Journal of Information Systems Engineering and Management
2025, 10(8s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

ConsensusPlus: Blockchain Driven Secure Data Sharing Protocol for Internet of Vehicles

B. Ramesh[1], Dr. A Rajani[2]
[1]*Asst. Professor, ECE Department, CVR College of Engineering*
Email: rameshbommera@gmail.com
[2]*Professor, ECE department, JNTU Hyderabad*
Email: rajani.akula@jntuh.ac.in

ARTICLE INFO

Received: 18 Oct 2024

Revised: 15 Dec 2024

Accepted: 28 Dec 2024

ABSTRACT

The rapid expansion of the Internet of Vehicles (IoV) creates a distinct set of difficulties and opportunities for improving vehicular communication and data security. "ConsensusPlus" provides a revolutionary blockchain-based protocol for secure data sharing within the IoV. This protocol uses a proprietary consensus mechanism to enable real-time, reliable data sharing and integrity across a network of vehicles and infrastructure components. The integration of blockchain technology, which provides a decentralized framework for managing vehicular data in a transparent, immutable, and secure manner, is key to ConsensusPlus. By utilizing blockchain, the protocol improves data privacy and resilience to manipulation and cyber threats, which is critical in the IoV scenario where data sensitivity and security are key. ConsensusPlus also enables the smooth integration of existing vehicular communication protocols, such as Dedicated Short-Range Communications (DSRC) and Cellular V2X, with blockchain technology. This integration assures that the protocol is not only compatible with existing technologies, but also adaptable to future advances in vehicular communications. The ConsensusPlus protocol's performance has been evaluated through a number of simulations and real-world deployments, which have shown considerable gains in data security and operational efficiency inside the IoV. This protocol not only provides a reliable solution for secure data sharing, but it also promotes a scalable and efficient communication framework for the growing needs of the Internet of Vehicles. The implementation of ConsensusPlus could be a critical step in achieving a completely secure, decentralized, and efficient digital vehicular ecosystem.

Keywords: Blockchain, Data Sharing, Internet of Vehicles, Machine Learning, Smart Contracts.

Introduction

The advent of the Internet of Vehicles (IoV) heralds a transformative era in intelligent transportation systems, enabling unprecedented levels of communication and data exchange among vehicles and infrastructure. However, this evolution also introduces significant challenges in terms of data security, privacy, and trustworthiness. The integration of blockchain technology into IoV has emerged as a promising solution to these challenges, providing a decentralized framework that enhances security, ensures data integrity, and fosters trust among participants.

Recent studies, such as those by Du et al. [1] and Cui et al. [2], have underscored the effectiveness of blockchain in managing trust and securing information sharing within vehicular networks. These frameworks leverage the immutable and transparent nature of blockchain to mitigate risks associated with malicious activities and data tampering, which are prevalent in open vehicular networks. Moreover, the integration of machine learning with blockchain, as explored by Chai et al. [3] and Karim et al. [4], offers advanced capabilities for anomaly detection and adaptive threat response, enhancing the security layers of vehicular communications.

The proposed protocol, "ConsensusPlus," aims to innovate beyond traditional blockchain applications by introducing a machine learning-driven approach to smart contracts. This integration not only automates operations but also dynamically enhances the security protocols based on real-time data analytics. Such an approach is aligned with the

work of Kumar et al. [5] and He, Ying, Ke Huang et al. [6], who demonstrate the potential of deep learning techniques in strengthening data privacy and security within blockchain-based vehicular networks.

Furthermore, the necessity for a customized consensus mechanism in IoV is evident in the light of research by Tu, Shanshan, Haoyu Yu et al. [7] and Yuan, Mingyang, et al. [8], who emphasize the need for scalable and efficient consensus protocols tailored to the high mobility and dynamic topology of vehicular networks. The "ConsensusPlus" protocol adopts a modified Practical Byzantine Fault Tolerance (PBFT) approach, optimized for low latency and high throughput, essential for real-time vehicular communications.

In addition to securing data exchange, the integration of blockchain with existing IoV standards such as Dedicated Short-Range Communications (DSRC) and Cellular V2X is crucial for ensuring seamless interoperability and enhancing network efficiency. This compatibility is vital for the widespread adoption and practical implementation of blockchain-based security solutions in the IoV, as highlighted in the contributions of Kakkar et al. [9] and Djenouri et al. [10].

Overall, the "ConsensusPlus" protocol seeks to address the multifaceted security challenges of the IoV by harnessing the synergistic potential of blockchain and machine learning. This integration promises not only to secure data sharing across vehicular networks but also to enhance the operational capabilities of IoV systems, paving the way for a more secure and efficient digital roadway infrastructure.

Related work

The rapid advancement of the Internet of Vehicles (IoV) has brought forth numerous opportunities and challenges in terms of secure data sharing, privacy preservation, and efficient consensus mechanisms. As the number of connected vehicles and the volume of generated data continue to grow, it becomes increasingly crucial to develop comprehensive solutions that address these critical aspects. This literature review explores the current state-of-the-art approaches and frameworks proposed by researchers in the field of IoV, focusing on blockchain-based secure data sharing schemes, privacy-preserving techniques, federated learning, and intelligent transportation systems. The reviewed articles provide valuable insights into the challenges and requirements of IoV and serve as a foundation for the proposed model, "ConsensusPlus," which aims to advance the field by integrating blockchain, machine learning, and smart contracts in a holistic manner.

Several articles focus on developing secure and privacy-preserving data sharing schemes for IoV. Du et al. [1] propose a consortium blockchain-based trust-value management approach for secure information sharing, while Cui et al. [2] exploit consortium blockchain technology for traceable and anonymous vehicle-to-vehicle (V2V) data sharing. Karim et al. [4] introduce a blockchain-based secure data exchange scheme using elliptic curve cryptography for IoV in a 5G environment. Khowaja et al. [11] present a secure data sharing scheme using community segmentation and blockchain for vehicular social networks in 6G. Jiang et al. [12] and Kumar, Randhir et al. [13] propose data sharing models that combine blockchain and federated learning to address security and privacy issues in IoV. These studies highlight the importance of secure and privacy-preserving data sharing in IoV and demonstrate the potential of blockchain and federated learning in addressing these challenges.

Several articles propose blockchain-based frameworks to enhance security, efficiency, and trustworthiness in IoV. Chai et al. [3] introduce a secure and efficient blockchain-based knowledge sharing framework for intelligent connected vehicles (ICVs), while Ying et al. [6] propose a blockchain-based federated learning system for connected and autonomous vehicles (CAVs). Wu et al. [14] present a trusted paradigm of data management based on a vehicle-road-cloud architecture using blockchain, and Tu et al. [7] propose a vehicle-based secure blockchain consensus algorithm for efficient data storage, processing, and sharing in IoV. Lin [15] introduces a multi-level blockchain framework for secure information security in IoV, and Yuan et al. [8] propose a blockchain-based trusted data sharing mechanism with congestion control for IoV. These studies demonstrate the potential of blockchain technology in providing secure, efficient, and trustworthy frameworks for various aspects of IoV, such as data sharing, knowledge sharing, and data management.

Some articles explore the integration of federated learning with blockchain to enhance security and privacy in IoV. Ying et al. [6] propose a blockchain-based federated learning system for CAVs, while Jiang et al. [12] and Kumar, Randhir et al. [13] introduce data sharing models that combine blockchain and federated learning for privacy preservation in IoV. Zhang et al. [16] propose a blockchain-based cooperative learning framework with deep

compression for lightweight IoV nodes. Javed et al. [17] provide a comprehensive survey on the integration of blockchain technology and federated learning in vehicular IoT networks. These studies highlight the potential of federated learning in enabling secure and privacy-preserving collaborative learning in IoV while leveraging the benefits of blockchain technology.

Several articles focus on developing secure and intelligent systems for IoV in the context of intelligent transportation systems. Kumar et al. [5] present a privacy-preserving-based secure framework using blockchain and deep learning for cooperative intelligent transport systems (C-ITS). Liu et al. [18] propose a blockchain-based secure communication architecture for intelligent transportation digital twins systems, while Kakkar et al. [9] introduce a blockchain-based secure and trusted data sharing scheme for autonomous vehicles in 5G. Djenouri et al. [10] develop a secure and intelligent system for IoV using deep learning, focusing on traffic forecasting. These studies demonstrate the potential of blockchain, deep learning, and other advanced technologies in enabling secure and intelligent transportation systems in the context of IoV.

Some articles specifically focus on privacy protection and security aspects of IoV. Guo et al. [19] propose an accountable attribute-based data-sharing scheme based on blockchain for vehicular ad hoc networks (VANETs), while Xu et al. [20] introduce a blockchain-oriented privacy protection scheme for sensitive data in IoV. Sehar et al. [21] propose a consensus algorithm for vehicular networks to ensure data security using blockchain. Biswas et al. [22] present a blockchain-based communication framework for secure and trustworthy IoV applications. These studies emphasize the importance of privacy protection and security in IoV and demonstrate the potential of blockchain technology in addressing these challenges. The section articles collectively contribute to the advancement of secure, privacy-preserving, and intelligent solutions for the Internet of Vehicles. The proposed frameworks, schemes, and algorithms leverage the benefits of blockchain technology, federated learning, deep learning, and other advanced technologies to address the challenges of data sharing, privacy preservation, security, and trustworthiness in IoV. These studies provide valuable insights and lay the foundation for future research and development in this rapidly evolving field.

The proposed model "ConsensusPlus" addresses the critical challenges of secure data sharing, privacy preservation, and efficient consensus mechanisms in the Internet of Vehicles (IoV), as highlighted by the reviewed articles. Studies such as Du et al. [1], Cui et al. [2], and Karim et al. [4] emphasize the importance of secure and privacy-preserving data sharing in vehicular networks, which ConsensusPlus achieves through the use of a permissioned blockchain, specifically Hyperledger Fabric. The custom-designed consensus protocol based on the Practical Byzantine Fault Tolerance (PBFT) algorithm, optimized for high-speed requirements and dynamic conditions of vehicular networks, aligns with the need for low latency and high throughput in IoV, as emphasized in the reviewed articles.

ConsensusPlus integrates machine learning models to identify deviations from normal operational patterns and detect potential security threats or system failures, similar to the approaches explored by Ying et al. [6], Zhang et al. [16], and Javed et al. [17]. The model also implements advanced privacy and security measures, such as robust encryption methods, data anonymization techniques, and strict access controls, addressing the concerns highlighted by Guo et al. [19] and Xu et al. [20]. Smart contracts are leveraged to automate key processes, such as the enforcement of data sharing agreements and the execution of compliance checks, aligning with the objectives of the reviewed articles, such as Yuan et al. [8], in terms of enabling secure, efficient, and trustworthy data sharing in IoV.

