

Secure Vehicle Communication and Data Integrity Using Blockchain and Machine Learning

Project ID: 24-25J-206

Project Proposal Report

Dissanayake D.J.R

B.Sc. (Hons) Degree in Information Technology Specializing in Data
Science

Department of Computer Science
Sri Lanka Institute of Information Technology Sri Lanka

August 2024

Secure Vehicle Communication and Data Integrity Using Blockchain and Machine Learning

Project ID: 24-25J-206

Project Proposal Report

Dissanayake D.J.R – IT21313370

Supervised by Mr. Samadhi Rathnayake

Co-supervised by Mr. Nelum Rathnayake

B.Sc. (Hons) Degree in Information Technology Specializing in Data
Science

Department of Computer Science

Sri Lanka Institute of Information Technology Sri Lanka

August 2024

DECLARATION


I declare that this is my own work, and this proposal does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.



Signature

Dissanayake D.J.R – IT21313370

Date: 8/23/2024



Signature of the Supervisor

(Mr. Samadhi Rathnayake)

Date: 8/23/2024

Signature of the Co-Supervisor

(Mr. Nelum Amarasena)

Date: 8/23/2024

ACKNOWLEDGEMENT

Those who contributed to the effective completion of this research proposal should be respectfully recognized. Mr. Samadhi Rathnayake and Mr. Nelum Amarasinghe, the project's supervisors, deserve special thanks for their tremendous assistance, support, and encouragement throughout the project. Dr. Junius Anjana, an expert in Blockchain, is to be acknowledged for his contribution and support in the research.

Participants in the research project should be recognized and appreciated for their time and willingness to participate. Their important contributions are vital to the study's success. The Faculty of Computing staff should be recognized and thanked for their guidance and encouragement throughout the academic journey.

The teammates' efforts should be recognized, since their teamwork and brainstorming sessions have extended their understanding of the issue. Lastly, the family, friends, and coworkers of the individual who undertook the research are to be recognized for their support and understanding during the period of the project.

ABSTRACT

The past decade has seen rapid advancements in autonomous vehicle technology, driven by innovations in sensors, communication systems, computational hardware, and AI. A critical component of this progress is Vehicle-to-Everything (V2X) communication, which allows vehicles to interact with each other and their surroundings. This technology is essential for enhancing road safety and transportation efficiency, making it a key focus in autonomous vehicle research.

Despite the sophistication of modern Intelligent Vehicles (IVs), the Controller Area Network (CAN) bus system, which manages communication between electronic control units (ECUs), remains vulnerable due to its lack of security mechanisms for authentication and authorization. This weakness exposes vehicles to potential attacks, such as Denial of Service (DoS), Fuzzing, and Spoofing, where malicious actors can manipulate CAN messages, compromising the vehicle's safety.

The significance of secure communication in vehicles is further emphasized by the high incidence of road accidents caused by sudden braking, loss of control, and other factors. To mitigate these risks, Vehicle-to-Vehicle (V2V) safety applications have been developed, offering solutions like emergency brake warnings, failure alerts, and collaborative driving aids. These applications rely on V2X services, including Dedicated Short-Range Communications (DSRC) and cellular networks, which, despite their benefits, face significant security challenges in protecting user privacy and ensuring reliable communication.

As autonomous and connected vehicles become more integrated into transportation systems, the potential for cyberattacks increases, posing serious safety concerns. Addressing these challenges requires ongoing research to develop secure, resilient communication frameworks that can protect the integrity of these vehicles, ensuring a safer and more reliable future for autonomous mobility.

Keywords: V2X, CAN Bus, Blockchain, Autonomous, Dedicated Short Range Communication, ECU, DoS, IVs

TABLE OF CONTENTS

CONTENTS

DECLARATION	3
ACKNOWLEDGEMENT	4
ABSTRACT	5
TABLE OF CONTENTS	6
LIST OF TABLES	8
LIST OF FIGURES	9
LIST OF ABBREVIATIONS	10
INTRODUCTION	11
BACKGROUND & LITERATURE SURVEY	12
RESEARCH GAP.....	14
RESEARCH PROBLEM.....	17
RESEARCH OBJECTIVES	18
Main Objectives	18
Specific Objectives	19
METHODOLOGY	21
METHODOLOGY INCLUDING THE SYSTEM DIAGRAM.....	21
SYSTEM ARCHITECTURE	27
SYSTEM DIAGRAM	29
COMPONENT DIAGRAM.....	30
COMMERCIALIZATION OF THE PRODUCT	31
1. Research Overview	31
2. Target Market and Audience	31
3. Key Features and Benefits.....	31
4. Business Model and Revenue Streams	32
5. Go-to-Market Strategy	32
6. Marketing and Sales	32
7. Risk Management and Mitigation.....	32

8. Conclusion	33
SOFTWARE SPECIFICATIONS, RESEARCH REVIEW OR DESIGN COMPONENTS	34
PROJECT REQUIREMENTS.....	34
Functional requirements.....	34
Non-Functional Requirements	36
EXPECTED TEST CASES.....	38
PROJECT PLAN	42
BUDGET AND BUDGET JUSTIFICATION	43
CONCLUSION.....	44
REFERENCES.....	45

