Secure Authentication Mechanism of Internet of Vehicles Using Blockchain Technology

MS.S. AARTHI[1], K. KAVYA VARSHITHA[2], K. BHARGAVI LAKSHMI[3], T. SASANK SURYA[4]
Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, India

***Abstract*—A secure authentication mechanism for the Internet of Vehicles (IoV) using blockchain ensures that communication between vehicles, infrastructure, and users is protected from unauthorized access and data tampering, aims to develop decentralized, tamper-proof authentication system using blockchain's distributed ledger technology. By leveraging smart contracts, each vehicle and device in the network can authenticate securely without relying on a central authority, reducing vulnerabilities and enhancing trust. The system ensures transparency, immutability, and security while maintaining low latency, crucial for real-time vehicular communications. It addresses key challenges such as scalability, privacy, and efficient consensus protocols to enable secure, fast, and reliable interactions within the IoV ecosystem.**

The rapid advancement of intelligent transportation systems has given rise to the Internet of Vehicles(IoV), enabling seamless communication between vehicles, infrastructure, and networks. However, the open and dynamic nature of IoV exposes it to significant security threats, particularly in the areas of authentication, data integrity, and trust management. This project proposes a novel secure authentication mechanism that integrates Blockchain technology with the Byzantine Fault Tolerance (BFT) algorithm to address these challenges. Blockchain provides a decentralized and immutable ledger that ensures transparency and resistance to tampering, while BFT ensures reliable consensus even in the presence of malicious or faulty nodes. By leveraging these technologies, the proposed system enables secure and efficient mutual authentication among vehicles and network components, without relying on centralized authorities. Additionally, smart contracts are utilized to automate authentication processes and enforce security policies dynamically.

The proposed solution enhances security, scalability, and trust within the IoV ecosystem. Simulation results confirm that the system significantly reduces authentication delays and provides strong resilience against various cyber-attacks, making it a practical and robust approachfor real-world IoV implementations.

***Index Terms*—Internet of Vehicles, Blockchain Technology, Secure Authentication, Vehicular Networks, Decentralized Systems. Byzantine Fault Tolerance, Network Security, Smart Transportation, Consensus Mechanism.**

I. INTRODUCTION

The Internet of Vehicles (IoV) plays a key role in smart transportation networks by allowing vehicles to exchange information with one another, roadside infrastructure, and cloud services for enhanced traffic management and safety. With the growing reliance on real-time data exchange in IoV networks, security and privacy have become major concerns. Unauthorized access, identity spoofing, and data tampering pose serious threats to both vehicle functionality and user safety. Traditional authentication mechanisms, which often depend on centralized authorities, struggle to meet the dynamic, distributed nature of IoV. To overcome these limitations.

This investigates the use of Blockchain technology combined with the Byzantine Fault Tolerance (BFT) algorithm to achieve secure and decentralized authentication. potentially causing accidents or traffic jams. Moreover, privacy concerns are paramount as sensitive user information could be exposed or misused, posing a direct threat to the safety and privacy of drivers and passengers. Blockchain provides transparency and safeguards data integrity, while BFT improves the system’s resilience to faults and ensures reliable consensus across distributed nodes.

To address these issues, a robust, scalable, and secure authentication system is critical for IoV. Traditional centralized authentication models, which rely on a single authority to manage and validate identities, are susceptible to single points of failure and are not well-suited for the large-scale, decentralized nature of IoV. The complexity of

mobile services in IoV demands a more sophisticated solution that can handle real-time authentication with low latency and high resilience to attacks. Blockchain technology, with its decentralized structure and robust cryptographic foundations, addresses key security challenges by ensuring data integrity and protection. It provides an immutable and tamper-resistant ledger, where every transaction or authentication event is securely recorded. The use of consensus mechanisms guarantees that these records are validated by the network, preventing unauthorized alterations.

