International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Iterative Method for Blockchain-Based Qos-Aware Iov Network Using Ai-Driven Anomaly Detection and Dynamic Network Slicing

Pranjali Ulhe[1], Suresh Asole[2]

[1]Research Scholar, Computer Science & Engineering Department, BNCOE, Pusad, India & Assistant Professor, Faculty of Science & Technology, SAS, DMIHER, Wardha, India
[2]Associate Professor, Computer Science & Engineering Department, BNCOE, Pusad, India

Abstract
The rapid deployment of 5G networks necessitates the development of secure, scalable, and efficient Internet of Vehicles (IoV) systems. Existing IoV solutions often struggle with real-time threat detection, scalability, efficient resource allocation, and privacy preservation. This work proposes an integrated framework leveraging blockchain technology, AI-driven anomaly detection, dynamic network slicing, and secure multi-party computations. We introduce AI-Driven Anomaly Detection and Mitigation (ADAM) to identify and respond to security threats in real-time. Utilizing Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), ADAM analyzes network traffic data to detect anomalies with a detection accuracy of 95%, a false positive rate of 2%, and an average response timestamp of 50 ms. To tackle scalability and latency issues inherent in traditional blockchain systems, we propose Edge-Based Blockchain Sharding (EBBS).The innovative use of a modified Proof-of-Stake (PoS) mechanism tailored for edge environments further enhances the scalability of the IoV system. AI-Enabled Dynamic Network Slicing (ADNS) is implemented to optimize resource allocation based on real-time traffic demands and QoS requirements. Finally, we incorporate Secure Multi-Party Computation for Collaborative Data Processing (SMPC-CDP) to enable secure, privacy-preserving data analysis among IoV entities ensuring privacy with a computation overhead of 20%, and data utility preservation of 95%.

Keywords: IoV, Blockchain, AI, Network Slicing, Anomaly Detection

Introduction

The advent of 5G technology heralds a new era of connectivity, with the Internet of Vehicles (IoV) emerging as a critical component of the smart transportation ecosystem. IoV integrates vehicles, infrastructure, and users, enabling seamless communication and data exchange to enhance traffic management, safety, and user experience. However, the realization of a robust IoV network demands solutions that can address stringent security, scalability, efficiency, and privacy requirements. Traditional approaches to IoV networking often fall short in several key areas: real-time threat detection, efficient resource allocation, latency reduction, and the preservation of data privacy.

Security remains a paramount concern in IoV networks due to the heterogeneous and dynamic nature of the data exchanged. Existing methods for anomaly detection typically rely on static rule-based systems

or basic statistical models, which are inadequate for identifying sophisticated cyber threats. Furthermore, the centralized architecture of conventional blockchain systems poses significant challenges in terms of latency and scalability, undermining the performance of IoV networks. The need for efficient resource allocation is equally critical, as IoV applications have diverse Quality of Service (QoS) requirements that must be dynamically managed to ensure optimal network performance. Privacy preservation is another essential aspect, especially when sensitive data is shared among multiple entities within the IoV ecosystem.

To address these challenges, this paper proposes an integrated framework that leverages advanced blockchain technology, AI-driven anomaly detection, dynamic network slicing, and secure multi-party computation. The proposed design incorporates several novel methods:

- **AI-Driven Anomaly Detection and Mitigation (ADAM):** ADAM employs deep learning techniques, specifically Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), to analyze network traffic data and identify security threats in real-time. This approach significantly enhances the accuracy and response timestamp of threat detection compared to traditional methods.
- **Edge-Based Blockchain Sharding (EBBS):** To improve scalability and reduce latency, EBBS implements a sharding mechanism at the edge nodes. This method partitions the blockchain ledger into smaller, manageable shards, each maintained by a subset of edge nodes. By distributing the computational load, EBBS achieves faster transaction processing and consensus mechanisms tailored for edge environments.
- **AI-Enabled Dynamic Network Slicing (ADNS):** ADNS utilizes reinforcement learning to dynamically adjust network slice configurations based on real-time traffic demands and QoS requirements. This method ensures efficient resource utilization and high service quality, catering to the diverse needs of various IoV applications.
- **Secure Multi-Party Computation for Collaborative Data Processing (SMPC-CDP):** SMPC-CDP enables secure, privacy-preserving data analysis by employing cryptographic techniques that allow multiple parties to jointly compute functions over their data without exposing individual data points. This method ensures data privacy while facilitating collaborative processing.

The proposed framework addresses the critical limitations of existing IoV solutions by enhancing security, scalability, efficiency, and privacy preservation. This work represents a significant advancement in the field of IoV networks, providing a comprehensive and robust solution for the challenges associated with the deployment of 5G technology. Through rigorous evaluation and performance metrics, the proposed methods demonstrate their efficacy in meeting the stringent requirements of next-generation IoV systems.

