Blockchain-Enhanced Machine Learning for Dynamic Routing and Secure Communications in Autonomous Vehicle Networks

Usama Arshad[1,2], Abdallah Tubaishat[3], Abrar Ullah[4], Zahid Halim[2], Sajid Anwar[5]

[1]CRADLE Lab, FAST School of Management, National University of Computer and Emerging Sciences, Islamabad, Pakistan
[2]Department of Information Management, National Yunlin University of Science and Technology, Douliou, Yunlin 64002, Taiwan
[3]College of Technological Innovation, Zayed University, UAE
[4]School of Mathematical & Computer Sciences, Heriot-Watt University, Dubai, UAE
[5]Center of Excellence in Information Technology, Institute of Management Sciences, Peshawar, Pakistan
usama.arshad@isb.nu.edu.pk, Abdallah.Tubaishat@zu.ac.ae, a.ullah@hw.ac.uk, zahidh@yuntech.edu.tw, sajid.anwar@imsciences.edu.pk

Abstract

The advent of autonomous vehicles (AVs) marks a significant milestone in urban transportation, promising to enhance safety, reduce congestion, and improve environmental sustainability. However, deploying AVs on a mass scale comes with critical challenges related to secure and efficient vehicular communication. This research proposes a novel framework that combines the security features of blockchain technology with the adaptive capabilities of machine learning (ML) to address these major challenges. Integrating a blockchain-based protocol ensures tamper-proof and transparent communication within AV networks, protecting against a wide array of cyber threats. Concurrently, ML algorithms are employed to optimize real-time routing decisions based on comprehensive traffic data and environmental conditions. Through simulation in realistic urban scenarios, our framework demonstrates a significant improvement in communication security and routing efficiency, indicating a promising avenue for achieving scalable and reliable AV networks. Operational cost assessments further reveal the economic viability of the proposed model, underscoring its potential to deliver long-term savings through enhanced efficiency and reduced human intervention. Thus an efficient solution in terms of security, dynamic routing, and scalability with respect to traditional models.

Introduction

The rise of autonomous vehicles (AVs) is reshaping the landscape of urban transportation, presenting a future where the way we commute is fundamentally transformed (Zhao et al. 2023). Due to its ability to go from one location to another without requiring human assistance, research suggests that autonomous cars present a new mobility paradigm (Rahman and Thill 2023). The concept of a transportation mode identifies and addresses a number of the main issues that arise in urban transportation systems, such as traffic jams and accidents caused by human error as well as the environmental impact of emissions (Orieno et al. 2024). Due to their advanced sensors and intricate algorithms, autonomous cars are able to make judgments quickly, adapt to changes in their environment, and thrive in urban areas. Autonomous cars are expected to lessen traffic bottlenecks when they are deployed in cities because they will be able to interact with one another to improve traffic management (Alhaj et al. 2023). This potential for synchronized movement can lead to smoother rides and less time spent on the road. Furthermore, by removing the possibility of human error, which is responsible for a significant portion of road accidents, AVs could drastically improve road safety (Sohail et al. 2023). Environmental sustainability is another critical area where AVs could make a significant impact. With the potential to be powered by clean energy sources and optimized for fuel efficiency through intelligent routing, AVs could contribute to a reduction in carbon emissions and urban air pollution (Duman et al. 2023). This follows global actions striving to fight climate change and encourage a healthier lifestyle among citizens of large cities. Nevertheless, the use of AVs in urban transportation creates a series of adverse issues. This includes the necessity to utilize unique communication systems and ensure the timely transfer of data (Laghari et al. 2023). It is essential for a proper operational pattern of AVs, as they are programmed to collect and process information on their surroundings at all times. Moreover, the security of these communication systems is crucial. As AVs depend heavily on the exchange of data, they are potentially vulnerable to cyber threats that could compromise the safety and privacy of passengers (Yoshizawa et al. 2023). Unauthorized access or manipulation of vehicular data could lead to severe consequences, highlighting the need for robust security measures (Wu et al. 2023). The dynamic nature of urban environments poses a constant challenge, requiring real-time data sharing for navigation and safety. Traditional systems struggle to keep up, leading to inefficiencies and potential safety risks (Novak and Ivanov 2023). As vehicles increasingly rely on digital communication, they become prime targets for cyber-attacks. Data manipulation and unauthorized access can severely compromise the safety and privacy of passengers, making robust security protocols nonnegotiable (Anwar et al. 2023). Moreover, ensuring reliable connectivity in dense urban areas, where signal interference and physical obstructions are common, remains a daunting task. This can disrupt the flow of critical data between vehi-