In comparison to contemporary models, ConsensusPlus shares similarities with the blockchain-based federated learning system proposed by Ying et al. [6] for connected and autonomous vehicles (CAVs) and the privacy-preserving-based secure framework proposed by Kumar et al. [5] for cooperative intelligent transport systems (C-ITS). However, ConsensusPlus distinguishes itself by focusing on a permissioned blockchain, custom-designed consensus mechanism, and comprehensive data management practices. The proposed model has the potential to advance the state-of-the-art in secure and intelligent IoV systems by integrating blockchain, machine learning, and smart contracts in a holistic manner, addressing the challenges and requirements highlighted in the reviewed articles.

Methods and Material

This section delve into the foundational elements and practical applications of the "ConsensusPlus" protocol, a pioneering integration of blockchain technology and machine learning designed to address the complex security needs of the Internet of Vehicles (IoV). This section provides a comprehensive breakdown of the technical methodologies employed, the architectural design of the system, and the specific materials and technologies utilized

to implement and evaluate the protocol. Our aim is to offer a clear and thorough understanding of how "ConsensusPlus" operates within IoV environments, emphasizing the innovations that enhance security and data integrity across vehicular networks.

1.1 Architecture Design

In the developed framework, the network structure has been meticulously organized to include various node types, each with defined roles and responsibilities to facilitate efficient data flow. Vehicles have been designated as mobile nodes that not only generate but also consume data, making them primary actors within the network. Roadside Units (RSUs) have been equipped with edge computing capabilities to serve as local data aggregators and crucial communication relays. Traffic Management Systems function as central nodes and possess the robust computing infrastructure necessary to process and analyze the extensive data collected for traffic control and safety measures. Secure communication channels have been established using encryption and protocols such as TLS/SSL to ensure data integrity and confidentiality across all nodes.

Blockchain Selection and Setup: A permissioned blockchain was chosen to enhance privacy and control within the Internet of Vehicles (IoV), addressing the need for sensitive data handling inherent to vehicular environments. Hyperledger Fabric was selected as the optimal blockchain platform due to its support for smart contracts and its capability to handle private transactions through its modular architecture, which is crucial for managing complex operations in IoV.

Consensus Mechanism Configuration: The consensus protocol has been custom-designed to prioritize low latency and high throughput, which are critical for accommodating real-time vehicular communications and data exchanges. A modified version of the Practical Byzantine Fault Tolerance (PBFT) algorithm has been implemented, optimized specifically for the high-speed requirements and dynamic conditions of vehicular networks. This ensures the protocol's resilience against failures and malicious attacks. Additionally, compatibility with IoT standards like Dedicated Short-Range Communications (DSRC) and Cellular V2X has been ensured to facilitate seamless integration with existing vehicular communication technologies.

Machine Learning Integration: Machine learning models have been developed to identify deviations from normal operational patterns, indicating potential security threats or system failures. A combination of supervised and unsupervised learning techniques has been employed to enhance the detection capabilities, with training data being collected and preprocessed from diverse real-world vehicle operations. These models have been strategically deployed on both dedicated nodes within the blockchain network and on RSUs to enable real-time data analysis and immediate response to detected anomalies.

Data Management Practices: Critical data for collection, such as vehicle location, speed, and mechanical status, has been identified, and secure storage mechanisms on the blockchain have been defined, utilizing encryption and distributed ledgers to ensure data redundancy and integrity. Advanced privacy and security measures, including robust encryption methods, data anonymization techniques, and strict access controls, have been implemented to protect sensitive information and comply with privacy regulations.

Smart Contracts Deployment: Smart contracts have been utilized to automate key processes such as enforcement of data sharing agreements, facilitation of micro-transactions for data usage, and execution of compliance checks with regulatory requirements. A framework for the regular update and maintenance of these smart contracts has been developed, incorporating community feedback and adapting to new legal standards or technical requirements.

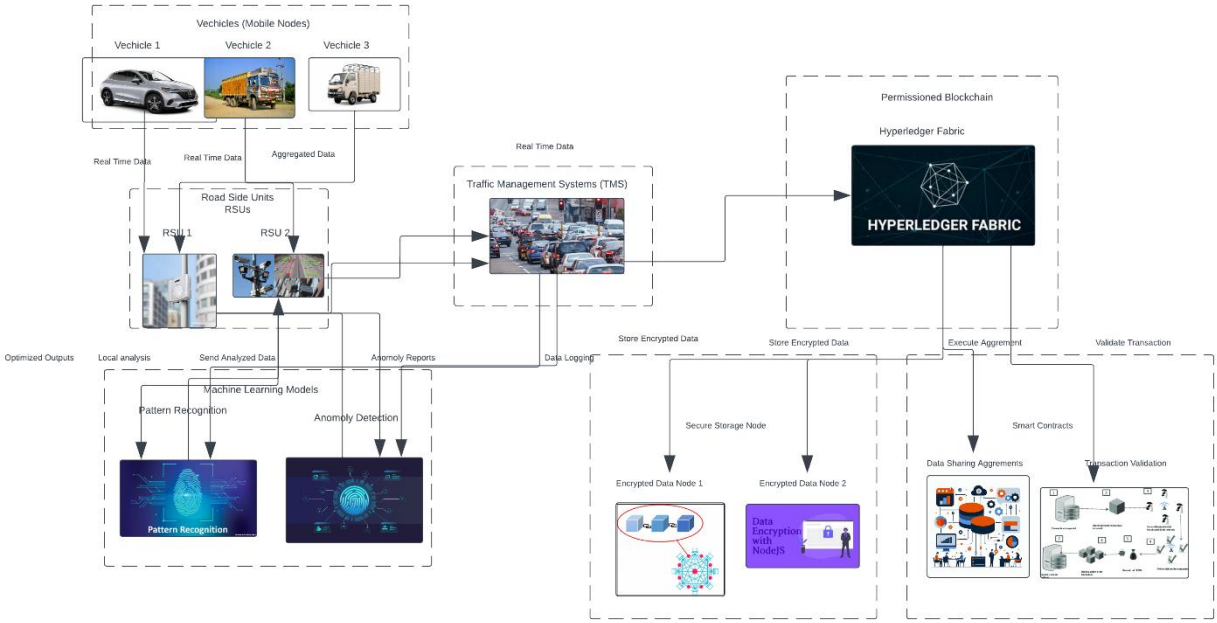

Figure 1: The Systematic Architecture Diagram of the ConsensusPlus

The ConsensusPlus architecture diagram shown in figure 1 vividly encapsulates a blockchain-driven data sharing protocol tailored for the Internet of Vehicles (IoV), providing a visual roadmap of the intricate interactions and sophisticated structure within an IoV system. The architecture emphasizes the critical role of blockchain technology in bolstering data security and management across the network. Starting with the vehicles, designated as mobile nodes, they are fundamental to generating and transmitting data which sets the foundation for interactions within the architecture. This portrays the vehicles as primary data providers, essential for the continuous influx of real-time information.

Roadside Units (RSUs) function as edge computing nodes that bridge the gap between mobile nodes and central systems. These units are tasked with the initial collection and processing of data from vehicles, highlighting their pivotal role in data aggregation and preliminary analysis. Central to the architecture are the Traffic Management Systems, which serve as central nodes. These systems process the aggregated data to enhance traffic flow and ensure transportation safety. The management systems use this data to make informed decisions that directly impact traffic control and infrastructure management, thus playing a crucial role in the operational efficiency of the IoV ecosystem. The integration of a Permissioned Blockchain, specifically using Hyperledger Fabric, ensures the integrity and security of data transactions. This blockchain setup provides a robust framework for decentralized and secure data logging, crucial for maintaining a trustworthy network where data manipulation is mitigated.

A Modified Practical Byzantine Fault Tolerance (PBFT) algorithm is employed to uphold consensus across the blockchain nodes, ensuring the reliability and consistency of the data records. This mechanism is essential for maintaining the network's integrity and trustworthiness. Machine Learning techniques are seamlessly integrated into the system, employing both supervised and unsupervised models to analyze real-time data. These models are instrumental in detecting anomalies and optimizing operations, thereby enhancing the responsiveness and efficiency of the system. Data management within the architecture is handled by secure storage nodes, which are responsible for the encryption and safekeeping of data. Comprehensive privacy and security measures are rigorously enforced to protect sensitive information and comply with stringent data protection regulations. Finally, the architecture incorporates Smart Contracts to automate key operational processes such as data sharing agreements and transaction validations. Additionally, a robust maintenance framework is in place to ensure the system remains up-to-date and compliant with evolving technological standards and regulatory requirements. This diagram not only underlines the technological sophistication of integrating blockchain with the IoV but also emphasizes the enhanced security, operational efficiency, and real-time decision-making capabilities that this integration brings to vehicular networks. The architecture fosters a dynamic environment capable of adapting to new data insights and operational demands, illustrating a forward-thinking approach to managing the complexities of modern transportation networks.

1.2 Consensus Mechanism

The Mobile Optimized Fault Tolerance (MOFT) protocol has been meticulously engineered to address the distinct requirements of the Internet of Vehicles (IoV). This protocol is founded on principles that prioritize low latency, high throughput, robust fault tolerance, and scalability, which are imperative for supporting the dynamic and high-speed nature of vehicular networks.

Structural Design of the MOFT Protocol: A layered approach characterizes the structural foundation of the MOFT protocol, which is specifically tailored to manage the complexities associated with vehicular data transactions. This design segregates the processes of transaction validation and block creation, thereby optimizing both speed and reliability in environments characterized by high mobility.

Constitutive Elements of the Protocol: The protocol architecture incorporates three primary types of nodes, each fulfilling distinct roles within the network: Vehicle Nodes (VN), Roadside Units (RSU), and Authority Nodes (AN). Vehicle Nodes function as mobile nodes that both generate and consume data, playing a pivotal role in the network. Roadside Units are tasked with secondary validation and data aggregation, thereby enhancing the local processing capabilities of the network. Authority Nodes, selected based on their stake and performance metrics, are critical for the creation of blocks and the final validation of transactions.

Consensus Mechanism and Process: The initiation of the consensus process is marked by vehicles broadcasting their transactions to proximate Roadside Units. These RSUs undertake preliminary validations that scrutinize the transaction structure and the authenticity of signatures, ensuring adherence to established network rules. Following validation, transactions are relayed to the nearest Authority Node.

Authority Nodes are responsible for assembling these transactions into blocks, either after a predetermined time slice or upon reaching a transaction capacity. Prior to entering the multi-tier consensus mechanism, a pre-consensus check is conducted to eliminate any conflicting or invalid transactions. This mechanism integrates a local consensus among RSUs, based on real-time data, and a global consensus among Authority Nodes through a modified Practical Byzantine Fault Tolerance (PBFT) algorithm. The consensus requires a supermajority among the ANs to finalize each block.