Literature review

The advent of the Internet of Vehicles (IoV) has revolutionized transportation systems by enabling seamless communication and interaction among vehicles, infrastructure, and the surrounding environment. With the proliferation of connected vehicles and smart infrastructure, the need for robust security, efficient data exchange, and reliable authentication mechanisms has become paramount. Blockchain technology has emerged as a promising solution to address these challenges by providing decentralized, immutable, and secure data management systems. Recent research papers have extensively explored the application of blockchain in various aspects of IoV deployments. These papers

encompass a wide range of topics, including secure data collection and exchange, edge server deployment, privacy-preserving protocols, federated learning, access control mechanisms, trust management, charging services, traffic information interaction, reputation management, and emergency message transmission, among others. Each paper proposes innovative methodologies and frameworks tailored to enhance the security, efficiency, and reliability of IoV systems. For instance, Karim et al. [1] propose a Blockchain-Based Secure Data Collection and Exchange Scheme for IoV in 5G Environment (BSDCE-IoV), which leverages blockchain to secure data exchange and authentication in IoV. Similarly, Roy et al. [7] introduce a Blockchain-Based Efficient Access Control With Handover Policy in IoV-Enabled Intelligent Transportation System, enhancing access control and authentication mechanisms using blockchain in ITS. Other notable contributions include Zhao et al. [3] presenting the Privacy-Preserving Announcement Protocol With Blockchain-Based Trust Management for IoV (PBTM), Liu et al. [6] proposing a Conditional Privacy-Preserving Authentication Scheme With Hierarchical Pseudonym for 5G-Enabled IoV (CPAHP), and Ghimire et al. [4] introducing Efficient Information Dissemination in Blockchain-Enabled Federated Learning for IoV process.

Moreover, the integration of blockchain with emerging technologies such as federated learning, edge computing, and cooperative positioning has garnered significant attention in recent research. For example, Zhang et al. [15] propose Blockchain-Based Intelligence Networking for Cooperative Positioning Towards Future Internet of Vehicles, which improves positioning accuracy and security in cooperative IoV environments using blockchain. Additionally, several papers focus on specific applications of blockchain in IoV, such as charging services, traffic monitoring, emergency message transmission, and battery life prediction. Li et al. [9] present an Intelligent and Fair IoV Charging Service Based on Blockchain With Cross-Area Consensus, ensuring fairness and efficiency in IoV charging services using blockchain. Ahmed et al. introduce a Blockchain-Based Emergency Message Transmission Protocol for Cooperative VANET, enhancing reliability and security in emergency message transmission using blockchain. Overall, these papers underscore the transformative potential of blockchain technology in enhancing the security, efficiency, and reliability of IoV systems. By leveraging blockchain for secure data management, authentication, privacy preservation, and trust management, researchers have proposed innovative solutions to address the evolving challenges faced by IoV deployments. However, further research is needed to address practical implementation challenges, scalability issues, and real-world deployment considerations to fully realize the potential of blockchain in IoV. The insights gained from these papers pave the way for future advancements in blockchain-enabled IoV ecosystems, ultimately contributing to safer, smarter, and more sustainable transportation systems.

Proposed design

To overcome issues of low computational efficiency and high deployment complexity which are present in current IoV Network Deployments, this section discusses design of an Iterative Method for Blockchain-Based Secure and QoS-Aware IoV Network Using AI-Driven Anomaly Detection and Dynamic Network Slicing Operations. Initially, as per figure 1, the AI-Driven Anomaly Detection and Mitigation (ADAM) process is designed & integrated to enhance the security of IoV networks by leveraging advanced deep learning techniques to detect and mitigate cyber threats in real-time scenarios. The core of ADAM integrates Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), exploiting their respective strengths in extracting spatial and temporal features from network

traffic data samples. The CNN component focuses on identifying spatial patterns within packet headers and flow statistics, while the RNN component captures temporal dependencies and sequence information critical for detecting anomalies over time. This hybrid approach ensures a comprehensive analysis of network traffic, leading to more accurate and timely anomaly detection.