The Internet of Vehicles is highly vulnerable to various security threats, especially during the authentication process, where malicious actors can impersonate vehicles or manipulate data. Existing centralized authentication systems create single points of failure and are not well-suited for the decentralized and mobile environment of IoV. These weaknesses can lead to unauthorized access, data breaches, and communication disruptions, compromising the safety and efficiency of transportation systems. Therefore, there is a critical need for a secure, decentralized authentication mechanism that can ensure trust, scalability, and fault tolerance in IoV networks

This aims to develop a secure and decentralized authentication mechanism tailored for the dynamic environment of IoV. It ensures trusted identity verification between vehicles and infrastructure without relying on a central authority. The integration of blockchain provides data immutability and transparency, while the BFT consensus algorithm enables secure agreement even in the existence of malicious nodes. This solution is scalable and suitable for real-time vehicular networks, offering improved resilience against cyber-attacks. It lays the groundwork for future advancements in intelligent transportation systems with enhanced security and privacy measures.

II. LITERATURE REVIEW

This chapter offers a comprehensive analysis of existing research and scholarly articles related to the project's theme. It outlines key findings, technological advancements, and the progression of methodologies in the field. Through this review, various techniques and models are critically assessed and compared, providing a strong foundation for understanding the current state-of-the-art and identifying potential gaps or opportunities for further exploration and innovation. This section plays a vital role in positioning the project within a broader academic context by leveraging insights and outcomes from previous studies

Zhong Xiaoyu et al. (2023) conducted an extensive survey on location privacy protection technologies within the Internet of Vehicles (IoV). The study highlights the criticality of safeguarding location information, as unauthorized tracking can lead to severe privacy breaches. The authors classified location privacy protection mechanisms into categories such as cryptographic methods, pseudonym exchange, and spatial cloaking techniques. They emphasized the need for context-aware and lightweight protocols to match the real-time nature of vehicular networks. The paper also points out challenges in balancing privacy, system efficiency, and service accuracy, suggesting a shift toward blockchain and AI-assisted privacy-preserving solutions for future IoV systems.

Sruthi Chavali et al. (2023) provided an overview of the core components and technologies powering autonomous vehicles while addressing their associated security and privacy requirements. The study discussed elements like sensors, embedded systems, vehicle-to-everything (V2X) communication, and cloud integration, all of which are susceptible to security threats. The authors detailed several types of attacks such as GPS spoofing, sensor manipulation, and remote-control hijacking.

Deng Yukang et al. (2022) focused on the foundational properties of vehicular networking and presented a classification and summary of various protection schemes. The authors categorized these properties into communication reliability, low latency, and high mobility, which together create a complex environment for maintaining security. They then analyzed current protection mechanisms such as authentication protocols, intrusion detection systems, and secure data aggregation techniques.

Zhou Jianhua et al. (2022) explored the typical application scenarios in the intelligent connected automobile industry, including autonomous driving, smart traffic systems, and vehicle-to-infrastructure

(V2I) communications. The study outlined the architecture of intelligent vehicles and their reliance on data-intensive technologies, making them prime targets for cyber-attacks. The authors emphasized the need for robust data authentication and identity management systems, particularly in large-scale deployment scenarios.

Al Shareeda M A et al. (2022) reviewed existing security of Vehicular Ad Hoc Networks (VANETs), which form the communication backbone of IoV. The paper detailed various types of security threats such as, and denial-of-service attacks. It also evaluated defensive strategies including trust-based models, public key infrastructure (PKI), and anomaly detection algorithms. The authors concluded that while many proposed methods enhance security, there is still a need for lightweight, scalable, and real-time solutions.

XIAO et al. (2021) reviewed the development status of vehicle networking both domestically and internationally. The paper highlighted the rapid growth of intelligent vehicle networks and the challenges faced in standardization, cross-border compatibility, and infrastructure readiness. The authors discussed the gap in adopting uniform security policies and emphasized the necessity for integrated frameworks that combine communication protocols, hardware security modules, and cloud services. They also stressed the importance of international cooperation in building globally interoperable and secure IoV systems.

