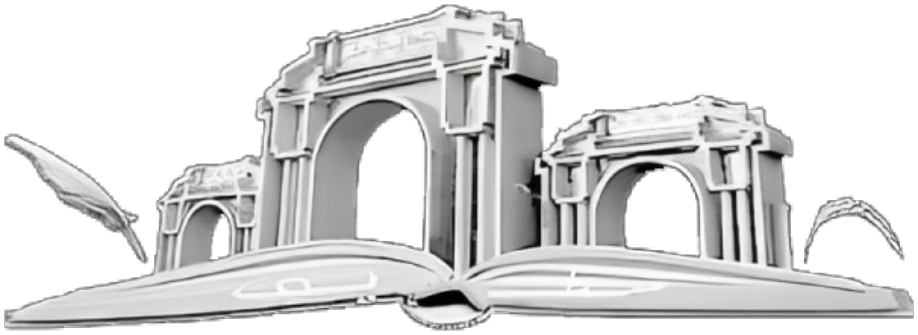
PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

Ministry of Higher Education and Scientific Research

UNIVERSITY SÉTIF 1 FERHAT ABBAS

Faculty of Sciences

Department of Computer Science



جامعة سطيف 1

UNIVERSITY OF SETIF 1

For the obtainment of the degree of

Master in Networks and Distributed Systems

Blockchain-Enabled Trust Management for Secure Data Exchange in Internet of Vehicles

---

Prepared by:

Djelili Tassaadit

Djidjik EL-Djida

Supervised by:

Dr. Cherbal Sarra

Academic Year: 2025–2026

Abstract

The Internet of Vehicles (IoV) enables continuous communication between vehicles and infrastructure, but its open and dynamic nature exposes it to severe security and trust challenges. Existing blockchain-based trust management solutions address these issues only partially, suffering from passive-only detection, static trust update mechanisms, absence of RSU monitoring, monolithic blockchain designs, and lack of fairness toward honest vehicles.

This memoir proposes **ADBT-IoV** (*Adaptive Dual-Blockchain Trust Framework for Secure Data Exchange in Internet of Vehicles*), a unified trust management framework implemented as Solidity smart contracts on an Ethereum blockchain. ADBT-IoV integrates cryptographic vehicle authentication, cross-verification-based message confidence scoring, active probing for hidden malicious behaviour detection, an adaptive AIMD trust update with recidivism memory, RSU anomaly monitoring via the Trust Outlier Factor (TOF) with automatic handover, graduated vehicle management through grey and black lists with a rehabilitation mechanism, broadcast priority proportional to trust, and a Soft Actor-Critic (SAC) deep reinforcement learning agent for dynamic parameter optimization.

Experimental evaluation on a Ganache local blockchain demonstrates that the SAC agent achieves **99.2%** accuracy, **98.6%** detection rate, and **0.6%** false positive rate. Smart contract benchmarks show write latency averaging 61.13 ms and read throughput reaching 182.48 TPS, with CPU consumption below 0.01%, confirming real-time suitability for resource-constrained IoV environments. A comparative analysis shows that ADBT-IoV is the only solution simultaneously addressing all identified limitations of existing approaches.

Keywords: Internet of Vehicles, Blockchain, Trust Management, Smart Contracts, Deep Reinforcement Learning, SAC, AIMD, Roadside Unit, Security.

Résumé

L'Internet des Véhicules (IoV) permet une communication continue entre les véhicules et l'infrastructure, mais sa nature ouverte et dynamique l'expose à de graves défis en matière de sécurité et de gestion de la confiance. Les solutions existantes basées sur la blockchain ne traitent ces problèmes que partiellement, souffrant d'une détection uniquement passive, de mécanismes de mise à jour de confiance statiques, d'une absence de surveillance des unités de bord de route, de conceptions blockchain monolithiques et d'un manque d'équité envers les véhicules honnêtes.

Ce mémoire propose **ADBT-IoV** (*Adaptive Dual-Blockchain Trust Framework for Secure Data Exchange in Internet of Vehicles*), un cadre unifié de gestion de la confiance implémenté sous forme de contrats intelligents Solidity sur une blockchain Ethereum. ADBT-IoV intègre l'authentification cryptographique des véhicules, le calcul d'un score de confiance des messages par vérification croisée, la détection active des comportements malveillants par messages sondes, une mise à jour adaptative de la confiance de type AIMD avec mémoire de récidive, la surveillance des unités de bord de route via le facteur d'anomalie TOF avec basculement automatique, une gestion graduée des véhicules suspects via liste grise et liste noire avec mécanisme de réhabilitation, une priorité de diffusion proportionnelle à la confiance, et un agent d'apprentissage par renforcement profond Soft Actor-Critic pour l'optimisation dynamique des paramètres.

