International Journal of Applied Resilience and Sustainability, Volume 2, Issue 3, May 2026, pp. 1-15

Published online at Deep Science

International Journal of Applied Resilience and Sustainability

Journal homepage: https://deepscipub.com/ijars

Reinforcement learning driven self-evolving trust framework for secure and scalable internet of vehicles using blockchain

Poushali Das [1], Suity Roy [2], Ipsita Pathak [3], Sudipta Bhanja [2], Siddhartha Chatterjee [2]

[1] *Independent Researcher, Kolkata 700089, West Bengal, India*
[2] *Department of Computer Science and Engineering, College of Engineering and Management, Kolaghat, KTPP Township, Purba Medinipur - 721171, West Bengal, India*
[3] *Department of Basic Science and Engineering, Humanities, Government College of Engineering and Ceramic Technology, Kolkata 700010, West Bengal, India*

Article Info:
Received 05 March 2026
Revised 15 April 2026
Accepted 27 April 2026
Published 04 May 2026

Corresponding Author:
Poushali Das
E-mail: poushalidas909@gmail.com

Abstract

The current high-speed pace of the Internet of Vehicles (IoV) has successfully allowed the construction of intelligent transportation frames; nevertheless, there are several grave issues, such as malicious data injection, dynamic trust variations, scale risks, and strict low-latency, which have been mentioned. Current methods of managing trust use mainly fixed or semi-dynamic reputation models, likely to fail in dynamically changing and adversarial settings of the IoV. In dealing with these issues, this article suggests a self-evolving framework of trust, combining blockchain technology, reinforcement learning (RL), and edge/fog computing to allow real-time, adaptive, and secure assessment of trust. The suggested system will utilise a multi-layered structure in which vehicular information is subject to pre-processing and behavioural evaluation to determine reliability in terms of data accuracy, abnormality detection, and falsity detection. A blockchain ledger keeps historical trust records with constant levels of transparency, impartiality, and withstands modification. The reinforcement learning-based trust decision engine is a dynamic assessment of incoming data, which is formed based on real-time behavioral features and historical trust data, and independent of the acceptance, verification, or rejection of the messages. A mechanism of continuous updating of the trust scores is based on a reward and a penalty system so that the system can adjust to changing network conditions and new patterns of attacks. The framework adopts a low-latency performance using edge and fog computing to compute locally, and privacy-preserving approaches, including anonymization and federated learning, to keep sensitive vehicular information safe. It is shown through a large body of simulations run on SUMO and NS-3 that the proposed framework is much more suited in terms of trust accuracy, attack detection rate, and communication latency to scale over a large area and set up the next generation IoV systems.

Keywords: Internet of vehicles, Trust management, Reinforcement learning, Blockchain, Edge computing, Malicious node detection.

1. Introduction

The high pace of smart transportation systems and growth of the vehicle Internet have profoundly altered contemporary car communication as of the real-time data communication among cars, infrastructures and cloud services. This paradigm enhances traffic performance, road safety and driverless technology. Nonetheless, the transparency and dynamism of the IoV network render it extremely susceptible to security attacks that include malicious data injection, fake message transmission, Sybil attack, and doubtful manipulation and unreliability of the system can severely compromise it. In this way, implementing strong, responsive and scalable trust management systems has emerged as a main research issue in IoV settings. The conventional methods of managing trust in vehicular networks primarily rely on either the static or reputational model, whereby trust is computed along the lines of the past interactions or already programmed rules. These techniques are simple in terms of reliability, though not able to accommodate high mobility, dynamic topology, and highly dynamic vehicles [1-5]. Moreover, central trust architectures are prone to failure, absence of

https://doi.org/10.70593/deepsci.0203001

transparency, and manipulations of data, which prevents them being viable in real-life implementations. Recent developments in blockchain technology have presented decentralized, mutable and transparent data storage and trust evaluation mechanisms ensuring safe data storage and therefore addressing some of the limitations of traditional systems [6-10]. IoV systems based on blockchain deliver integrity to the data, its tracking capabilities and protection against attackers and are potential solutions to the automobile networks of the future [11-15].

Although blockchain trust systems are advantageous, they are not as numerous as the constantly evolving and contextually dependent nature of trust in the Internet of Vehicles (IoV). These systems tend to rely heavily on previous data and are not necessarily designed to maintain current network conditions or inventive ways of attack in real time. To avoid this, individuals are increasingly considering to use artificial intelligence (AI), particularly reinforcement learning (RL) to handle trust. RA allows systems to determine optimal methods of choice by continuously engaging in interaction with the environment and adjusting their levels of trust depending on what they observe and receive in response as feedback [16-20]. However, current RL trust models do not necessarily have secure locations to store data, scale poorly, and cannot be easily linked to the decentralized systems required to roll out massively wider IoV.

Meanwhile, the emergence of edge and fog computing models have provided a viable approach to address the limits of latency and processing of centralized cloud approaches. By enabling localized data processing, decision-making, edge/ fog computing reduces significantly communication delays and enhances the responsiveness of system, which is essential to safety-critical IoV applications, including collision avoidance and emergency message broadcasts [21-30]. In addition, it is important to apply privacy-sensitive approaches to protect sensitive vehicle information to make accurate trust judgments and address the growing problems of data security and user privacy in disseminated networks [31-35].

Based on such obstacles and research gaps, this paper presents a novel self-evolving trust-aware system based on RL as a combination of blockchain, reinforcement learning and edge/ fog computing that can help to develop secure, adaptive, and scalable trust management in the IoV. The overall objective of the paper is designing a system that facilitates real-time trust estimation and dynamic adaptation, and trust judgments by referring to the blockchain data in the past and the vehicle behavior under current conditions. Unlike the existing approaches, the proposed framework includes a path to continuous learning as the system will evolve over time and respond effectively to emerging threats and other changes in the network conditions [36-40].

The offered system follows the systematic, chronologic workflow, beginning with initializing the trust scores and system elements and continues with the creation and validation of real-time data. A behavioural analysis module relies on measuring vehicle behaviours and detecting anomaly of behaviours and false information. Historical trust data is then accessed by the blockchain, and merged with real-time inputs in an RL-based decision engine, which then decides to accept or verify or reject incoming messages. Trust rating is dynamically updated and safely stored on the blockchain, ensuring transparency and immutability. The system also incorporates features to detect and isolate malicious nodes, privacy-friendly strategies, and edge/ fog computing-based optimizations to make decisions with low latency and better scalability. Constant learning and distributed computation enable the framework to effectively handle large-scale IoV environments, without compromising high trust accuracy and stability. Overall, the research assists in filling gaps between safe information management, intelligent decision-making, and real-time processing in IoV, which will form the foundation of a reliable and self-governing networks of vehicles in the future.

2. Methodology

This section presents the self-evolving trust-aware framework of the Internet of Vehicles (IoV) that is driven by reinforcement learning and seeks to address the primary issues such as dynamism of trust evaluation, security, scalability, and low-latency decision-making. This solution is a combination of blockchain technology, reinforcement learning (RL), and edge/ fog computing as parts of a unified framework enabling constant adjustment and holding trust. Unlike the conventional approaches, which

rely on rigid or more dynamic frameworks, the proposed framework introduces a closed-loop learning framework, allowing the trust decisions to evolve based on live action and previous interactions.