III. METHODOLOGY

In proposed system addresses these challenges by introducing a decentralized authentication mechanism using blockchain technology and the Byzantine Fault Tolerance (BFT) consensus algorithm. Each vehicle and roadside unit is securely registered onto a permissioned blockchain network, where it is assigned a unique cryptographic identity. Authentication requests are broadcast across the network and validated through the BFT algorithm, which ensures consensus even if some nodes behave maliciously or unpredictably. This will thereby improving fault tolerance and system availability. They are enforce authentication policies and control access to vehicle resources autonomously. The blockchain ledger ensures that all transactions are recorded immutably, supporting transparency and auditability. The system provides a scalable, real- time solution that enhances data integrity, user privacy, and communication security across the IoV ecosystem.

Architecture Diagram

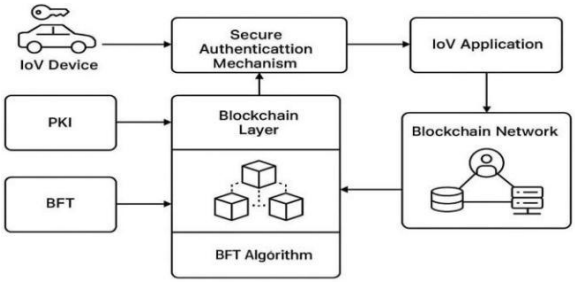
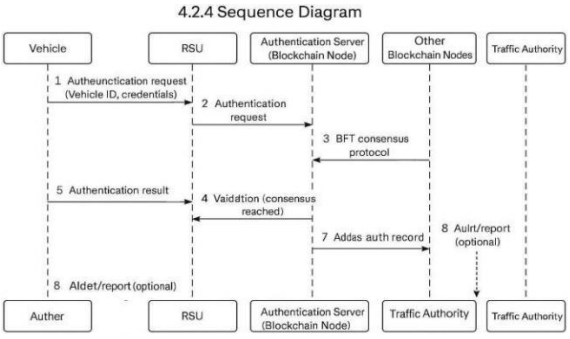


Figure illustrates a Vehicles send authentication requests to Roadside Units (RSUs), which forward them to a blockchain network where the BFT algorithm validates and records transactions. Smart contracts manage access control, ensuring secure, real-time communication within the IoV ecosystem.

In the design stage, various models and diagrams are developed to illustrate different aspects of the system, including its structure, behavior, and data movement. Tools such as UML, sequence diagrams, use case diagrams, and data flow diagrams are utilized to effectively represent the system's architecture and operations to both stakeholders and development teams. Overall, this phase plays ensuring the software solution is designed to meet its intended goals efficiently and accurately

Sequence Diagram



A. Modules amd Module description:

1. MODULE 1- Authentication Module: Authentication request is cross- checked with blockchain-stored identities to prevent spoofing or unauthorized access. The decentralization ensures that no single point of failure can be exploited.is

handles the identity verification of vehicles using cryptographic credentials embedded in blockchain transactions.

2. MODULE 2- Blockchain Integration Module: Blockchain Integration module enables secure interaction with the blockchain network, where each authenticated transaction is stored immutably. It utilizes smart contracts to automate authentication policies and access control decisions. Byzantine Fault Tolerance (BFT) is implemented to maintain consensus, even when some nodes may be malicious or faulty. This ensures the reliability and trustworthiness of recorded authentication data

3. MODULE 3- Detection and Response Module: Detection and Response Module constantly monitors network traffic and vehicle behavior to detect anomalies such as replay attacks, Sybil attacks, or unusual communication patterns. Machine learning or rule- based techniques can be integrated to enhance detection accuracy. Upon identifying suspicious activity, the module triggers alerts and initiates a BFT-based consensus for deeper validation. It helps maintain system integrity by isolating or blocking compromised nodes.

