How blockchain technologies can serve distributed access control

SUPERVISORS:
clara.bertolissi@lis-lab.fr (LIS, Marseille)
Maryline.Laurent@telecom-sudparis.eu (Télécom SudParis, Evry)

Keywords: cloud, blockchain, dynamic and contextual access control.

Le cloud offre une exposition accrue aux menaces telles que les violations de données, les attaques par élévation de privilèges, ou encore le manque de traçabilité. La blockchain se présente comme une solution pertinente pour renforcer la sécurité et le contrôle d'accès dans les environnements cloud [1,2,6]. En tant que registre distribué et immuable, elle permet de garantir la traçabilité et l'intégrité des transactions, notamment les actions liées à l'accès et à la gestion des données.
Le contrôle d'accès repose souvent sur des modèles tels que RBAC ou ABAC, mais ces modèles sont généralement centralisés, avec un administrateur ou une autorité centrale qui contrôle l'accès aux ressources.
Avec la blockchain, il est possible de décentraliser ce processus en enregistrant les règles d'accès sous forme de contrats intelligents (smart contracts). Ces contrats intelligents, stockés et exécutés sur la blockchain, permettent d' automatiser l'exécution des politiques de contrôle d'accès : lorsqu'un utilisateur tente d'accéder à une ressource, les conditions d'accès sont vérifiées automatiquement par le smart contract avant d'autoriser ou de refuser l'accès [7].

Dans un contexte ouvert et distribué comme le cloud, la gestion des accès est souvent dynamique, et les règles doivent s'adapter à des conditions changeantes, comme la révocation ou la modification des attributs utilisateur ou des conditions dynamiques comme un contexte particulier (e.g. la géolocalisation, l'heure de la requête, l'appareil utilisé, la robustesse de l'authentification) [3].
L'objectif de ce stage est d'étudier comment la blockchain peut jouer un rôle en enregistrant ces informations contextuelles et en les reliant aux politiques d'accès.
On peut imaginer que les contrats intelligents soient configurés pour inclure ces aspects contextuels dans les règles d'accès. Par exemple, une règle pourrait spécifier qu'un utilisateur a accès à une ressource uniquement s'il se connecte à partir d'un réseau spécifique ou s'il

présente des preuves d'authentification multi-facteurs.
L'un des objectifs du stage est aussi de déterminer comment utiliser efficacement cette technologie pour renforcer l'auditabilité et la traçabilité des actions effectuées sur les données sensibles.
Chaque tentative d'accès est enregistrée sur la blockchain, garantissant une auditabilité. Cela est particulièrement utile dans les environnements multi-locataires du cloud où plusieurs organisations peuvent accéder aux mêmes ressources [4,5].

Une poursuite en thèse dans le cadre du projet TrustinCloud du PEPR Cloud peut être envisagé à la fin du stage.

References :

[1] Fariba Ghaffari, Emmanuel Bertin, Noel Crespi, and Julien Hatin. Distributed ledger technologies for
authentication and access control in networking applications : A comprehensive survey. Computer
Science Review, 50 :100590, 2023
[2] Aarti Punia, Preeti Gulia, Nasib Singh Gill, Ebuka Ibeke, Celestine Iwendi, and Piyush Kumar Shukla.
A systematic review on blockchain-based access control systems in cloud environment. Journal of
Cloud Computing, 13(1) :146, 2024.
https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-024-00697-7
[3] Matthias Hummer, Michael Kunz, Michael Netter, Ludwig Fuchs, and Gunther Pernul. Adaptive
identity and access management—contextual data based policies. EURASIP Journal on Information
Security, 2016(1) :19, 2016.
[4] Worachet Uttha, Clara Bertolissi, Silvio Ranise: Modeling Authorization Policies for Web Services in Presence of Transitive Dependencies. SECRYPT 2015: 293-300
[5] Clara Bertolissi, Jerry den Hartog, Nicola Zannone: Using Provenance for Secure Data Fusion in Cooperative Systems. SACMAT 2019: 185-194
[6] S.Dramé-Maigné, M.Laurent, L.Castillo, H.Ganem, "Centralized, Distributed and Everything in-between: Reviewing Access Control Solutions for the IoT », Computing Survey (CSUR), DOI 10.1145/3465170, 2021
[7] S. Dramé-Maigné, M. Laurent, L. Castillo, “Distributed access control solution for the IoT based on multi-endorsed attributes and smart contracts”, International Wireless Communications & Mobile Computing Conference (IWCMC 2019),Tangier, Morocco, DOI 10.1109/IWCMC.2019.8766478, June 24-28, 2019