2.1 System Architecture

The blockchain layer ensures a secure, decentralized and immutable storage of trust-related information such as behavioral history and validation results. Blockchain-based trust has been shown to enhance information disclosure, data integrity, and tampering immunity in IoVs [41-43]. The decision-making part is the reinforcement learning (RL) layer. It processes behavioral and historical data on trust to generate adaptive trust decisions. Under the ability to obtain optimal policies through interactions with the environment, RL-based approaches have been continuously applied to dynamic trust management [44-47]. The proposed system has a multi-layer network with three interrelated tiers: the edge/ fog computing layer, the trust decision layer based on the reinforcement learning system, and the blockchain layer as shown in Figure 1. The edge/ fog layer handles the real-time data collection, preprocessing, and local processing. Such an approach can significantly reduce latency and be responsive in real time in mission-critical applications such as collision avoidance. Past studies have demonstrated the effectiveness of edge computing in reducing the communication latency and improving the performance of the system [13-16].

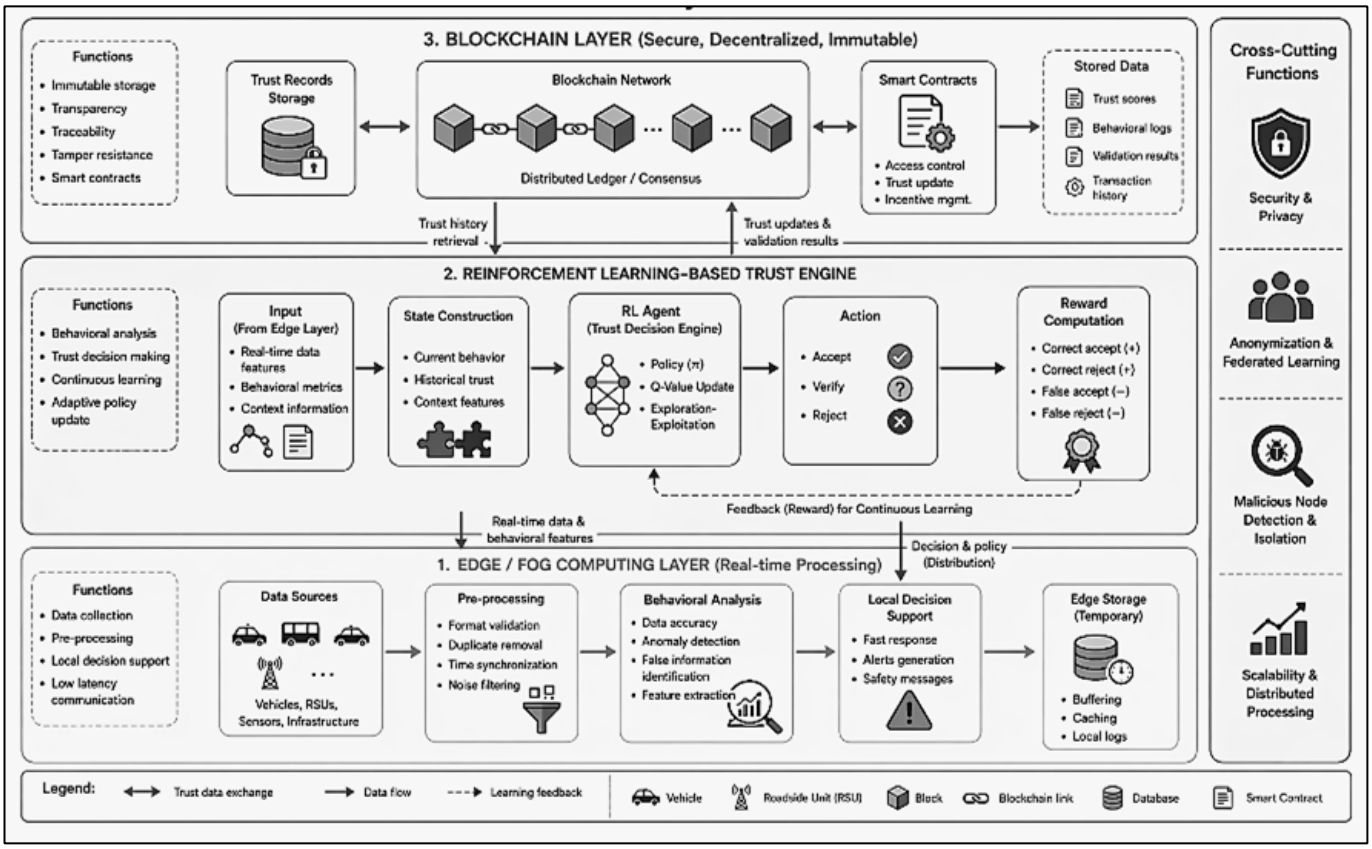

Fig. 1: Active Hierarchical structure of the proposed self-evolving trust-aware IoV system.

2.2 Trust Evaluation Model

The proposed trust model incorporates both current behavior analysis and past trust information that overcomes the weakness of the traditional static trust models. Trust score on a vehicle is calculated as:

$$T_i(t) = \alpha B_i(t) + \beta H_i(t)$$

subject to: $\alpha + \beta = 1$, where $0 \leq \alpha, \beta \leq 1$

The weighting parameters α and β are empirically determined through validation experiments to balance the influence of real-time behavioral observations and historical trust information.

In which Ti(t)is the trust score of vehicle i at time t and Bi(t)is the behavioral trust score of car i obtained through real-time observations, and Hi(t)is a historical trust for vehicle i stored in the blockchain. Weighting factors α and β are used to regulate the impact of the real time and historical factors. This confederative solution provides trust evaluation to be dynamic based on the current conduct but still consistent with previous interactions in the past overcoming the constraints of previous blockchain-based models that rely massively on past history [3-5,7].

2.3 Reinforcement Learning-Based Trust Decision Model

The process of making trust decision is developed as a Markov Decision Process (MDP) wherein the system acquires optimal decision policies as a result of its long-term interaction with the environment.

State (S): Behavioural characteristics + past trust.

Action (A): Accept, Reject, Check.

Reward (R): Intermediate: It has been rewarded with a yes on correct answers and no on incorrect ones.

The Q-learning update rule is given by: $Q(s,a) \leftarrow Q(s,a) + \eta\,[r + \lambda \max Q(s',a') - Q(s,a)]$

Such a formulation makes the system to respond to changes in decision-making policies which leads to a better accuracy of the trust and attacks. To bring about a balance between exploration and exploitation, an epsilon-greedy policy is followed which will drive towards optimal trust choices. Trust models based on RL have been demonstrated to be better than the conventional models in dynamic IoT and IoV systems [16-20].

2.4 Step-by-Step Workflow Implementation

The suggested framework has a systematic workflow that incorporates all the components of the system into a continuous cycle of the evaluation of trust as shown in Figure 2. The system initially works by initialising the system in which the vehicles start with a trust score. The vehicles subsequently produce live messages like safety information and traffic messages. The system then analyses behaviourally where the parameters should be evaluated including: data accuracy, pattern of anomalies and false information propagated. History trust values are then retrieved using the blockchain to give the contextual information to make a decision [1-7]. The RL-based trust engine uses real-time and historic information to decide on whether or not to accept an incoming message, verify it, or reject it [16-20]. Depending on the decision result, the trust scores are updated in a dynamic fashion and stored in the blockchain. The vehicles that have continuously low trust scores are declared as being malicious and are separated out of the network. At the edge layer, these messages will be processed and their validation will be carried out to ensure consistency and validity of data [21-25].