B. STEPS OF IMPLEMENTATION:

I.Pre-Processing of Data:
Clean the raw IoV data by removing missing values, duplicates, and inconsistent entries to maintain data quality. Normalize numerical features like speed, time, and distance to a standard scale (e.g., 0 to 1) for better model performance. Encode categorical variables such as vehicle type, region ID, and status using one-hot encoding or label encoding. Convert and format timestamps consistently, and extract additional time-related features like hour, minute, or weekday. Apply noise reduction techniques to sensor data to filter out random errors or fluctuations in the readings. Map the preprocessed vehicle data to blockchain entries using identifiers like transaction hashes and block IDs for secure linkage

II. Split the Data:
The processed vehicle data is divided into three subsets for model development and evaluation.

- Training Set (70%): Utilized to train the authentication model using the extracted features and sketches of vehicles.
- Validation Set (15%): Employed to adjust model parameters and identify the most effective configuration.
- Testing Set (15%): Applied to evaluate the model's performance on new, unseen data to ensure its reliability.

III. Build the Model:
To develop a machine learning-based authentication model that verifies vehicle identity using image/sketch features.

- Input Layer:

Inputs include vehicle ID, timestamp, location data, cryptographic signatures, and sensor data (e.g., speed, proximity). Additional blockchain metadata like block number, transaction hash, and node ID can also be included

- Encoder Section:

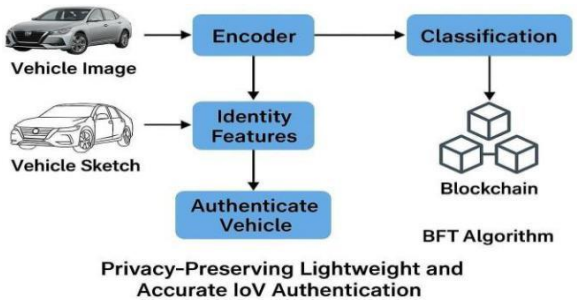
Use CNNs or dense layers to extract key patterns from input data (especially for spatial features like location). Implement LSTM/GRU layers to encode temporal dependencies (e.g., movement pattern of a vehicle over time). Reduce feature space while retaining key characteristics using dense layers or attention mechanisms. Extract encoded representation of digital signatures or hashed credentials for secure comparison

- Decoder Section:

The Decoder Section takes the encoded features and reconstructs them into a recognizable format, such as a sketch or number plate pattern, for comparison and verification. It ensures that the compressed data still accurately represents the original vehicle identity. This helps validate the authentication before final storage on the blockchain, enhancing both accuracy and security in the system

- Module Creation:

The model is created to authenticate vehicles by analyzing images or sketches and extracting unique identity features. It begins with an input layer that receives processed vehicle data, followed by an encoder that compresses the data into feature vectors. These vectors are classified using a machine learning or deep learning algorithm to determine authenticity. Optionally, a decoder verifies feature consistency. Finally, the authentication result is validated through BFT consensus and stored securely on the blockchain



IV. IMPLEMENTATION

The model is compiled using an appropriate optimizer (e.g., Adam), loss function (e.g., categorical cross entropy), and performance metrics like accuracy. The training process uses the pre-split training dataset (70%) to learn vehicle features and identities. Validation data (15%) is used to tune the model and prevent overfitting. The model is trained over multiple epochs with defined batch size to improve learning performance. Once trained, it is evaluated on the test set and prepared for integration with the blockchain layer for secure authentication.

