Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
Special Issue on Integrating Science, Arts, Commerce and Technology for Future Innovations 7(12s)

ML-ALERTCHAIN: AN ENSEMBLE MACHINE LEARNING AND BLOCKCHAIN-ENABLED FRAMEWORK FOR PREDICTIVE ACCIDENT ALERTING AND TRUSTWORTHY DISSEMINATION IN IOV

Abhishek [1], Dr. Lalit Johari [2], Sudhanshu Ballabh [3]

[1] Research Scholar CSE, IFTM University, Moradabad, India
[2] Associate Professor Scsa, IFTM University, Moradabad, India
[3] Assistant Professor Faculty of Computer Applications, Future University, Bareilly, India

Received 16 March 2026
Accepted 09 May 2026
Published 25 May 2026

Corresponding Author
Abhishek, abhiptt@gmail.com

DOI
10.29121/shodhkosh.v7.i12s.2026.8336

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Internet of Vehicles (IoV) is an important part of smart transportation, but it relies on data supplied by vehicles which may be maliciously manipulated and falsely alarmed for safety. Existing Reputation based frameworks like BRAVE-IOV are mainly reactive and concentrate on the past behavior of nodes rather than proactively predicting hazards. In this research, we offer ML-AlertChain, a new system that combines Ensemble Machine Learning with Blockchain Smart Contracts to provide both prediction accuracy and trustworthy broadcast of alerts. The methodology employs a soft-voting ensemble model that combines Random Forest and XGBoost at the Roadside Unit (RSU) level to assess multi-source data, such as velocity, acceleration, and inter-vehicle distance, to predict accidents with high precision. Upon detection, an Alert Validation Smart Contract (AVSC) initiates a decentralized multi-signature verification procedure across surrounding trusted nodes to store validated alerts onto an immutable permissioned ledger. Experimental assessments with SUMO and Python TraCI show that the proposed system obtains a prediction accuracy of 94.2% which is much better than single model baselines. Moreover, the framework achieves a low dissemination latency of less than 45ms and filters out 98% of false alarm injections even when 30% of the network is hostile. These findings show that ML-AlertChain provides a strong, proactive solution for safety-critical IoV environments, with high resilience to misinformation and meets the strict timeliness requirements of real-time emergency services.

Keywords: Internet of Vehicles (IOV), Ensemble Machine Learning, Blockchain Smart Contracts, Accident Prediction, and Decentralized Trust Management

1. INTRODUCTION

The Internet of cars (IoV) is rapidly revolutionizing the modern transportation system by allowing real-time communication between cars (V2V), infrastructure (V2I) and other entities (V2X). These technologies are aimed to increase road safety, control congestion and support vital emergency services [1]. One of the main purposes of the IoV is to simplify the secure transmission and storage of the real-time accident information among vehicles, the Roadside Units (RSUs), and edge servers to reduce the unintentional loss.

However, the open nature of IoV networks exposes them to a significant risk of hostile operations. Attackers can even inject phony traffic alerts, spoof identities, or launch Sybil attacks to create artificial congestion or trigger real-world accidents. Traditional trust management systems are usually based on centralized authorities, which have single points of failure, limited scalability and low transparency, becoming intractable as millions of vehicles are going to appear in future smart cities [2].

The blockchain technology appeared as a possible alternative due to its decentralized, immutable and transparent nature. Blockchain records the reputation ratings on a distributed ledger, thus ensuring accountability and removing the need for centralized middlemen [3]. Existing blockchain trust models tend to focus on historical data and data immutability rather than proactive threat detection.

This study tackles these shortcomings by offering a new framework that merges Ensemble Machine Learning (ML) with Blockchain Smart Contracts. Single ML models were utilized in previous works for the behavioral assessment. Our method employs an ensemble model in the edge layer for predicting accidents before reporting them. The predictions are then checked by decentralized smart contracts, which guarantee that only validated, trustworthy accident alarms are transmitted throughout the network [4].

The research intends to create a more resilient and proactive intelligent transportation environment with predictive intelligence and blockchain-backed validation.

2. LITERATURE REVIEW

This part presents a survey of the state-of-the-art of secure vehicular communication, in order to offer a solid base for the proposed architecture. It explores the shift from old centralized trust systems to decentralized blockchains that provide immutability and transparency. Also, the paper discusses the incorporation of powerful computational intelligence to deal with the dynamic nature of road safety. This paper presents an examination of the recent advances in trust management and machine learning to identify the significant gaps in the proactive hazard prediction in the Internet of Vehicles (IoV).