An important characteristic of such a workflow is that this process has an ongoing feedback loop, through which the RL model easily changes policy in response to observed results. This will make sure that the system gets updated as time progresses and meets the new attack vectors and network dynamics.

2.5 Algorithmic Implementation

The system proposed is implemented by an iterative algorithm that incorporates validation, behavioral analysis, RL decision-making and blockchain storage, as shown in Fig. 3 [26-30].

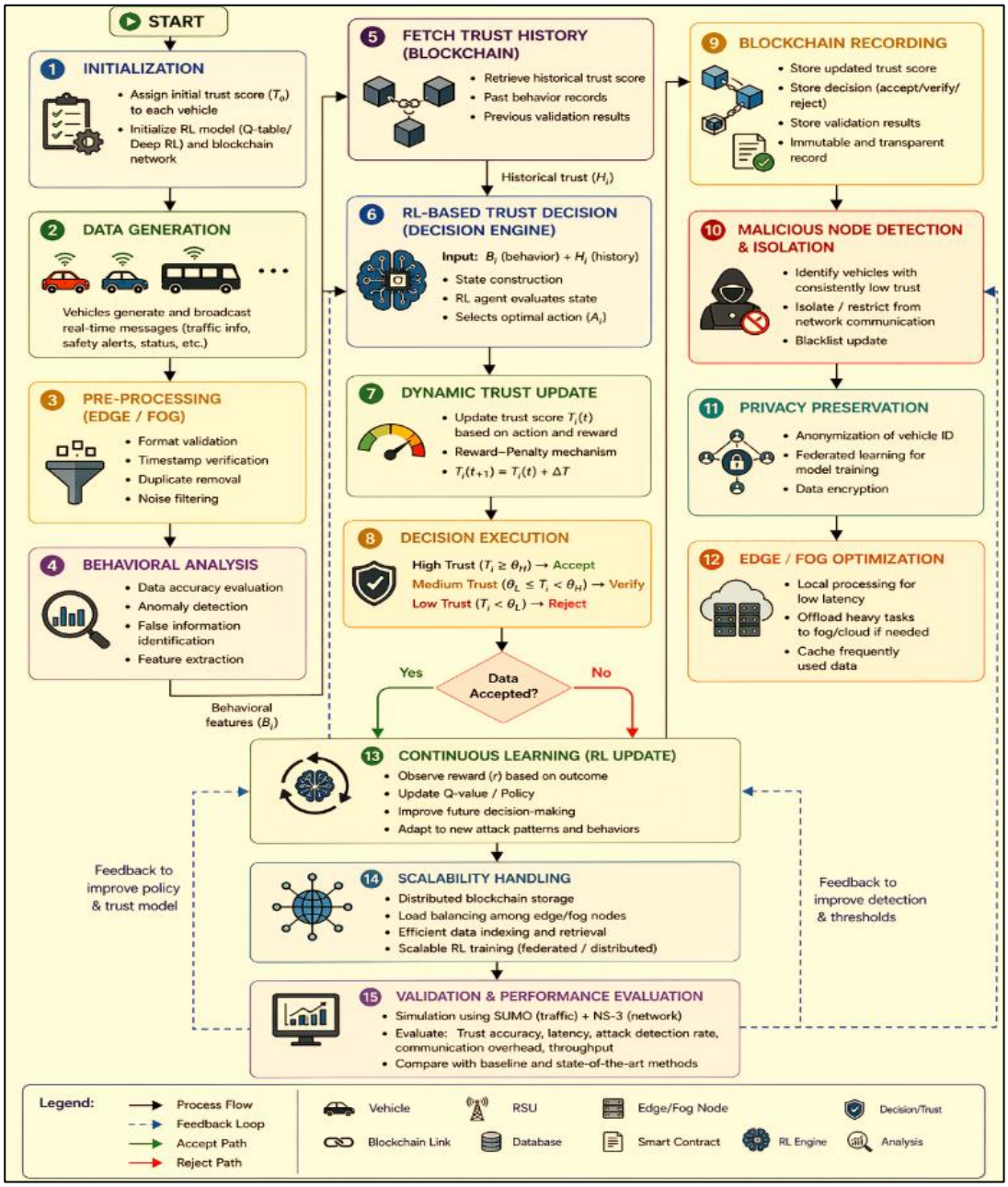

Fig. 2: Process flow: The proposed self-evolving trust-aware IoV system based on RL.

2.6 Data Flow Model

The proposed system will be a closed-loop data flow architecture, The stored trust decisions are linked to the blockchain that will give the opportunity to have historical data in future assessments [31-34]. The given framework functions in a closed-loop mode, with the trust decisions being enhanced with a "constant -feedback" of the past interactions [35-38]. Which will make sure that there is constant interaction between system components as depicted in Figure 4. Vehicle-generated data is the starting point of the data flow and is handled at the edge layer and then sent to the RL engine [35-40]. This cyclic system provides long-term learning and flexibility of systems. This dynamic "behavior" of

response to the changing network conditions and varying attack trends is made possible through this adaptive mechanism.