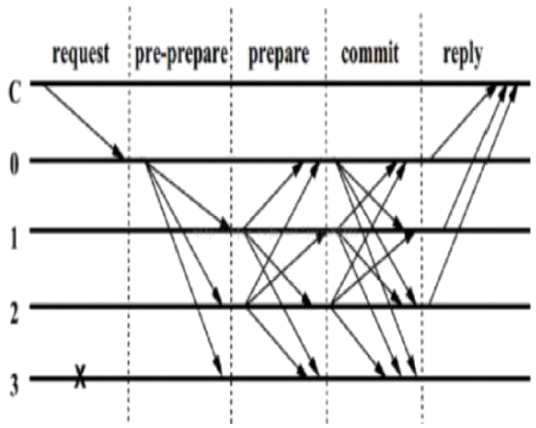
The structure illustrates the interconnection of blocks in a blockchain, where each block contains a unique hash that is derived from both its transaction data and the hash of the preceding block. This design ensures a secure linkage between blocks, as any alteration in the data of one block would result in a change in its hash, thereby affecting all subsequent blocks. Each block also stores critical identifiers, such as a pseudo identity and a public key, associated with the vehicles or entities involved in the transactions. This chaining mechanism establishes an immutable ledger, enhancing the integrity and security of the blockchain, making it resistant to tampering and unauthorized modifications. The combination of transaction details and cryptographic identifiers facilitates secure communication and authentication, which is vital for applications like the Internet of Vehicles.

C. Byzantine Fault Tolerance Algorithm:

The scenario outlines a consensus process in a distributed system that employs the Byzantine Fault Tolerance (BFT) algorithm to ensure reliable communication and agreement among nodes. In this setup, a requester node, labeled C, interacts with several server nodes, including servers 0, 1, 2, and 3. Among these, server 3 is marked as being offline, which introduces a challenge for reaching consensus on requests.

The protocol initiates when node C sends a request to server
0. Upon receiving this request, server 0 broadcasts it to the other servers (1, 2, and 3). During the next phase, known as Prepare, the active servers (0, 1, and 2) confirm receipt of the request by broadcasting it again to one another. However, server 3, being down, cannot participate in this communication, which emphasizes the system's ability to function even with some nodes failing to respond.

For the system to successfully reach consensus, a majority of servers must agree on the request during the Commit phase. Once a sufficient number of identical requests are acknowledged, the servers enter the Commit phase, where they broadcast their approval. After this stage, the servers send feedback to requester C, confirming the request's execution. The effectiveness of this approach relies on the condition $N \geq 3F+1N \geq 3F + 1N \geq 3F+1$, where NNN represents the total number of nodes in the system and FFF indicates the maximum number of nodes that can fail or behave incorrectly. This ensures that there are enough operational nodes to achieve consensus despite any failures, thereby maintaining the integrity and reliability of the distributed system.



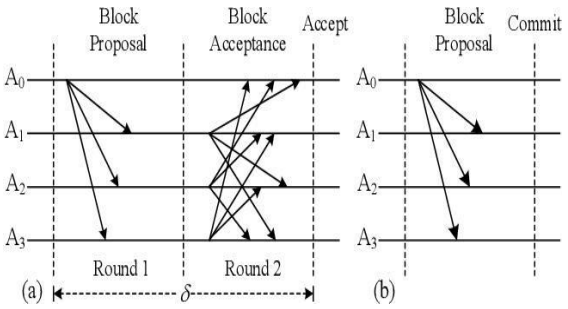
D. Proof of Authority:

In a Proof of Authority (PoA) scenario, a consensus mechanism is established among a designated group of trusted validators, each playing a critical role in the transaction approval process. Initially, the validators engage in a block proposal phase, where one of the authorized nodes submits a proposed block of transactions to the network. This proposal is then communicated to all other validators, creating an opportunity for each participant to assess the legitimacy and integrity of the proposed

transactions. The communication during this phase is essential, as it sets the stage for collaborative verification and enhances the transparency of the entire process.

Following the proposal phase, the diagram transitions into the "Block Acceptance" stage, where nodes engage in a voting process to reach consensus on which proposed block should be added to the blockchain. The arrows indicate the communication paths between nodes, showing how they relay their acceptance or rejection of the proposals. The interactions across multiple rounds demonstrate a robust mechanism where nodes can adjust their votes based on the information received from other validators. This adaptability is crucial for maintaining consensus, as it enables nodes to respond to the dynamics of the network while ensuring that only valid and agreed-upon transactions are recorded.