LIST OF TABLES

Table 1. Research Gap Table.....	16
Table 2. Overall Budget	43

LIST OF FIGURES

Figure 1.CAN-BUS Shield	24
Figure 2. OBD2-to-DB9 Adapter Cable Port.....	25
Figure 3. OBD2-to-DB9 Adapter Cable Port Actual View	25
Figure 4. OBD2-to-DB9 Adapter Cable	26
Figure 5. USB Extension Cable	26
Figure 6. Vehicle Dash Camera.....	26
Figure 7. Overall System Diagram	29
Figure 8. Component Diagram	30
Figure 9. Gantt Chart	42

LIST OF ABBREVIATIONS

Keyword	Meaning
V2X	Vehicle-to-Everything
CAN	Controller Area Network
BC	Blockchain
DSRC	Dedicated Short Range Communication
ECU	Electronic control units
DoS	Denial of Service
IVs	Intelligent Vehicles

INTRODUCTION

In the evolving landscape of autonomous and connected vehicles, secure and efficient communication is critical to ensuring safety and reliability. "Secure Vehicle Communication with Hybrid Solutions," focuses on developing a robust communication protocol that integrates advanced technologies and edge computing to facilitate real-time data exchange between vehicles and infrastructure. This hybrid protocol aims to provide low-latency and high-reliability communication, which is essential for the seamless operation of vehicular networks.

At the core of this component is the collection and analysis of data from various communication streams, including intra-vehicle communication through sensors, and inter-vehicle communication such as Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Pedestrian (V2P) interactions. Utilizing visible light, GPS, and LiDAR systems, this data will be processed through machine learning algorithms to predict vehicle behavior and critical events. The inclusion of blockchain technology further enhances the security and reliability of these predictions by providing a secure logging mechanism for critical event data.

The hybrid communication protocol developed in this component integrates both traditional and modern communication methods. This integration enables real-time data exchange while ensuring secure and efficient processing of information. By leveraging blockchain, the protocol not only enhances the accuracy of models used for object detection in V2V, V2I, and V2P communications but also ensures that all data exchanges are securely logged and protected against potential cyber threats.

This component represents a significant step toward the development of secure and resilient vehicular communication systems. By combining advanced communication technologies with machine learning and blockchain, the hybrid protocol aims to optimize the safety and efficiency of autonomous and connected vehicles, paving the way for a more secure and reliable future in transportation.

BACKGROUND & LITERATURE SURVEY

This decade has seen a major focus in the development of autonomous vehicles around the world. Various types of sensors, communication systems, computational hardware, and the emerging AI technologies play key roles in advancing the research and development of autonomous and connected mobility. Researchers are actively working on technologies that enable vehicles to communicate with each other and with surrounding devices in the environment, which is collectively known as vehicle-to-everything (V2X) communication [1].

The modern Intelligent Vehicle (IV) is a complex technological marvel that heavily relies on the Controller Area Network (CAN) bus system to enable seamless communication among different electronic control units (ECUs). However, the CAN bus system lacks security mechanisms for authentication and authorization, leaving it vulnerable to various attacks. Malicious actors can freely broadcast CAN messages without protection, making the system susceptible to DoS, Fuzzing, and Spoofing attacks [2].

Statistics of road accidents show that road accidents occurred mainly due to the following reasons. The frontier vehicle suddenly stop or slow down, The vehicle is loss of control, The vehicle changes lanes, The vehicle drives across the roads junction where is, absent of traffic signal lights, The vehicle does not follow the traffic rules, The road is congestion or abnormal, The vehicle breaks down in the middle of the road, When a vehicle detects some risks, it issues the, warning message. If a vehicle hears the warning message, it receives it and processes it by the corresponding safety application. According to the above risks, vehicle-to-vehicle safety applications can be classified into 7 applications. such as the application of emergency brake warning, The application of failure warning, The application of collaborative driving, The application of converse driving warning, The application of abnormal road warning, The application of road congestion warning, Application of asking for help [3].

In recent studies, vehicular networks have been considered as a promising solution to achieve better traffic management and to improve the driving experience of drivers. In vehicular networks, vehicle-to-everything (V2X) services, e.g. on-road traffic information exchange and location-based services, are provided to facilitate road safety for vehicles and traffic management for the relevant authorities. Dedicated Short Range Communications is specifically designed for V2X communications, and recently the cellular network has shown great potential to support V2X with better performance and more applications. Due to the wireless nature of V2X communications, how to secure V2X communications and guarantee the privacy of users are great challenges that have hampered the implementation of vehicular services [4].

The general communication framework for emerging connected and autonomous vehicles poses a severe security challenge as its safety can be compromised by several diverse types of cyberattacks. Moreover, there are still a lot of uncertainties and doubts about cause-effect relationships and mechanisms of vehicles' cybersecurity [5].