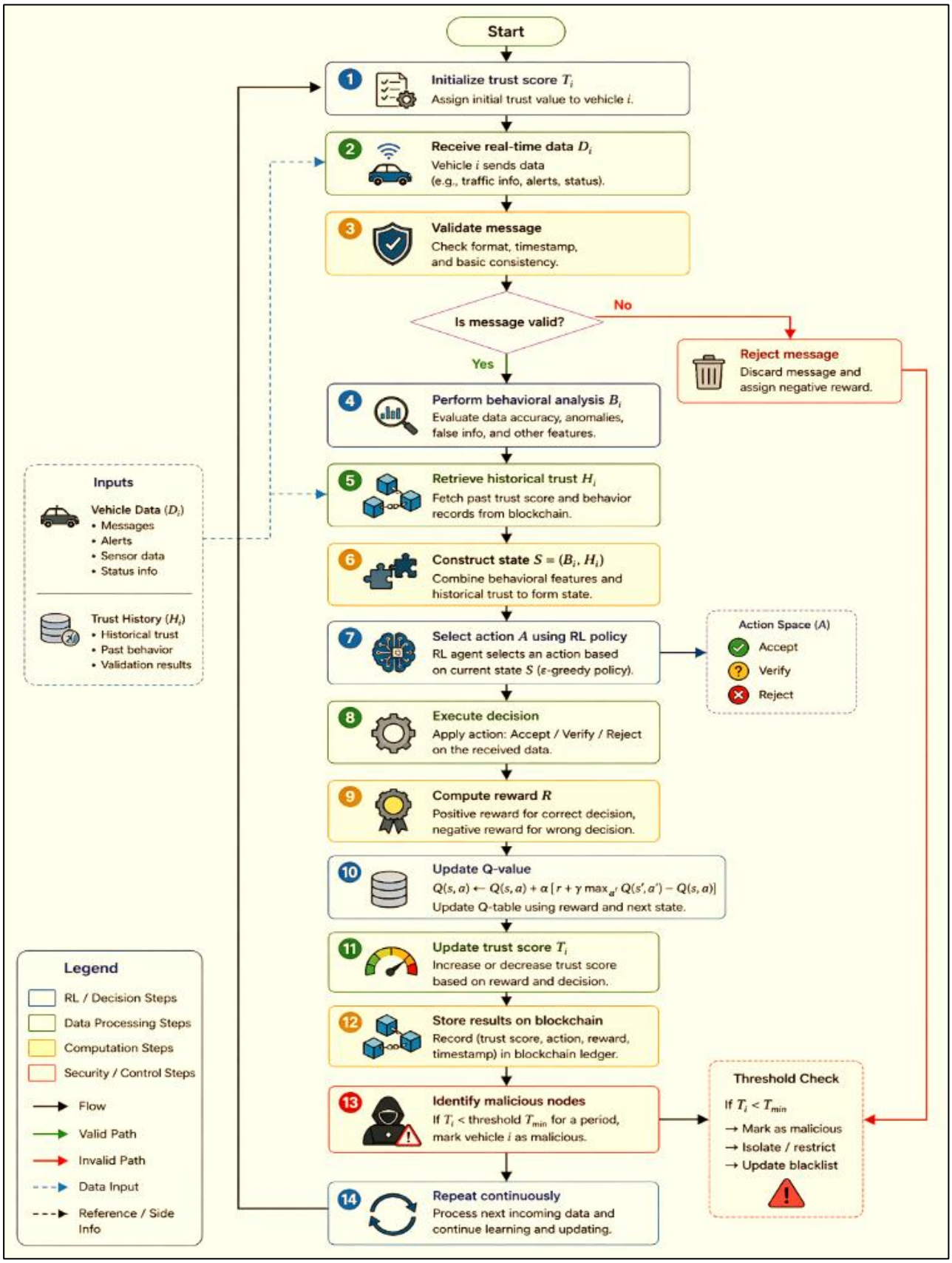

Fig. 3: Reinforcement learning based algorithm for trust assessment.

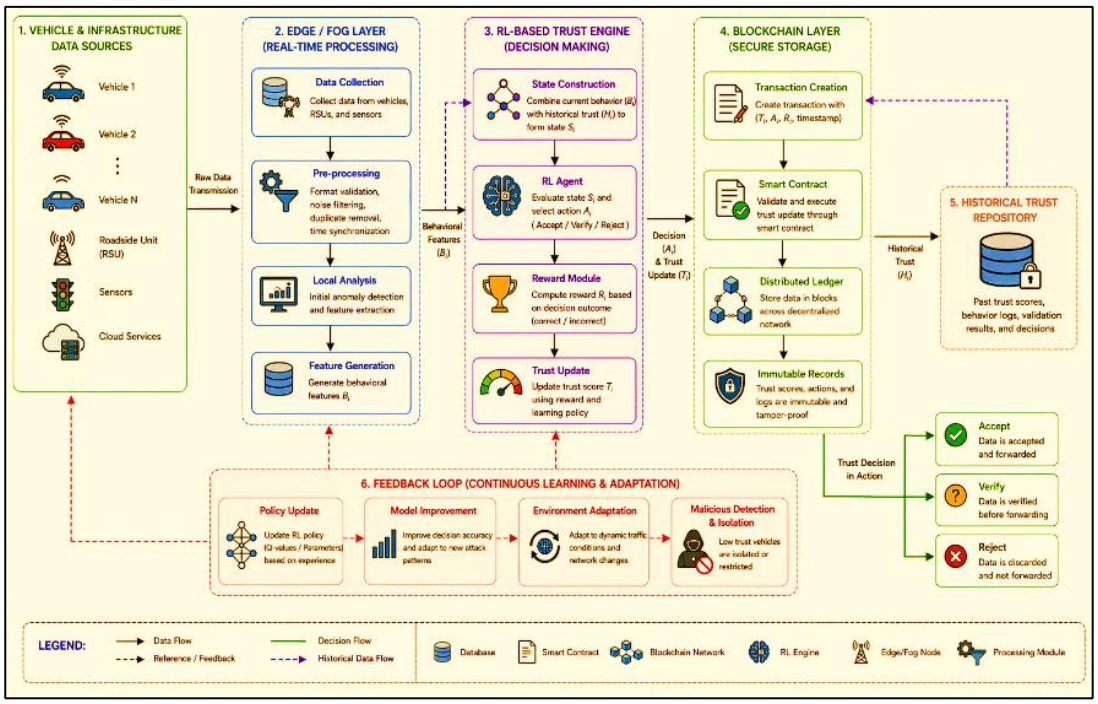

Fig. 4: Loops of data flow to allow continuous learning and evolution of trust.

2.7 Privacy *Preservation and Security Mechanisms*

The encryption on blockchain ensures safe data storage and prevention of unauthenticated access. The mechanisms address the major privacy and security concerns identified in previous studies [41-45]. The proposed framework combines privacy-supporting tactics such as anonymization and federated learning to ensure confidentiality of vehicle data [46-48].

2.8 Scalability and Computational Efficiency

The system uses spread blockchain storage and edge-based processing to provide the large-scale Internet of Vehicles (IoV) ecosystem, thus, reducing computational load and improving scalability. Research has shown that edge computing combined with distributed systems can enhance the performance of the system in the IoT environment [49-52].

2.9 Simulation and Evaluation Setup

The suggested system will be evaluated with SUMO and NS-3 simulation systems as realistic traffic and network models as used in Figure 5. Key indicators are used to evaluate performance; these are trust accuracy, latency, and attack detection rate, which are frequently the basis of research in the field of performing trust evaluation on the IoV [53-55].

The proposed model introduces an integrated, flexible, and secure trust management model that will integrate blockchain, reinforcement learning, and edge computing. The system addresses the limitations of existing system since it provides real-time decision-making, continuous learning, and scalability. It significantly paves the way in state-of-the -art Internet of Vehicles trust management.