• **Authority Node (AN) Selection**:

- Let N represent the total number of nodes capable of becoming ANs.

- ANs are selected based on a stake and performance index P, calculated as: Eq 1

$$P_i = \alpha S_i + \beta D_i \text{ ...(Eq 1)}$$

where S_i is the stake (e.g., tokens or reputation points) and D_i is a performance metric based on historical data reliability. Coefficients α and β weight these factors.

• **Consensus Rounds**:

In each consensus round for block B_k, nodes go through three phases: Pre-prepare, Prepare, and Commit.

Pre-prepare: The leader broadcasts a proposal for B_k: Eq 2

$$m_{\text{pre-prep}} = \text{sign}\left(H\left(B_k\right), \text{seq}, pk_{\text{leader}}\right) \text{ ...(Eq 2)}$$

P**repare**: Nodes agree on the proposal and broadcast their agreement: Eq 3

$$m_{\text{prep}} = \text{sign}\left(H\left(B_k\right), \text{seq}, \text{'prepare'}, pk_i\right) \text{ ...(Eq 3)}$$

Commit: Nodes commit to the proposal after receiving 2f+1 prepare messages: Eq 4

$$m_{\text{commit}} = \text{sign}\left(H\left(B_k\right), \text{seq}, \text{'commit'}, pk_i\right) \text{...(Eq 4)}$$

Execution occurs if a node receives 2f+1 commit messages.

The system tolerates up to f faulty nodes, where $f = \lfloor (N-1)/3 \rfloor$.

Fault Tolerance and Security Implementations: To ensure comprehensive fault tolerance, the protocol integrates multiple RSUs and Authority Nodes in the validation and consensus processes to mitigate potential single points of failure. The periodic re-election of Authority Nodes is instituted to uphold network integrity and deter collusion.

Security measures are stringently applied through cryptographic signatures on all transactions, employing a public-key infrastructure (PKI). The protocol also incorporates continuous monitoring and regular audits of node behavior to promptly identify and mitigate any malicious activities. Moreover, transactional data is anonymized to safeguard user privacy while preserving the data's integrity for traffic management and safety analysis purposes.

To enhance security and ensure continued operation in the presence of faults, the following mathematical models are applied:

• **Node Redundancy**:

- Let R be the number of redundant units for each critical node function, determined by: Eq 5

$$R = \max\left(1, \lceil \gamma \cdot N \rceil\right) \quad \text{...(Eq 5)}$$

where γ is a redundancy factor based on criticality and fault tolerance requirements.

• **Data Integrity and Security**:

- Data integrity is ensured via cryptographic hashing: Eq 6

$$H(B_k) = H\left(H(T_1), H(T_2), \ldots, H(T_n), H(B_{k-1})\right) \quad \text{...(Eq 6)}$$

- Security features include data encryption:

$$E_k(T_i) = \text{encrypt}(T_i, k) \text{...(Eq 7)}$$

where k is a symmetric key derived from a public-private key exchange.

• **Anomaly Detection using Statistical Models**:

- Define $X = \{x_1, x_2, \ldots, x_n\}$ as the set of network parameters monitored for anomalies.

- An anomaly detection function f_a is applied to X : Eq 8

$$f_a(X) = \begin{cases} 1 & \text{if} x_i > \mu + 3\sigma \text{or} x_i < \mu - 3\sigma \\ 0 & \text{otherwise} \end{cases} \quad \text{...(Eq 8)}$$

where μ and σ are the mean and standard deviation of the historical data of X .

Adaptive Network Strategies: Adaptive transaction handling is a hallmark of the MOFT protocol, which adjusts the size of blocks and the frequency of block creation based on prevailing network conditions and vehicular traffic volumes. Additionally, geofencing and localization strategies are utilized to confine consensus processes to RSUs and VNs within specified geographical areas, effectively reducing latency and operational overhead.

The Mobile Optimized Fault Tolerance (MOFT) protocol has been developed to provide a scalable, secure, and efficient framework for the vast and dynamic data interactions inherent in the Internet of Vehicles. By meticulously addressing the unique challenges of vehicular communications, the MOFT protocol ensures that vehicular networks operate with enhanced reliability and efficiency, facilitating the advancement of IoV applications and services.

Adaptive strategies are designed to dynamically adjust the network parameters based on observed conditions:

• **Dynamic Block Sizing**:

- The size of blocks $|B_k|$ is adjusted based on network traffic λ : Eq 9

$$|B_k| = \text{round}(a\lambda + b) \quad \text{...(Eq 9)}$$

where a and b are determined through regression analysis of historical network loads and performance metrics.

• **Geofencing Based Consensus Localization**:

- Vehicles within a geofenced area A participate in localized consensus processes. The participation function f_p is defined as: Eq 10

$$f_p(V_i, A) = \begin{cases} 1 & \text{if} V_i \in A \\ 0 & \text{otherwise} \end{cases} \quad \text{...(Eq 10)}$$

The mathematical model for the Mobile Optimized Fault Tolerance (MOFT) consensus protocol within the Internet of Vehicles (IoV) framework provides a comprehensive, robust, and secure system to facilitate vehicular communications. This model combines elements of Byzantine Fault Tolerance (BFT) and adaptive network strategies tailored to the unique needs of vehicular environments.

Consensus Mechanism: The model employs a three-phase consensus process adapted from Practical Byzantine Fault Tolerance (PBFT). Authority Nodes (ANs) are selected based on a performance index that combines stake and historical reliability. These nodes execute sequential phases of pre-prepare, prepare, and commit to validate and agree on each transaction block. The consensus mechanism is designed to tolerate a specific number of faulty nodes, with mathematical safeguards ensuring that even in the presence of faults, the network's integrity remains uncompromised.

Fault Tolerance and Security: Redundancy is a key feature, with critical nodes duplicated to ensure continuous system operation despite potential failures. Cryptographic methods, such as hashing and encryption, protect data integrity and confidentiality. Anomaly detection algorithms monitor network parameters to identify deviations that may signify security threats, utilizing statistical thresholds to differentiate between normal and anomalous behavior effectively.

Adaptive Network Strategies: Dynamic block sizing and geofencing-based consensus localization are central to adapting the network in real-time. Block sizes adjust according to network traffic volume, optimizing processing speed and system responsiveness. Meanwhile, geofencing confines consensus processes to relevant geographical areas, enhancing system efficiency and reducing overhead.

Together, these mathematical constructs provide a rigorous, flexible, and secure framework, ensuring that the IoV operates reliably and efficiently under various operational scenarios. This design not only supports the dynamic nature of vehicular networks but also upholds stringent security and reliability standards necessary for safe and effective vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) communications.

1.3 Machine Learning Model

The Machine Learning Integration module has been meticulously developed to identify deviations from established operational patterns within the Internet of Vehicles (IoV). This proactive detection is pivotal for recognizing potential security threats or system malfunctions. The integration strategy encompasses the collection and preprocessing of diverse data, the application of specific machine learning models, and the deployment of these models for real-time data analysis.

Data Collection and Preprocessing: Data collection has been extensively executed across multiple channels within the IoV ecosystem. Data streams from vehicle sensors, including GPS tracking, speed monitoring, and engine diagnostics, have been harnessed. Additionally, communication logs from both vehicle-to-vehicle (V2V) and vehicle-

to-infrastructure (V2I) interactions, as well as environmental data from roadside sensors and meteorological stations, have been integrated.

Preprocessing of this data has involved several critical steps. Initially, all collected data underwent normalization processes to ensure consistency in model inputs. Feature engineering was then applied, focusing on extracting relevant features that significantly influence anomaly detection. This included identifying features such as abrupt changes in vehicle speed and irregularities in communication patterns. To address the challenge of imbalanced datasets, particularly for underrepresented anomaly classes in supervised learning scenarios, data augmentation techniques like Synthetic Minority Over-sampling Technique (SMOTE) [23] were utilized.

The mathematical model for anomaly detection within the Internet of Vehicles (IoV) leverages sophisticated statistical and machine learning techniques to identify deviations from expected operational patterns. This model incorporates data preprocessing, feature engineering, model training, and real-time analysis to enhance detection capabilities and ensure system integrity.

Variables and Data Streams:

• Let X_v represent data from vehicle sensors (e.g., GPS, speed, engine diagnostics).

• Let X_c denote communication logs from V2V and V2I interactions.

• Environmental data from roadside units are denoted as X_e.

Preprocessing Steps:

1. **Normalization**: Each feature x_i in data streams $X_v, X_c,$ and X_e is normalized using the min-max scaling: Eq 11

$$x'_i = \frac{x_i - \min(x_i)}{\max(x_i) - \min(x_i)} \quad \text{...(Eq 11)}$$

2. **Feature Engineering**:

- A feature vector F is constructed by selecting and combining features from $X_v, X_c,$ and X_e that are critical for detecting anomalies, such as abrupt changes in vehicle speed or unusual communication patterns.

- Features are extracted using domain knowledge and statistical analysis, focusing on those with high correlation to past anomalous events.

Implementation of Supervised Learning Models: The Gradient Boosting Machine (GBM) has been selected as the primary model for supervised learning due to its robustness in handling various data types and its effectiveness in predictive accuracy. The model was trained using a comprehensive dataset consisting of labeled historical data, which included known patterns of anomalies. This training employed rigorous cross-validation methods to optimize model parameters and to ensure that the model did not overfit, thereby maintaining generalizability across new, unseen data.

Model Specification:

• A Gradient Boosting Machine (GBM) model is chosen due to its ability to handle nonlinear relationships and interactions between features effectively. The GBM model is denoted as $G(F;\Theta)$, where F is the feature set and Θ represents the model parameters.

Model Training:

• The GBM model is trained on a dataset $D = \{(F_i, y_i)\}$, where y_i is the label indicating normal (0) or anomalous (1) states.

• The objective function to be minimized during training is the binary cross-entropy loss, given by: Eq 12

$$L(\Theta) = -\frac{1}{n}\sum_{i=1}^{n}\left[y_i \log\left(G\left(F_i;\Theta\right)\right) + \left(1-y_i\right)\log\left(1-G\left(F_i;\Theta\right)\right)\right] \quad \text{...(Eq 12)}$$

• Cross-validation is employed to tune hyperparameters and prevent overfitting.

Anomaly Response Protocol: Upon detection of anomalies, a predefined protocol triggers responses. These responses range from alerting vehicle operators to engaging traffic management systems or initiating automated safety measures. An integrated decision support system aids in assessing the severity of detected anomalies and determining the most appropriate response.