Finally, the "Commit" phase represents the conclusion of the consensus process, where the accepted block is finalized and added to the blockchain. At this point, all participating nodes have reached an agreement on the proposed transactions, ensuring that the state of the blockchain is consistent across the network. This two-phase approach enhances the efficiency and security of the PoA mechanism, as it minimizes the risk of forks and maintains a clear line of authority among trusted validators. In the context of the IoV, this enables quick and reliable transactions between vehicles and infrastructure, supporting real-time applications such as traffic management and autonomous driving. Overall, the diagram encapsulates the effectiveness of the PoA algorithm in facilitating secure, swift, and efficient consensus among trusted nodes in the Internet of Vehicles.



V. RESULT

E. Image of the subject:

- Input: Pre-processed vehicle images or sketches, along with extracted feature vectors.
- Output: Authentication status (e.g., Verified, Rejected), and secure logging on the blockchain ledger.
- The system checks whether the vehicle matches registered identities using the trained model and BFT verification

Data Sheet of Vehicle

F. Efficiency of Proposed System:

The proposed system enhances the security and efficiency of the Internet of Vehicles (IoV) by integrating Blockchain technology with the Byzantine Fault Tolerance (BFT) algorithm. Blockchain ensures tamper-proof data sharing among vehicles, while BFT guarantees consensus even in the presence of malicious or faulty nodes. This hybrid approach reduces the chances of unauthorized access and data manipulation. Compared to traditional methods, the proposed system offers faster authentication and secure communication between vehicles and infrastructure.

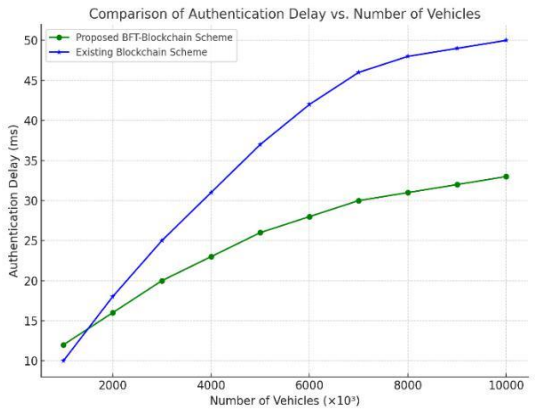
The decentralized structure eliminates the need for a central authority, reducing system downtime and vulnerability. Additionally, the latency is minimized due to the lightweight nature of the BFT algorithm. The system ensures reliability, scalability, and real-time performance, which are crucial in dynamic vehicular environments. It also supports the seamless exchange of data while preserving privacy. Simulation results show improved throughput and reduced computational overhead. Overall, the system increases trust among IoV participants and paves the way for smarter transportation networks

Communication Between Vehicles in Hash Tables

G. Comparison of Experimental Results:

Figure X presents a comparative analysis of authentication delay between the proposed BFT-based blockchain authentication scheme and a conventional blockchain mechanism, evaluated across varying numbers of vehicles in an IoV environment. As the number of vehicles increases from 1,000 to 10,000, both schemes exhibit a growth in delay due to network load and consensus overhead. However, the proposed scheme consistently outperforms the traditional approach. For instance, at 5,000 vehicles, the delay for the BFT-based method is approximately 26 ms, whereas the existing method reaches nearly 38 ms.

The improvement is primarily attributed to the use of the Byzantine Fault Tolerance (BFT) consensus algorithm, which significantly reduces the time required to reach consensus without compromising security. Traditional blockchain schemes, often reliant on PoW or similar mechanisms, tend to suffer from higher latency as network size increases. In contrast, the BFT algorithm allows for faster agreement among trusted nodes, enabling quicker validation and reduced authentication overhead. This makes the proposed architecture highly suitable for real-time IoV applications where low latency and high reliability are critical, such as autonomous driving coordination, emergency vehicle routing, and vehicular data sharing.