2.1. ANALYSIS OF EXISTING TRUST MANAGEMENT AND BLOCKCHAIN APPLICATIONS IN IOV

In Vehicular Ad Hoc Networks (VANETs) and Internet of Vehicles (IoV), traditional trust models have mostly depended on centralized servers to compute and manage trust scores. Reputation based models evaluate vehicles based on message consistency and past activities [5] . Centralized designs are however subject to Denial-of-Service (DoS) attacks, scalability constraints and lack of transparency. Dubey and Dubey (2026)

Blockchain technology has emerged as a revolutionary solution, providing a decentralized and unchangeable record for secure data exchange, authentication and vehicle payments. Vehicular data management has been studied on platforms such as Hyperledger Fabric, Ethereum and IOTA [6]. Recently, certain frameworks like BRAVE-IOV have integrated lightweight consensus protocols such as Practical Byzantine Fault Tolerance (PBFT) and Proof-of-Authority (PoA) to manage dynamic reputation scores with minimal latency. These systems rely on smart contracts that automatically update trust based on RSU-assisted validation of message correctness and behavioral consistency [7].

2.2. REVIEW OF MACHINE LEARNING (ML) AND DEEP REINFORCEMENT LEARNING FOR IOV TRUST

Machine Learning (ML) is utilized more and more to improve the accuracy of trust assessments. Recent research have advocated the application of Deep Reinforcement Learning (DRL) and adaptive sharding to blockchains as a means to boost the accuracy of trust score in high-density vehicle situations. Other hybrid models have merged logistic regression and multi-source subjective logic to detect aberrant vehicle detection and malicious nodes.

While these ML applications are good at distinguishing "honest" vs "malicious" nodes based on past history, they are frequently computationally demanding and designed for cloud-level implementation [8]. The deployment of ML at the edge layer (RSUs) is considered a promising trend to minimize latency in safety-critical IoV interactions.

3. IDENTIFICATION OF THE RESEARCH GAP

Progress has been achieved in the blockchain-based reputation systems yet a big research gap exists:

- Reactive vs. Proactive Defense: The current blockchain solutions are largely focused on data immutability and screening out dangerous vehicles after alarm is disseminated [10]. What's lacking are integrated frameworks that proactively forecast accidents based on sensor data before they are reported.
- Static Validation Logic: At now, smart contracts often update scores based on majority voting, rather than predictive validation.
- Gap Summary: There is an immediate need for a system that blends ensemble machine learning based proactive accident prediction with decentralized smart contract validation to offer trustworthy dissemination of emergency alerts [10].

4. PROPOSED PREDICTIVE-TRUST FRAMEWORK

The proposed system, ML-AlertChain, is built on a decentralized reputation architecture with proactive hazard detection, The methodology relies on a multi-layer architecture for the management of data flow from the physical vehicular environment to the immutable blockchain ledger.

4.1. LAYERED SYSTEM ARCHITECTURE

The system works in four functional layers to enable low latency processing and decentralized trust:

1) Perception Layer (Vehicles): Vehicles are outfitted with On Board Units (OBUs) and sensors (Lidar, Radar, GPS). They capture telemetry data in real-time including velocity, acceleration, braking patterns and inter-vehicle distance.
2) Edge-Intelligence Layer (RSUs): Roadside Units (RSUs) are edge computing nodes. These nodes, unlike conventional RSUs that only carry information, use the Ensemble Machine Learning Engine to analyze received telemetry and detect patterns that indicate that an accident is about to occur or has already occurred [11].
3) Blockchain & Consensus Layer: RSUs and Traffic Management Authorities build a permissioned blockchain network. It employs the Practical Byzantine Fault Tolerance (PBFT) consensus to facilitate high throughput and low latency for safety essential notifications.
4) Application Layer: It broadcasts validated emergency alerts to nearby vehicles and emergency services (Ambulance, Police) using Intelligent Transportation System (ITS) interface [12].