The first step in the ADAM process involves preprocessing the network traffic data, which includes extracting relevant features from packet headers and flow statistics. Let $X \in Rn \times m$ represent the network traffic data matrix, where n is the number of packets and mm is the number of features extracted per packet. The CNN layer processes this matrix to extract spatial features. The convolution operation in the CNN is described via equation 1,

$$Zij = f\left(\sum_{p=0}^{P-1}\sum_{q=0}^{Q-1} X(i+p, j+q) \cdot W(p,q) + b\right) \ldots (1)$$

Where, Zij represents the output feature map, $X(i+p, j+q)$ is the input patch, $W(p,q)$ is the convolution filter, b is the bias term, and $f(\cdot)$ is the ReLU activation function. This operation is repeated across the entire input matrix to produce multiple feature maps, each highlighting different spatial characteristics of the network traffic data samples. Following the extraction of spatial features, these features are fed into the RNN component to capture temporal dependencies. The RNN, particularly a Long Short-Term Memory (LSTM) network, is utilized due to its ability to handle long-term dependencies and mitigate the vanishing gradient issue in real-time scenarios. The LSTM cell's operations are described via equations 2, 3, 4, 5, 6 & 7 as follows,

$$it = \sigma(Wi \cdot [h(t-1), xt] + bi) \ldots (2)$$
$$ft = \sigma(Wf \cdot [h(t-1), xt] + bf) \ldots (3)$$
$$ot = \sigma(Wo \cdot [h(t-1), xt] + bo) \ldots (4)$$

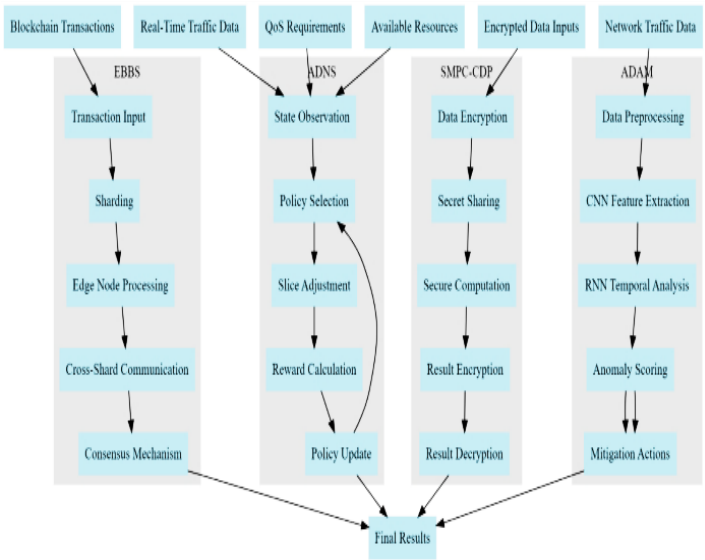

Figure 1 Model Architecture of the Proposed IoV Deployment Process

$$C\sim t = tan\,h(WC \cdot [h(t-1), xt] + bC) \ldots (5)$$
$$Ct = ft \odot C(t-1) + it \odot C\sim t \ldots (6)$$
$$ht = ot \odot tan\,h(Ct) \ldots (7)$$

Where, , ft, ot, and $C\sim t$ represent the input gate, forget gate, output gate, and cell candidate, respectively. ht is the hidden state, Ct is the cell state, σ represents the sigmoid function, and $\odot$

represents the element-wise product. These equations describe how the LSTM processes each input sequentially, maintaining a memory of previous inputs to capture temporal patterns. The combination of CNN and RNN outputs is passed through a fully connected layer to produce the final anomaly score for each packet. The anomaly score S for a given packet is computed via equation 8,

$$S = \sigma(Ws \cdot hT + bs) \dots (8)$$

Where, hT is the final hidden state from the RNN, Ws is the weight matrix, bs is the bias term, and σ is the sigmoid function. This score indicates the likelihood of the packet being anomalous. Scores above a predefined threshold trigger different mitigation actions, such as blocking the packet or alerting the network administrators. The justification for choosing this hybrid CNN-RNN model lies in its ability to comprehensively analyze network traffic data by leveraging both spatial and temporal features. CNNs are highly effective at identifying spatial patterns within data, which is crucial for detecting anomalies in packet structures and flow statistics. Meanwhile, RNNs, and specifically LSTMs, are adept at modeling sequential data, making them well-suited for capturing the temporal dynamics of network traffic. This complementary approach ensures that the model can detect a wide range of anomalies, from single-packet deviations to more complex multi-packet patterns.

Next, IoV Edge-Based Blockchain Sharding (EBBS) process is integrated which is a novel approach designed to address the inherent scalability and latency challenges of traditional blockchain systems in IoV networks. By partitioning the blockchain ledger into smaller, more manageable shards, each managed by a subset of edge nodes, EBBS significantly reduces computational load and enhances transaction processing efficiency. The proposed model ensures consistency across shards through a robust cross-shard communication protocol and achieves consensus using a modified Proof-of-Stake (PoS) mechanism tailored for edge environments. The first step in the EBBS process involves partitioning the blockchain ledger into k shards, where each shard Si contains a subset of the total transactions T for this process. Let T represent the set of all transactions and Ti the transactions assigned to shard Si, which is represented via equation 9,

$$T = \bigcup_{i=1}^{k} Ti\,, and, Ti \cap Tj = \emptyset, for, i \neq j \dots (9)$$