cles and infrastructure, affecting decision-making processes and overall traffic management (Tian et al. 2023). Lastly, the integration of AVs into existing road networks requires vehicular communication systems to adapt to a mix of human-driven and autonomous vehicles. Achieving seamless communication in such mixed traffic conditions is essential for safety and efficiency but remains a complex issue to address.

Gaps in Current Research

While previous works have laid a solid foundation in the fields of vehicular communication systems, blockchain technology in AV networks, and ML applications for dynamic routing, several gaps remain unaddressed:

- Research on blockchain and ML integration for enhancing both security and routing in AV networks is sparse, with most studies not exploring the synergistic benefits of combining these technologies.
- Scalability and the need for computational efficiency in blockchain and ML applications within AV networks are often underexplored, hindering real-time performance in urban settings.
- Comprehensive security models leveraging blockchain for AV network data exchanges, covering privacy, integrity, and cyber threat resistance, remain undeveloped.
- Existing studies fall short in addressing AV integration challenges within mixed-traffic urban environments, critical for achieving seamless communication and AV adoption.

In response to these challenges, our study introduces a novel approach that combines the strengths of blockchain technology with machine learning (ML). Blockchain offers a secure and transparent platform for vehicular communication, ensuring the integrity and confidentiality of data exchanged within AV networks. Its decentralized nature makes it resistant to tampering and unauthorized access, providing a solid foundation for secure communications. Simultaneously, ML algorithms are employed to enhance the dynamic routing capabilities of AVs. By analyzing vast amounts of traffic data and environmental conditions in real time, ML enables AVs to make optimized routing decisions, further improving traffic flow and reducing travel times.

Main contributions and novelty

- We introduced a framework integrating blockchain with ML for secure, efficient AV network routing, enabling tamper-proof communications and real-time, data-informed decisions.
- Blockchain ensures our framework's security and transparency, safeguarding against cyber threats and unauthorized data access, crucial for AV technology acceptance.
- ML algorithms in our framework adaptively optimize routing based on live traffic and environmental data, significantly enhancing traffic flow and reducing travel times.
- Addressing scalability, our approach proves viable for large-scale urban deployment, maintaining real-time performance through optimized blockchain protocols and algorithms.
- Designed for mixed traffic conditions, our framework supports both autonomous and human-driven vehicles, promoting smoother integration into evolving urban mobility landscapes.

Proposed Model

Framework Overview

The dawn of autonomous vehicle (AV) technology introduces transformative potential for urban mobility, aiming to significantly enhance road safety, traffic efficiency, and environmental sustainability. However, the realization of this potential is dependent upon overcoming substantial challenges in vehicular communication and routing. Current systems face threats from cybersecurity risks and dynamic traffic conditions, which compromise the safety and efficiency of AV operations. To address these challenges, our research proposes an innovative framework that integrates blockchain technology with machine learning (ML) algorithms within AV networks. The essence of this integration lies in harnessing blockchain's unparalleled security features for vehicular communication and leveraging ML's capability to adapt and optimize routing decisions in real time.

Theoretical Foundation The proposed framework operates on two fundamental premises:

- Blockchain Technology for Secure Communication: Utilizing a decentralized ledger system, blockchain technology ensures the integrity and privacy of data exchanges in AV networks. Let $\mathcal{B}$ denote the blockchain system, where each transaction and data exchange is recorded as a block $b_i \in \mathcal{B}$. These blocks are linked using cryptographic principles, ensuring a secure and tamper-proof chain.

$$b_i = \text{encrypt}(data_i, key_{i-1}) \tag{1}$$

  where $data_i$ is the information transmitted in block i, and key_{i-1} is the cryptographic link to the previous block.