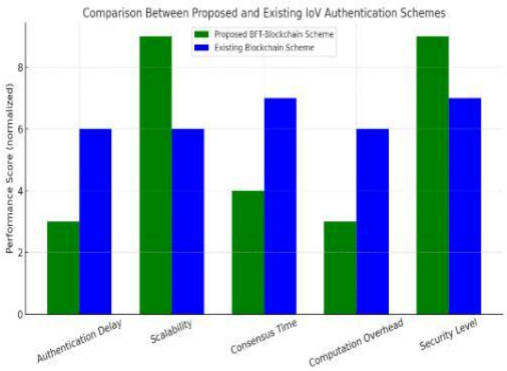
Comparison of Experimental Curves

VI.CHALLENGES AND SOLUTIONS

Figure provides a qualitative comparison between the proposed secure IoV authentication scheme based on Blockchain with BFT consensus and an existing conventional blockchain approach. The comparison is made across five key metrics: authentication delay, scalability, consensus time, computation overhead, and security level, each normalized on a scale of 0 to 10 for consistency

As depicted, the proposed scheme outperforms the existing method in terms of authentication delay, scalability, and computational overhead, attributed to the lightweight and deterministic nature of BFT consensus. While the consensus time remains slightly higher in traditional approaches due to their reliance on probabilistic or energy-intensive methods, the proposed model shows better optimization across all critical dimensions, making it more suitable for real-time and scalable IoV environments.

Comparison of Proposed and Exisisting System



The existing authentication systems in IoV are typically centralized, making them vulnerable to single points of failure and cyber-attacks. They often rely on traditional cryptographic methods which may not scale well with the growing number of vehicles and data exchanges. In contrast, the proposed system uses Blockchain, which provides decentralized, immutable, and transparent data handling, enhancing security. The BFT algorithm ensures consensus without requiring high computational power like Proof of Work (PoW). This results in lower energy consumption and faster processing. While existing systems suffer from scalability and real-time challenges, the proposed model offers high throughput and reduced delay.

VII. CONCLUSION

The proposed secure authentication mechanism for IoV using Blockchain and the BFT algorithm provides a robust and decentralized solution to address security and trust issues in vehicular networks. By eliminating the reliance on centralized servers and incorporating a fault-tolerant consensus mechanism, the system ensures reliable, fast, and tamper-proof communication. The approach significantly improves data integrity, node authentication, and resilience to attacks. This work demonstrates the potential of Blockchain-based systems to transform IoV communication into a more secure and efficient environment.

Additionally, blockchain technology offers effective solutions for identity authentication and counterfeiting challenges within multi-node systems in IoV. By combining blockchain with Public Key Infrastructure (PKI), the proposed approach successfully tackles identity verification issues among vehicles, servers, and Roadside Units (RSUs) while streamlining user account management. The encryption features inherent in blockchain safeguard sensitive vehicle identity information, thus mitigating data breach risks. This research contributes to advancing blockchain applications in IoV by introducing innovative mechanisms for key distribution, node joining, and vehicle identity authentication through blockchain consensus. Experimental results demonstrate that the enhanced authentication framework significantly improves verification quality, effectively resisting malicious attacks and ensuring a secure and efficient IoV ecosystem.

The findings show that blockchain can significantly transform vehicle communication in the IoV ecosystem. By removing the need for centralized control, blockchain creates a decentralized system that enhances trust and security. It ensures the integrity and privacy of data exchanged between vehicles and infrastructure. This approach makes IoV networks more resilient and reliable. The proposed authentication scheme not only fortifies the network against unauthorized access but also streamlines the communication processes, enabling seamless interactions among diverse nodes. As IoV continues to expand, the integration of blockchain technology can facilitate safer and more efficient transportation systems, ultimately contributing to smarter cities and improved quality of life for users. This study sets a foundation for future research, encouraging exploration of additional blockchain applications and optimizations tailored to the evolving challenges of the Internet of Vehicles.

