

# Blockchain security enforcement based on artificial intelligence in vehicular networks

**Co-supervisors:** Samiha Ayed (University of Technology of Troyes - UTT)

Lamia Chaari (Sfax University – US )

*Le sujet est rédigé en anglais et en français*

## Version en anglais :

The rapid uptake of the intelligent vehicle and the rising popularity of its services, like Collision Avoidance, Cooperative Driving, Traffic Optimization and Payment Services, lead to unprecedented security requirements. The vehicular networks continue presenting many security challenging that may disrupt the users safety. Considering the criticality context of the use of intelligent vehicles, many research efforts are focusing on improving and proposing security solutions to guarantee the user security and safety. These solutions have to consider the different constraints of the traffic volume, real-time exchanges and the mobility. Fulfilling the security requirements of such systems is challenging since the vehicular environments are increasingly complex and evolving. Many directions are possible to deal with this issue. One potential solution is to resort to the blockchain technology. The main advantage of this technology concerning security is the enhancement of the integrity and the traceability properties based on its distributed databases. However, properties like confidentiality, privacy, access control and trust are not directly considered and have to be integrated through specific approaches. The blockchain technology offers the smart contract concept that can be used to integrate new requirements. To enhance the management of the missing security properties based on the blockchain technology, we can make use of the smart contracts combined to the advanced artificial intelligence techniques.

In this context, this thesis proposal aims to design and to validate new blockchain-based approaches to manage security in the vehicular networks context. Several scenarios and road situations have to be defined to pinpoint the different security requirements and test the proposed solutions. Different intelligent approaches based on artificial intelligence techniques (machine learning, deep learning, game theory, etc.) could be considered and combined with the blockchain technology to optimize the proposals.

## Tasks planning

- 1) Task 1: Elaborate a state of the art related to proposed security solutions to solve **access and trust management** issues in vehicular networks.  
This task should be validated at least by one survey paper.
- 2) Task 2: Elaborate a state of the art related to the use of the **blockchain technology and the artificial intelligence techniques** in enhancing the security properties in vehicle networks context. The focus should be on the access control and the trust properties.  
This task should be validated at least by one survey paper.

- 3) Task 3: Design and validate a **new blockchain-based trust approach** to improve and secure intra and inter communications in the vehicular networks. One of the artificial intelligence techniques (game theory, machine learning, deep learning algorithms, ...) can be used to enforce the proposed solution.

This task should be validated at least by one journal paper and one conference paper.

- 4) Task 4: Propose, specify and validate a **new trust-based access control model** considering the task 3. The security policy should be dynamic and contextual to take into account the mobility and distributed aspects of vehicular networks.

This task should be validated at least by one journal paper and one conference paper.

- 5) Task5: To study the **performance evaluation** of the whole proposition in task 3 and task 4 through different **practical scenarios**.

This task should be validated at least by one journal paper or one conference paper.

#### **Possible simulations environments for the blockchain technology:**

Ethereum Testnet, SimBlock, BLOCKBENCH

#### **Version en Français :**

L'émergence rapide des véhicules intelligents et la popularité de leurs services comme la « Collision Avoidance », « Cooperative Driving », « Traffic Optimization » et « Payment Services », a conduit à des nombreuses exigences de sécurité. Les réseaux véhiculaires continuent à présenter des défis qui peuvent perturber la sécurité des utilisateurs. Considérant la criticité de ce contexte, plusieurs travaux de recherche se sont concentrés sur la proposition et l'amélioration de solutions de sécurité pour garantir la sécurité des utilisateurs. Ces solutions doivent prendre en considération les différentes contraintes liées au volume du trafic, aux échanges en temps réel et à la mobilité. Répondre à ces exigences de sécurité pour ces systèmes représente un vrai défi vu leur complexité croissante. Plusieurs approches sont possibles pour traiter ce sujet. Une solution possible est d'avoir recours à l'usage de la technologie de la blockchain. Le principal avantage de cette technologie est qu'elle améliore les propriétés de sécurité d'intégrité et de traçabilité à travers ses bases de données distribuées. Par contre, les propriétés comme la confidentialité, la privacy, le contrôle d'accès et la gestion de la confiance ne sont pas prises en compte et doivent être intégrées en se basant sur des approches spécifiques. La technologie de la blockchain propose le concept des contrats intelligents qui peuvent être utilisés pour intégrer des nouveaux besoins fonctionnels ou non fonctionnels. Pour améliorer les propriétés de sécurité au niveau de la technologie de la blockchain on peut combiner l'usage des contrats intelligents aux techniques de l'intelligence artificielle.