- Machine Learning for Dynamic Routing: The framework employs ML algorithms to analyze traffic data $\mathcal{D}$, predicting patterns and optimizing routes for AVs in real time. The function $f : \mathcal{D} \rightarrow \mathcal{R}$ represents the ML model that maps input data to optimal routing decisions, where $\mathcal{R}$ is the set of possible routes.

$$\mathcal{R}_{opt} = \arg\min_{r \in \mathcal{R}} \text{Cost}(r, \mathcal{D}) \tag{2}$$

  $\text{Cost}(r, \mathcal{D})$ evaluates the efficiency of route r based on current traffic data $\mathcal{D}$, selecting the route with minimal associated cost.

The goal of this framework is to enhance the secure communication and dynamic, efficient routing capabilities of AV networks, addressing critical challenges and setting the stage for a new era of urban mobility. Through this integrated approach, we aim to achieve a seamless, secure, and efficient transportation system, paving the way for the widespread adoption of AV technology in urban environments.

Table 1: Comparison - Proposed Model vs Previous Models

Ref.	Data Processing	Verification	Pattern Analysis	Security	Decentralized Tech	Dynamic Routing	Decision Making	Adaptive Network
(Han et al. 2023)	✓	✓	X	✓	X	X	X	X
(Anbalagan et al. 2023)	✓	✓	X	✓	X	X	X	X
(Yao et al. 2023)	✓	✓	✓	✓	X	X	✓	✓
(Feng et al. 2023)	✓	✓	X	✓	✓	X	X	X
(Ali et al. 2023)	✓	X	✓	X	X	✓	✓	✓
Proposed Model	✓	✓	✓	✓	✓	✓	✓	✓