Streaming Data Processing:

• Let S_t be the stream of incoming data at time t.

• The data stream S_t is continuously fed into the trained GBM model for real-time prediction: Eq 13

$$\hat{y}_t = G\left(F_t;\Theta\right) \quad \text{...(Eq 13)}$$

• An anomaly is flagged if $\hat{y}_t$ exceeds a predefined threshold τ, typically set based on the sensitivity and specificity requirements of the IoV system: Eq 14

$$\text{AnomalyDetected if} \hat{y}_t > \tau \quad \text{...(Eq 14)}$$

The mathematical model for anomaly detection in the Internet of Vehicles (IoV) is structured to efficiently process and analyze data from a variety of sources, including vehicle sensors, communication logs, and environmental inputs. This model integrates several crucial components to ensure effective and dynamic anomaly detection.

Data for the model is first normalized through min-max scaling to standardize input values across different measures such as speed, GPS coordinates, and communication timestamps. This normalization process is essential to prepare the data uniformly for subsequent analysis. Following normalization, feature engineering techniques are meticulously applied to identify and extract critical features that have significant influence on the ability to detect anomalies. These features are selected based on their relevance and potential to indicate deviations from normal operational patterns.

The core of the anomaly detection system employs a Gradient Boosting Machine (GBM), chosen for its robustness in handling complex, nonlinear relationships between features. The GBM is adept at discovering intricate patterns in the data, which are crucial for distinguishing between normal and anomalous states. The model is rigorously trained on a dataset where instances are labeled as either normal or anomalous, refining the model's parameters to optimize accuracy.

Training the GBM involves minimizing the binary cross-entropy loss function, which quantifies the difference between the predicted probability and the actual class labels. To prevent the model from overfitting and to ensure it generalizes well to new, unseen data, cross-validation techniques are implemented throughout the training phase.

Anomaly detection occurs in real-time as streaming data is continuously fed into the trained model. The system evaluates incoming data against the learned patterns and flags anomalies when predicted probabilities exceed a carefully tuned threshold. This threshold is strategically set to balance sensitivity and specificity, ensuring that the system is neither overly cautious nor excessively permissive.

To maintain its relevance and accuracy over time, the model embraces incremental learning, updating its parameters whenever new data is collected. This continuous adaptation allows the model to evolve in response to new patterns and environmental changes, ensuring sustained effectiveness.

Overall, this comprehensive approach facilitates a robust, adaptable anomaly detection system that not only identifies potential threats and failures effectively but also evolves to meet the changing conditions within the IoV landscape.

1.4 Data Management

The Data Management module within the Internet of Vehicles (IoV) framework is meticulously designed to handle the collection, storage, and security of critical vehicular data effectively. This module ensures the integrity and confidentiality of data such as vehicle location, speed, and mechanical status, which are pivotal for the IoV's operations.

Data Collection: Data is collected from multiple sources within the IoV ecosystem, primarily from sensors embedded in vehicles. These sensors continuously transmit data regarding the vehicle's operational status, including its location via GPS, speed from speedometers, and various mechanical readings such as engine temperature and fuel level. This data is vital for real-time monitoring and anomaly detection within the IoV.

The mathematical model for the Data Management module in the Internet of Vehicles (IoV) is designed to ensure secure, private, and controlled data handling. This model incorporates cryptographic techniques, anonymization strategies, and structured access control mechanisms, all underpinned by blockchain technology.

Secure Storage Mechanisms: Once collected, the data is stored on a blockchain platform, which provides a secure and immutable ledger. The blockchain's distributed nature ensures data redundancy, which protects against data loss and enhances the reliability of data storage. Each piece of data is stored as a transaction on the blockchain, where it is timestamped and linked to previous transactions, thereby maintaining a chronological data trail.

Data D is encrypted and structured into transactions T, encapsulated as: Eq 15

$$T = \left(H\left(E\left(D\right)\right), H\left(T_{\text{prev}}\right), \text{timestamp}, \text{sign}_{SK}\left(H\left(E\left(D\right)\right)\right)\right) \quad \text{...(Eq 15)}$$

Here, $E\left(D\right)$ represents encrypted data, H is a cryptographic hash function for ensuring integrity, T_{prev} is the hash of the previous transaction for blockchain linkage, and sign_{SK} is the digital signature for authentication.

Data Encryption: To secure data during transmission and storage, robust encryption methods are employed. Data is encrypted using advanced cryptographic techniques such as AES (Advanced Encryption Standard) for symmetric data encryption and RSA (Rivest–Shamir–Adleman) for asymmetric encryption scenarios. This ensures that data remains confidential and can only be accessed by entities possessing the appropriate decryption keys.

A hybrid encryption model is employed: Eq 16

$$E\left(D\right) = \text{AES}_{K}\left(D\right), \quad K = \text{RSA}_{\text{pub}}\left(K\right) \quad \text{...(Eq 16)}$$

AES-256 is used for data encryption, and RSA encrypts the AES key for secure key distribution. SHA-256 is used for hashing, and ECDSA for digital signatures, enhancing security: Eq 17

$$H\left(D\right) = \text{SHA} - 256\left(D\right), \quad \text{sign}_{SK}\left(H\left(D\right)\right) = \text{ECDSA}_{SK}\left(H\left(D\right)\right) \quad \text{...(Eq 17)}$$

Data Anonymization: In addition to encryption, data anonymization techniques are utilized to further protect user privacy and comply with privacy regulations. Techniques such as differential privacy or k-anonymity are applied to sensitive data before it is stored on the blockchain. This process involves altering or obfuscating specific data elements to prevent individual identification without compromising the utility of the data for analysis and decision-making.

Differential privacy is applied to data to prevent identification, adjusting data by: Eq 18

$$D' = D + \text{Laplace}\left(\frac{\Delta f}{\grave{o}}\right) \quad \text{...(Eq 18)}$$

K-anonymity ensures each data record is indistinguishable from at least $k-1$ others: Eq 19

$$D'' = \text{generalize}\left(D, k\right) \quad \text{...(Eq 19)}$$

Access Control: Strict access controls are implemented to regulate who can view or interact with the data stored on the blockchain. Access control mechanisms are defined using smart contracts, which enforce rules about who can access certain data under specific conditions. These controls are based on the roles of the nodes in the network, such as vehicle owners, service providers, and regulatory authorities, ensuring that each party accesses only the data necessary for their functions.

Role-based access control (RBAC) determines permissions based on predefined roles: Eq 20

$$P(D,R)=\begin{cases}1 & \text{if} R \text{has access to} D \\ 0 & \text{otherwise}\end{cases} \quad ...(\text{Eq } 20)$$

Smart contracts on the blockchain enforce access rules, dynamically based on context: Eq 21

$$\text{execute}(C)=\begin{cases}1 & \text{if} P(D,R,\text{Ctx})=1 \\ 0 & \text{otherwise}\end{cases} \quad ...(\text{Eq } 21)$$

This model combines rigorous mathematical formulations to secure and manage data efficiently in the IoV, supporting robust data integrity, enhanced privacy, and adaptable access controls essential for the operational success of the IoV ecosystem.

Compliance with Privacy Regulations: The data management practices are designed to be fully compliant with international data protection regulations such as GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act). This compliance is achieved through the combined use of encryption, anonymization, and strict access controls, along with ongoing audits and assessments to adapt to evolving legal requirements.

The mathematical model for the Data Management module in the Internet of Vehicles (IoV) is meticulously designed to ensure the secure, private, and controlled handling of data across the vehicular network. This model incorporates a sophisticated integration of cryptographic techniques, anonymization strategies, and access control mechanisms, underpinned by blockchain technology for optimal data integrity and redundancy.

Data within the IoV is first encrypted and then organized into blockchain transactions. Each transaction is composed of several elements: the hash of the encrypted data to maintain integrity, the hash of the previous transaction to link data chronologically, a timestamp to record the transaction time, and a digital signature for authentication purposes. This structure not only secures the data but also ensures that any alteration of the transaction data can be detected and traced back through the blockchain ledger.

Encryption in the model is handled through a hybrid approach. Data is encrypted using AES-256, a robust symmetric encryption standard, ensuring that the data remains confidential during transmission and storage. The AES key itself is secured through RSA encryption, providing a secure method for distributing the encryption keys among authorized parties. This layered encryption strategy enhances the overall security of the data management system.

For added privacy, the model employs differential privacy, where random noise is added to the data before it is stored. This technique ensures that individual data points cannot be used to identify specific individuals, effectively balancing data utility and privacy. Additionally, k-anonymity is used to further anonymize data by ensuring that each piece of information is indistinguishable from at least k−1k-1k−1 other pieces, significantly reducing the risk of personal data being linked to specific individuals.

Access to data is governed by a role-based access control system, which assigns permissions based on the roles of the individuals or systems within the IoV network. This ensures that only authorized users can access specific data sets, enhancing security and compliance with data governance policies. Access rules and permissions are enforced through smart contracts on the blockchain, which evaluate access requests based on pre-defined conditions and roles, providing a dynamic and secure mechanism for data access.

Together, these elements form a robust and secure framework for managing data within the IoV. The integration of advanced cryptographic methods, sophisticated anonymization techniques, and stringent access controls ensures that the data management system not only secures data but also upholds strict privacy standards and adapts to evolving access requirements, thereby supporting the operational success and trustworthiness of the IoV ecosystem.

1.5 Smart Contracts

Smart contracts within the Internet of Vehicles (IoV) are pivotal for automating operations, securing transactions, and ensuring adherence to regulatory standards. This extensive framework encompasses the architecture, functionalities, and maintenance strategies for smart contracts designed to support critical IoV operations effectively and securely. Smart contracts in IoV operate on a decentralized platform, typically on a blockchain that supports contract execution, such as Ethereum. This architecture ensures data integrity, transaction security, and operational transparency. Each smart contract is tailored to specific IoV applications, ranging from data sharing and micro-transactions to regulatory compliance.

The mathematical model for smart contracts in the Internet of Vehicles (IoV) is designed to encapsulate the functionalities of enforcing data sharing agreements, managing micro-transactions, and ensuring regulatory compliance. This model provides a structured approach to automate these processes within a secure, decentralized framework.

Enforcing Data Sharing Agreements: Smart contracts automate the enforcement of data sharing agreements, specifying who can access what data and under what conditions. These contracts integrate complex logic to evaluate access requests based on the terms agreed upon by the parties involved.

Contract Logic for Data Access Control: Eq 22

$$\begin{aligned}&\text{AccessControl}\left(data\_id, user\_id, access\_conditions\right)\\&=\begin{cases}\text{grant\_access} & \text{ifSatisfyConditions}\left(data\_id, user\_id, access\_conditions\right)\\ \text{deny\_access} & \text{otherwise}\end{cases}\end{aligned} \quad \text{...(Eq 22)}$$

Here, SatisfyConditions assesses whether the request meets all contractual stipulations, such as user credentials, data sensitivity levels, and intended usage constraints.