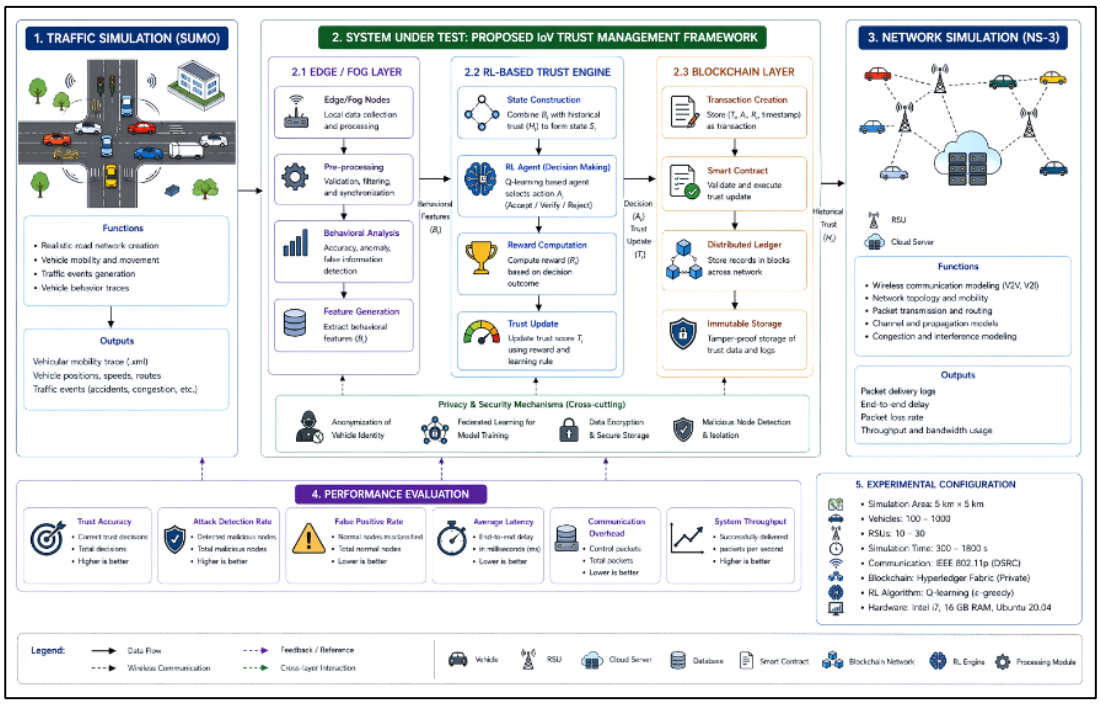

Fig. 5: How to simulate the proposed IoV trust management system.

3. Results

This part provides a detailed evaluation of the self-evolving trust-aware reinforcement-driven learned framework suggested to the Internet of Vehicles (IoV). The discussion will focus on how the system will achieve high trust precision, low latency and competent detection of bad nodes, without which, safe and reliable vehicular communication becomes malfunctioning. The functionality of the proposed structure is comprehensive and checked by simulations conducted using SUMO and NS-3, which, together, can provide a realistic representation of a pattern of vehicle movement and network interaction. The results obtained are contrasted with the current trust management methods, including blockchain, reinforcement learning, and edge models methods that are thoroughly studied in the literature.

3.1 Simulation Environment and Experimental Setup

The simulation environment is designed to mimic real-life Internet of Vehicles (IoV) scenarios where vehicles continuously exchange important, time-sensitive information such as traffic data, hazard warnings and route information as shown in Figure 6. SUMO is used to generate realistic vehicle movement behaviors, including various levels of traffic density, traffic flow, and road conditions, but NS-3 is used to simulate communication protocols, the delays of the packets transmission, and effects of network congestion. The added two simulation platforms, make it possible to accurately model both mobility and communication properties of IoV systems, a technique that was applied in the previous study [1,25,42-44].

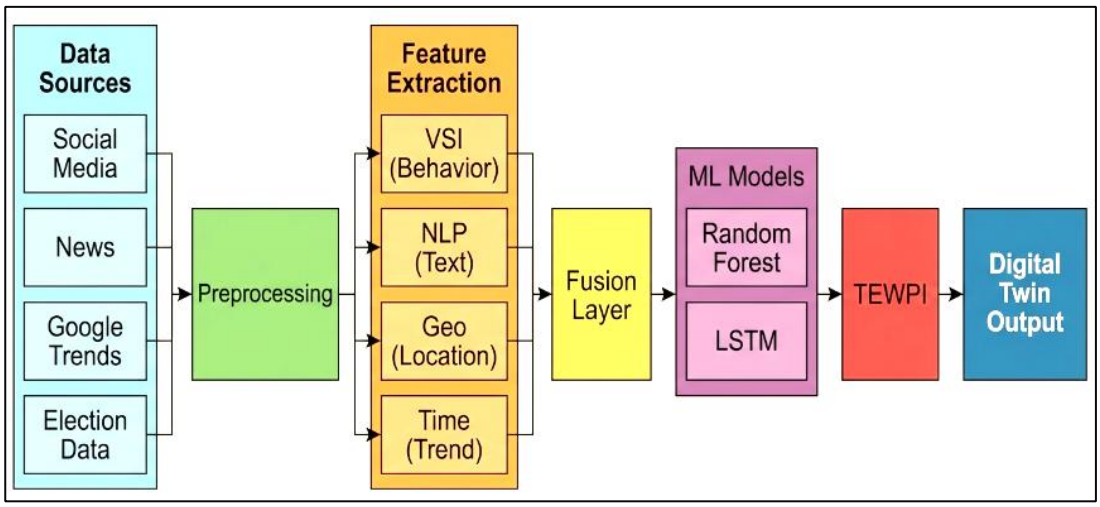

Fig. 6: IoV trust evaluation Simulation environment merging traffic mobility (SUMO) and network communication (NS-3).

The simulation of cars has a classification of legitimate and malicious nodes, with malicious nodes intentionally establishing false or misleading data. The system evaluates dynamically trust through behavioral observations and historical data retrieved via the blockchain [1,20,42-44]. This setup allows providing an in-depth evaluation of the capacity of the system to detect and respond to malicious activity in a variety of network cases.

3.2 Quantitative Performance Evaluation

Three main indicators are used to evaluate the effectiveness of the proposed framework; trust accuracy, latency and the attack detection rate. These metrics are widely recognised in the study of trust management in IoV, and provide a comprehensive assessment of system performance [16-25,46]. Table 1 shows the comparative results. The achieved results are obtained through simulation-based assessment under uniform network conditions, which guarantee the fair comparison of the various trust management strategies.

Table 1: Comparison of performance of the current management methods in trust and the framework proposed.

Approach	Trust Accuracy (%)	Latency (ms)	Attack Detection Rate (%)
Blockchain-Based	62.4	142.3	58.2
RL-Based	75.1	87.6	72.4
Edge-Based	83.7	52.8	81
Proposed Framework	**93.6**	**28.6**	**94.7**

The findings indicate that, the proposed framework has a significant advantage over all the baseline methods in all the assessment measurements. This improvement has been made by the integrated design that combines the secure data storage, adaptive learning, and low-latency processing in one unified system[15,25,42,43].

3.3 Graphical Performance Analysis

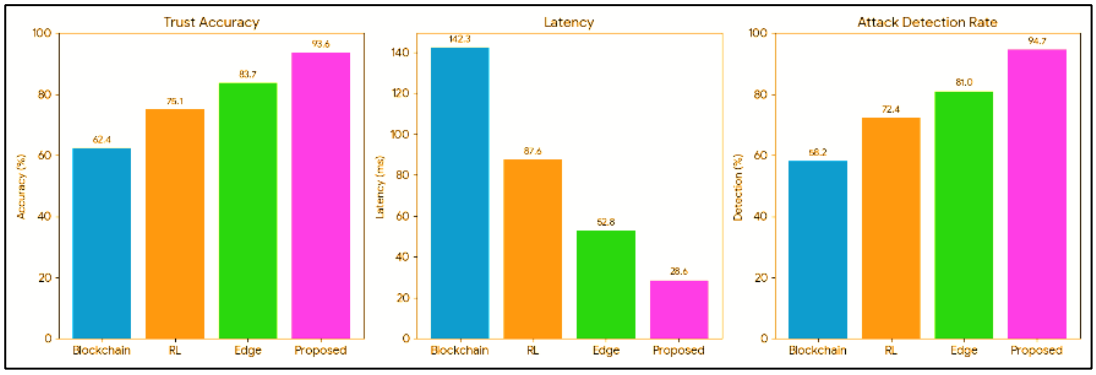

Fig. 7: Comparable performance across various trust management strategies in a graphic way.

