Authorization and Interoperability in Access Control Systems

Rajeshwari Gadathas Krishna Babu
Institute of Computer Sciences
Georg-August-Universität Göttingen
Email: r.gadathaskrishnab@stud.uni-goettingen.de

Aytaj Badirova
Institute of Computer Sciences
Georg-August-Universität Göttingen
Email: aytaj.badirova@gwdg.de

Faraz Fatemi Moghaddam
Senior Cyber Security Manager
GWDG, Germany
Email: ffatemi@gwdg.de

Philipp Wieder
Deputy head of GWDG
Institute of Computer Sciences
Georg-August-Universität Göttingen
Email: philipp.wieder@gwdg.de

Ramin Yahyapour
Managing Director of GWDG
Institute of Computer Sciences
Georg-August-Universität Göttingen
Email: ramin.yahyapour@gwdg.de

***Abstract*—A robust policy management framework is necessary to provide strong authorization in access control systems. This study focuses on addressing the authorization and interoperability challenges in access control systems in a collaborative environment. The main purpose of this work is to harmonize the various user identities (roles or attributes) issued by different identity providers, translate them to the right security levels, and grant access to the appropriate resources. This is accomplished using internal broker policy mapping. The broker is a dependable security solution that is managed by the service provider. It assigns appropriate security levels to users while also controlling resource access. The user is recognized using their specified identity, which is further classified based on the possession of identity assurance profiles, credential assurance, or the type of authentication method used. The service provider and the broker reach an agreement on organizational policy and grant authorized users access to the services.**

I. Introduction

Federated single sign-on can also be called Federated Identity Management. It is a trust-based association between separate institutions, and service or resource providers, to exchange identities and authorize users in a multi-domain environment. The eduGAIN is one such identity federation. This inter-federation system integrates identity federations worldwide, facilitating the ability for the global academic and research community to access content, services, and resources [1]. Digital services are becoming critical for science and engineering. Many web services are used by students, lecturers, scientists, and institution employees to cooperate. Providing students and faculty with a simple and easy way to access services is an important criterion for offering services. However, in a multi-domain collaborative environment with different access control measures in place, authorizing users to the appropriate resources might be challenging. This problem may be solved by employing an internal broker policy mapping mechanism, which not only protects the model's privacy but also the security of the collaborative model. In section 2, we will discuss a few literature studies of existing research works. Section 3 introduces the proposed model with the internal broker policy design. Section 4 illustrates a few application scenarios for assessing the model. Finally, section 5 concludes the report.

II. Related Studies

The rapid progress in the domain of security and cloud computing in recent times has prompted several studies on authentication and authorization in access control systems. Few of the existing works in this field have been reviewed in this section. While numerous studies have been conducted in the authentication and access control fields, the majority of the works focus on a single access control model without always integrating diverse models in a heterogeneous environment.

In study [2], the researchers developed an access control framework to be used in a non-dynamic IoT infrastructure. The main advantage of their work is the enhancement of the OAuth 2.0 authorization protocol to conveniently exchange resources and simplify token administration. However, their work did not address the dynamicity which is a very important factor when it comes to interoperability in heterogeneous environments. Therefore, these existing flaws will be addressed by the proposed framework suggested in this paper as it enhances the security, scalability, and interoperability of the system [2]. In [3], the researchers suggested a multi-domain access control mechanism for hybrid environments upon a federation design in which, every organization stays accountable for the access control of their services. However, the study did not evaluate the performance and scalability factors. The work does not involve any assurance levels for users. The work described in study [3] suggest utilizing *Extensible Access Control Markup Language* (XACML) to translate domain access control frameworks into *Attribute based access control*

(ABAC) and applying the generated policy to remote requests to provide interoperability between diverse access control models in the federation. The literature has provided several solutions to the variety of authorization attributes [4]. The attribute mapping proposed in [6] comprises transforming local attributes via derivation criteria into federated variables, which are domain defined but accepted by the federation. The study [5] proposes a scalable architecture based on the ABAC concept to enable multi-internal domain access control methods. However, the preference is to authorize access to a service based on the collaboration contract. While this method protects domain autonomy, it does not fully support authorization alterations.