RESEARCH GAP

Identifying research gaps is an important element of any research project. A research gap is a piece of knowledge that has not yet been examined in a certain subject. The identification of research gaps assists researchers in deciding the scope of the study and in exploring new topics of inquiry. Several unique aspects of the suggested system have been found in this study, including Hybrid communication approach, Edge Computing with hybrid approach, Intra Vehicle and Network communication, Inter vehicle and communication within the network. In comparison to the proposed system, several selected research papers have been analyzed in this study to identify research gaps and explore new areas of research.

The first research shows the challenges of implementing V2X communication, such as the high cost of DSRC installations and the difficulty in achieving time synchronization between devices. Despite these challenges, the results showed that V2V communication could significantly improve vehicle safety, with applications like emergency brake lights and collision warnings effectively alerting drivers to potential hazards.

The second research focuses on enhancing the security of in-vehicle networks, specifically Controller Area Networks (CANs), against cyberattacks. It introduces HybridSecNet, a hybrid model combining Long Short-Term Memory (LSTM) networks and Convolutional Neural Networks (CNN) to detect and mitigate cyber threats within CANs. and Suggestions for future research include refining the model to handle more complex attack scenarios and exploring its integration into other vehicular communication systems. In this case our approach for security enhancement is considered as an architectural solution as an overall project solution.

The third research outlines key safety applications, designs safety messages and communication requirements, and proposes performance metrics for V2V communication. It categorizes safety applications into seven types, such as emergency brake warning and road congestion warning, and emphasizes the need for reliable and timely message transmission. The study also discusses the communication range necessary for different safety messages and suggests metrics like reception reliability and transmission delay to evaluate V2V communication performance. These findings are intended to guide the development of V2V safety communication protocols. We have recognized that this approach contains a risk of conveying messages due to single model using for the application, we suggest the multi model approach with edge computing to fill the gap of this research paper.

The fourth research discusses the potential of vehicular networks, particularly vehicle-to-everything (V2X) services, in improving traffic management and driving experience. V2X communications facilitate road safety and traffic management, with

Dedicated Short-Range Communications (DSRC) being specifically designed for this purpose. Recently, cellular networks have shown promise in supporting V2X with enhanced performance and more applications. Intra vehicle communications connected to the network can be identified as a lack of this approach. So, we suggest networked intra vehicle communication for this.

The final research paper discusses modern approaches to securing CAVs, including machine learning, federated learning, and blockchain technology. These methods are used to enhance intrusion detection systems and develop other countermeasures to safeguard CAVs. The article concludes by identifying research challenges and future directions in the field of CAV cybersecurity. As an overall solution we suggest architectural changes such as using multi model approach and using cloud storage, blockchain and edge computing to avoid the issues related to the related delays.

Research Research Gap Feature	01	02	03	04	05	Proposed Research Solution
Hybrid Communication approach with blockchain and machine learning	✗	✗	✗	✓	✓	✓
Enhance security measures using blockchain	✗	✓	✓	✓	✓	✓
Edge computing combined with cloud and blockchain stored models	✗	✗	✗	✗	✗	✓
Networked intra vehicle communication	✓	✓	✗	✓	✓	✓
Inter vehicle communication using ad-hock communication technologies and web-based network	✓	✓	✗	✓	✓	✓

Table 1. Research Gap Table

RESEARCH PROBLEM

Research Problem: What strategies can be implemented to Enhance security and data integrity in an effective way in vehicular communication Networks through hybrid blockchain and machine learning.

The challenge of secure vehicular communication centers around the significant security challenges associated with vehicular networks, particularly in vehicle-to-everything (V2X) communications. As autonomous and connected vehicles become increasingly integrated into modern transportation systems, the reliance on these networks for real-time data exchange between vehicles and infrastructure grows. However, this interconnectedness introduces vulnerabilities, notably the susceptibility of the Controller Area Network (CAN) bus system to various cyberattacks such as Denial of Service (DoS), Fuzzing, and Spoofing.

The fundamental issue lies in the lack of robust security mechanisms within current vehicular communication frameworks. The CAN bus system, a critical component of Intelligent Vehicles (IVs), was not designed with adequate authentication and authorization protocols, making it an easy target for malicious actors. As a result, unauthorized access to this system can lead to catastrophic consequences, compromising the safety and functionality of autonomous vehicles.

Moreover, the wireless nature of V2X communications exacerbates the problem, presenting additional challenges in ensuring data privacy and integrity. Existing solutions have not fully addressed these vulnerabilities, leaving a gap in the secure implementation of vehicular networks.

Also, identifying objects using inter vehicular communication techniques and intra vehicular communication takes a main role in this scenario. After the identification of the environmental status, it needs to be taken the necessary actions according to the situations. So that communication itself should identify the critical situation in an efficient manner.

The research proposes a hybrid approach that integrates blockchain technology with machine learning to enhance the security and data integrity of these networks. Blockchain's decentralized and immutable ledger provides a reliable method for storing and auditing vehicular events, while machine learning algorithms can analyze real-time data to detect anomalies and reduce verification times. This dual approach aims to create a more resilient vehicular communication system capable of withstanding various cyber threats, ultimately contributing to safer and more efficient transportation systems.