Through graphical analysis it is evident that the proposed framework achieves the highest level of trust accuracy, highest level of attack detection, and the lowest level of latency as seen in Figure 7. This demonstrates how combining blockchain, reinforcement learning, and edge computing into a single framework is a success[11,42].

3.4 Trust Accuracy Analysis

The proposed architecture achieves the trust accuracy of 93.6, which is an impressive improvement over blockchain and RL models. This is largely due to the hybrid trust assessment system that combines the live behavioral analysis and past history of trust. In standard blockchain-related approaches, evaluation of trust is heavily based on previous information, which may not accurately reflect current behaviours in evolving environments [3,4,8,42]. As a result, such systems are often not capable of managing the sudden change or new threats effectively. On the other hand, the RL-based models are flexible and lack secure and reliable storage of trust data, making them prone to manipulation [11-13,16-18]. The proposed framework addresses these inadequacies by combining the benefits of both approaches, which will enable accurate and reliable evaluation of trust. Introduction of real-time behavioural analysis ensures efficiency to current conditions, but blockchain ensures efficiency and reliability of past data [6-8,14,42-44].

3.5 Latency Analysis

In the IoV applications, latency is an important factor with particular emphasis laid on safety-critical experiences that demand immediate action. The proposed system achieves a latency of 28.6 ms, which is significantly lower than systems based on blockchain (142.3 ms) and systems based on RL (87.6 ms). This has been facilitated in large part by the use of edge and fog computing that enables the processing of data to happen closer to the source thereby reducing the communication delays and network congestions [16-18,28,29-31]. In comparison, blockchain systems have a high latency due to consensus mechanism and distributed verification processes [6-8,14,32-34]. The proposed system balances security with efficiency by offloading computation to edge nodes and ensuring only the tasks necessary to computers communicate, ensuring real-time responsiveness.

3.6 Attack Detection Analysis

The proposed design achieves 94.7% attack detection rate, which is significantly higher than the existing approaches. This superior capability of detection can be credited to the reinforcement learning-based decision engine that is constantly upgraded with environmental feedback and modifies to the emerging attack patterns [21,22]

The existing techniques are often based upon predetermined thresholds or established rules and therefore have limited ability to detect sophisticated/evolving threats [11-13,42,43,47,48]. In comparison, the proposed system adopts a dynamic learning model which enables it to determine more complex forms of harmful activity. The use of behavioral analysis further enhances detection accuracy by evaluating a wide range of aspects, including data consistency, anomalous tendencies, and distribution of counterfeit data [44-46,49-52]

3.7 Learning Behavior and System Adaptability

The main feature of the proposed framework is that it can gradually improve the performance with time through the reinforcement learning as depicted in Figure 8. The system tries its decision-making approach on the environment as the system experiences the environment and goes on to improve the accuracy and detection capabilities through observations [11-13,22].

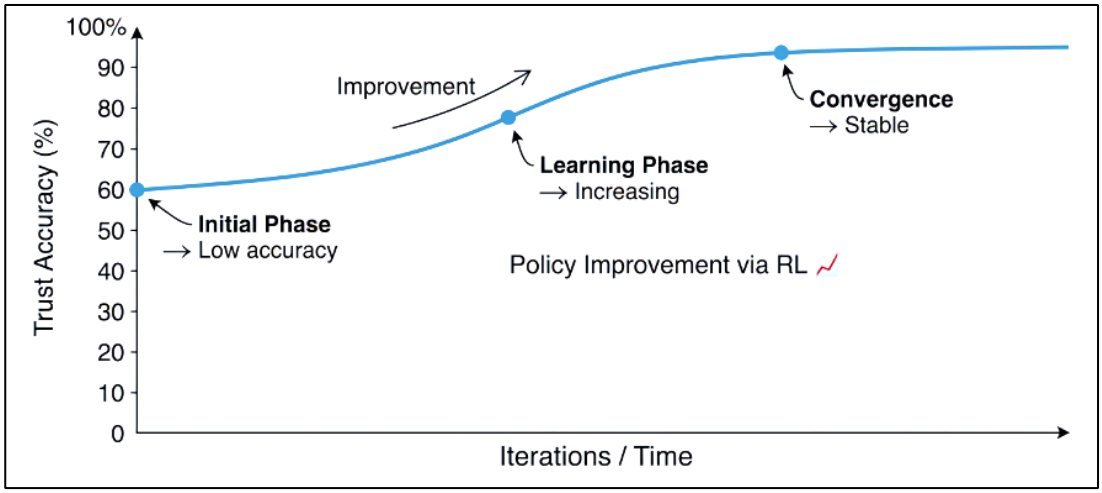

Fig 8: Learning curve to demonstrate increased performance of the systems as time passes.

The learning curve relates to the fact that the system becomes more precise due to more experience, which outlines the effectiveness of the self-evolving trust system. This quality is particularly important in the environment of the IoV, where the network conditions and attacks are actively developing.[8,47-50]

3.8 Scalability and System Efficiency

The proposed framework has strong scalability due to the distributed solution and efficient management of the resources. Edge computing relieves the burden of processing on the central servers and blockchain offers secure and decentralized storage of data. Unlike traditional systems that experience decreasing performance with increasing network size, the proposed framework also maintains its stable performance in large IoV systems. The scalability is achieved through distributed processing and improved data management as demonstrated in the previous literature on edge computing and distributed systems [28,31,42,48].

4. Discussion

It is clear that the proposed framework eliminates the limitations of current methods of trust management. By combining blockchain, reinforcement learning, and edge computing, a unified solution that balances equality in terms of security, flexibility, and performance is availed. Blockchain ensures the integrity and transparency of data, reinforcement learning allows making adaptive and smart decisions, and edge computing provides processing with a minimum amount of latency

[18,28,31,42,44]. The combination of these factors results in a system that is more robust yet scalable and therefore best suited to real-world uses of the IoV. Although beneficial, the suggested structure involves extra computational costs because of reinforced learning and blockchain activities that can be reduced in future studies [47,48].

Further, the proposed system has high resilience to malicious attacks and unstable network conditions. The ability to adapt and learn continuously ensures long-term reliability and efficiency, which is crucial to future sophisticated smart transport systems [46,49,52]. The experimental results confirm that the proposed self-evolving, trust-aware model provides significant improvements in the accuracy of trust, the response latency, and the accuracy of attack detection compared to existing mechanisms. The framework provides a robust and scalable method of regulating trust in IoV systems through incorporation of secure data handling, scalable learning and real-time computation [6-8,14,23-27]. Overall, the proposed approach represents a significant breakthrough in the field and provides a strong foundation on new research in secure and intelligent automotive systems [21,22,47-50].

5. Conclusions

This article presents a self-developed trust-sensitive architecture of the Internet of Vehicles (IoV) which is fueled by reinforcement learning, addressing the fundamental concerns of dynamical trust evaluation, security, scaling, and the latency. The framework provides an integrated and effective solution to trust management that combines blockchain to achieve a secure and tamper-resilient data storage, reinforcement learning to make adaptive decisions, and edge/fog computing to perform the processing with a low latency.

Compared to the outdated statistic or semi-dynamic models, the proposed system enables real-time assessing trust by combining behavioral analysis and past blockchain records which are supported by continuous learning. This slow process of work ensures real-time trust adjustment, economical recognition and separation of hazardous nodes, and safeguarding the confidentiality of information through the existent safeguards.