L'évaluation expérimentale sur une blockchain locale Ganache démontre que l'agent SAC atteint **99,2%** de précision, **98,6%** de taux de détection et **0,6%** de taux de faux positifs. Les benchmarks des contrats intelligents montrent une latence d'écriture moyenne de 61,13 ms et un débit de lecture atteignant 182,48 transactions par seconde, avec une consommation processeur inférieure à 0,01%, confirmant l'adéquation temps réel pour les environnements à ressources limitées. Une analyse comparative montre qu'ADBT-IoV est la seule solution traitant simultanément toutes les limitations identifiées.

Mots-clés : Internet des Véhicules, Chaîne de Blocs, Gestion de la Confiance, Contrats Intelligents, Apprentissage par Renforcement Profond, SAC, AIMD, Unité de Bord de Route, Sécurité.

ملخص

يُتيح إنترنت المركبات التواصلَ المستمر بين المركبات والبنية التحتية، غير أنّ طابعه المفتوح والديناميكي يُعرّضه لتحديات أمنية جسيمة تتعلق بإدارة الثقة. تعالج الحلول القائمة على تقنية سلسلة الكتل هذه المشكلات بصورة جزئية فحسب، إذ تعاني من اقتصار الكشف على المراقبة السلبية، وآليات تحديث ثابتة للثقة، وغياب مراقبة وحدات الطرف، وتصاميم أحادية لسلسلة الكتل، وانعدام الإنصاف تجاه المركبات الأمينة.

تقترح هذه المذكرة إطاراً موحداً لإدارة الثقة مُنفَّذاً على شكل عقود ذكية فوق سلسلة كتل لامركزية. يدمج هذا الإطار المصادقةَ التشفيرية للمركبات، وحساب درجة ثقة الرسائل عبر التحقق المتقاطع، والكشف النشط عن السلوكيات الخبيثة المخفية باستخدام رسائل الاستجواب، وتحديثاً تكيّفياً للثقة مع ذاكرة للتكرار، ومراقبةَ وحدات الطرف عبر معامل الشذوذ مع تحويل تلقائي، وإدارةً متدرّجة للمركبات المشبوهة من خلال قائمة رمادية وقائمة سوداء مع آلية إعادة تأهيل، وأولويةَ بث متناسبة مع درجة الثقة، وعاملَ تعلم معزز عميق لتحسين المعاملات بصورة ديناميكية.

يُثبت التقييم التجريبي على سلسلة الكتل المحلية أنّ عامل التعلم المعزز يحقق دقةً بلغت **99,2%**، ومعدل كشف **98,6%**، ومعدل إيجابيات كاذبة **0,6%** فحسب. كما تُظهر معايير العقود الذكية متوسطَ زمن استجابة كتابة بلغ 61,13 ميلي ثانية وإنتاجية قراءة وصلت إلى 182,48 معاملة في الثانية، مع استهلاك للمعالج أقل من 0,01%، مما يؤكد ملاءمة النظام للاشتراطات الزمنية الفعلية في بيئات إنترنت المركبات المحدودة الموارد. ويتّضح من التحليل المقارن أنّ الإطار المقترح هو الحل الوحيد الذي يعالج في آنٍ واحد جميع القيود المُحدَّدة في الحلول القائمة.

الكلمات المفتاحية: إنترنت المركبات، سلسلة الكتل، إدارة الثقة، العقود الذكية، التعلم المعزز العميق، خوارزمية المحاكاة اللينة للعامل والناقد، الزيادة الجمعية والتخفيض الضربي، وحدة الطرف، الأمن.

Contents

Acknowledgments **1**

Abstract **4**

Résumé **5**

6 **ملخص**

Contents **10**

List of Figures **12**

List of Tables **12**

List of Algorithms **13**

List of Abbreviations **14**

General Introduction **16**

1 Blockchain, IoV, and Trust: Background **19**

1.1 Introduction 19

1.2 Blockchain 19

1.2.1 Definition 19

1.2.2 Types of Blockchain 21

1.2.3 Characteristics of Blockchain 22

1.2.4 Classification of Application Domains 23

1.2.5 Consensus Mechanism 26

1.3 Internet of Vehicles (IoV) 28

1.3.1 Definition 28

1.3.2 Types of IoV Communication 29

1.3.3 IoV Architectures 30

1.3.4 Areas of Application 32

1.3.5 Challenges of the IoV 33

1.4 Trust Management in IoV . . . 35
1.4.1 Definition . . . 35
1.4.2 The Concept of Trust . . . 35
1.4.3 Limitations of Centralized Trust Management in IoV . . . 35
1.4.4 Importance of Trust for Data Security and Integrity . . . 36
1.5 Conclusion . . . 37