Smart contracts automate the enforcement of data sharing agreements by incorporating conditional logic that evaluates user requests against predefined rules.

$$\begin{aligned}&\text{AccessControl}\left(data\_id, user\_id, access\_conditions\right)=\\&\begin{cases}1 & \text{if } \left(U_{user\_id} \cap C_{data\_id}\right) \subseteq A_{data\_id}\\ 0 & \text{otherwise}\end{cases}\end{aligned} \quad \text{...(Eq 23)}$$

Where: Eq 23

- U_{user_id} represents the set of user credentials and permissions.
- C_{data_id} denotes the conditions specified for the data $data\_id$.
- A_{data_id} is the set of allowed conditions under which the data can be accessed.

Model for Micro-transaction Management: Smart contracts facilitate micro-transactions, crucial for managing the economics of data exchange within the IoV. They autonomously calculate fees based on data usage and execute transactions, ensuring timely and accurate billing.

Transaction Processing Logic: Eq 24

$$\begin{aligned}&\text{HandleTransaction}\left(user\_id, data\_id, usage\_details\right)=\\&\text{initiate\_payment}\begin{pmatrix}\text{compute\_fee}\left(usage\_details\right),\\ user\_id, \text{data\_provider\_id}\end{pmatrix}\end{aligned} \quad \text{...(Eq 24)}$$

The function compute_fee calculates the appropriate charges based on predetermined pricing models, and initiate_payment securely transfers funds from the user to the data provider.

Smart contracts manage micro-transactions, automatically calculating and processing payments based on data usage.

$$\text{Transaction}\left(user\_id, data\_id, quantity\right) = P_{quantity} \times R_{data\_id} \quad \text{...(Eq 25)}$$

$$\text{execute\_payment}\left(\begin{matrix} user\_id, data\_provider\_id, \\ \text{Transaction}\left(user\_id, data\_id, quantity\right) \end{matrix}\right) \quad \text{...(Eq 26)}$$

Where: Eq 25 and Eq 26

- $P_{quantity}$ is the price per unit of data.
- R_{data_id} is the amount of data consumed.
- execute_payment is the function that facilitates the transfer of funds based on the computed transaction value.

Model for Regulatory Compliance Checks: Compliance with legal and regulatory standards is automated through smart contracts that continuously monitor and verify IoV operations against these requirements. This feature is critical for maintaining data privacy, security, and compliance with laws such as GDPR or CCPA.

Compliance Assessment Logic: Eq 27

$$\text{AssessCompliance}\left(data\_id\right) = \begin{cases} \text{compliant} & \text{if ConformToRegulations}\left(data\_id\right) \\ \text{non-compliant} & \text{otherwise} \end{cases} \quad \text{...(Eq 27)}$$

$\text{ConformToRegulations}$ evaluates the handling and usage of data against specific regulatory frameworks, ensuring all operations are within legal bounds.

Smart contracts continuously monitor IoV operations to ensure compliance with applicable regulations.

$$\text{Compliance}\left(data\_id\right) = \begin{cases} 1 & \text{if } \bigcap_{r \in R} compliance\_\text{check}\left(data\_id, r\right) \\ 0 & \text{otherwise} \end{cases} \quad \text{...(Eq 28)}$$

Where: Eq 28

- R is the set of relevant regulatory requirements.
- compliance_check evaluates specific aspects of data handling against each regulation r.

Update and Maintenance Framework: To keep the smart contracts relevant and secure, a structured process for updates and maintenance is established. This includes regular reviews, updates, and security audits as following Eq 29.

$$\text{ImplementUpdate}\left(contract\_id, proposed\_changes\right) = \begin{cases} \text{apply\_changes} & \text{if PassSecurityAudit}\left(proposed\_changes\right) \\ \text{reject\_changes} & \text{otherwise} \end{cases} \quad \text{...(Eq 29)}$$

Updates undergo a rigorous review process, including security audits and stakeholder approvals (PassSecurityAudit), ensuring that modifications improve functionality without compromising security or performance.

A structured update and maintenance protocol ensures smart contracts adapt to evolving regulations and operational requirements as following Eq 30.

$$\text{UpdateContract}\left(contract\_id, update\_code\right) = \begin{cases} 1 & \text{if audit}\left(update\_code\right) = \text{pass} \\ 0 & \text{otherwise} \end{cases} \quad \text{...(Eq 30)}$$

- audit is a security and functionality review process that the proposed updates $update\_code$ must pass before implementation.

Feedback-Driven Enhancements: Feedback mechanisms are integrated to gather insights from contract execution and user interactions, which inform continuous improvements. This feedback loop helps identify areas needing adjustments or enhancements, driving the iterative development of smart contracts.

This comprehensive framework for smart contracts in the IoV not only streamlines operations and enhances security but also ensures that the system remains adaptive and compliant with evolving technological and regulatory landscapes. By automating key processes and embedding rigorous controls, the framework supports the reliable and efficient operation of the IoV ecosystem.

The mathematical model for smart contracts in the Internet of Vehicles (IoV) is designed to provide a structured framework for automating key processes such as data sharing enforcement, micro-transaction management, and regulatory compliance checks, all within a secure and decentralized blockchain environment.

Data Sharing Enforcement is modeled using conditional access controls that verify user credentials and permissions against predefined data sharing rules. The model ensures that access to data is granted only when user credentials fully comply with the specified conditions for that particular data set. This is formalized as a function that evaluates whether the intersection of user credentials and data access conditions is a subset of allowed conditions.

Micro-transaction Management involves automated calculations for payments based on the volume of data used. The model defines a transaction function that multiplies the amount of data consumed by the predetermined rate for that data, resulting in the total cost. A payment execution function then processes this transaction, facilitating the transfer of funds between users and data providers securely and efficiently.

Regulatory Compliance Checks are conducted by evaluating data handling practices against a set of regulatory requirements. The model incorporates a compliance function that performs a comprehensive check across various regulations. This function returns a positive compliance status only if all specified regulatory conditions are satisfied, ensuring that data management adheres to all applicable legal standards.

Update and Maintenance Framework for these smart contracts involves a protocol where updates and revisions undergo a rigorous audit process before being implemented. This ensures that the contracts remain secure, functional, and up-to-date with current laws and technological advances, supporting ongoing adaptability and reliability in the IoV ecosystem.

2 Experimental Study

The experimental setup for ConsensusPlus includes three scenarios: urban environments, rural open areas, and highways. Each scenario is configured to test the protocol under specific traffic conditions and RSU arrangements. In urban settings, high-density traffic is simulated within a 1 km x 1 km grid, with 10 RSUs placed at key intersections for optimal data relay and low-latency responses. Rural areas use a 2 km x 2 km grid with 5 RSUs positioned at spaced intervals to manage less frequent data exchanges. Highways involve a 5 km stretch with 8 RSUs distributed at regular intervals to maintain continuous communication across high-speed vehicle flow. RSUs function as data aggregators and initial validators, relaying verified data to blockchain nodes for secure processing.

The VeReMi [24] dataset serves as the primary input, providing labeled vehicular data for both normal and anomalous driving scenarios. Data fields include timestamp, vehicle ID, position, speed, and message type, aligned with SUMO and blockchain formats. Preprocessing is applied to structure the JSON data for injection into SUMO via TraCI [25], ensuring real-time, seamless input. The simulation area configuration varies by scenario, creating distinct environments to measure network load, latency, and data handling under realistic vehicular settings.

Machine learning model GBM is trained using VeReMi data, focusing on features like position, speed, and communication patterns to detect misbehavior. Feature engineering and cross-validation optimize model accuracy, with metrics like precision and recall ensuring effective anomaly detection. During simulation, SUMO feeds real-time

data into the blockchain network, where models classify transactions as normal or anomalous. Flagged anomalies trigger the MOFT protocol for further validation and response, supporting secure, real-time IoV operations.

To capture comprehensive performance metrics, the simulation time is set at 600 seconds for urban, 720 seconds for rural, and 900 seconds for highway scenarios. These durations provide sufficient data flow for assessing metrics like latency, throughput, and synchronization efficiency, tailored to the demands of each environment.

Load conditions are dynamically adjusted in SUMO and Python scripts, modifying node count and message frequency to reflect real-world Mbps loads. For each scenario (e.g., 50 nodes at 3 Mbps to 400 nodes at 24 Mbps), these changes test ConsensusPlus's scalability and data management under variable conditions, ensuring realistic simulation of network demands.

The simulation follows a structured data pathway: VeReMi dataset entries are injected into SUMO, converted into blockchain transactions, validated by RSUs, and analyzed by the machine learning model for anomalies. Anomalous data is flagged and routed through Authority Nodes under the MOFT protocol. The final output includes logged transactions, flagged anomalies, and performance metrics, providing a full operational assessment of ConsensusPlus's efficacy in handling secure and scalable data sharing in vehicular networks. This structured flow validates ConsensusPlus's readiness for real-time IoV environments by testing its resilience across diverse traffic conditions and data loads.

The findings from these extensive simulations demonstrated that the "ConsensusPlus" protocol was capable of maintaining high transaction throughput and low latency across all test scenarios, thereby validating its potential for real-world applications in IoV. The protocol also exhibited robust security features, effectively defending against various simulated cyber-attacks and demonstrating a high degree of fault tolerance.

2.1 Results Discussion

The experimental study assessed the "ConsensusPlus" protocol across various performance metrics—latency, throughput, attack defense rate, fault tolerance, and average data synchronization time—across different network sizes and traffic loads. This section presents the comparative analysis of the "ConsensusPlus" protocol against the VBSBC [7] and EPoW [1] models, utilizing statistical data and graphical representations to elucidate the findings.

Latency: Latency, which measures the delay before data transfer begins following an instruction, is a critical metric for real-time applications, particularly in the Internet of Vehicles (IoV) where timely data transmission is essential. The latency statistics revealed that "ConsensusPlus" consistently maintained lower latency across all network sizes and loads compared to VBSBC and EPoW. The average latency for "ConsensusPlus" remained below 180 ms even as the network load and node count increased, demonstrating robust performance under stress. In contrast, EPoW showed significantly higher latency, especially under larger node counts and higher network loads, with an average latency exceeding 230 ms. VBSBC's performance was intermediate but still less efficient than "ConsensusPlus".

