Invitation - Soutenance de thèse de doctorat

Titre : Architecture de partage et stockage des données dans un environnement cloud computing basée sur la technologie Blockchain.

Présenté par : Houaida GHANMI, Doctorante au L2TI.

Date et heure : Vendredi 05 Décembre 2025 à 14h

Lieu : Amphithéâtre Darwin

Jury :

- **BOUZEFRANE Samia** : Professeur, CNAM Paris, Examinatrice
- **IDOUDI Hanen** : Professeur, ENSI Manouba, Examinatrice
- **KHATOUN Rida** : Professeur, Télécom Paris, Rapporteur
- **KHOUKHI Lyes** : Professeur, CNAM Paris, Rapporteur
- **HAJLAOUI Nasreddine** : Docteur**,** FSG Gabes, Encadrant
- **TOUATI Haifa** : Maître de Conférences HDR**,** FSG Gabes, Directrice de thèse
- **BOUDJIT Saadi** : Professeur**,** Université de Rouen Normandie, Directeur de thèse
- **SAIDI Mohand Yazid** : Maître de Conférences HDR**,** USPN, Directeur de thèse

---

Résumé:

Le cloud est une révolution technologique largement considérée comme l'une des innovations modernes les plus importantes, permettant aux organisations d'exploiter leurs ressources informatiques à distance via Internet. Cette thèse se concentrera spécifiquement sur les mécanismes de partage et de stockage sécurisé des données dans le cloud, tout en éliminant la dépendance à des tiers de confiance. Ces mécanismes nécessitent plus de précautions en termes de transparence, d'intégrité, de traçabilité et de confidentialité. Notre objectif principal est donc de proposer une approche hybride combinant stockage on-chain et offchain, tout en maximisant l'efficacité globale en terme de sécurité, performance et coûts de stockage.

Pour résoudre les problèmes de centralisation et de manque de transparence, nous avons proposé une architecture blockchain sécurisée permettant le stockage et le partage décentralisés des données dans un environnement cloud, en s'appuyant sur des contrats intelligents, afin de garantir que seuls les utilisateurs autorisés y aient accès. Ce système répond aux exigences de sécurité en matière de confiance, d'authentification, de confidentialité, d'intégrité et de gestion transparente du contrôle d'accès. De plus, une combinaison d'algorithmes cryptographiques, tels que AES pour le chiffrement des données, ECC pour la gestion des clés et ECDSA pour la signature numérique, est utilisée pour garantir la confidentialité, l'intégrité et la non-répudiation des transactions. Les résultats de simulation démontrent que notre architecture constitue une approche prometteuse pour garantir un contrôle d'accès fiable et atteindre des performances significatives en termes de coûts de calcul et de communication.

Nous avons également évalué le débit des transactions afin d'analyser les performances et l'évolutivité du système proposé. De plus, la robustesse du mécanisme a été confirmée par des analyses formelles utilisant Ban Logic et l'outil AVISPA. Nous avons également proposé une approche d'audit décentralisée et traçable dans un environnement cloud, garantissant que les données stockées dans le cloud n'ont été ni supprimées, ni modifiées. Afin de respecter le critère de confidentialité, nous avons notamment utilisé une application bilinéaire pour vérifier

l'intégrité des données sans révéler d'informations personnelles sur leur propriétaire. Les tâches d'audit sont assignées aléatoirement aux nœuds ou aux utilisateurs du réseau via des contrats intelligents, garantissant une répartition équitable et transparente des responsabilités. Nous avons évalué le temps de traitement de différentes opérations cryptographiques, notamment celles reposant sur l'application bilinéaire, ainsi que le coût total en gaz lié à l'exécution des fonctions des contrats intelligents, mettant en évidence le compromis entre robustesse de la sécurité et performance. Les résultats de cette évaluation confirment la robustesse des améliorations de sécurité que nous proposons.

Mots-clés: Stockage cloud sécurisé, Partage de données, Blockchain, Contrôle d'accès, Audit décentralisé.

Abstract:

Cloud computing is a technological revolution widely regarded as one of the most important modern innovations, enabling organizations to leverage their computing resources remotely via the Internet. This thesis specifically focuses on secure data sharing and storage mechanisms in the cloud, while eliminating reliance on trusted third parties. These mechanisms require increased rigor in terms of transparency, integrity, traceability, and confidentiality. Our main objective is therefore to propose a hybrid approach that combines on-chain and off-chain storage, while ensuring an optimal trade-off between security, performance, and storage costs.

To address the centralization and lack of transparency issues, we have proposed a secure blockchain architecture to ensure decentralized data storage and sharing in a cloud environment through smart contracts, guaranteeing that only authorized users have access. This system meets the security requirements for trust, authentication, confidentiality, integrity, and transparent access control management. In addition, a combination of cryptographic algorithms, such as AES for data encryption, ECC for key management, and ECDSA for digital signatures, is used to ensure transaction confidentiality, integrity, and non-repudiation. Simulation results demonstrate that our architecture is a promising approach to ensuring reliable access control while achieving significant performance in terms of computation and communication costs. We also evaluated transaction throughput to analyze the performance and scalability of the proposed system. Moreover, the robustness of the mechanism was confirmed through formal analyses using BAN Logic (Burrows Abadi Needham Logic.) and the AVISPA tool.

Moreover, the robustness of the mechanism was confirmed by formal analyses using Ban Logic and the AVISPA tool. Moreover, we have proposed a decentralized and traceable auditing approach in a cloud environment, ensuring that data stored in the cloud has neither been deleted, nor modified, nor tampered with. To comply with confidentiality requirements, we employed a bilinear application to verify data integrity without revealing any personal information about the data owner. Auditing tasks are randomly assigned to network nodes or users via smart contracts, ensuring a fair and transparent distribution of responsibilities. We evaluated the processing time of various cryptographic operations, particularly those relying on the bilinear application, as well as the total gas cost associated with the execution of smart contract functions, highlighting the trade-off between security robustness and performance. The results of this approach confirm the strength of the security enhancements we propose.

Keywords: Secure cloud storage; Data sharing; Blockchain; Access control; Decentralized auditing.

Pot : La soutenance sera suivie d'un **pot amical**, pour lequel vous êtes tous chaleureusement conviés. Ce sera une belle occasion d'échanger dans un cadre convivial après la présentation.