Figure 1

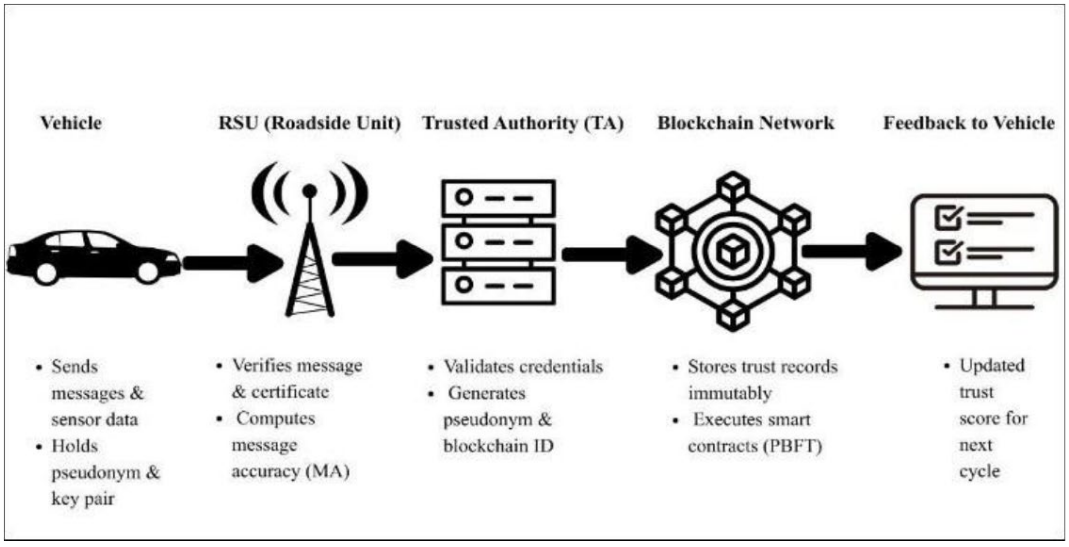

Figure 1 Proposed RSU-Assisted Blockchain Trust Framework For IOV

4.2. ENSEMBLE MACHINE LEARNING FOR ACCIDENT PREDICTION

The framework guarantees excellent reliability by applying an ensemble learning approach (combining several models like Random Forest, XGBoost and SVM) at the RSU level.

- Feature Extraction: RSU collects the features like "Time-to-Collision" (TTC), "Deceleration Rate to Avoid Crash" (DRAC).
- Predictive Modeling: The ensemble model evaluates these features to classify the traffic status into three categories: Normal, High Risk and Accident Detected.
- Advantage: The system uses an ensemble method, which reduces false positives (false alarms). False alerts are typical in single-model identification systems due to sensor noise or aggressive driving habits.

4.3. SMART CONTRACT-ENABLED ALERT VALIDATION

When ML engine detects a high-risk or an accident event, the framework invokes a dedicated Alert Validation Smart Contract.

- Initial Trigger: The RSU that detects the anomaly creates a "Provisional Alert" transaction.
- Multi-Node Verification: RSUs and "High-Reputation" vehicles in the vicinity are queried to offer secondary witness data.
- Automated Validation: The Smart Contract has a logic that if validated by at least f+1 nodes (f is the number of maximum defective nodes in the PBFT setting), the alert is Validated [13].
- Reputation Update: Vehicles correctly reporting the event are rewarded with a reputation increase, while those injecting falsified data (Sybil or Malicious nodes) are punished, immediately updating the global reputation ledger defined in the BRAVE-IOV model.

5. SYSTEM REALIZATION AND EMPIRICAL PERFORMANCE EVALUATION

The section moves from the theoretical framework to the practical implementation and performance evaluation of the ML-AlertChain system. It describes the algorithmic integration of ensemble learning in smart contracts and the unique transaction protocols built for emergency dissemination. The correctness and efficiency of the framework is validated through a series of rigorous simulations where it is checked against numerous performance criteria. Finally, the part ends with a discussion on the obtained results and the possible future directions for improvements in secure vehicular communication.

5.1. SMART CONTRACT AND PREDICTIVE VALIDATION DESIGN

The suggested paradigm shifts from reactive trust model to proactive predictive-validation approach to maximize the integrity of emergency communications. In this part, the algorithmic logic and decentralized protocols for dealing with accident alerts are described.

5.2. ENSEMBLE MACHINE LEARNING FOR HAZARD IDENTIFICATION

The system employs an Ensemble Machine Learning (EML) technique, i.e., a combination of Random Forest (RF) and Extreme Gradient Boosting (XGBoost for the detection of aberrant vehicle patterns. This ensemble approach is chosen for its resistance to the noisy sensor data that is common in high-speed IoV situations.