RESEARCH OBJECTIVES

Main Objectives

The primary goal of this study is to create an efficient communication system with the use of blockchain enhancing the security and integrity of communication. Successful identification of the seven critical events which can lead to road accidents will help to prevent sudden collisions and protect the life of the users.

1. The frontier vehicle suddenly stops or slow down,
2. the vehicle is loss of control, the vehicle changes lanes,
3. the vehicle drives across the roads junction where is,
4. absent of traffic signal lights,
5. the vehicle does not follow the traffic rules,
6. the road is congestion or abnormal,
7. the vehicle breaks down in the middle of the road

are the seven events which are identified by the system through intra and inter vehicular communication. For identifying these scenarios intra vehicular communication using CAN bus system and inter vehicular communication using cameras and sensors and the networks are taking main roles. For reading intra vehicular data use of CAN bus data reader and for reading inter vehicular data external cameras and sensors needs to be used and for the inter vehicular communication. Also, connected networks will be identified through the internet as well as online applications. The priority for the resource allocation should be based on the situation as well.

Specific Objectives

Specific

- Using CAN bus data reader device, collect CAN bus data
- Using camera collect object data
- Train machine learning models using collected data to identify seven critical events
- Use blockchain and store the models
- Use cloud storage for storing models

Measurable

- Check the efficiency of the machine learning models
- Assess the speed and resource allocation time
- Measuring the reduction in communication latency and increase in data transmission reliability after implementing the hybrid protocol.
- Assessing the percentage of vehicles and infrastructure systems successfully implementing the new hybrid protocol.

Achievable

- Ensuring that the necessary technological resources (e.g., blockchain infrastructure, machine learning models) are accessible and can be effectively implemented.
- Leveraging the skills of the research team and collaborating with industry experts to achieve the technical goals

Relevant

- Addressing the increasing demand for secure communication in autonomous and connected vehicles.
- Aligning the project with current advancements in blockchain and AI technologies, ensuring it remains cutting-edge
- Ensuring the solution meets all necessary industry standards and legal requirements for vehicular communication systems.

Time-bound

- Collect vehicle object identifying data from available sources and train basic ML models within 2 months
- Read CAN bus data and build ML models which read CAN bus data within the first two months of the project.

- Getting stored data from blockchain and train ML models for identifying the location wise critical grounds to handle
- Completing the prototype within the first three months with camera installation and CAN bus data reader.

The goal of the research is to gather vehicle data using open-source data sets and with necessary field visits based on the requirements to train ML models to identify specific features of vehicle and vehicular communication data, such as intervehicle communication with camera, sensors and network. As a final output this project identifies in detail features of vehicles and environment to build meaningful communication in the network and identify the critical events using intra vehicle and inter vehicle communications.

METHODOLOGY

METHODOLOGY INCLUDING THE SYSTEM DIAGRAM

REQUIREMENT GATHERING

The process of gathering requirements is an important phase in the development of the proposed system. It includes gathering and evaluating data from stakeholders and users to define the system's functional and non-functional needs.

The primary objective of this research is to secure vehicle-to-everything (V2X) communication through the development and implementation of a hybrid solution integrating blockchain technology and machine learning algorithms. The success of this component hinges on thorough requirement gathering, which will ensure the development of a robust and secure communication protocol that meets the needs of modern vehicular networks. This description outlines the key requirements necessary for the successful execution of the research project.

The first step in requirement gathering is identifying the stakeholders who will contribute to and benefit from the secure communication protocol. Key stakeholders include:

- **Automotive Manufacturers:** Companies developing autonomous and connected vehicles that require secure communication channels.
- **Insurance Providers:** Companies that offer vehicle insurance policies, potentially involved in assessing risks and claims related to V2X communication incidents.
- **Regulatory Bodies:** Government agencies that set standards for vehicular communication and cybersecurity.
- **End Users:** Drivers and passengers who rely on secure and reliable vehicle communication systems for safety and convenience.

Also, it takes a major role for technical requirements gathering in this research. Usage of blockchain and cloud storage and machine learning model implementation using real world data and historical data take crucial role as well as the other requirements.

Technical requirements are critical for the design and implementation of the hybrid solution:

- **Blockchain Integration:** The system must incorporate a decentralized blockchain network to store and verify vehicular data securely, providing an immutable audit trail.

- **Machine Learning Models:** Development and training of machine learning models are required to analyze data in real-time, enabling quick detection of anomalies and reducing verification times.
- **Interoperability:** The protocol must be compatible with existing vehicular communication systems and capable of integrating with various automotive and infrastructure technologies.

Also, it takes a major role that comes to the topic of risk management and mitigation when dealing with cybersecurity threats, technology limitations and regulatory changes.

To ensure the project's success, it is essential to identify potential risks and develop strategies to mitigate them:

- **Cybersecurity Threats:** Address potential vulnerabilities that could be exploited by cyber attackers, ensuring that the protocol includes robust defense mechanisms.
- **Technological Limitations:** Recognize and address limitations in current blockchain and machine learning technologies, ensuring that the solution remains effective and reliable.
- **Regulatory Changes:** Monitor and adapt to any changes in industry regulations that could impact the implementation of the communication protocol.