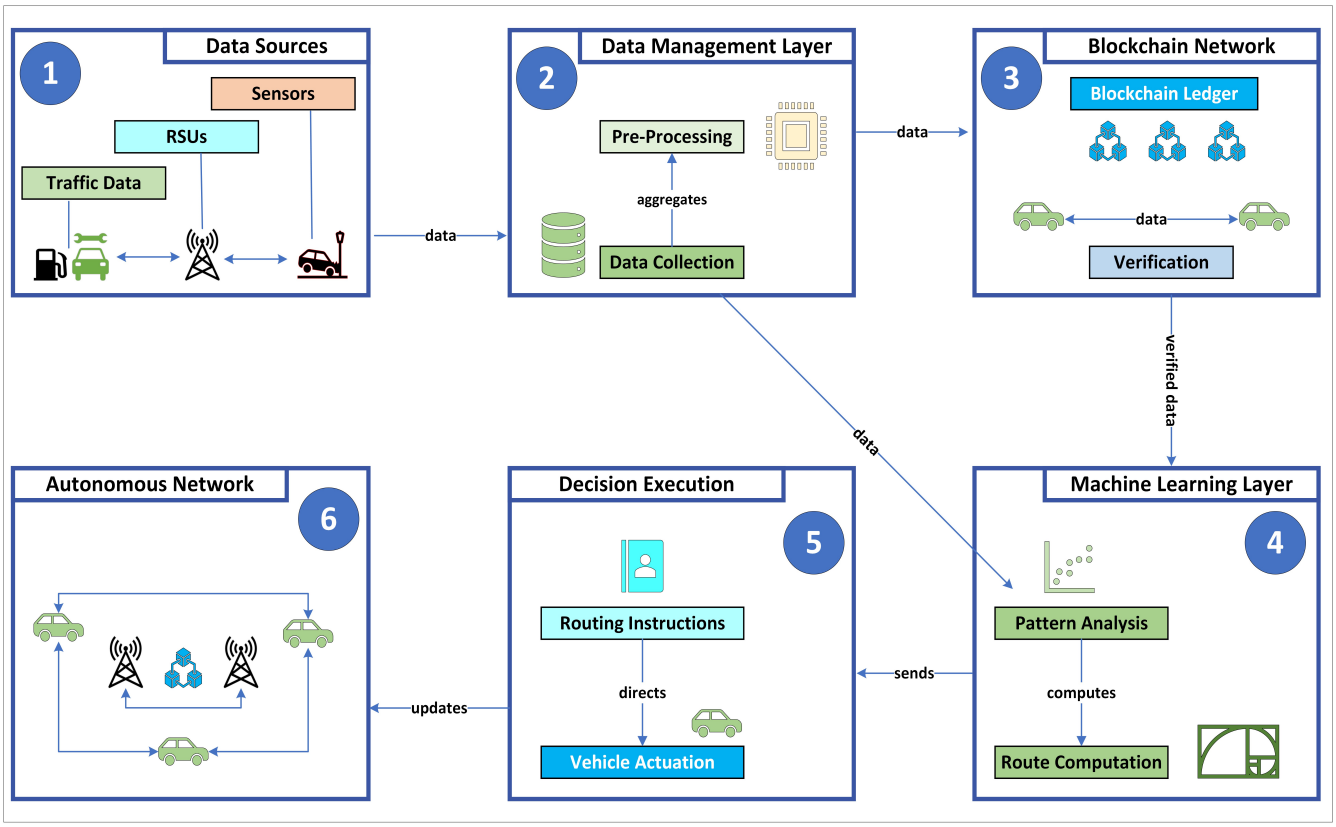

Figure 1: Proposed Architecture.

Decentralization and Data Integrity

The decentralized nature of blockchain eliminates the need for a central authority, thereby reducing vulnerabilities to single points of failure and potential security breaches. In a blockchain network, each participant, or node, holds a copy of the ledger, contributing to the system's resilience against tampering and cyber-attacks. Data integrity is maintained through cryptographic hash functions, which ensure that each block is securely linked to its predecessor. This linkage creates an immutable chain of blocks, where altering the information in any single block would require changing all subsequent blocks, a feat practically impossible to achieve without detection. The mathematical representation of this concept is as follows:

$$H(b_i) = \text{hash}(H(b_{i-1}) + data_i + nonce_i) \tag{3}$$

where $H(b_i)$ is the hash of block i, $H(b_{i-1})$ is the hash of the previous block, $data_i$ represents the information stored in block i, and $nonce_i$ is a nonce value that, when hashed with the previous block's hash and the block's data, meets the network's difficulty target.

Transparency and Security

The transparency feature of blockchain allows all participants of the network to verify and audit transactions independently. This promotes trust between the entities in the AV ecosystem. In addition, blockchain's transparency and the security provided by its nature build strong protection against various cyber threats, including data manipulations and unauthorized access. Another security-enhancing mechanism is the use of consensus algorithms to verify transactions and reach an agreement of all nodes on the state of the ledger. Such popular consensus mechanisms as Proof of Stake provide security for the blockchain network and allow everybody to have a vote in approving transactions, which makes the entire system more secure and resistant to attacks.

$$\text{Valid}(b_i) = \begin{cases} 1, & \text{if } H(b_i) < \text{target} \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

where $\text{Valid}(b_i)$ determines the validity of block i based on whether its hash is below a certain target.

Dynamic Routing

Machine learning (ML) algorithms have emerged as an important technology in the development of dynamic routing systems for autonomous vehicle (AV) networks. By leveraging real-time traffic data and environmental conditions, ML algorithms facilitate the optimization of routing decisions, thereby enhancing travel efficiency and mitigating congestion. The core of ML-driven dynamic routing lies in its ability to process and analyze vast amounts of data from various sources, including traffic sensors, GPS devices, and environmental monitoring systems. This data encompasses a wide range of parameters such as vehicle speed, traffic volume, road conditions, and weather patterns. The function $\mathcal{F}$, representing an ML model, processes this data to predict traffic conditions and determine optimal routes as follows:

$$\mathcal{R}_{opt} = \mathcal{F}(x; \theta) \tag{5}$$

where x represents the input data (e.g., current traffic and environmental conditions), θ denotes the parameters of the ML model, and $\mathcal{R}_{opt}$ is the output representing the optimal route.

