PhD thesis : Authorization specification and management in multi-cloud infrastructures

8 février 2025

Keywords : distributed security policies, cloud, blockchain, dynamic and contextual access control.
Contact :
Clara Bertolissi, clara.bertolissi@lis-lab.fr
Maryline Laurent, maryline.laurent@telecom-sudparis.eu
Hosting institution :
Aix-Marseille Université (https://www.univ-amu.fr/)
Laboratoire d'Informatique et Systèmes, LIS, UMR 7020, Campus de Luminy, Marseille, France (http://www.lis-lab.fr)

Objectives : The final objective of this thesis is to develop a formal framework for authorization specification and management in multi-cloud infrastructures, as well as the development of mechanisms to detect privilege abuse via a learning-based approach.

Context : In this thesis, we focus on authorization management models and mechanisms in multi-cloud environments. An authorization system must satisfy the key security properties of confidentiality (preventing unauthorized disclosure of resources), integrity (preventing modification of resources without authorization), and availability (ensuring access to a resource by legitimate users when necessary). Cloud-Edge environments are characterized by limited trust, variable computing power, and the involvement of multiple actors with different goals, which complicates the enforcement of security and privacy policies. Multi-cloud brings greater complexity to roles and accountability, and requires even more rigorous management and accountability. There is a need for security mechanisms that ensure control over data and its use.

This thesis aims to develop a scalable authorization framework for cloud applications. Also, abusive access detection will be used to both dynamically limit unauthorized information disclosure and allow access control policies refinement in order to make the principle of least privilege effective.

Part 1 : *Access control models and mechanisms.*

Models that rely on user identities are not fully suited to decentralized and distributed systems. Our goal is to provide a formal access control framework to specify operations and decision-making procedures in a distributed and federated cloud system [4]. The proposed model will be inspired by attribute-based access control and support the notions of contextual information, user groups and relationships between entities (causal, social, defined by the application, etc.)[5]. The model we aim to develop will provide a more fine-grained control w.r.t. traditional models. In particular, different users may have different relationships with the same resources, and resources (or applications) may have dependencies between them. Furthermore, in open and distributed environments such as multi-cloud, access management is inherently dynamic, requiring rules to adapt to evolving conditions. These may include changes in user attributes, revocations, or contextual factors such as geolocation, time of access, device type, or authentication strength [6].

Nowadays, most of the existing authorization solutions rely on a centralized authorization module, which can include policy administration and credential management for authorization decisions (e.g., the authorization server in the case of OAuth2.0 or the PDP/PEP module in the case of XACML) [1]. On the other hand, blockchain has emerged in recent years as a relevant solution to strengthen security and access control in cloud environments [3, 8]. As a distributed and immutable ledger, it guarantees the traceability and integrity of transactions, particularly actions related to access and management of data. With blockchain, it is possible to decentralize the access evaluation process by enforcing access control rules in the form of smart contracts [2]. We aim to explore how blockchain technology can facilitate the recording of contextual information and its integration into access control policies. Smart contracts, stored and executed on the blockchain, make it possible to automate the execution of access control policies. We aim to study how they can be designed to incorporate contextual parameters into the access rules.

Another objective of the research will be an assessment of how blockchain can improve the auditability and traceability of access to sensitive data. By recording each access attempt on the blockchain, the system ensures full transparency and accountability, which is particularly valuable in multi-tenant cloud environments where multiple organizations share access to common resources [9].

Part 2 : *Privilege Abuse and Mitigation Measures.*

The level of security offered by an access control system mainly depends on the correctness of the access control policies used. To this end, several principles to guide the specification of access control policies have been proposed (least privilege, separation of duties, etc.). However, once access privileges are assigned to a user, there is no guarantee that the user will not misuse them. We want to study a proactive solution to detect privilege abuse by complementing the access control system with an anomaly detection system. We would like to exploit learning approaches for the detection of abnormal user behaviors, in order to

learn the behavioral profiles of users accessing resources and to accurately refine the policies [7]. There may be different behavioral profiles, to be determined based on the analysis of contextual knowledge concerning users and resources. Such knowledge has proven to be a valuable source of information for approaches dedicated to improving the detection of internal threats to systems and access control. In particular, the anomaly detection system must check whether access requests are abnormal according to the requester's access behavior profile and, in this case, react by triggering an alert indicating a possible misuse of privileges.

This thesis is part of the France2030 national project ANR-23-PECL-0009 "TRUSTINCloudS" funded by the French National Research Agency. During his thesis, the doctoral student will be required to participate in working groups, summer schools and other activities supported by the project.

Références

[1] S. Dramé-Maigné, M. Laurent, L. Castillo, and H. Ganem. Centralized, distributed, and everything in between : Reviewing access control solutions for the iot. *ACM Comput. Surv.*, 54(7), September 2021.

[2] S. Dramé-Maigné, M. Laurent-Maknavicius, and L. Castillo. Distributed access control solution for the iot based on multi-endorsed attributes and smart contracts. *Proc. of IWCMC'19*, pages 1582–1587, 2019.

[3] F. Ghaffari, E. Bertin, N. Crespi, and J. Hatin. Distributed ledger technologies for authentication and access control in networking applications : a comprehensive survey. *Computer Science Review*, 50 :100590, 2023.

[4] Lewis Golightly, Paolo Modesti, Rémi Garcia, and Victor Chang. Securing distributed systems : A survey on access control techniques for cloud, blockchain, iot and sdn. *Cyber Security and Applications*, 1 :100015, 2023.

[5] Yanchun Zhang Hua Wang, Jinli Cao. *Access Control Management in Cloud Environments*. Springer Cham, 2020.

[6] M. Hummer, M. Kunz, M. Netter, L. Fuchs, and G. Pernul. Adaptive identity and access management—contextual data based policies. *EURASIP Journal on Information Security*, 2016(1) :19, 2016.

[7] Lopamudra Praharaj Mahmoud Abdelsalam Ram Krishnan Ravi Sandhu Mohammad Nur Nobi, Maanak Gupta. Machine learning in access control : A taxonomy and survey. Technical report, arXiv :2207.01739, 2023.

[8] A. Punia, P. Gulia, N. S. Gill, E. Ibeke, C. Iwendi, and P. K. Shukla. A systematic review on blockchain-based access control systems in cloud environment. *Journal of Cloud Computing*, 13(1) :146, 2024.

[9] Worachet Uttha, Clara Bertolissi, and Silvio Ranise. Modeling authorization policies for web services in presence of transitive dependencies. In *Proc. of SECRYPT, (ICETE 2015)*, pages 293–300. INSTICC, SciTePress, 2015.