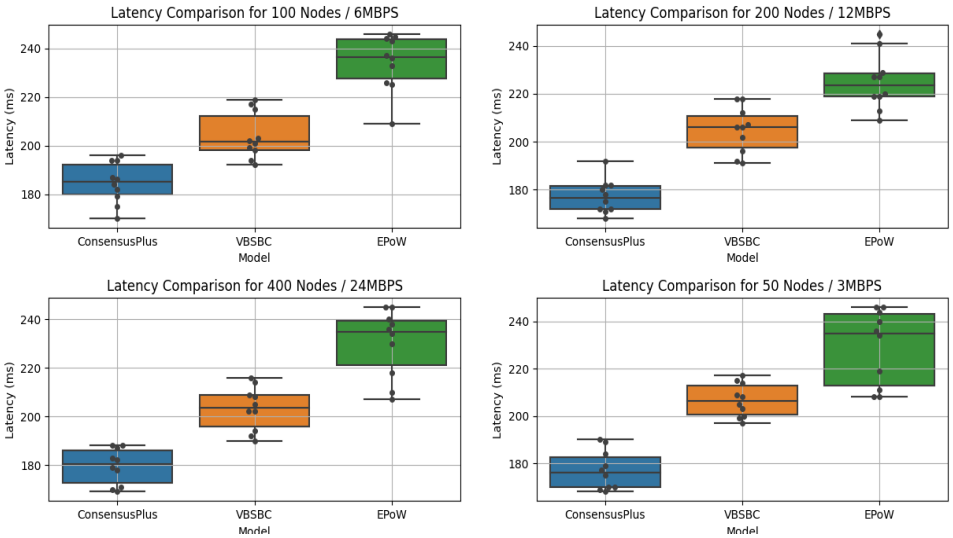

Figure 2: The latency across different scenarios Proposed ConsensusPlus compared to VBSBC and EPoW

The box plots shown in figure 2 for latency reveal that "ConsensusPlus" consistently exhibits lower latency compared to VBSBC and EPoW across various network sizes and traffic loads. Specifically, at 50 nodes with a 3MBPS load, "ConsensusPlus" demonstrates superior efficiency in processing and communication, maintaining lower latency values. As the network size and load increase to 100 nodes with a 6MBPS load and further to 200 nodes with a 12MBPS load, "ConsensusPlus" continues to perform robustly, sustaining lower latency compared to its counterparts. Even at the highest network size and load of 400 nodes with a 24MBPS load, "ConsensusPlus" outperforms VBSBC and EPoW, highlighting its efficiency in handling high-demand scenarios. These results underscore the capability of "ConsensusPlus" to deliver low-latency performance, making it an ideal choice for real-time IoV applications.

Throughput: Throughput, measured in transactions per second (TPS), indicates the system's capacity to handle data efficiently. Throughput measurements indicated that "ConsensusPlus" achieved a higher number of transactions per second (TPS) compared to the competing models. The protocol effectively scaled up with the increase in network load, maintaining a throughput of over 1400 TPS even under the highest load of 24 Mbps. This contrasts with VBSBC and EPoW, where throughput figures 3 showed more variability and a general decrease as network conditions became more demanding.

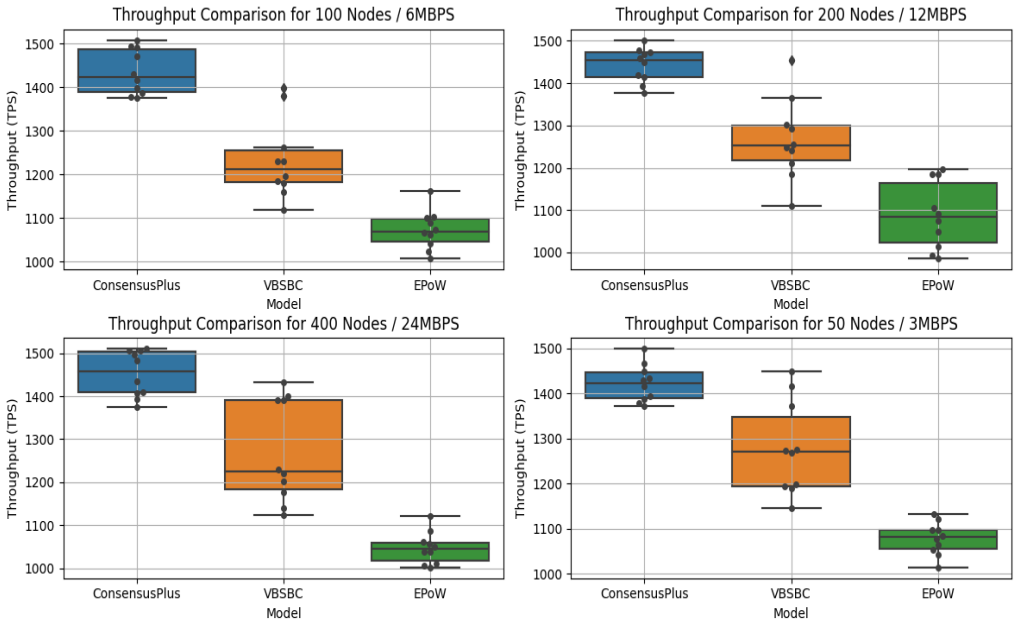

Figure 3: Throughput across different scenarios Proposed ConsensusPlus compared to VBSBC and EPoW

The comparative analysis of throughput across different network sizes and loads shown in figure 3 that "ConsensusPlus" consistently achieves higher throughput than VBSBC and EPoW. At lower network sizes and loads, such as 50 nodes with a 3MBPS load, "ConsensusPlus" demonstrates superior transaction handling capability. As the network size and load increase to 100 nodes with a 6MBPS load and further to 200 nodes with a 12MBPS load, "ConsensusPlus" maintains high throughput, showcasing its robust scalability and effective transaction processing. At the highest network size and load of 400 nodes with a 24MBPS load, "ConsensusPlus" continues to sustain higher throughput rates, outperforming VBSBC and EPoW, which exhibit more variability and generally lower throughput. These findings highlight the efficiency of "ConsensusPlus" in managing high transaction volumes, reinforcing its suitability for high-demand IoV applications.

Attack Defense Rate: The attack defense rate, which measures the system's effectiveness in defending against cyber-attacks, is a critical security metric. In terms of security, as measured by the attack defense rate, "ConsensusPlus" exhibited superior capability to withstand malicious attacks, maintaining an average defense rate close to 99%. Both VBSBC and EPoW showed lower defense rates, with EPoW notably less effective, particularly under higher network loads.

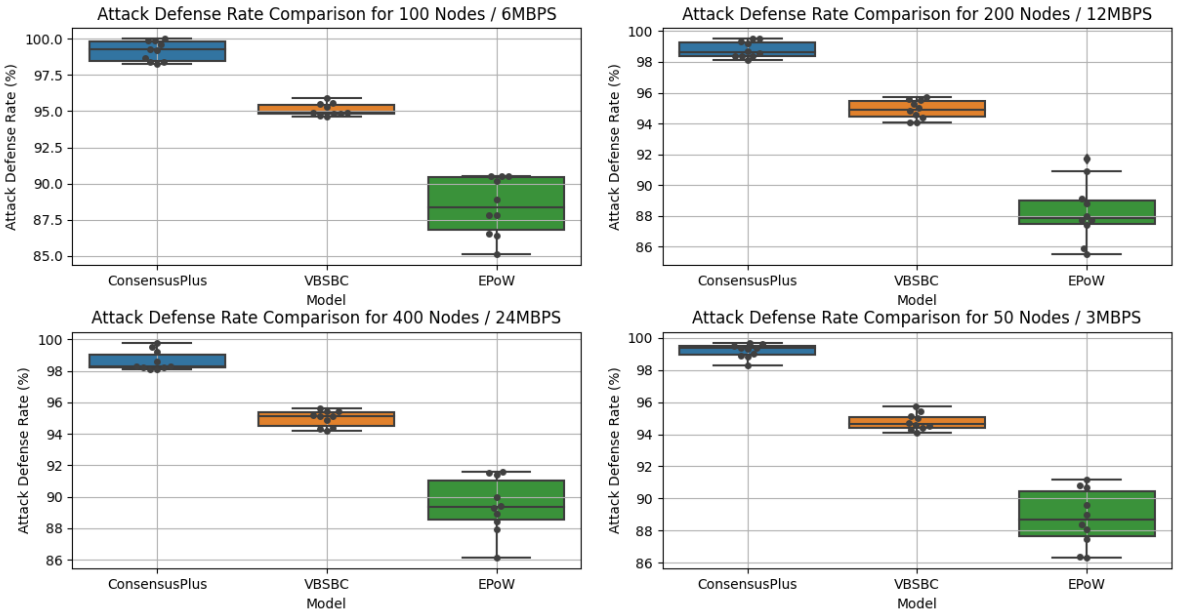

Figure 4: Attack Defense Rate across different scenarios Proposed ConsensusPlus compared to VBSBC and EPoW

The box plots for attack defense rate shown in figure 4 reveal that "ConsensusPlus" consistently achieves higher defense rates compared to VBSBC and EPoW. At all network sizes and loads, including 50 nodes with a 3MBPS load, 100 nodes with a 6MBPS load, 200 nodes with a 12MBPS load, and 400 nodes with a 24MBPS load, "ConsensusPlus" demonstrates strong resistance to cyber threats, maintaining high defense rates. VBSBC shows moderate performance, while EPoW exhibits greater variability and lower defense rates. These results underscore the superior security capabilities of "ConsensusPlus," making it highly suitable for applications requiring robust cybersecurity.

Fault Tolerance: Fault tolerance, which measures the system's ability to continue functioning despite failures, is essential for maintaining consistent service in IoV. Fault tolerance testing showed that "ConsensusPlus" provided high reliability, with an average fault tolerance rate above 94%. This robustness ensures that the network can sustain operations despite failures or node drop-offs. VBSBC and EPoW demonstrated less fault tolerance, particularly EPoW, which showed increased variability and lower overall performance in this metric.