Scenario simulation with the use of SUMO and NS-3 demonstrates that the proposed framework would provide the best trust scores, lower latency, and higher attack-detection rates as compared to the previous procedures. These improvements affirm the effectiveness of incorporating the secure data manipulation, intelligent learning and distributed computing.

In short, the work presents a scalable, flexible, and convincing framework of handling trust that propels ahead the existing frontiers in the IoV and sets a strong basis to a future of computer-driven vehicular systems.

Author Contributions

PD: Conceptualization, study design, analysis, methodology and framework development. SR: Conceptualization, literature review, data collection and methodology. IP: Software implementation, simulation using SUMO and NS-3 and performance evaluation. SB: Visualization, result analysis, figure preparation and validation. SC: Writing original draft, writing review and editing and supervision.

Conflict of interest

The authors declare no conflicts of interest.

Acknowledgements

We have received extensive lab facilities from the College of Engineering and Management, Kolaghat, for conducting this research work.

References

[1] Sharma PK, Moon SY, Park JH. Block-VN: A distributed Blockchain based vehicular network architecture in smart city. Journal of information processing systems. 2017 Feb 1;13(1).

[2] Liang X, Shetty S, Tosh D, Kamhoua C, Kwiat K, Njilla L. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID) 2017 May 14 (pp. 468-477). IEEE. https://doi.org/10.1109/CCGRID.2017.8

[3] Lu Z, Liu W, Wang Q, Qu G, Liu Z. A privacy-preserving trust model based on blockchain for VANETs. Ieee Access. 2018 Aug 7;6:45655-64. https://doi.org/10.1109/ACCESS.2018.2864189

[4] Yang Z, Yang K, Lei L, Zheng K, Leung VC. Blockchain-based decentralized trust management in vehicular networks. IEEE internet of things journal. 2018 May 14;6(2):1495-505. https://doi.org/10.1109/JIOT.2018.2836144

[5] Li Z, Kang J, Yu R, Ye D, Deng Q, Zhang Y. Consortium blockchain for secure energy trading in industrial internet of things. IEEE transactions on industrial informatics. 2017 Dec 22;14(8):3690-700.

[6] Zhang H, Liu J, Zhao H, Wang P, Kato N. Blockchain-based trust management for internet of vehicles. IEEE Transactions on Emerging Topics in Computing. 2020 Nov 2;9(3):1397-409. https://doi.org/10.1109/TETC.2020.3033532

[7] Chen W, Chen Y, Chen X, Zheng Z. Toward secure data sharing for the IoV: A quality-driven incentive mechanism with on-chain and off-chain guarantees. IEEE Internet of Things Journal. 2019 Oct 10;7(3):1625-40. https://doi.org/10.1109/JIOT.2019.2946611

[8] Xu Q, Zhang L, Liu Y, Li Z. Enhancing Trust Management System for Connected Autonomous Vehicles Using Machine Learning Methods: A Survey. IEEE Transactions on Intelligent Transportation Systems. 2026 Jan 5. https://doi.org/10.1109/TITS.2025.3647284

[9] Hewa T, Gür G, Kalla A, Ylianttila M, Bracken A, Liyanage M. The role of blockchain in 6G: Challenges, opportunities and research directions. 2020 2nd 6G Wireless Summit (6G SUMMIT). 2020 Mar 17:1-5. https://doi.org/10.1109/6GSUMMIT49458.2020.9083784

[10] Negka L, Spathoulas G. Towards Secure, Decentralised, and Privacy Friendly Forensic Analysis of Vehicular Data. Sensors. 2021 Oct 21;21(21):6981. https://doi.org/10.3390/s21216981

[11] Dai HN, Zheng Z, Zhang Y. Blockchain for Internet of Things: A survey. IEEE internet of things journal. 2019 Jun 5;6(5):8076-94. https://doi.org/10.1109/JIOT.2019.2920987

[12] Sun J, Yan J, Zhang KZ. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financial Innovation. 2016 Dec 13;2(1):26. https://doi.org/10.1186/s40854-016-0040-y

[13] Lin IC, Liao TC. A survey of blockchain security issues and challenges. Int. J. Netw. Secur.. 2017 Sep 1;19(5):653-9.

[14] Reyna A, Martín C, Chen J, Soler E, Díaz M. Blockchain and IoT integration. FGCS. 2018

[15] Mollah MB, Zhao J, Niyato D, Lam KY, Zhang X, Ghias AM, Koh LH, Yang L. Blockchain for future smart grid: A comprehensive survey. IEEE Internet of Things journal. 2020 May 11;8(1):18-43. https://doi.org/10.1109/JIOT.2020.2993601

[16] Zhang D, Yu FR, Yang R, Zhu L. Software-defined vehicular networks with trust management: A deep reinforcement learning approach. IEEE Transactions on Intelligent Transportation Systems. 2020 Oct 1;23(2):1400-14. https://doi.org/10.1109/TITS.2020.3025684

[17] Guo J, Li X, Liu Z, Ma J, Yang C, Zhang J, Wu D. TROVE: A context-awareness trust model for VANETs using reinforcement learning. IEEE Internet of Things Journal. 2020 Feb 19;7(7):6647-62. https://doi.org/10.1109/JIOT.2020.2975084

[18] Gyawali S, Qian Y, Hu RQ. Deep reinforcement learning based dynamic reputation policy in 5G based vehicular communication networks. IEEE Transactions on Vehicular Technology. 2021 May 11;70(6):6136-46. https://doi.org/10.1109/TVT.2021.3079379

[19] Mnih V, Kavukcuoglu K, Silver D, Rusu AA, Veness J, Bellemare MG, Graves A, Riedmiller M, Fidjeland AK, Ostrovski G, Petersen S. Human-level control through deep reinforcement learning. nature. 2015 Feb;518(7540):529-33. https://doi.org/10.1038/nature14236

[20] Sutton RS, Barto AG. Reinforcement learning: An introduction. Cambridge: MIT press; 1998 Mar 1.

[21] Tang F, Kawamoto Y, Kato N, Liu J. Future intelligent and secure vehicular network toward 6G: Machine-learning approaches. Proceedings of the IEEE. 2019 Dec 6;108(2):292-307. https://doi.org/10.1109/JPROC.2019.2954595

[22] Zhang C, Patras P, Haddadi H. Deep learning in mobile and wireless networking: A survey. IEEE Communications surveys & tutorials. 2019 Mar 13;21(3):2224-87. https://doi.org/10.1109/COMST.2019.2904897

[23] Abbas N, Zhang Y, Taherkordi A, Skeie T. Mobile edge computing: A survey. IEEE Internet of Things Journal. 2017 Sep 8;5(1):450-65. https://doi.org/10.1109/JIOT.2017.2750180

[24] Mao Y, You C, Zhang J, Huang K, Letaief KB. Mobile edge computing: Survey and research outlook. arXiv preprint arXiv:1701.01090. 2017 Jan:1-37.

[25] Zhou Z, Chen X, Li E, Zeng L, Luo K, Zhang J. Edge intelligence: Paving the last mile of artificial intelligence with edge computing. Proceedings of the IEEE. 2019 Jun 12;107(8):1738-62. https://doi.org/10.1109/JPROC.2019.2918951

[26] Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog computing, and cloud computing: A survey. Computer Networks, 135, 1-15.