The requirement gathering process for this research is a critical phase that lays the foundation for developing a secure, reliable, and scalable vehicular communication protocol. By engaging with stakeholders, defining clear functional and non-functional requirements, and addressing technical and risk management considerations, the project is well-positioned to deliver a solution that meets the needs of modern automotive networks and enhances overall vehicular safety and security.

CAN bus adapter devices

The Controller Area Network (CAN) bus is a robust vehicle bus standard designed to facilitate communication between various electronic control units (ECUs) within a vehicle. As modern vehicles become increasingly complex, with numerous sensors and control systems, the CAN bus plays a critical role in ensuring seamless communication across these components. A CAN bus adapter data reading device is an essential tool that interfaces with the CAN bus, allowing for real-time monitoring, data extraction, and analysis of the signals transmitted across the network.

This device is crucial for diagnostics, performance tuning, and the development of advanced vehicular systems, such as autonomous driving and vehicle-to-everything (V2X) communication. By capturing and interpreting the data exchanged between ECUs, the CAN bus adapter enables engineers, technicians, and developers to gain valuable insights into vehicle operations, identify potential issues, and optimize performance.

Additionally, the device can be used in research and development to test new automotive technologies, ensuring they are compatible with existing systems. With the rise of smart and connected vehicles, the CAN bus adapter data reading device has become an indispensable tool in the automotive industry, contributing to the advancement of safer, more efficient, and technologically advanced vehicles.

Benefits of Using a Dash Cam Device for Object Data Identification

In the context of vehicular research, particularly in the development of advanced driver assistance systems (ADAS) and autonomous vehicles, the use of a dash cam device for object data identification offers significant benefits. Dash cams, typically mounted on the windshield of a vehicle, continuously record the road ahead, capturing high-quality video footage that can be analyzed for various research purposes.

One of the primary advantages of using a dash cam is its ability to provide real-time visual data that complements the information gathered from other sensors, such as LIDAR or radar. This visual data is crucial for object recognition and classification, allowing researchers to identify and track various objects on the road, such as vehicles, pedestrians, and traffic signs. The dash cam's footage can be processed using computer vision algorithms to detect and analyze these objects, aiding in the development of more accurate and reliable object detection systems.

Furthermore, dash cams are relatively easy to install and can operate continuously, making them an efficient tool for collecting large volumes of data over extended periods. This extensive dataset is invaluable for training machine learning models, testing new algorithms, and validating the performance of object recognition systems in diverse driving conditions.

Using dash cam footage also enhances the ability to simulate real-world scenarios, providing researchers with the visual context needed to understand how vehicles interact with their environment. This is particularly important for improving the safety and decision-making capabilities of autonomous vehicles, as it ensures that the systems can accurately identify and respond to dynamic road situations.

Overall, the integration of a dash cam device into vehicular research enables comprehensive object data identification, contributing to the advancement of more intelligent and safer automotive technologies.

