verification protocol belonging to ABGS runs by using the AA_2 public certificate generated by CAO, and receives signature plus the access structure τ defined by their PDP. Hence, the algorithm verifies the validity of signature if the access structure and group certificate belong to CAO.

For the second step, the ABGS algorithm also enables the authorization administration to open the signature if, and only if the signature verifies where the output is a subset of the user's attributes. To open the signature, the protocol requires the verified signature and the group public certificate generated by CAO. The output of this algorithm is a set of the user's attributes where it is used to satisfy the access structure. Thus, the user's attributes are extracted from the signature while the signature is verified and opened by the administration of domain. The user's attributes is then forwarded to the PDP for final evaluation.

In the third step, the received attributes are evaluated by the PDP and suitable permissions are generated for the user if, and only if the user's attributes can satisfy the access structure define by authorization system; otherwise, the access request is denied. Using the concept of ABGS enables our access control model to obtain accurate attributes as the signers of a message need to process certain attributes to satisfy the access structure while the ABGS protocol runs in AA_2. The sequence diagram of our model is depicted in Fig. 3.

IV. Security Analysis

We now present a specific security evaluation and analysis of the proposed DMA-ABAC model to demonstrate and highlight the strengths of the proposed scheme.

A. Replay attack:

We presume that there is an adversarial user who intercepted a message belonging to a user. Lets say the adversary sends a request to access healthcare data with the appropriate set of attributes that can, which can satisfy the access policy. To do this, the adversary needs to authenticate him/herself with the authorization system located in AA_1. The authentication

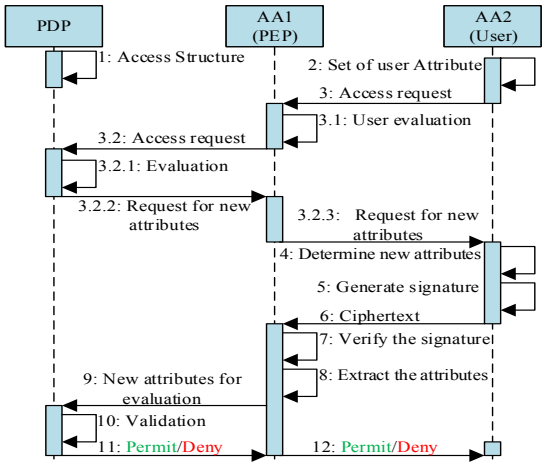

Fig. 3. Sequence diagram of our proposed model.

will be refused while the system recognises that the certificate of the adversary is not matching the certificate of the user belonging to AA_2. This is checked by using the attribute owned by the user and the certificate shared between domains. In addition to this, the generated signature minimises the replay attack while the authorization engine must validate the signature before processing the attributes.

B. Attribute collusion:

Protection against attribute collusion is required as this increases the privacy of the system and prevents illegal access to healthcare data because it generates attributes for two users with either same authority is totally different. This also prevents the authorities from revealing attributes to any authority that should not receive the attributes. Lets say AA_3 and AA_4 handle the set of attributes called ω_3, ω_4 and the healthcare data. In addition, we presume that there are two users called U_3 and U_4 from different domains (AA_3 and AA_4). The ω_3 and ω_4 are denoted as a set of attributes for each user belonging to their respectively authority. For this, we assume that U_3 is interested in accessing the healthcare resource using both ω_3 and ω_4. In this step, the security parameters of U_3 validate the eligibility of the user using the corresponding signature. The system recognizes the user is not valid as his/her attributes do not match with attribute in the system. Hence, this attack will not happen in our system model.

C. Access control and privacy:

A suitable access control framework proposed based on the use of cross-domains presented with the following future to meet the requirements presented model. Our model supports the use of a cross-domain, which can provide both a centralized and decentralized access control model without relying on third party control over healthcare data. As we presented, a user needs to prove his eligibility and evidence to get access to healthcare resources. Here, we presume that the σ cannot forged with any adversary. Hence, the critical information such as attributes will disclosure to corresponding authority where this increase the privacy of sensitive data.

D. Selective attribute:

Selective attribute requires the selection of the least number of attributes to be used in access control models, while satisfying the access structure defined by the patient. The ABGS enables the user to sign a message using certain attributes required for the access structure and then the verifier who is manager of attribute authority accepts the message and attributes if, and only if the associated signature prove that this message is signed by the user who possess adequate attributes to satisfies the given access structure define on access policy.