III. Proposed Model

This section presents the proposed model design which deals with internal broker organizational policies. Figure 1 has 'n' number of Identity Providers and 'n' number of corresponding service providers. The Identity provider is responsible for user authentication. The service embedded inside the IdP is called the 'Broker' which is a service offered by the corresponding service provider. This broker is the crucial component that does the mapping of user roles or attributes and designates the users with the appropriate security levels and forwards the request to the service providers

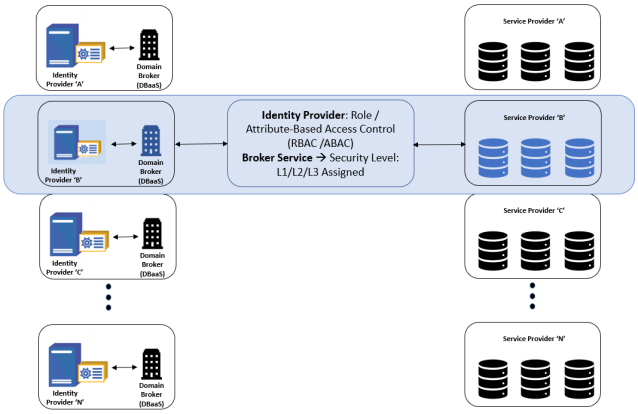

Fig. 1. Model Overview Design

The service provider and the broker service agree on the broker policy. The service provider should concur with the security level that the broker gives to the organizational policy mappings based on their shared understanding. Figure 2 represents the broker policy in detail. The roles or attributes can be classified into three types namely, the type of authentication used, the user's Identity assurance profiles, and the type of credential assurance. The figure is explained in three categories. The first category highlights the different types of authentication methods used. These include memorized passwords, Two-factor authentication, multi-factor authentication, and certificate issued by the identity provider. The second category of classification includes the kind of identity assurance profiles the user possesses. The different types of identity assurance profiles introduced in this policy layout include InCommon profiles: Silver and Bronze and The Voice of Research and Education Identity Federations (REFEDS) profiles: Espresso and Cappuccino. The type of credential assurance, which incorporates knowledge-based confirmation, physical conformation, and Identity provider confirmation, constitutes the final category. The identity provided by the user will be evaluated against these three categories, checked against the policy, and assigned the appropriate security level to access the associated resources as shown in the below figure.

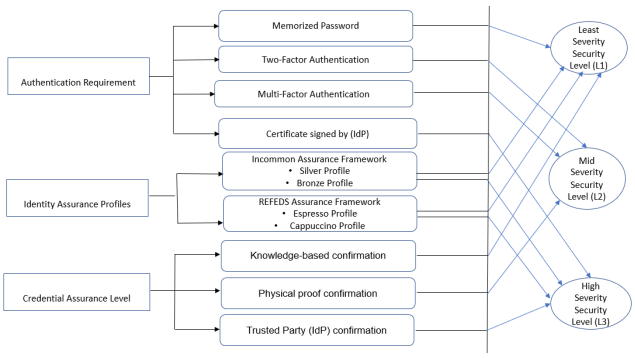

Fig. 2. Broker Policy Mapping

For example, in the first situation, when a user authenticates with a *'Memorized Secret'*, as per the broker policy the user will be assigned with *'Low'* severity privilege level. Therefore the user is assigned security level 'L1' by the broker. Similarly, the security level L2, L3, L4 applies to two factor, multi factor and authentication using certificates issued by identity providers where L4 being the more critical and L1 being least critical privileges. The suggested model takes the advantage of two popular identity assurance profiles namely InCommon and REFEDS. REFEDS supports two types of profiles [8]. They are the REFEDS Espresso profile and REFEDS Cappuccino profile [8]. If the user possesses an Espresso assurance profile, they will be assigned with 'L2' Privilege level by the broker. Espresso profiles are claimed to be more secure than Cappuccino profiles since they incorporate multi-factor authentication. As a result, the broker is alleged to have assigned a security level of 'L3' to users who have Cappuccino profiles so they may access the services. On the other hand, the model also incorporates the InCommon assurance framework. Two distinct types of identity assurance profiles—InCommon Silver and InCommon Bronze profiles—with varying degrees of assurance are made available to users as a result. The National Institute of Standards and Technology (NIST) standard is the foundation of the InCommon Assurance architecture. According to [9] the InCommon silver profile offers identity verification, registrations, etc. It demands credentials that are tough to predict, Sensitive authentication information, improved credential administration, relatively well-verified personal

details about each user, and distinctive subject identifiers. The conditions for the InCommon Bronze profile are lower than those for the InCommon Silver profile [7]. These identity assurance profiles can have differing demands for the same requirement, with the Bronze profile standards being less demanding than the Silver profile standards [7].