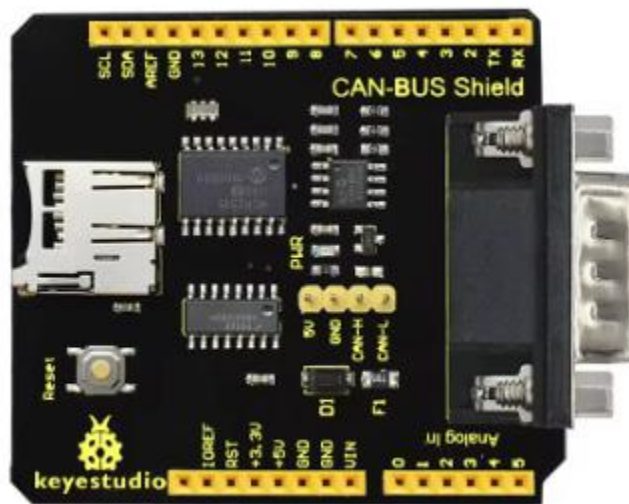


Figure 1.CAN-BUS Shield

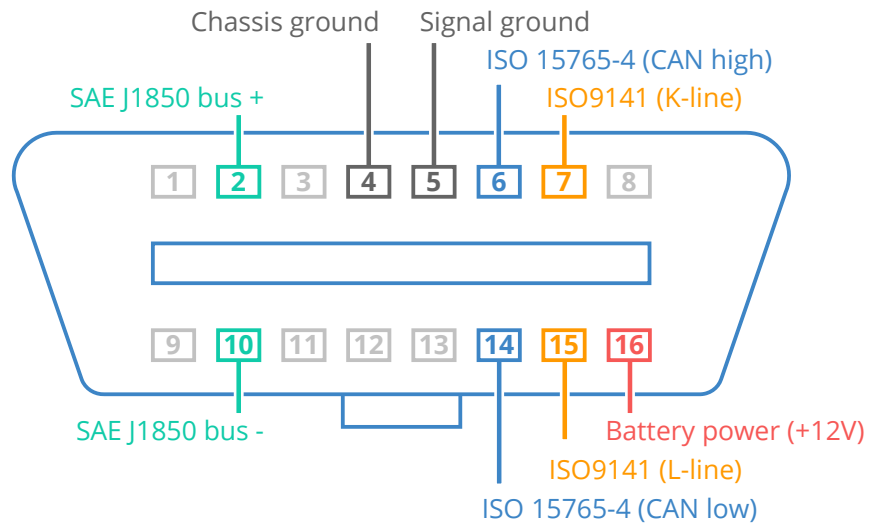


Figure 2. OBD2-to-DB9 Adapter Cable Port



Figure 3. OBD2-to-DB9 Adapter Cable Port Actual View



Figure 4. OBD2-to-DB9 Adapter Cable



Figure 5. USB Extension Cable



Figure 6. Vehicle Dash Camera

SYSTEM ARCHITECTURE

The proposed system architecture is intended to provide a cost effective and scalable solution for detecting vehicle event critical situations using machine learning, blockchain and cloud-based system integrated with edge computing capabilities.

Data Collection

The data collection component is responsible for aggregating diverse sources of information from within and between vehicles. This includes tapping into the CAN bus for intra-vehicle communication to capture vital data on vehicle status, performance metrics, and driver inputs. Additionally, it involves utilizing cameras and sensors for inter-vehicle communication to monitor surrounding traffic conditions, detect other vehicles, pedestrians, and obstacles. The collected data also includes environmental conditions and real-time vehicle interactions. The data is obtained from various sources such as onboard cameras, radar, lidar, and existing open-source datasets, enabling comprehensive and nuanced information gathering.

Data Processing

Data processing involves preparing and refining the collected data for further analysis. This step focuses on filtering out noise and irrelevant information from the CAN bus data, camera feeds, and sensor inputs. It involves the integration of raw data from different sources into a cohesive dataset, suitable for analysis. Advanced data cleaning techniques are employed to handle discrepancies and ensure that the data is accurate and consistent. Machine learning methods are used to preprocess and format the data, making it ready for model training and validation.

Object and Motion Detection

The object and motion detection component are tasked with analyzing the processed data to identify and track objects within the vehicle's environment. This involves using machine learning models trained on open-source datasets to recognize and classify various objects such as other vehicles, pedestrians, and obstacles. The component employs advanced algorithms, including convolutional neural networks (CNNs) for image analysis and motion tracking techniques, to detect and follow the movement of these objects. The system aims to enhance situational awareness and support decision-making processes by accurately identifying and interpreting dynamic elements in the vehicle's surroundings.

Model Training and Evaluation

Model training and evaluation leverage open-source datasets to develop and refine algorithms for object recognition and motion analysis. This includes using pre-existing data to train models in identifying and predicting object behaviors and movements. The

research involves applying various machine learning techniques to enhance model accuracy and efficiency. Continuous evaluation and refinement are performed to ensure the models' performance aligns with real-world scenarios, making them robust and reliable for practical applications in vehicular communication systems.

Application and Integration

The application and integration phase focuses on deploying the trained models into the vehicular communication system. This involves integrating the object and motion detection capabilities with existing vehicle control and communication systems. The goal is to enable real-time responses and interactions based on the detected information, improving vehicle safety and efficiency. This phase also includes validating the system's effectiveness in various driving conditions and ensuring seamless operation within the vehicle's architecture.