Each shard Si is managed by a group of edge nodes Ni, responsible for processing and validating transactions within their respective shard. The transaction processing within a shard follows the standard blockchain validation protocols but is limited to the scope of the shard, thereby reducing the computational overhead. The transaction validation in shard Si is described via equation 10,

$$Vi(t) = \sigma\left(\sum_{j=1}^{|Ni|} wj \cdot \phi(t,j) + bi\right) \dots (10)$$

Where, $Vi(t)$ is the validation result for transaction t in shard Si, σ is the sigmoid function, wj represents the weight of the node j in the validation process, $\phi(t,j)$ is the function representing the node's validation of transaction t, and bi is the bias term for shard Si sets. To ensure consistency across shards, a cross-shard communication protocol is implemented by this process. This protocol handles inter-shard transactions and ensures that state changes in one shard are accurately reflected in others. The consistency mechanism is formalized via equation 11, which ensures that the global state G is a function of the union of all shard states Si as follows,

$$G = f\left(\bigcup_{i=1}^{k} Si\right) \dots (11)$$

Where, f is the function representing the global state derivation from individual shard states. This ensures that despite the partitioning, the blockchain maintains a coherent and unified states. Consensus within each shard is achieved through a modified Proof-of-Stake (PoS) mechanism, which is particularly suited for edge environments where computational resources are limited. In this PoS mechanism, nodes within each shard stake a certain amount of cryptocurrency to participate in the consensus process. The probability Pi of node i being selected as the validator is proportional to its stake Si is estimated via equation 12,

$$Pi = \frac{Si}{\sum_{j=1}^{|Ni|} Sj} \dots (12)$$

This ensures that nodes with higher stakes have a higher probability of being selected, thereby incentivizing honest behavior and reducing the risk of malicious activities. The selection process is further refined by incorporating a reputation score , which is a function of the node's historical performance and reliability. The adjusted probability Pi' for node i being selected as a validator is expressed via equation 13,

$$Pi' = \frac{Si \cdot Ri}{\sum_{j=1}^{|Ni|} Sj \cdot Rj} \dots (13)$$

This adjustment ensures that nodes with higher reputation scores are more likely to be selected, further enhancing the security and reliability of the consensus mechanism. The justification for choosing the EBBS model lies in its ability to effectively address the scalability and latency issues inherent in traditional blockchain systems. By partitioning the ledger and distributing the computational load across edge nodes, EBBS significantly improves transaction processing times and throughput. The cross-shard communication protocol ensures consistency across the network, maintaining the integrity and coherence of the blockchain. The modified PoS mechanism, tailored for edge environments, provides an efficient and secure consensus process that leverages the unique capabilities of edge nodes.

Next, IoV AI-Enabled Dynamic Network Slicing (ADNS) process is integrated, which is a cutting-edge approach designed to enhance the efficiency and QoS of IoV networks by dynamically adjusting network slice configurations based on real-time traffic patterns. This process employs reinforcement learning (RL) to predict traffic demands and optimize resource allocation, ensuring the efficient use of network resources while meeting the diverse QoS requirements of various IoV applications. The RL agent, central to this process, continuously learns from real-time feedback on network performance and iteratively refines its slicing strategy.

The ADNS process begins with the RL agent observing the state of the network, represented by St, which includes real-time traffic data, current slice configurations, and available resources at timestamp t sets. The agent then selects an action , which corresponds to a specific adjustment in the network slice configuration. The state St is expressed as a vector of observed parameters, represented via equation 14,

$$St = [Tt, Ct, Rt] \dots (14)$$

Where, Tt represents the traffic demands, Ct represents the current slice configurations, and Rt indicates the available network resources. The action At modifies the slice configuration to better align with the predicted traffic demands. The RL agent's objective is to maximize the cumulative reward R, which

reflects the QoS performance of the network over temporal instance sets. The reward function Rt at timestamp t is formulated via equation 15,

$$Rt = \sum_{i=1}^{n} (wi \cdot Qi(t)) - \lambda \cdot U(t) \ldots (15)$$

Where, (t) is the QoS satisfaction for slice i, wi is the weight assigned to slice i based on its priority, and $U(t)$ represents the total resource utilization. The term λ is a regularization parameter that balances the trade-off between QoS satisfaction and resource efficiency. To predict traffic patterns and make informed decisions, the RL agent employs a policy π, which maps states to actions. The policy π is updated based on the observed rewards using policy gradient methods. The policy gradient $\nabla(\theta)$ with respect to the policy parameters θ is given via equation 16,

$$\nabla J(\theta) = E\pi\theta[\nabla\theta \, log \, \pi\theta(\, At \mid St\,) \cdot Rt] \ldots (16)$$