Optimization and Adaptation of Routing Decisions The objective of ML algorithms in this context is to minimize travel time and avoid congestion by dynamically adjusting routing decisions based on predicted traffic patterns. This is achieved through the optimization of a cost function $\mathcal{C}$, which evaluates the efficiency of a given route based on several criteria, including travel distance, expected traffic delays, and environmental factors:

$$\min_{\mathcal{R}} \mathcal{C}(\mathcal{R}; x, \theta) = \text{Travel Time}(\mathcal{R}) + \lambda \cdot \text{Congestion}(\mathcal{R}; x) \tag{6}$$

where $\mathcal{R}$ represents a set of possible routes, $\text{Travel Time}(\mathcal{R})$ calculates the estimated travel time for route $\mathcal{R}$, $\text{Congestion}(\mathcal{R}; x)$ assesses the expected level of congestion based on current data x, and λ is a weighting factor that balances the importance of minimizing travel time against avoiding congested routes. To enhance the accuracy of traffic predictions and routing optimizations, ML models employ adaptive learning techniques that continuously update the model parameters θ based on new data. This iterative process ensures that the routing system remains responsive to changing traffic conditions and environmental factors, thereby improving the reliability and efficiency of AV navigation over time.

$$\theta_{new} = \theta_{old} - \alpha \nabla_\theta \mathcal{C}(\mathcal{R}; x, \theta) \tag{7}$$

where α is the learning rate, and $\nabla_\theta \mathcal{C}$ represents the gradient of the cost function with respect to the model parameters, guiding the update process to minimize routing inefficiencies.

System Architecture and Data Flow

The system architecture comprises three main components: the blockchain network, the machine learning module, and the data management layer. These components interact to form an integrated system that addresses the challenges of security and routing efficiency in AV networks.

- Blockchain Network: Serves as the backbone for secure data exchange among AVs and infrastructure, storing transactions and data exchanges in an immutable ledger.
- Machine Learning Module: Analyzes real-time traffic data and environmental conditions to optimize routing decisions, continuously learning and adapting to changing patterns.
- Data Management Layer: Facilitates the collection, storage, and distribution of data between the blockchain network and the ML module, ensuring data integrity and availability.

Data flow within the integrated system follows a structured path, ensuring that information is effectively captured, processed, and utilized:

1. Data Collection: Traffic data, environmental conditions, and vehicular communications are collected through sensors and IoT devices, and then transmitted to the data management layer.
2. Data Storage and Sharing: Collected data is stored in the data management layer, where it is pre-processed and made available for both the blockchain network and the ML module. Blockchain technology ensures that shared data remains secure and tamper-proof.
3. Data Processing and Analysis: The ML module accesses real-time data to perform analysis and generate routing decisions. This process involves data-driven algorithms that predict traffic patterns and identify optimal routes.
4. Decision Implementation: Routing decisions are communicated back to AVs and relevant infrastructure through the blockchain network, ensuring that the information is securely and efficiently distributed.

The interaction between the blockchain network and the ML module is mediated by the data management layer, which ensures that data integrity and security are maintained throughout the process. This layered architecture allows for:

$$\text{SecureDataExchange}(D_b) = \text{encrypt}(D_m, K_b) \quad (8)$$

where D_b represents data for the blockchain, D_m denotes data from the ML module, and K_b is the encryption key, ensuring secure data exchange between components.

$$\text{RoutingDecision}(R_{opt}, D_m) = \mathcal{F}(D_m; \theta) \quad (9)$$

where R_{opt} is the optimal routing decision, D_m is the input data from sensors, and θ represents the parameters of the ML model.