2 Literature Review **39**

Literature Review **39**
2.1 Introduction . . . 39
2.2 Research Works on IoV Security . . . 39
2.2.1 Trust-based Approaches in IoV . . . 39
2.2.2 Blockchain-based Trust Approaches for IoV Security . . . 41
2.3 Comparative Analysis . . . 43
2.3.1 Comparative Analysis between Trust-Based and Blockchain-Based Approaches in IoV . . . 43
2.4 Related work . . . 45
2.4.1 Blockchain-based Trust Management in IoT and Industrial IoT . . . 45
2.4.2 Blockchain-based Trust Management in IoV and Vehicular Networks . . . 46
2.5 Conclusion . . . 49

3 Proposed approach **51**
3.1 Introduction . . . 51
3.2 Motivation . . . 51
3.3 System Overview . . . 52
3.4 System Entities . . . 53
3.4.1 Vehicles . . . 53
3.4.2 Roadside Units (RSUs) . . . 54
3.4.3 Cloud Certification Authority (Cloud CA) . . . 54
3.4.4 Local Blockchain (RSU Level) . . . 55
3.4.5 Global Blockchain (Cloud Level) . . . 55
3.4.6 DRL Agent . . . 55
3.5 System Architecture . . . 56
3.5.1 Edge Tier – Authentication and Communication Layer . . . 57
3.5.2 Fog Tier – Verification and Detection Layer . . . 57
3.5.3 Fog Tier – Trust Management and RSU Monitoring Layer . . . 57
3.5.4 Cloud Tier – Storage and Intelligence Layer . . . 58
3.6 Trust Model . . . 60
3.6.1 Vehicle Authentication . . . 60

3.6.2 Message Confidence Score . . . 60
3.6.3 Historical Trust Score . . . 60
3.6.4 Active Trust Score . . . 61
3.6.5 Behavioural Trust Fusion . . . 61
3.6.6 Final Trust Score . . . 62
3.6.7 Adaptive Trust Update (AIMD with Recidivism Memory) . . . 62
3.6.8 RSU Anomaly Detection (Trust Outlier Factor) . . . 63
3.6.9 Rehabilitation . . . 64
3.7 Operational Workflow . . . 64
3.7.1 Vehicle Registration and Authentication . . . 64
3.7.2 Message Validation and Trust Computation . . . 64
3.7.3 Trust Score Initialisation and Evolution . . . 65
3.7.4 Grey List and Black List Management . . . 65
3.7.5 Rehabilitation of Blacklisted Vehicles . . . 65
3.7.6 Active Probing for Malicious Behaviour Detection . . . 65
3.7.7 RSU Monitoring using the Trust Outlier Factor . . . 65
3.7.8 Automatic Handover for Compromised RSUs . . . 66
3.7.9 V2V Permission and Broadcast Priority . . . 66
3.7.10 Dual Blockchain Storage and Consensus . . . 67
3.8 Algorithms . . . 68
3.9 Attack Resilience of ADBT-IoV . . . 76
3.9.1 Compromised RSU . . . 77
3.9.2 False Data Injection . . . 77
3.9.3 Sybil / Impersonation . . . 77
3.9.4 On-Off Attack . . . 77
3.9.5 False Consensus . . . 78
3.9.6 RSU-Vehicle Collusion . . . 78
3.9.7 Replay Attack . . . 78
3.10 Conclusion . . . 78

4 Implementation and Evaluation 81
4.1 Introduction . . . 81
4.2 Implementation Tools . . . 81
4.2.1 NPM . . . 81
4.2.2 Node.js . . . 81
4.2.3 Web3.js (Ethereum JavaScript API) . . . 82
4.2.4 Ganache . . . 82
4.2.5 Truffle . . . 82
4.2.6 Solidity . . . 82

4.2.7 MetaMask . . . 83
4.2.8 Python Language . . . 83
4.3 Platform Development Tools . . . 83
4.4 Comparison of Deep Reinforcement Learning Models . . . 84
4.4.1 Performance Metrics of SAC . . . 84
4.4.2 Experimental Setup and Parameter Configuration . . . 85
4.5 Performance Evaluation . . . 89
4.5.1 Performance Metrics . . . 89
4.6 Performance Results . . . 91
4.6.1 Throughput Analysis . . . 91
4.6.2 Latency Analysis . . . 92
4.6.3 CPU Usage Analysis . . . 92
4.6.4 Discussion of Results . . . 93
4.7 Performance comparison . . . 93
4.8 Comparison of ADBT-IoV Approach with Existing Implementations . . . 94
4.9 Backend Implementation . . . 95
4.9.1 Observer API . . . 95
4.9.2 Enterprise API . . . 95
4.10 User Interface Presentation . . . 95
4.10.1 Landing Page . . . 95
4.10.2 Enterprise Authentication . . . 96
4.10.3 Observer Interface . . . 97
4.10.4 Enterprise Dashboard . . . 98
4.11 Conclusion . . . 102

Bibliography **110**

A Annexe Startup **111**