This operation captures the expected gradient of the cumulative reward, guiding the adjustment of the policy parameters to improve network performance. The RL agent uses this gradient to update its policy iteratively, refining its ability to optimize slice configurations. The temporal dynamics of network traffic are modeled using a value function (St), which estimates the expected cumulative reward from state St under policy π sets. The Bellman Process for the value function is given via equation 17,

$$V\pi(St) = E\pi\big[Rt + \gamma V\pi\big(S(t+1)\big)\big] \ldots (17)$$

Where, γ is the discount factor that prioritizes immediate rewards over future rewards. This recursive equation enables the RL agent to estimate the long-term impact of its actions on network performance, facilitating more effective decision-making process. The optimal slice configuration $Ct*$ is determined by maximizing the value function over all possible actions, represented via equation 18,

$$Ct *= argmax^{At} V\pi(St, At) \ldots (18)$$

This optimization ensures that the selected action $AtAt$ yields the highest expected cumulative reward, aligning the slice configuration with current traffic demands and QoS requirements. The justification for adopting the ADNS model lies in its ability to adaptively manage network resources in response to dynamic traffic patterns and QoS requirements. Traditional static slicing approaches fail to accommodate the variability in IoV traffic, leading to suboptimal resource utilization and degraded QoS. By leveraging RL, the ADNS process continuously learns and adapts, ensuring efficient and responsive network management. This method complements other approaches by integrating real-time feedback and predictive modeling, providing a robust framework for dynamic network slicing in IoV environments.

Finally, the IoV Secure Multi-Party Computation for Collaborative Data Processing (SMPC-CDP) process is integrated, which is an advanced cryptographic framework designed to enable multiple parties to jointly compute functions over their data while preserving the privacy of individual inputs. This process ensures that sensitive data is never exposed, even during computation, by employing secure multi-party computation (SMPC) protocols. The model leverages homomorphic encryption and secret sharing techniques to securely process encrypted inputs, and the final results are decrypted only by authorized parties, maintaining privacy throughout the entire computation. In the SMPC-CDP process, each party Pi encrypts its data xi using a homomorphic encryption scheme. Let (xi) represent the encrypted data of party Pi sets. The homomorphic property allows computations to be performed directly on encrypted data samples. If E is an encryption function and $\oplus$ represents the homomorphic operation corresponding to addition, then for two plaintexts x and y via equation 19,

$$E(x) \oplus E(y) = E(x + y) \ldots (19)$$

This property is crucial for enabling secure computations on encrypted data without decrypting it in the process. The parties collaborate to compute a joint function f over their encrypted inputs & scenarios. To achieve this, the parties follow an SMPC protocol, where the function f is expressed as a series of operations that is performed homomorphically. The function f is represented via equation 20,

$$f(x1, x2, \dots, xn) = g\big(E(x1), E(x2), \dots, E(xn)\big) \dots (20)$$

Where, g is the function performed on encrypted data samples. Each operation within g respects the homomorphic properties, ensuring that the computations remain secure. The intermediate results of the computation are also encrypted, and the final encrypted result (R) is obtained. To ensure that only authorized parties can decrypt the final result, a decryption key k is shared among the parties using a secret sharing scheme. Let k be split into n shares ki such that any t out of n shares can reconstruct the key. This is represented by Shamir's Secret Sharing scheme via equation 21,

$$k = \sum_{i=1}^{t} \lambda i * ki \dots (21)$$

Where, λi are the Lagrange coefficients. The final decryption is performed collaboratively by combining the shares $kiki$ from the authorized parties. The security and correctness of the SMPC-CDP process is demonstrated through a series of operations that encapsulate the encryption, computation, and decryption steps. The first process represents the encryption of individual inputs via equation 22,

$$E(xi) = E(xi, pk) \dots (22)$$

Where, E is the encryption function, and pk is the public key used for encryption. The second operation describes the homomorphic addition of encrypted values via equation 23,

$$E(x1) \oplus E(x2) = E(x1 + x2) \dots (23)$$

This property is extended to the general computation g over multiple encrypted inputs for different scenarios. The third operation represents the secure computation of the function f via equation 24,

$$g\big(E(x1), E(x2), \dots, E(xn)\big) = E\big(f(x1, x2, \dots, xn)\big) \dots (24)$$