The broker service inside the identity provider conducts the roles and attribute mapping based on one of the three major determinants presented by the user. Initially, the user is authenticated by the Identity provider. The user input is then evaluated and analysed based on the access control mechanism implemented by the respective organization. If the user presents a role (for example Tutor) to the identity provider, the broker retrieves the user roles from the same organizational repository and assigns the security level to the user based on their authentication factor or possession of assurance profiles or credential assurance confirmation. On the other hand, if the user submits an attribute (for example a matriculation number), then the broker retrieves all the relevant attributes of the user from the same organization and follows the same process as mentioned earlier in the previous case.

IV. Evaluation and Discussion

The proposed model is examined using a security analysis in this section. We will assess a few user-experience situations and analysis this design and determine their benefits and drawbacks.

A. Security Evaluation

Theorem 1: *Institution A assigns the user role 'Tutor' to its students while Institution B assigns the user role 'Tutor' to its staff*

Proof: Although the users have been granted the role of 'Tutor' in both institutions, their method of authentication, credential assurances, and the level of assurances provided is unique. Therefore, the user can be a student in one institution while being a staff in another institution. These policies are defined inside the internal broker inside their respective identity providers.

Theorem 2: *User Bob from Organization A provides an attribute '2996', a matriculation number to an organization implemented with RBAC framework and User Alice from Organization A provides the role 'Professor' to an organization implemented with ABAC framework*

Proof: When Bob provides an attribute to an RBAC-based institution, the broker service of the institution translates the provided attribute matriculation number to a corresponding role in the institution based on security level assignation. When Alice provides a role to an ABAC-based institution, the role is translated to the corresponding user level and granted access to the required resources. This depends completely on the level assigned by the broker based on organizational internal mapping policies.

Theorem 3: *The organization's privacy policies are not exposed to external organizations*

Proof: Since the identity Providers support a broker service that is offered by the corresponding service provider, the institution's policies will not be exposed to other institutions in a collaborative environment. All the internal broker policy mappings, organizational privacy standards, and user databases are completely secure and cannot be accessed by external domain users.

Therefore, we can state that the proposed model can be considered more flexible, secure, and reliable when compared to other existing models in the current research systems. Therefore, we can state that the proposed model can be considered as more flexible, secure and reliable when compared to other existing models in the current research systems.

V. Conclusion

In a multi-domain environment that employs several access control frameworks, it is challenging to authorize users to the appropriate services or resources. This study introduced a new internal broker mapping policy technique to accurately map resources to users. The policy specifies different levels of authentication for distinct user and service hierarchies. The incorporation of identity assurance profiles and the possession of physical proofs and certificates for critical resource access in broker policy mapping strengthens the security of the proposed approach. The broker is a service administered by the service provider but hosted by the identity provider within each institution. As a result, inside the heterogeneous environment, organizational policies are not shared with external entities, thereby ensuring privacy. Therefore, by assigning security levels, the user roles or attributes are effectively translated and processed utilizing broker internal mapping. This proposed technique may be effectively deployed in a multi-organizational context and offers a flexible identity-translating access control framework.

References

[1] eduGAIN. Enabling Worldwide Access.

[2] Oh, Se-Ra, Young-Gab Kim, and Sanghyun Cho. "An interoperable access control framework for diverse IoT platforms based on oauth and role." Sensors 19.8 (2019).

[3] Abdramane et al. Federation of Services from Autonomous Domains with Heterogeneous Access Control Models.

[4] Preuveneers, D., Joosen, W., Ilie-Zudor, E.: Policy reconciliation for access control in dynamic cross-enterprise collaborations. Enterprise Information Systems 12(3) (March 2018) .

[5] Haguouche, S., Jarir, Z.: Managing Heterogeneous Access Control Models CrossOrganization. In Lopez, J., Ray, I., Crispo, B., eds.: Risks and Security of Internet and Systems. Volume 8924. Springer International Publishing, Cham (2015).

[6] Fragoso-Rodriguez, U., Laurent-Maknavicius, M., Incera-Dieguez, J.: Federated Identity Architectures. In: Proc. 1st Mexican.

[7] InCommon Identity Assurance Profiles : Bronze and Silver.

[8] REFEDS Assurance Framework: Espresso and Cappuccino.

[9] A. Badirova et al. "A Secure and Flexible Method of Permission Delegation Between Different Account Types," 2021 8th International Conference on Future Internet of Things and Cloud (FiCloud), Rome, Italy, 2021.