[27] Dorri A, Kanhere SS, Jurdak R. Towards an optimized blockchain for IoT. InProceedings of the second international conference on Internet-of-Things design and implementation 2017 Apr 18 (pp. 173-178). https://doi.org/10.1145/3054977.3055003

[28] Huang X, Yu R, Kang J, He Y, Zhang Y. Exploring mobile edge computing for 5G-enabled software defined vehicular networks. IEEE Wireless Communications. 2018 Jan 4;24(6):55-63. https://doi.org/10.1109/MWC.2017.1600387

[29] Liu J, Wan J, Zeng B, Wang Q, Song H, Qiu M. A scalable and quick-response software defined vehicular network assisted by mobile edge computing. IEEE Communications Magazine. 2017 Jul 14;55(7):94-100. https://doi.org/10.1109/MCOM.2017.1601150

[30] Zhang K, Mao Y, Leng S, He Y, Zhang Y. Mobile-edge computing for vehicular networks: A promising network paradigm with predictive off-loading. IEEE vehicular technology magazine. 2017 Apr 24;12(2):36-44. https://doi.org/10.1109/MVT.2017.2668838

[31] Satyanarayanan M. The emergence of edge computing. computer. 2017 Jan 5;50(1):30-9. https://doi.org/10.1109/MC.2017.9

[32] Liu J, Wan J, Zeng B, Wang Q, Song H, Qiu M. A scalable and quick-response software defined vehicular network assisted by mobile edge computing. IEEE Communications Magazine. 2017 Jul 14;55(7):94-100. https://doi.org/10.1109/MCOM.2017.1601150

[33] Conti M, Kumar ES, Lal C, Ruj S. A survey on security and privacy issues of bitcoin. IEEE communications surveys & tutorials. 2018 May 31;20(4):3416-52. https://doi.org/10.1109/COMST.2018.2842460

[34] Zhang Y, Kasahara S, Shen Y, Jiang X, Wan J. Smart contract-based access control for the internet of things. IEEE internet of things journal. 2018 Jun 15;6(2):1594-605. https://doi.org/10.1109/JIOT.2018.2847705

[35] Gupta S, Vanteru K, Reddy S, Madupati B. AI-Enhanced Blockchain Networks for Climate Change Monitoring and Carbon Credit Verification. InProceedings of the 2025 4th International Conference on Frontiers of Artificial Intelligence and Machine Learning 2025 Apr 25 (pp. 31-37). https://doi.org/10.1145/3748382.3748389

[36] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Integration of blockchain and cloud of things: Architecture, applications and challenges. IEEE Communications surveys & tutorials. 2020 Aug 28;22(4):2521-49.

[37] Dorri A, Kanhere SS, Jurdak R. Blockchain in internet of things: challenges and solutions. arXiv preprint arXiv:1608.05187. 2016 Aug 18.

[38] Chatterjee S, Nandan M, Ghosh A, Banik S. Dtnma: identifying routing attacks in delay-tolerant network. InCyber Intelligence and Information Retrieval: Proceedings of CIIR 2021 2021 Sep 29 (pp. 3-15). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-16-4284-5_1

[39] Zhou Z, Chen X, Li E, Zeng L, Luo K, Zhang J. Edge intelligence: Paving the last mile of artificial intelligence with edge computing. Proceedings of the IEEE. 2019 Jun 12;107(8):1738-62. https://doi.org/10.1109/JPROC.2019.2918951

[40] Xu X, Pautasso C, Zhu L, Gramoli V, Ponomarev A, Tran AB, Chen S. The blockchain as a software connector. In2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA) 2016 Apr 5 (pp. 182-191). Ieee. https://doi.org/10.1109/WICSA.2016.21

[41] Atzori L, Iera A, Morabito G. The internet of things: A survey. Computer networks. 2010 Oct 28;54(15):2787-805. https://doi.org/10.1016/j.comnet.2010.05.010

[42] Kouicem DE, Bouabdallah A, Lakhlef H. An efficient architecture for trust management in IoE based systems of systems. In2018 13th Annual Conference on System of Systems Engineering (SoSE) 2018 Jun 19 (pp. 138-143). IEEE. https://doi.org/10.1109/SYSOSE.2018.8428732

[43] Yan Z, Zhang P, Vasilakos AV. A survey on trust management for Internet of Things. Journal of network and computer applications. 2014 Jun 1;42:120-34. https://doi.org/10.1016/j.jnca.2014.01.014

[44] Zhang J, Cui J, Zhong H, Chen Z, Liu L. PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. IEEE Transactions on Dependable and Secure Computing. 2019 Mar 10;18(2):722-35. https://doi.org/10.1109/TDSC.2019.2904274

[45] Raya M, Hubaux JP. The security of vehicular ad hoc networks. InProceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks 2005 Nov 7 (pp. 11-21). https://doi.org/10.1145/1102219.1102223

[46] Nguyen DC, Ding M, Pathirana PN, Seneviratne A. Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: A survey. Ieee Access. 2021 Jun 30;9:95730-53. https://doi.org/10.1109/ACCESS.2021.3093633

[47] Wang S, Zhang X, Zhang Y, Wang L, Yang J, Wang W. A survey on mobile edge networks: Convergence of computing, caching and communications. Ieee Access. 2017 Mar 21;5:6757-79. https://doi.org/10.1109/ACCESS.2017.2685434

[48] Abdel-Basset M, Manogaran G, Mohamed M, Rushdy E. Internet of things in smart education environment: Supportive framework in the decision-making process. Concurrency and Computation: Practice and Experience. 2019 May 25;31(10):e4515. https://doi.org/10.1002/cpe.4515

[49] Zhang Y, Wen J. The IoT electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Networking and Applications. 2017 Jul;10(4):983-94. https://doi.org/10.1007/s12083-016-0456-1

[50] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. IEEE access. 2016 May 10;4:2292-303. https://doi.org/10.1109/ACCESS.2016.2566339

[51] Kshetri N. Can blockchain strengthen the internet of things?. IT professional. 2017 Aug 17;19(4):68-72. https://doi.org/10.1109/MITP.2017.3051335

[52] Hussain R, Zeadally S. Autonomous cars: Research results, issues, and future challenges. IEEE Communications Surveys & Tutorials. 2018 Sep 10;21(2):1275-313. https://doi.org/10.1109/COMST.2018.2869360

[53] Zhang L, Luo M, Li J, Au MH, Choo KK, Chen T, Tian S. Blockchain based secure data sharing system for Internet of vehicles: A position paper. Vehicular Communications. 2019 Apr 1;16:85-93 https://doi.org/10.1016/j.vehcom.2019.03.003

[54] El Hadraoui H, Ouahabi N, El Bazi N, Laayati O, Zegrari M, Chebak A. Toward an intelligent diagnosis and prognostic health management system for autonomous electric vehicle powertrains: A novel distributed intelligent digital twin-based architecture. IEEE Access. 2024 Aug 9;12:110729-61. https://doi.org/10.1109/ACCESS.2024.3441517

[55] Chatterjee S, Nandan M, Ghosh A, Banik S. Dtnma: identifying routing attacks in delay-tolerant network. InCyber Intelligence and Information Retrieval: Proceedings of CIIR 2021 2021 Sep 29 (pp. 3-15). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-16-4284-5_1