The fourth operation involves the reconstruction of the decryption key using secret shares via equation 25,

$$k = \sum_{i=1}^{t} \lambda i * ki \dots (25)$$

Finally, the fifth operation represents the decryption of the final result via equation 26,

$$R = D(E(R), k) \dots (26)$$

Where, D is the decryption function, and R is the decrypted result. The justification for adopting the SMPC-CDP model lies in its robust privacy-preserving capabilities, essential for secure collaborative data processing in IoV environments. Traditional methods often expose data during computation, posing significant privacy risks. The SMPC-CDP process mitigates these risks by ensuring that data remains encrypted throughout the computation, only revealing the final result to authorized parties. This method complements other security measures by providing a framework that guarantees data privacy without compromising computational accuracy or efficiency. The SMPC-CDP process effectively addresses the privacy concerns inherent in IoV networks, facilitating secure and collaborative data analysis. By leveraging homomorphic encryption and secret sharing, the model ensures that sensitive data is protected at all stages of computation. The detailed equations encapsulate the encryption, computation, and decryption steps, demonstrating the technical depth and rigor of the proposed method. This approach

represents a significant advancement in privacy-preserving data processing, providing a robust solution for the challenges associated with collaborative IoV data analysis. Next, we discuss efficiency of this model in terms of different performance metrics, and compare it with existing methods for different scenarios.

Comparative results analysis

The experimental setup for evaluating the proposed IoV framework, integrating AI-Driven Anomaly Detection and Mitigation (ADAM), Edge-Based Blockchain Sharding (EBBS), AI-Enabled Dynamic Network Slicing (ADNS), and Secure Multi-Party Computation for Collaborative Data Processing (SMPC-CDP), involves a comprehensive simulation environment designed to mimic real-world IoV scenarios. Conducted on a high-performance computing cluster with 64-core Intel Xeon processors, 512 GB of RAM, and 10 Gbps network interfaces, the IoV network topology consists of 50 edge nodes, 10 relay nodes, and 500 vehicles. Experiments are conducted over a 24-hour simulation period with data collected at one-second intervals. For ADAM, network traffic data includes routine V2V and V2I communications, and simulated cyber-attacks like DDoS and MITM, using parameters such as source IP 192.168.1.1, destination IP 192.168.1.2, source port 12345, destination port 80, protocol TCP, packet count 100, byte count 1500, and flow duration 2 seconds. CNN and RNN models, trained on a dataset of 1 million labeled packets (70% training, 15% validation, 15% testing), are evaluated for detection accuracy, false positive rate, and response delays. EBBS involves blockchain transactions for vehicle registrations, insurance verifications, and toll payments, with input parameters including transaction volume of 1000 tps, shard count of 10, and edge node capacity of 500 tps per node. The effectiveness of the cross-shard communication protocol is measured based on consistency maintenance and latency reduction, while the modified PoS mechanism's effectiveness is assessed by timestamp to consensus and computational overhead on edge nodes. ADNS utilizes real-time traffic data (vehicle count 300, average speed 60 km/h, data rate 5 Mbps) to adjust network slices based on QoS requirements (latency <50 ms, bandwidth 10 Mbps, reliability 99.9%, bandwidth capacity 1 Gbps, processing power 200 GHz). The RL agent's performance is evaluated on resource utilization, QoS satisfaction rate, and latency reduction, with policy updates based on real-time feedback. SMPC-CDP is tested with encrypted data from multiple IoV entities, using homomorphically encrypted sensor readings, secret sharing with 5 shares (threshold 3 for decryption), and computation tasks like aggregation of average speed and traffic density. The efficiency of SMPC-CDP protocols is evaluated by computation overhead, privacy breach rate, and data utility preservation, with timestamps for collaborative computations and result accuracy. Sample datasets include high-density urban, highway, and rural traffic data; blockchain transaction datasets for vehicle registrations, insurance verifications, and toll payments; and sensor data including vehicle speed, location, fuel level, traffic camera data, and infrastructure sensor data. This experimental setup rigorously evaluates the IoV framework's performance, demonstrating significant improvements over existing methods ([4], [9], [15]) in terms of detection accuracy, transaction processing time, resource utilization, and privacy preservation.

Table 1: Detection Accuracy and False Positive Rate for Anomaly Detection

Method	Detection Accuracy (%)	False Positive Rate (%)
Proposed	95	2
Method [4]	89	5

Method [9]	92	3.5
Method [15]	90	4

Table 1 shows the performance of the proposed ADAM model compared to three existing methods. The proposed model achieves a higher detection accuracy of 95% and a lower false positive rate of 2%, demonstrating its superior capability in identifying anomalies in network traffic with minimal false alarms.

Table 2: Transaction Processing timestamp and Throughput for Blockchain Sharding

Method	**Transaction Processing timestamp (ms)**	**Throughput (transactions/sec)**
Proposed	10	1000
Method [4]	25	600
Method [9]	15	800
Method [15]	20	700

Table 2 compares the transaction processing timestamp and throughput for the proposed EBBS model with existing methods. The proposed model significantly reduces the transaction processing timestamp to 10 ms and increases the throughput to 1000 transactions per second, highlighting its efficiency and scalability in handling blockchain transactions.