SYSTEM DIAGRAM

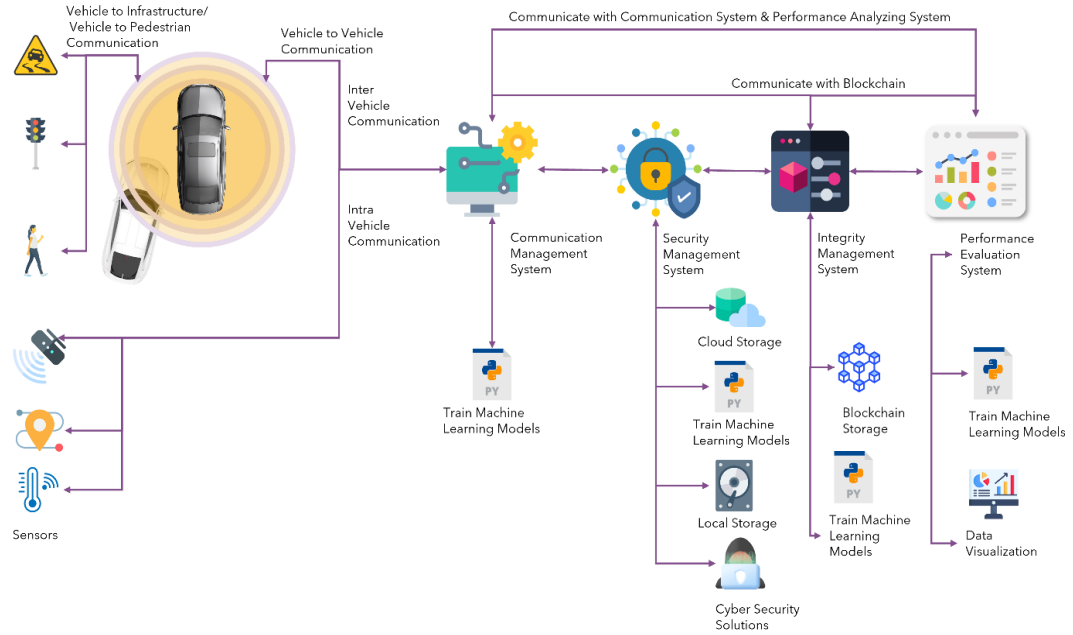


Figure 7. Overall System Diagram

COMPONENT DIAGRAM

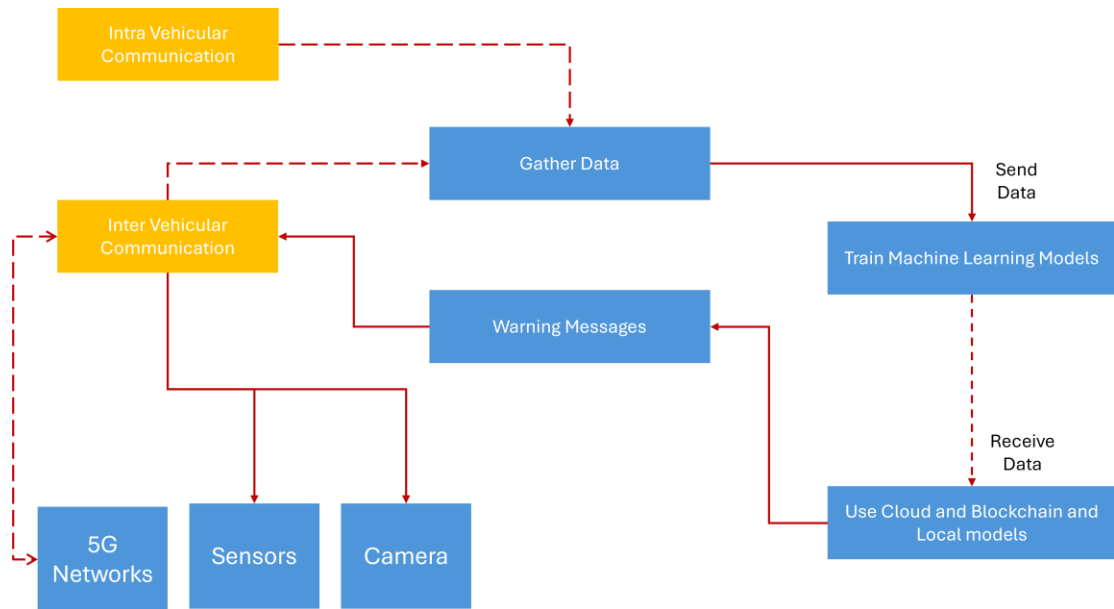


Figure 8. Component Diagram

COMMERCIALIZATION OF THE PRODUCT

1. Research Overview

The research aims to secure vehicle-to-everything (V2X) communication through a hybrid solution that integrates blockchain technology and machine learning algorithms. The goal is to develop a robust and secure communication protocol suitable for modern vehicular networks, enhancing data security, real-time decision-making, and anomaly detection.

2. Target Market and Audience

- **Automotive Manufacturers:** Companies developing autonomous and connected vehicles that require secure communication channels.
- **Regulatory Bodies:** Government agencies setting standards for vehicular communication and cybersecurity.
- **Fleet Operators:** Businesses managing large vehicle fleets needing secure and efficient communication systems.
- **Insurance Providers:** Companies that offer vehicle insurance policies, potentially involved in assessing risks and claims related to V2X communication incidents.

3. Key Features and Benefits

- **Blockchain Integration:** Provides decentralized, secure data storage and verification, ensuring an immutable audit trail.
- **Machine Learning Algorithms:** Enables real-time detection of anomalies and threats, improving network security.
- **Low Latency Communication:** Supports minimal delay in data transmission, crucial for timely decision-making and safety.
- **Scalability:** Designed to accommodate a growing number of connected vehicles and infrastructure without sacrificing performance.
- **Compliance:** Adheres to industry standards and regulatory requirements for vehicular communication and cybersecurity.

4. Business Model and Revenue Streams

- **Licensing:** Offer the technology as a licensed product to automotive manufacturers and infrastructure providers.
- **Subscription Service:** Provide ongoing updates, support, and enhancements through a subscription-based model.
- **Custom Solutions:** Develop tailored solutions for specific clients or industries with unique needs.

5. Go-to-Market Strategy

- **Partnerships:** Establish strategic alliances with key stakeholders such as automotive manufacturers and infrastructure providers to build credibility and market presence.
- **Pilot Programs:** Implement pilot projects with select clients to demonstrate the effectiveness and benefits of the research.
- **Industry Events:** Participate in automotive and technology conferences to showcase the research and network with potential clients.