V. Discussion

This paper introduced the DMA-ABAC model relying on multiple authorities where a user is required to access healthcare resources in cross-domain. This scheme supports the use of a cross-domain, which can provide both a centralized and decentralized access control model without relying on third party control on sensitive resources. We investigated the concept of ABAC approaches, which led us to propose our authorization system model. Our proposed model is a decentralized ABAC approach, which is useful for collaborative healthcare environments. Practically, the proposed model is built based on classical and cryptographic cross-domain access control setting, with each of the authorities responsible to handle and distribute the attributes and necessary security parameters for their entities. According to our model, the access decision making in the domain that the healthcare data located. This increase the privacy of healthcare data against outsider attacker like third party attacker. This also enables the authority to manage and update security and privacy requirements of the respective domain where this can reduce the illegal revealing of healthcare data against internal and external malicious users. Not only does our proposed model enable the access control to achieve what we discussed above, but it also achieves resistance against replay attacks, attribute collusion, privacy and selective attribute. Hence, in contrast to previous work [12], our current proposed model is decentralized and has the ability for dynamic authorization, which directly authorize cross-domain users to access data without relying on a third party and central policy agreement and also without revaluing the privacy and attribute to illegal users and authorities.

VI. Conclusion and Future Work

In this paper, we presented an overview of the current state of knowledge about ABAC problems and the existing relevant models based on single and multiple domain in the healthcare environment. For the first time, a cross-domain framework and access control policy model have been proposed in a model we call DMA-ABAC. This model allows the user

to gain access to healthcare data in a way that fulfills the security and privacy regulations of the NIST and local and international organizations such as HIPAA. We construct the first DMA-ABAC and prove it along with relative security requirements. We achieved a DMA-ABAC scheme which is able to provide flexible access control with resistance against replay attacks, attribute collusion, and privacy of attributes. We believe that this paper proposes an appropriate access control policy model that would be applicable for collaborative healthcare application in distributed environments.

Moving forward from this research paper, we plan to extend and formulate this model to develop an efficient authorization protocol based on the proposed model and given solution. We will evaluate the feasibility of our model by applying the outcomes of this study with further security proof (e.g., attribute anonymity and user anonymity, user and domain traceability and collusion resistance attributes) and analyses and then compare this work with current studies. We plan to develop this model to meet the security and privacy requirements of distributed networks in real healthcare environments.

REFERENCES

[1] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *Communications Surveys Tutorials, IEEE*, vol. 16, no. 3, pp. 1658–1686, Third 2014.

[2] 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.

[3] S. A. Salehi, M. 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.

[4] S. A. Salehi, M. Razzaque, P. Naraei, and A. Farrokhtala, "Security in wireless sensor networks: Issues and challanges," in *2013 IEEE International Conference on Space Science and Communication (IconSpace)*. IEEE, 2013, pp. 356–360.

[5] 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.

[6] J. Grimson, W. Grimson, and W. Hasselbring, "The si challenge in health care," *Communications of the ACM*, vol. 43, no. 6, pp. 48–55, 2000.

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

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] V. Kuchta, G. Sharma, R. A. Sahu, and O. Markowitch, "Generic framework for attribute-based group signature," in *International Conference on Information Security Practice and Experience*. Springer, 2017, pp. 814–834.

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

[15] 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.

[16] S. Bugiel, S. Heuser, and A.-R. Sadeghi, "Flexible and fine-grained mandatory access control on android for diverse security and privacy policies." in *USENIX Security Symposium*. Washington, DC, 2013, pp. 131–146.

[17] 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.

[18] 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.

[19] V. C. Hu, D. R. Kuhn, and D. F. Ferraiolo, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, 2015.

[20] 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.

[21] 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.

[22] 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.

[23] 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*, 2015.

[24] 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.

[25] W. W. Smari, J. Zhu, and P. Clemente, "Trust and privacy in attribute based access control for collaboration environments," in *Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services*. ACM, 2009, pp. 49–55.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

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

[33] 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.

[34] M. Bellare, H. Shi, and C. Zhang, "Foundations of group signatures: The case of dynamic groups," in *Cryptographers Track at the RSA Conference*. Springer, 2005, pp. 136–153.

[35] D. Khader, "Attribute based group signatures." *IACR Cryptology ePrint Archive*, vol. 2007, p. 159, 2007.