Implementation details

The Algorithm 1 describes the brief implementation details. The simulations and results were produced using Python on a device with a Core-I7 12 Generation processor and 16 GB RAM. Remix IDE is used for testing different scenarios. The decision tree is used as an ML model for predictions and dynamic routing on the dataset (Žunić 2019) for testing scenarios. However, simulation data was used for the results.

Algorithm 1: Algorithm for Secure and Efficient AV Network Communication

$\mathcal{V} \leftarrow$ Set of vehicles, $\mathcal{S} \leftarrow$ Set of sensors, $\mathcal{R} \leftarrow$ Set of routes Optimized route assignments $\mathcal{R}_{opt}$ for vehicles $\mathcal{B} \leftarrow$ Initialize blockchain network $\mathcal{M} \leftarrow$ Initialize ML model for traffic prediction $\mathcal{L} \leftarrow$ Initialize ledger $v \in \mathcal{V}$ $d_v \leftarrow$ Collect data from vehicle v Store d_v in $\mathcal{L}$ using $\mathcal{B}$ $\mathcal{D} \leftarrow \bigcup_{s \in \mathcal{S}} d_s$ $d \in \mathcal{D}$ $\mathcal{B}$.validate(d) $\mathcal{P} \leftarrow \mathcal{M}$.predict$(\mathcal{D})$ $v \in \mathcal{V}$ $\mathcal{R}_{opt} \leftarrow$ Optimize$(\mathcal{P}, v, \mathcal{R})$ Assign route $\mathcal{R}_{opt}$ to vehicle v $\mathcal{F} \leftarrow$ Collect feedback from all $v \in \mathcal{V}$ $\mathcal{M}$.update$(\mathcal{F})$
return $\mathcal{R}_{opt}$

Simulations and Results

The results of our simulations and analyses reveal significant improvements across several key metrics for the proposed model, which integrates blockchain technology and machine learning (ML) for enhanced communication security and dynamic routing in autonomous vehicle networks.

Communication Security

Fig. 2 demonstrated that the proposed model significantly enhances communication security, with the number of successful secure transactions steadily increasing to a near-perfect success rate of 99.8%. This is in contrast to the existing model, which plateaued at a success rate of 96% in specific scenarios. Additionally, the proposed model proved highly effective in detecting and thwarting unauthorized access attempts, showcasing its superior security capabilities against potential cyber-attacks and data breaches.

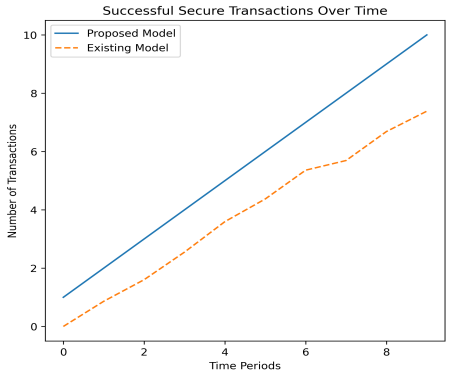

Figure 2: Communication Security.

Dynamic Routing Efficiency

The efficiency of the proposed model in computing optimal routes under various traffic conditions was markedly superior as shown in Fig. 3. It consistently required less time to compute routes across all levels of traffic, particularly excelling in heavy traffic scenarios. Moreover, the implementation of the proposed model resulted in a noticeable reduction

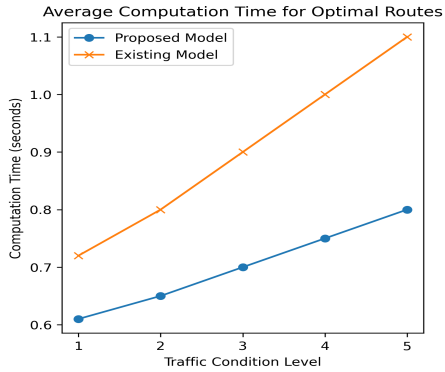

Figure 3: Dynamic Routing Efficiency.

in average travel times, up to 20%, underscoring the model's effectiveness in improving traffic flow and minimizing congestion.