Dans ce contexte, cette thèse a comme objectif de concevoir et de valider une nouvelle approche basée sur la blockchain pour gérer la sécurité dans le cadre des réseaux véhiculaires. Plusieurs scénarios doivent être définis pour spécifier les besoins en sécurité et tester les solutions proposées. Les approches basées sur les techniques de l'intelligence artificielle peuvent être utilisées pour optimiser les solutions proposées.

## **Découpage en tâches**

- 1) Tâche 1: Etude de l'état de l'art concernant les travaux de gestion de la confiance et du contrôle d'accès dans le cadre des réseaux véhiculaires.  
Cette tâche doit être validée au moins par un article survey.
- 2) Tâche 2: Etude de l'état de l'art lié à l'usage de la technologie de la blockchain et de l'intelligence artificielle pour améliorer la sécurité des réseaux véhiculaires. Le focus doit être fait sur le contrôle d'accès et la gestion de la confiance.  
Cette tâche doit être validée au moins par un article survey.
- 3) Tâche 3: Concevoir et valider une nouvelle approche basée sur la gestion de la confiance pour sécuriser les communications intra et inter un réseau véhiculaire. Une technique d'intelligence artificielle (game theory, machine learning, deep learning algorithms, ...) peut être utilisée pour renforcer la proposition.  
Cette tâche doit être validée au moins par un article journal et un article de conférence.
- 4) Tâche 4: Proposer, spécifier et valider un nouveau modèle de contrôle d'accès basé sur la gestion de la confiance en considérant la proposition faite pour la tâche 3. La politique de sécurité doit être dynamique et contextuelle pour prendre en compte la mobilité des réseaux véhiculaires.  
Cette tâche doit être validée au moins par un article journal et un article de conférence.
- 5) Tâche 5: Etudier l'évaluation de performance de la proposition de la tâche 3 et 4 à travers plusieurs scénarios pratiques.  
Cette tâche doit être validée au moins par un article journal ou un article de conférence.

## **Environnement de simulation possibles pour la technologie blockchain :**

Ethereum Testnet, SimBlock, BLOCKBENCH

## **References :**

- [1] Y. Fu, F. R. Yu, C. Li, T. H. Luan and Y. Zhang, "Vehicular Blockchain-Based Collective Learning for Connected and Autonomous Vehicles," in *IEEE Wireless Communications*.
- [2] Dinh, Thang & Thai, My. (2018). AI and Blockchain: A Disruptive Integration. *Computer*. 51. 48-53. 10.1109/MC.2018.3620971.
- [3] Tanwar, Sudeep & Bhatia, Qasim & Patel, Pruthvi & Kumari, Aparna & Singh, Pradeep & Hong, Wei-Chiang. (2020). Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward. *IEEE Access*. 2020. 474. 10.1109/ACCESS.2019.2961372.

[4] Outchakoucht, Aissam & ES-SAMAALI, Hamza & Philippe, Jean. (2017). Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things. International Journal of Advanced Computer Science and Applications. 8. 10.14569/IJACSA.2017.080757.

[5] K. Salah, M. H. U. Rehman, N. Nizamuddin and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," in IEEE Access, vol. 7, pp. 10127-10149, 2019.

[6] Kim, Hyunil & Kim, Seung-Hyun & Hwang, Jung & Seo, Changho. (2019). Efficient Privacy-preserving Machine Learning for Blockchain Network. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2940052.