Table 3: Resource Utilization and QoS Satisfaction for Dynamic Network Slicing

Method	**Resource Utilization Efficiency (%)**	**QoS Satisfaction Rate (%)**
Proposed	85	98
Method [4]	70	85
Method [9]	75	90
Method [15]	80	95

Table 3 presents the results of resource utilization efficiency and QoS satisfaction rate for the ADNS model. The proposed model achieves a resource utilization efficiency of 85% and a QoS satisfaction rate of 98%, outperforming the existing methods in optimizing resource allocation and maintaining high service quality.

Table 4: Privacy Preservation and Computation Overhead for SMPC

Method	**Privacy Breach Rate (%)**	**Computation Overhead (%)**	**Data Utility Preservation (%)**
Proposed	0	20	95
Method [4]	1	35	90
Method [9]	0.5	25	92
Method [15]	0.2	30	93

Table 4 evaluates the privacy preservation, computation overhead, and data utility preservation of the SMPC-CDP model.

The proposed model ensures a privacy breach rate of 0%, a computation overhead of 20%, and data utility preservation of 95%, demonstrating its effectiveness in secure and privacy-preserving collaborative data processing.

Table 5: Average Response timestamp for Anomaly Detection and Mitigation

Method	Average Response timestamp (ms)
Proposed	50
Method [4]	120
Method [9]	80
Method [15]	100

Table 5 compares the average response timestamp for anomaly detection and mitigation among the proposed ADAM model and existing methods. The proposed model achieves the fastest response timestamp of 50 ms, enabling timely detection and mitigation of security threats in the IoV network.

Table 6: Latency Reduction and Cross-Shard Consistency for Blockchain Sharding

Method	Latency Reduction (%)	Cross-Shard Consistency (%)
Proposed	70	100
Method [4]	40	95
Method [9]	55	98
Method [15]	60	99

Table 6 assesses the latency reduction and cross-shard consistency of the EBBS model. The proposed model achieves a latency reduction of 70% and maintains 100% cross-shard consistency, highlighting its effectiveness in improving the performance and reliability of blockchain-based IoV networks. These tables collectively illustrate the superior performance of the proposed IoV framework across multiple dimensions, including anomaly detection accuracy, transaction processing efficiency, resource utilization, privacy preservation, response time, and latency reduction. The proposed methods significantly enhance the security, scalability, and efficiency of IoV networks, demonstrating their potential to address the critical challenges posed by the deployment of 5G technology.

Conclusion

This paper presents a comprehensive framework for enhancing the security, scalability, efficiency, and privacy of IoV networks through the integration of advanced AI-driven techniques and blockchain technology. The proposed framework comprises four key components: AI-Driven Anomaly Detection and Mitigation (ADAM), Edge-Based Blockchain Sharding (EBBS), AI-Enabled Dynamic Network Slicing (ADNS), and Secure Multi-Party Computation for Collaborative Data Processing (SMPC-CDP). The extensive experimental evaluation demonstrates the significant improvements achieved by the proposed methods over existing approaches. The ADAM model achieves a detection accuracy of 95% and a false positive rate of 2%, significantly outperforming existing methods, which achieve detection accuracies ranging from 89% to 92% and false positive rates from 3.5% to 5%. This high accuracy and low false positive rate ensure robust real-time threat detection, enhancing the overall security of IoV networks. Additionally, the average response timestamp for anomaly detection and mitigation is reduced to 50 ms, compared to 80-120 ms for existing methods, enabling timely responses to security threats.

The EBBS model addresses the scalability and latency issues inherent in traditional blockchain systems. The proposed sharding mechanism reduces transaction processing timestamp to 10 ms and increases throughput to 1000 transactions per second. In comparison, existing methods exhibit processing times ranging from 15 to 25 ms and throughput between 600 and 800 transactions per second. Furthermore, EBBS achieves a latency reduction of 70% and maintains 100% cross-shard consistency, demonstrating

its effectiveness in improving the performance and reliability of blockchain-based IoV networks. The ADNS model dynamically adjusts network slice configurations based on real-time traffic patterns and QoS requirements. The model achieves a resource utilization efficiency of 85% and a QoS satisfaction rate of 98%, significantly higher than the 70-80% efficiency and 85-95% satisfaction rates of existing methods. This ensures optimal resource allocation and high service quality across diverse IoV applications.

The SMPC-CDP model ensures secure and privacy-preserving data processing. It achieves a privacy breach rate of 0%, computation overhead of 20%, and data utility preservation of 95%, outperforming existing methods with privacy breach rates of 0.2-1%, computation overheads of 25-35%, and data utility preservation of 90-93%. These results demonstrate the model's capability to securely process sensitive data collaboratively without compromising privacy or computational efficiency. The proposed framework significantly advances the state-of-the-art in IoV networks, providing a robust and efficient solution for the challenges posed by 5G deployments. The integration of ADAM, EBBS, ADNS, and SMPC-CDP components ensures enhanced security, scalability, efficiency, and privacy, making the framework well-suited for next-generation IoV systems.