Scalability

Simulations on scalability represented by Fig. 4 demonstrated the proposed model's robust performance in accommodating increased loads, scaling effectively with the rising number of vehicles and transactions. System throughput

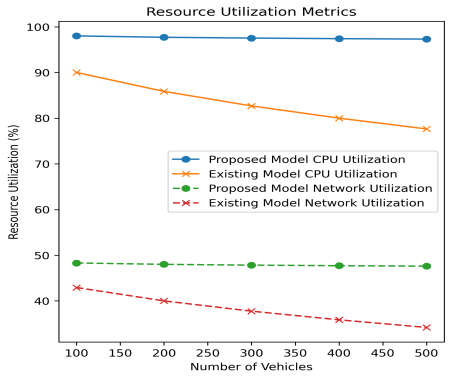

Figure 4: Scalability.

for the proposed model significantly outpaced that of the existing model, particularly under higher load conditions. Furthermore, resource utilization metrics indicated more efficient use of computational and network resources by the proposed model as the system scaled, affirming its scalability and efficiency.

Operational Cost

Comparisons of operational costs in Fig. 5 revealed the proposed model's ability to lower expenses over time, which in turn enhanced infrastructure efficiency, maintenance savings, and reduced energy consumption. A cost-benefit analysis further highlighted the long-term financial advantages of the proposed model, showing net savings that far exceeded those of the existing model, primarily due to improved efficiency and reduced necessity for human intervention.

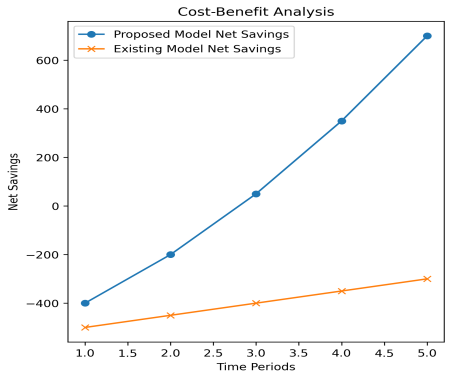

Figure 5: Operational Cost.

Conclusion

The integration of blockchain and machine learning (ML) technologies into autonomous vehicle (AV) networks represents a significant technological advancement in enhancing communication security, dynamic routing efficiency, and scalability. Our study's simulations have clearly demonstrated the proposed model's superior performance across these critical areas when compared to existing models. The model establishes a new benchmark in communication security with a near-perfect success rate in secure transactions and a marked improvement in handling unauthorized access attempts. Additionally, the efficiency gains in dynamic routing, evidenced by reduced computation times and travel durations, highlight the model's capability to optimize traffic flow and minimize congestion, even under varying traffic conditions. The scalability analysis further underscores the model's robustness in handling increased loads, showcasing its potential to accommodate the growing demands of smart transportation systems without compromising performance. Moreover, the operational cost assessment reveals the model's economic viability, with significant long-term savings achieved through enhanced efficiency and reduced human intervention. In conclusion, this study affirms the integration of blockchain and ML as a promising approach for advancing AV networks. By addressing the current limitations of vehicular communication systems, the proposed model not only enhances the security and efficiency of AV networks but also paves the way for future research and development. It invites a broader exploration into smart transportation solutions, with the potential to revolutionize urban mobility in the coming years.

Acknowledgments

References

Alhaj, A.; Zanoon, N.; Alrabea, A.; Alnatsheh, H.; Jawabreh, O.; Abu-Faraj, M.; and Ali, B. 2023. Improving the Smart Cities Traffic Management Systems using VANETs and IoT Features. *Journal of Statistics Applications & Probability*, 12(2): 405–414.

Ali, M. H.; Jaber, M. M.; Alfred Daniel, J.; Vignesh, C. C.; Meenakshisundaram, I.; Kumar, B. S.; and Punitha, P. 2023. Autonomous vehicles decision-making enhancement using self-determination theory and mixed-precision neural networks. *Multimedia Tools and Applications*, 1–24.