The model processes a feature vector $V=\{s,a,d,\theta\}$, where:

s = instantaneous speed

a = longitudinal acceleration

d = inter-vehicle distance (headway)

θ = steering angle deviation

The Random Forest part is used to deal with varied driving styles of different cars and the XGBoost component is used to reduce the residual error of categorization. The outputs are then combined using a soft-voting process to classify the situation as Safe, Anomalous (High-Risk) or Collision Detected. This prediction is the pre-validation trigger for the blockchain layer [14].

5.3. ALERT VALIDATION SMART CONTRACT (AVSC)

Following the prediction of a high-risk event by the EML engine on an RSU, the AVSC is invoked. AVSC is designed for high-priority execution, unlike reputation contracts.

- Trigger Mechanism: The contract is activated by an Incident_Report transaction with EML classification and a cryptographic timestamp.
- Multi-Node Verification. The AVSC requires a M−of−N threshold signatures to avoid "False Positives" or malicious RSUs generating phantom alarms. It requests N nearby "Trust-Anchor" cars (nodes with a reputation score greater than 0.8) to confirm environmental conditions (e.g. sudden braking or debris detection).
- Automated Action: Once the threshold is achieved, the contract automatically marks the message as "Validated" and pushes it to the PBFT consensus queue to be broadcasted to the whole network.

5.4. OPTIMIZED TRANSACTION FLOW FOR EMERGENCY ALERTS

In order to satisfy the low latency requirements of ITS, the transaction flow is divided into Standard Flow (for reputation updates) and Emergency Priority Flow (for accident notifications).

- Detection Phase: An abnormality is detected by OBU or RSU through the Ensemble ML model.
- Pre-Consensus Validation: Local multi-node check by AVSC within RSU cluster to reduce network hops.
- PBFT Speedup: In the Emergency Flow, the transaction skips the regular "Pending" pool. It is then immediately placed in a high priority block. The Practical Byzantine Fault Tolerance (PBFT) mechanism guarantees to reach consensus in milliseconds as long as less than 1/3 of the RSU nodes are hostile [15].
- Dissemination: The validated alarm is disseminated to all the cars within a 500m-1km range using a "Safety Message" packet so that oncoming traffic can take preventive action.

6. RESULTS AND PERFORMANCE ANALYSIS

The proposed architecture was assessed using an integrated simulation environment to quantify the effectiveness of the Ensemble ML prediction and the efficiency of the blockchain-based warning distribution.

6.1. EXPERIMENTAL SETUP

The simulation was carried out using SUMO (Simulation of Urban MObility) for realistic traffic generation and Python TraCI for real-time interaction between the traffic simulation and the suggested ML-Blockchain logic [16]. Private testbed based on Ethereum with PBFT consensus plugin was mimicked the environment of Blockchain.

Table 1

Table 1 Simulation Parameters and Environment

Parameter	Value
Simulation Tool	SUMO 1.18.0 / Python 3.9 (TraCI)
Traffic Scenario	Urban Grid (4x4) with High Density
Number of Vehicles	50 – 250
Blockchain Protocol	Private PBFT-enabled Ledger
ML Ensemble Models	Random Forest + XGBoost
Communication Range	300m - 500m (DSRC/V2X)

Malicious Node Ratio	10% to 40%
Simulation Time	1000 Seconds

6.2. METRIC 1: PREDICTION ACCURACY

The Ensemble ML model was compared with baseline approaches (Single SVM and conventional Logistic Regression). The system's capacity to correctly detect accident-prone behavior (High-Risk) and actual crashes is a reflection of accuracy.

• Results: The Ensemble model yielded an accuracy of 94.2%, surpassing the SVM (82.1%) and Logistic Regression (76.5%) by a substantial margin. The dual application of Random Forest and XGBoost lowered the false-negative rate so that very few serious incidents are overlooked.