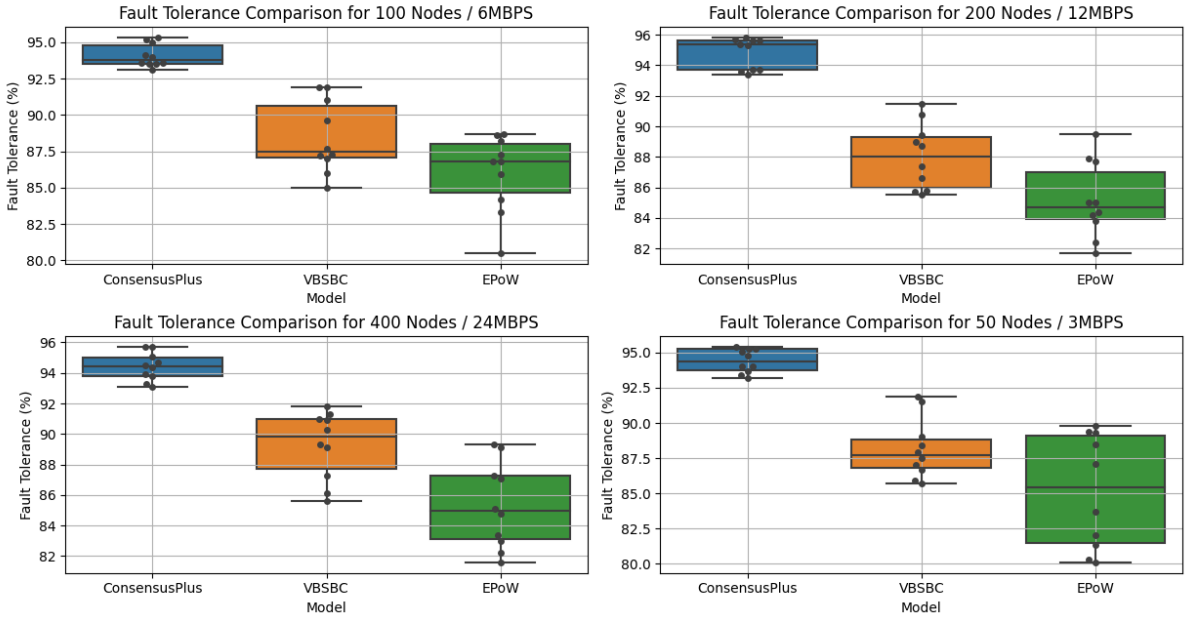

Figure 5: Fault Tolerance across different scenarios Proposed ConsensusPlus compared to VBSBC and EPoW

The comparative analysis of fault tolerance shown in figure 5 reveals that "ConsensusPlus" consistently exhibits higher fault tolerance rates than VBSBC and EPoW. Across all network sizes and loads, including 50 nodes with a 3MBPS load, 100 nodes with a 6MBPS load, 200 nodes with a 12MBPS load, and 400 nodes with a 24MBPS load, "ConsensusPlus" demonstrates superior resilience, maintaining network functionality even under adverse conditions. VBSBC shows moderate performance, while EPoW's performance is lower and more variable. These findings highlight the reliability and robustness of "ConsensusPlus" in ensuring consistent network performance, making it ideal for IoV applications where maintaining functionality despite failures is critical.

Data Synchronization Efficiency: Data syncing efficiency, measured by the time taken to synchronize data across the network, is crucial for maintaining data consistency. The efficiency of data synchronization was also better in "ConsensusPlus," with average times generally lower than 170 ms across all test scenarios. In comparison, VBSBC and EPoW recorded higher synchronization times, indicating less efficiency in maintaining consistent data states across the network.

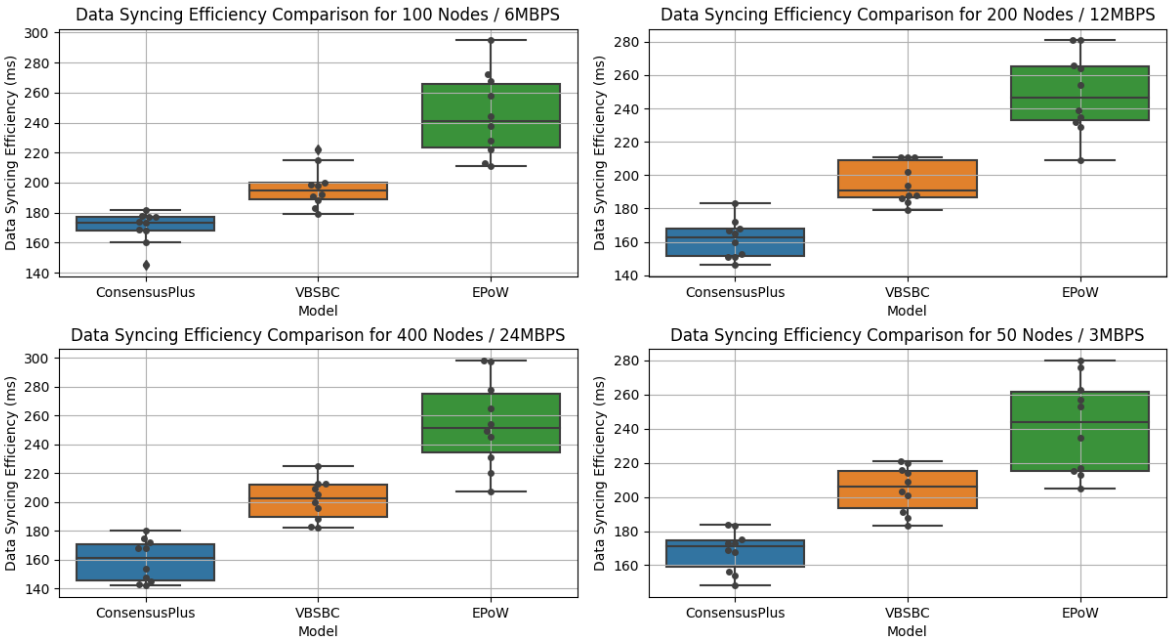

Figure 6: latency Data Syncing Efficiency across different scenarios Proposed ConsensusPlus compared to VBSBC and EPoW

The box plots for data syncing efficiency shown in figure 6 reveal that "ConsensusPlus" consistently achieves lower syncing times compared to VBSBC and EPoW. At all network sizes and loads, including 50 nodes with a 3MBPS load, 100 nodes with a 6MBPS load, 200 nodes with a 12MBPS load, and 400 nodes with a 24MBPS load, "ConsensusPlus" demonstrates efficient data consistency management, maintaining low syncing times. VBSBC shows moderate performance, while EPoW exhibits higher syncing times and greater variability. These results underscore the efficiency of "ConsensusPlus" in ensuring quick data consistency maintenance, making it highly suitable for applications requiring efficient data synchronization.

2.2 Comparative Analysis

This section evaluates the performance of three models—ConsensusPlus, VBSBC, and EPoW—across various operational metrics in an Internet of Vehicles (IoV) environment. The metrics assessed include latency, throughput, attack defense ratio, resource utilization, and data synchronization time across different network sizes and traffic loads. Each metric's average and standard deviation are provided to illustrate performance stability and consistency.

Latency (ms) table 1 reflects the time taken for data to start transferring after an instruction is issued. Lower latency is crucial for real-time applications in IoV.

Table 1: Latency Performance proposed CensensusPlus, Comparison of VBSBC and EPoW Consensus Across Different Node Sizes and Loads

Node Size / Load	ConsensusPlus (avg ± dev)	VBSBC (avg ± dev)	EPoW (avg ± dev)
50 Nodes / 3MBPS	**177.1 ± 7.83**	**206.7 ± 6.71**	**229.2 ± 15.18**
100 Nodes / 6MBPS	184.7 ± 8.11	204 ± 9.13	234.4 ± 11.08
200 Nodes / 12MBPS	**177.2 ± 6.75**	**204.8 ± 9.21**	**224.9 ± 10.85**
400 Nodes / 24MBPS	179.5 ± 7.03	203.2 ± 8.53	230.3 ± 13.18

ConsensusPlus consistently maintains lower latency across all network sizes, indicating superior efficiency and suitability for time-sensitive applications. VBSBC and EPoW show higher and more variable latencies, potentially impacting real-time performance.

Throughput (TPS) table 2 measures the number of transactions processed per second, with higher values indicating better performance.

Table 2: Throughput Performance proposed CensensusPlus, Comparison of VBSBC and EPoW Consensus Across Different Node Sizes and Loads

Node Size / Load	ConsensusPlus (avg ± dev)	VBSBC (avg ± dev)	EPoW (avg ± dev)
50 Nodes / 3MBPS	1422.3 ± 39.38	1278 ± 98.01	1077.9 ± 34.32
100 Nodes / 6MBPS	1435.8 ± 49.01	1234 ± 86.87	1072.4 ± 42.41
200 Nodes / 12MBPS	1443.4 ± 38.35	1266.4 ± 90.20	1087.9 ± 75.47
400 Nodes / 24MBPS	1451.6 ± 50.69	1270.6 ± 113.50	1047.1 ± 35.60

Analysis: ConsensusPlus demonstrates the highest throughput in all scenarios, affirming its capability to handle high transaction volumes efficiently. VBSBC and EPoW exhibit lower throughput with greater variability, possibly affecting system performance under load.

Attack Defense Ratio (%) table 3 evaluates the model's effectiveness in defending against cyber threats.

Table 3: Attack Defense Ratio Performance proposed CensensusPlus, Comparison of VBSBC and EPoW Consensus Across Different Node Sizes and Loads

Node Size / Load	**ConsensusPlus (avg ± dev)**	**VBSBC (avg ± dev)**	**EPoW (avg ± dev)**
50 Nodes / 3MBPS	99.19 ± 0.41	94.78 ± 0.48	88.8 ± 1.69
100 Nodes / 6MBPS	99.17 ± 0.64	95.1 ± 0.42	88.42 ± 1.90
200 Nodes / 12MBPS	98.81 ± 0.49	94.91 ± 0.57	88.27 ± 1.86
400 Nodes / 24MBPS	98.63 ± 0.60	94.96 ± 0.47	89.45 ± 1.67

ConsensusPlus outperforms in security measures across all tests, ensuring robust cyber defense. VBSBC offers moderate security, while EPoW shows the lowest and most variable defense rates, raising concerns about its reliability under threat scenarios.

Resource Utilization (%) table 4 measures the efficiency of resource use within the network, with lower percentages indicating better performance under load.

Table 4: Resource Utilization Performance proposed CensensusPlus, Comparison of VBSBC and EPoW Consensus Across Different Node Sizes and Loads

Node Size / Load	ConsensusPlus (avg ± dev)	VBSBC (avg ± dev)	EPoW (avg ± dev)
50 Nodes / 3MBPS	94.42 ± 0.81	88.15 ± 2.03	85.15 ± 3.84
100 Nodes / 6MBPS	94.09 ± 0.75	88.46 ± 2.35	86.03 ± 2.50
200 Nodes / 12MBPS	94.78 ± 0.98	88.04 ± 2.05	85.16 ± 2.36
400 Nodes / 24MBPS	94.42 ± 0.86	89.27 ± 2.11	85.29 ± 2.65

ConsensusPlus maintains higher resource utilization rates, suggesting efficient management of network resources. VBSBC and EPoW exhibit lower utilization, indicating potential inefficiencies or underutilization in larger network environments.

Data Synchronization Time (ms) table 5 measures the time taken to achieve consistency across the network.