In the future, the proposed system can be enhanced by incorporating Artificial Intelligence (AI) to enable adaptive decision-making for vehicle communication. Edge computing can be integrated to further reduce latency and support real-time analytics. Additionally, smart contract integration can automate access control and service delivery in IoV. Scalability can be improved to handle large-scale deployment across smart cities. Finally, extensive real-world testing can help fine-tune the model for various traffic and environmental conditions to achieve higher reliability and performance

REFERENCES

[1] X. Wang, Z. Ning, M. Zhou, X. Hu, L. Wang, Y. Zhang, F. R. Yu, and B.Hu, “Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions,” IEEE Communications Surveys & Tutorials, vol.21, no. 2, pp. 1314–1345, 2018.

[2] G. Xu, W. Zhou, A. K. Sangaiah, Y. Zhang, X. Zheng, Q. Tang, N. Xiong,K. Liang, and X. Zhou, “A security-enhanced certificateless aggregate signature authentication protocol for invanets,” IEEE Network, vol. 34, no. 2,pp. 22–29, 2020.

[3] W. Chen, Y. Chen, X. Chen, and Z. Zheng, “Toward secure data sharing for the iov: A quality-driven incentive mechanism with on-chain and off-chain guarantees,” IEEE Internet Things J., vol. 7, no. 3, pp. 1625–1640,2020.

[4] Y.Xia,L.Wu,Z.Wang,X.Zheng,andJ.Jin,“Clust er-enabled cooperative scheduling based on reinforcement learning for high-mobility vehicular networks,” IEEE Trans. Veh. Technol., vol. 69, no. 11, pp. 12664–12678,2020.

[5] S.Xie,Z.Zheng, W.Chen,J.Wu, H.-N.Dai,and M.Imran, “Blockchain for cloud exchange: A survey,” Computers & Electrical Engineering, vol. 81, p.106526, 2020.

[6] O.Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T.Lin, X. Liu, Internet of vehicles: Motivation, layered

architecture, network model, challenges, and future aspects, IEEE Access 4 (2016) 5356–5373(2016).

[7] L. Mendiboure, M. A. Chalouf, F. Krief, Towards a 5Gvehicular architecture, in: 14th International Workshop,Nets4Cars/Nets4Trains/Nets4Aircraft 2019, Springer, 2019, pp. 265–277 (2019).

[8] S. Tanwar, J. Vora, S. Tyagi, N. Kumar, M. S. Obaidat, A systematic review on security issues in vehicular ad hoc network, Security and Privacy1 (5) (2018) e39 (2018).

[9] L. Mendiboure, M. A. Chalouf, F. Krief, Towards a blockchain-based sd - iov for applications authentication and trust management, in: International Conference on Internet of Vehicles, Springer, 2018, pp. 265–277 (2018).

[10] Y. Park, C. Sur, K.-H. Rhee, A secure incentive scheme for vehicular de-lay tolerant networks using cryptocurrency, Security and Communication Networks 2018 (2018) 5932183:1–5932183:13 (2018).

[11] Y. Park, C. Sur, K.-H. Rhee, A secure incentive scheme for vehicular delay tolerant networks using cryptocurrency, Security and Communication Networks 2018 (2018) 5932183:1–5932183:13 (2018).

[12] Z. Lu, Q. Wang, G. Qu, Z. Liu, BARS: a blockchain-based anonymous reputation system for trust management in VANETs, arXiv preprint arXiv:1807.06159 (2018).

[13] A. Ali, M. A. Khan, M. A. Khan, BlockAuth: a blockchain-based framework for secure vehicle authentication and authorization, PLoS ONE 18(9): e0289876 (2023).

[14] M. Wagner, B. McMillin, An efficient blockchain authentication scheme for vehicular ad-hoc networks, in: Critical Infrastructure Protection XIV, IFIP Advances in Information and Communication Technology, vol. 596, Springer, Cham, pp. 65–80 (2020).