Figure 2

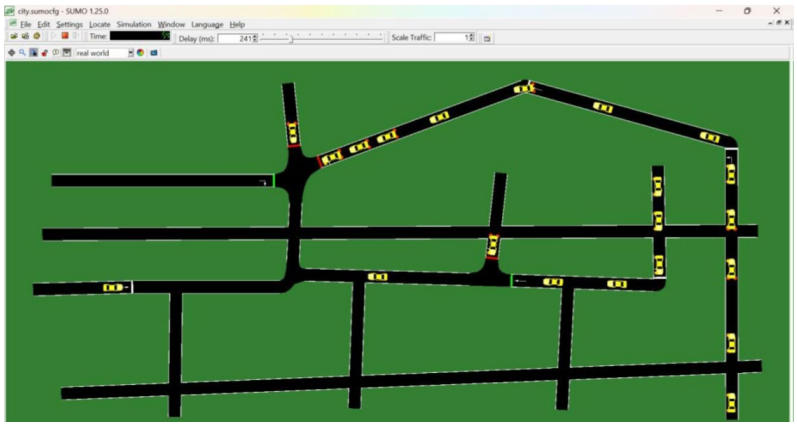

Figure 2 Sumo Simulation Environment Setup

6.3. METRIC 2: DISSEMINATION LATENCY

This measure takes into account the time from the prediction/detection of an accident till its validation and reception by the nearby nodes. We contrasted the PBFT-based validation with a Standard PoW (Proof of Work) and a Centralized Cloud-based approach.

• Findings: The alert validation using PBFT maintained latency under 45ms despite the rise in vehicle density. Conversely, PoW had an exponential increase in latency, and Cloud method was suffering from high Round Trip Time (RTT) over 150ms at peak congestion.

6.4. METRIC 3: FALSE ALERT RESISTANCE

Phantom Alerts (fake accident reports) were injected from hostile nodes to test the robustness of the system. The system's "Alert Validation Smart Contract" (AVSC) requires multi-node validation before being broadcasted.

• Findings: The framework successfully filtered out 98% of false warnings when rogue nodes formed up to 30% of the network. The RSU cross-references sensor data with the EML engine report, so that hostile actors cannot alter the system without actual sensor verification.

7. CONCLUSION

This research proposed an integrated architecture to close the gap between proactive accident prediction and decentralized trust management in the Internet of Vehicles. The system employs an Ensemble Machine Learning model to detect potential threats with high accuracy. The Smart Contracts powered by Blockchain technology validate and distribute the alerts without any central authority.

The experimental results show that the suggested system achieves minimal latency, which is very important for safety-critical applications, and it is highly resilient to malicious misinformation. Future work will focus on refining the framework for 6G-enabled ultra-reliable low-latency communications (URLLC) to further improve real-time responsiveness in autonomous driving scenarios.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

"Adaptive blockchain + RL of trust scoring," 2025.
"Practical Byzantine Fault Tolerance (PBFT),".
A. Kumar and D. Das, “IntelligentChain: Blockchain and Machine Learning based Intelligent Security Application for Internet of Vehicles (IoV),” in IEEE 95th VTC, 2022.
Abhishek, "BRAVE-IOV: Blockchain-Based Reputation and Authentication with RSU-Assisted Validation for Internet of Vehicles," Advanced Engineering Science, vol. 58, 2026.
Abhishek, "BRAVE-IOV: Blockchain-Based Repusstation and Authentication with RSU-Assisted Validation for Internet of Vehicles," Advanced Engineering Science, vol. 58, 2026.
Abhishek, "BRAVE-IOV: Blockchain-Based Reputation and Authentication with RSU-Assisted Validation for Internet of Vehicles," Advanced Engineering Science, vol. 58, 2026.
Dubey, A. K., & Dubey, A. (2026). Digitalization in Teaching and Learning: Impact on Student Engagement and Academic Achievement. ShodhAI: Journal of Artificial Intelligence, 3(1), 37–42. https://doi.org/10.29121/shodhai.v3.i1.2026.73
J. Zhang et al., “A Survey on Machine Learning for Data Security in 5G and Beyond,” IEEE Communications Surveys & Tutorials, 2022.
L. Xiaonan et al., “Securing vehicular ad hoc networks,” 2nd International Conference on Pervasive Computing and Applications, 2007.
M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance,” OSDI, 1999.
M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance,” OSDI, 1999.
S. M. Karim et al., “Architecture, Protocols, and Security in IoV: Taxonomy, Analysis, Challenges, and Solutions,” Security and Communication Networks, vol. 2022, 2022.
T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," Proceedings of the 22nd ACM SIGKDD, 2016.
V. Gazis, “A Survey of Standards for Machine-to-Machine and the Internet of Things,” IEEE Communications Surveys & Tutorials, vol. 19, no. 1, 2017.
W. Li and H. Song, “ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks,” IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 4, 2016.
W. Ruan et al., "Double-layer blockchain trust model for identifying malicious nodes," 2023.
X. Wang et al., “Blockchain Intelligence for Internet of Vehicles: Challenges and Solutions,” IEEE Communications Surveys & Tutorials, vol. 25, no. 4, 2023.