Anbalagan, S.; Raja, G.; Gurumoorthy, S.; Suresh, R. D.; and Dev, K. 2023. IIDS: Intelligent Intrusion Detection System for Sustainable Development in Autonomous Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 24(12): 15866–15875.

Anwar, A.; Anwar, A.; Moukahal, L.; and Zulkernine, M. 2023. Security assessment of in-vehicle communication protocols. *Vehicular Communications*, 44: 100639.

Duman, Z.; Mao, X.; Cai, B.; Zhang, Q.; Chen, Y.; Gao, Y.; and Guo, Z. 2023. Exploring the spatiotemporal pattern evolution of carbon emissions and air pollution in Chinese cities. *Journal of Environmental Management*, 345: 118870.

Feng, C.; Xu, Z.; Zhu, X.; Klaine, P. V.; and Zhang, L. 2023. Wireless Distributed Consensus in Vehicle to Vehicle Networks for Autonomous Driving. *IEEE Transactions on Vehicular Technology*, 72(6): 8061–8073.

Han, J.; Ju, Z.; Chen, X.; Yang, M.; Zhang, H.; and Huai, R. 2023. Secure Operations of Connected and Autonomous Vehicles. *IEEE Transactions on Intelligent Vehicles*, 8(11): 4484–4497.

Laghari, A. A.; Jumani, A. K.; Laghari, R. A.; and Nawaz, H. 2023. Unmanned aerial vehicles: A review. *Cognitive Robotics*, 3: 8–22.

Novak, A.; and Ivanov, A. 2023. Network security vulnerabilities in smart vehicle-to-grid systems identifying threats and proposing robust countermeasures. *Journal of Artificial Intelligence and Machine Learning in Management*, 7(1): 48–80.

Orieno, O. H.; Ndubuisi, N. L.; Ilojianya, V. I.; Biu, P. W.; and Odonkor, B. 2024. The future of autonomous vehicles in the US urban landscape: a review: analyzing implications for traffic, urban planning, and the environment. *Engineering Science & Technology Journal*, 5(1): 43–64.

Rahman, M. M.; and Thill, J.-C. 2023. Impacts of connected and autonomous vehicles on urban transportation and environment: A comprehensive review. *Sustainable Cities and Society*, 104649.

Sohail, A.; Cheema, M. A.; Ali, M. E.; Toosi, A. N.; and Rakha, H. A. 2023. Data-driven approaches for road safety: A comprehensive systematic literature review. *Safety science*, 158: 105949.

Tian, G.; Lu, W.; Zhang, X.; Zhan, M.; Dulebenets, M. A.; Aleksandrov, A.; Fathollahi-Fard, A. M.; and Ivanov, M. 2023. A survey of multi-criteria decision-making techniques for green logistics and low-carbon transportation systems. *Environmental Science and Pollution Research*, 30(20): 57279–57301.

Wu, J.; Zhang, M.; Xu, T.; Gu, D.; Xie, D.; Zhang, T.; Hu, H.; and Zhou, T. 2023. A review of key technologies in relation to large-scale clusters of electric vehicles supporting a new power system. *Renewable and Sustainable Energy Reviews*, 182: 113351.

Yao, Y.; Zhao, J.; Li, Z.; Cheng, X.; and Wu, L. 2023. Jamming and eavesdropping defense scheme based on deep reinforcement learning in autonomous vehicle networks. *IEEE Transactions on Information Forensics and Security*, 18: 1211–1224.

Yoshizawa, T.; Singelée, D.; Muehlberg, J. T.; Delbruel, S.; Taherkordi, A.; Hughes, D.; and Preneel, B. 2023. A survey of security and privacy issues in v2x communication systems. *ACM Computing Surveys*, 55(9): 1–36.

Zhao, X.; Fang, Y.; Min, H.; Wu, X.; Wang, W.; and Teixeira, R. 2023. Potential sources of sensor data anomalies for autonomous vehicles: An overview from road vehicle safety perspective. *Expert Systems with Applications*, 121358.

Žunić, E. 2019. Real-world VRP benchmark data with realistic constraints - input data and results - v2.