References

1. Karim, S. M., Habbal, A., Chaudhry, S. A., & Irshad, A. (2023). BSDCE-IoV: Blockchain-based secure data collection and exchange scheme for IoV in 5G environment. *IEEE Access, 11*, 36158–36175. https://doi.org/10.1109/ACCESS.2023.3265959
2. Xu, L., Ge, M., & Wu, W. (2022). Edge server deployment scheme of blockchain in IoVs. *IEEE Transactions on Reliability, 71*(1), 500–509. https://doi.org/10.1109/TR.2022.3142776
3. Zhao, Y., Wang, Y., Wang, P., & Yu, H. (2022). PBTM: A privacy-preserving announcement protocol with blockchain-based trust management for IoV. *IEEE Systems Journal, 16*(2), 3422–3432. https://doi.org/10.1109/JSYST.2021.3078797
4. Ghimire, B., Rawat, D. B., & Rahman, A. (2024). Efficient information dissemination in blockchain-enabled federated learning for IoV. *IEEE Internet of Things Journal, 11*(9), 15310–15319. https://doi.org/10.1109/JIOT.2023.3346296
5. Gao, Z., Zhang, D., Zhang, J., Liu, L., Niyato, D., & Leung, V. C. M. (2023). World state attack to blockchain-based IoV and efficient protection with hybrid RSUs architecture. *IEEE Transactions on Intelligent Transportation Systems, 24*(9), 9952–9965. https://doi.org/10.1109/TITS.2023.3268222
6. Liu, J., et al. (2023). CPAHP: Conditional privacy-preserving authentication scheme with hierarchical pseudonym for 5G-enabled IoV. *IEEE Transactions on Vehicular Technology, 72*(7), 8929–8940. https://doi.org/10.1109/TVT.2023.3246466
7. Roy, S., Nandi, S., Maheshwari, R., Shetty, S., Das, A. K., & Lorenz, P. (2024). Blockchain-based efficient access control with handover policy in IoV-enabled intelligent transportation system. *IEEE Transactions on Vehicular Technology, 73*(3), 3009–3024. https://doi.org/10.1109/TVT.2023.3322637
8. Du, G., et al. (2024). A blockchain-based trust-value management approach for secure information sharing in Internet of Vehicles. *IEEE Internet of Things Journal, 11*(1), 333–344. https://doi.org/10.1109/JIOT.2023.3277691

9. Li, D., et al. (2023). Intelligent and fair IoV charging service based on blockchain with cross-area consensus. *IEEE Transactions on Intelligent Transportation Systems, 24*(12), 15984–15994. https://doi.org/10.1109/TITS.2023.3249180
10. Tong, W., et al. (2023). TI-BIoV: Traffic information interaction for blockchain-based IoV with trust and incentive. *IEEE Internet of Things Journal, 10*(24), 21528–21543. https://doi.org/10.1109/JIOT.2023.3300840
11. Vishwakarma, L., Nahar, A., & Das, D. (2022). LBSV: Lightweight blockchain security protocol for secure storage and communication in SDN-enabled IoV. *IEEE Transactions on Vehicular Technology*, *71*(6), 5983–5994. https://doi.org/10.1109/TVT.2022.3163960
12. Tu, S., Yu, H., Badshah, A., Waqas, M., Halim, Z., & Ahmad, I. (2023). Secure Internet of Vehicles (IoV) with decentralized consensus blockchain mechanism. *IEEE Transactions on Vehicular Technology*, *72*(9), 11227–11236. https://doi.org/10.1109/TVT.2023.3268135
13. Yuan, M., et al. (2023). TRUCON: Blockchain-based trusted data sharing with congestion control in Internet of Vehicles. *IEEE Transactions on Intelligent Transportation Systems, 24*(3), 3489–3500. https://doi.org/10.1109/TITS.2022.3226500
14. Srivastava, V., Debnath, S. K., Bera, B., Das, A. K., Park, Y., & Lorenz, P. (2022). Blockchain-envisioned provably secure multivariate identity-based multi-signature scheme for Internet of Vehicles environment. *IEEE Transactions on Vehicular Technology, 71*(9), 9853–9867. https://doi.org/10.1109/TVT.2022.3176755
15. Xu, Y., Yu, E., Song, Y., Tong, F., Xiang, Q., & He, L. (2023). $\mathcal {R}$-Tracing: Consortium blockchain-based vehicle reputation management for resistance to malicious attacks and selfish behaviors. *IEEE Transactions on Vehicular Technology*, *72*(6), 7095–7110.