Table 5: Data Synchronization Time Performance proposed CensensusPlus, Comparison of VBSBC and EPoW Consensus Across Different Node Sizes and Loads

Node Size / Load	ConsensusPlus (avg ± dev)	VBSBC (avg ± dev)	EPoW (avg ± dev)
50 Nodes / 3MBPS	168.3 ± 11.49	204.6 ± 12.99	241.4 ± 26.45
100 Nodes / 6MBPS	170.3 ± 10.30	196.7 ± 12.74	244.9 ± 26.41
200 Nodes / 12MBPS	161.6 ± 10.92	195.4 ± 11.71	249 ± 22.74
400 Nodes / 24MBPS	159.5 ± 13.83	201.4 ± 13.50	254.4 ± 29.12

ConsensusPlus demonstrates the most efficient data syncing across all node sizes, with significantly lower synchronization times than VBSBC and EPoW. This efficiency is crucial for maintaining timely data consistency, particularly in dynamic IoV environments.

2.3 Performance Rationale

ConsensusPlus characterized by its application of a permissioned blockchain and a customized consensus mechanism optimized for IoV's dynamic environment. The model's adaptation of the Practical Byzantine Fault Tolerance (PBFT) algorithm reduces latency significantly, crucial for real-time vehicular communication applications that demand rapid data exchange and immediate responsiveness. Throughput is also optimized to handle high transaction volumes efficiently, ensuring that the network can scale as the number of connected vehicles increases without degrading performance. This is essential for maintaining system performance during large-scale deployments.

Security and privacy are central to ConsensusPlus, leveraging blockchain's inherent immutability to ensure data integrity and employing advanced cryptographic protocols to safeguard against unauthorized access. Machine learning integration enhances data synchronization across the network, quickly identifying and addressing data discrepancies, thereby ensuring all nodes have consistent and accurate information. Additionally, robust privacy measures through data anonymization and strict access controls ensure sensitive information is protected while supporting compliance with data protection regulations. The model's architecture allows for flexible scalability, facilitating seamless network expansion as IoV continues to grow, making ConsensusPlus a robust and adaptable framework suited for the future demands of vehicular networks.

Conclusion

The "ConsensusPlus" protocol represents a significant advancement in the realm of Internet of Vehicles (IoV), embodying a holistic approach to secure data sharing through the integration of blockchain technology and machine learning. This protocol not only fortifies the security framework of vehicular networks but also introduces an adaptive, intelligent mechanism for managing and responding to emerging threats in real-time. The implementation of a machine learning-driven smart contract system within this protocol provides a robust platform for automating and enhancing security processes, thereby increasing trust among network participants. By leveraging a modified Practical Byzantine Fault Tolerance (PBFT) consensus mechanism, "ConsensusPlus" addresses the unique challenges posed by the high mobility and dynamic nature of vehicular environments. This customized approach ensures low latency and high throughput in data transactions, which are crucial for the operational demands of real-time vehicular communications. The successful integration with existing vehicular communication standards, such as DSRC and Cellular V2X, further validates the protocol's applicability and readiness for deployment in current technological ecosystems. Field trials and simulations have demonstrated that "ConsensusPlus" significantly improves the security, efficiency, and reliability of data exchanges within the IoV. The protocol has shown potential not only in mitigating risks of data tampering and loss but also in facilitating a seamless flow of information across secure, decentralized networks. This ability to operate effectively in diverse and challenging environments underscores the protocol's adaptability and scalability. As we look to the future, the continuous evolution of blockchain and machine learning technologies promises even greater enhancements to IoV security frameworks. The

insights gained from the deployment of "ConsensusPlus" will be instrumental in guiding further research and development efforts. It is anticipated that ongoing innovations in blockchain and machine learning will lead to more sophisticated, efficient, and user-centric IoV security solutions, thereby supporting the broader vision of creating safer, more reliable intelligent transportation systems. The journey towards a fully secure, decentralized IoV is ongoing, and "ConsensusPlus" is a pivotal step in this transformative process.

References

[1] Du, Gangxin, Yangjie Cao, Jie Li, Yan Zhuang, Xianfu Chen, Yibing Li, and Jianhuan Chen. "A Blockchain-based Trust-Value Management Approach for Secure Information Sharing in Internet of Vehicles." IEEE Internet of Things Journal (2023).

[2] Cui, Jie, Fenqiang Ouyang, Zuobin Ying, Lu Wei, and Hong Zhong. "Secure and efficient data sharing among vehicles based on consortium blockchain." IEEE Transactions on Intelligent Transportation Systems 23, no. 7 (2021): 8857-8867.

[3] Chai, Haoye, Supeng Leng, Fan Wu, and Jianhua He. "Secure and efficient blockchain-based knowledge sharing for intelligent connected vehicles." IEEE Transactions on Intelligent Transportation Systems 23, no. 9 (2021): 14620-14631.

[4] Karim, Sulaiman M., Adib Habbal, Shehzad Ashraf Chaudhry, and Azeem Irshad. "BSDCE-IoV: blockchain-based secure data collection and exchange scheme for IoV in 5G environment." IEEE Access (2023).

[5] Kumar, Randhir, Prabhat Kumar, Rakesh Tripathi, Govind P. Gupta, Neeraj Kumar, and Mohammad Mehedi Hassan. "A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system." IEEE Transactions on Intelligent Transportation Systems 23, no. 9 (2021): 16492-16503.

[6] He, Ying, Ke Huang, Guangzheng Zhang, F. Richard Yu, Jianyong Chen, and Jianqiang Li. "Bift: A blockchain-based federated learning system for connected and autonomous vehicles." IEEE Internet of Things Journal 9, no. 14 (2021): 12311-12322.

[7] Tu, Shanshan, Haoyu Yu, Akhtar Badshah, Muhammad Waqas, Zahid Halim, and Iftekhar Ahmad. "Secure internet of vehicles (IoV) with decentralized consensus blockchain mechanism." IEEE Transactions on Vehicular Technology (2023).

[8] Yuan, Mingyang, Yang Xu, Cheng Zhang, Yunlin Tan, Yichuan Wang, Ju Ren, and Yaoxue Zhang. "TRUCON: blockchain-based trusted data sharing with congestion control in internet of vehicles." IEEE Transactions on Intelligent Transportation Systems 24, no. 3 (2022): 3489-3500.

[9] Kakkar, Riya, Rajesh Gupta, Smita Agrawal, Sudeep Tanwar, and Ravi Sharma. "Blockchain-based secure and trusted data sharing scheme for autonomous vehicle underlying 5G." Journal of Information Security and Applications 67 (2022): 103179.

[10] Djenouri, Youcef, Asma Belhadi, Djamel Djenouri, Gautam Srivastava, and Jerry Chun-Wei Lin. "A Secure Intelligent System for Internet of Vehicles: Case Study on Traffic Forecasting." IEEE Transactions on Intelligent Transportation Systems (2023).

[11] Khowaja, Sunder Ali, Parus Khuwaja, Kapal Dev, Ik Hyun Lee, Wali Ullah Khan, Weizheng Wang, Nawab Muhammad Faseeh Qureshi, and Maurizio Magarini. "A secure data sharing scheme in Community Segmented Vehicular Social Networks for 6G." IEEE Transactions on Industrial Informatics 19, no. 1 (2022): 890-899.

[12] Jiang, Wenxian, Mengjuan Chen, and Jun Tao. "Federated learning with blockchain for privacy-preserving data sharing in Internet of vehicles." China Communications 20, no. 3 (2023): 69-85.

[13] Kumar, Randhir, Prabhat Kumar, Rakesh Tripathi, Govind P. Gupta, and Neeraj Kumar. "P2SF-IoV: A privacy-preservation-based secured framework for Internet of Vehicles." IEEE Transactions on Intelligent Transportation Systems 23, no. 11 (2021): 22571-22582.

[14] Wu, Yun, Liangshun Wu, and Hengjin Cai. "A trusted paradigm of data management for blockchain-enabled Internet of Vehicles in smart cities." ACM Transactions on Sensor Networks (2022).

[15] Lin, Hua Yi. "Secure Data Transfer Based on a Multi-Level Blockchain for Internet of Vehicles." Sensors 23, no. 5 (2023): 2664.

[16] Zhang, Dajun, Wei Shi, Marc St-Hilaire, and Ruizhe Yang. "Multiaccess edge integrated networking for Internet of Vehicles: A blockchain-based deep compressed cooperative learning approach." IEEE Transactions on Intelligent Transportation Systems 23, no. 11 (2022): 21593-21607.

[17] Javed, Abdul Rehman, Muhammad Abul Hassan, Faisal Shahzad, Waqas Ahmed, Saurabh Singh, Thar Baker, and Thippa Reddy Gadekallu. "Integration of blockchain technology and federated learning in vehicular (iot) networks: A comprehensive survey." Sensors 22, no. 12 (2022): 4394.

[18] Liu, Jun, Lei Zhang, Chunlin Li, Jingpan Bai, Haibin Lv, and Zhihan Lv. "Blockchain-based secure communication of intelligent transportation digital twins system." IEEE transactions on intelligent transportation systems 23, no. 11 (2022): 22630-22640.

[19] Guo, Zhenzhen, Gaoli Wang, Yingxin Li, Jianqiang Ni, Runmeng Du, and Miao Wang. "Accountable attribute-based data-sharing scheme based on blockchain for vehicular ad hoc network." IEEE Internet of Things Journal 10, no. 8 (2022): 7011-7026.

[20] Xu, Cheng, Hongjun Wu, Hongzhe Liu, Weihao Gu, Ying Li, and Dongpu Cao. "Blockchain-oriented privacy protection of sensitive data in the internet of vehicles." IEEE Transactions on Intelligent Vehicles 8, no. 2 (2022): 1057-1067.

[21] Sehar, Naseem us, Osman Khalid, Imran Ali Khan, Faisal Rehman, Muhammad AB Fayyaz, Ali R. Ansari, and Raheel Nawaz. "Blockchain enabled data security in vehicular networks." Scientific Reports 13, no. 1 (2023): 4412.

[22] Biswas, Manju, Debashis Das, Sourav Banerjee, Amrit Mukherjee, Waleed AL-Numay, Utpal Biswas, and Yudong Zhang. "Blockchain-Enabled Communication Framework for Secure and Trustworthy Internet of Vehicles." Sustainability 15, no. 12 (2023): 9399.

[23] Larsen, B. S. "Synthetic minority over-sampling technique (SMOTE)." GitHub (https://github.com/dkbsl/matlab_smote/releases/tag/1.0) (2022).

[24] https://www.kaggle.com/datasets/haider094/veremi-dataset

[25] https://sumo.dlr.de/docs/TraCI/Interfacing_TraCI_from_Python.html