6. Marketing and Sales

- **Digital Marketing:** Utilize online channels, including social media, webinars, and industry forums, to promote the research findings and attract potential clients.
- **Sales Team:** Develop a skilled sales team to engage with potential clients, present the research outcomes, and negotiate contracts.
- **Case Studies and Testimonials:** Use success stories and feedback from pilot programs to build trust and demonstrate the value of the research.

7. Risk Management and Mitigation

- **Cybersecurity Risks:** Implement robust security measures and continuous monitoring to address potential cyber threats.
- **Technological Challenges:** Stay updated with advancements in blockchain and machine learning technologies, and address limitations through ongoing research and improvements.
- **Regulatory Changes:** Monitor changes in industry regulations to ensure the research remains compliant with evolving standards.

8. Conclusion

The commercialization of this research offers a transformative opportunity for vehicular communication by integrating cutting-edge technologies with practical applications. The hybrid approach, combining blockchain and machine learning, addresses key challenges in securing vehicle-to-everything (V2X) communication. This solution enhances data security through decentralized verification and provides real-time anomaly detection to mitigate potential threats.

The hybrid communication protocol promises significant benefits for various stakeholders. Automotive manufacturers gain a reliable system essential for autonomous and connected vehicles, while infrastructure providers can integrate it into existing roadside units, improving network efficiency. Regulatory bodies will appreciate the protocol's adherence to industry standards, supporting compliance and governance in vehicular communication.

Fleet operators managing extensive vehicle networks will benefit from enhanced communication security and operational efficiency, contributing to safer fleet management. The solution's scalability ensures it can accommodate the growing number of connected vehicles and infrastructure components, adapting to evolving transportation demands.

The go-to-market strategy emphasizes strategic partnerships, pilot programs, and targeted marketing efforts to establish credibility and demonstrate practical value. Engaging with stakeholders through industry events and pilot projects will facilitate the transition from research to real-world application. A subscription-based model and custom solutions offer flexible revenue streams while maintaining ongoing support and innovation.

Addressing cybersecurity threats and technological limitations is crucial for the commercialization effort's success. By implementing robust security measures, staying current with technological advancements, and adapting to regulatory changes, the research will remain effective and relevant in the evolving industry landscape.

In conclusion, this research's successful commercialization will advance vehicular communication technologies, enhancing the safety and efficiency of modern transportation networks. This secure, scalable, and compliant solution has the potential to set new standards in V2X communication, driving significant improvements across the automotive sector.

SOFTWARE SPECIFICATIONS, RESEARCH REVIEW OR DESIGN COMPONENTS

PROJECT REQUIREMENTS

Functional requirements

1. Secure Data Transmission:

- **Description:** The communication protocol must encrypt and authenticate all data exchanged between vehicles and infrastructure to ensure that only authorized entities can access and modify the data.
- **Objective:** To prevent unauthorized access and tampering of vehicular data, ensuring the integrity and confidentiality of communications.

2. Low Latency Communication:

- **Description:** The system must support real-time data transmission with minimal delay to ensure timely responses to critical situations such as collision avoidance and emergency braking.
- **Objective:** To enable vehicles and infrastructure to make quick decisions based on the most current data available.

3. Anomaly Detection:

- **Description:** The integration of machine learning algorithms must allow the system to continuously monitor communication networks for unusual patterns or anomalies and trigger appropriate responses to address potential threats.
- **Objective:** To detect and mitigate potential security breaches or system faults in real-time, enhancing overall network reliability.

4. Blockchain Integration:

- **Description:** The protocol must utilize a decentralized blockchain network to store and verify vehicular data, ensuring an immutable and tamper-proof audit trail for all transactions.
- **Objective:** To provide a transparent and secure record of all communication activities, which can be audited and verified as needed.

5. Interoperability:

- **Description:** The solution must be compatible with existing vehicular communication systems and infrastructure technologies, allowing for seamless integration and operation within diverse environments.
- **Objective:** To ensure that the new system can be effectively implemented alongside current technologies without requiring significant modifications.

6. Real-Time Data Analysis:

- **Description:** The system must be capable of processing and analyzing data from multiple sources in real-time, including CAN bus data, camera feeds, and sensor inputs, to support decision-making and situational awareness.
- **Objective:** To provide timely insights and responses based on up-to-date information from various vehicular and environmental sources.

Non-Functional Requirements

1. Scalability:

- **Description:** The communication protocol must be designed to handle an increasing number of connected vehicles and infrastructure units without a decline in performance or efficiency.
- **Objective:** To support the growth of vehicular networks and infrastructure as the number of connected devices expands.

2. Reliability:

- **Description:** The system must maintain high availability and consistent performance, even under high traffic conditions or during potential cyberattacks.
- **Objective:** To ensure that the communication protocol remains operational and effective in various scenarios, providing reliable data exchange and security.

3. Compliance:

- **Description:** The solution must adhere to industry standards and regulatory requirements related to vehicular communication and cybersecurity, including data protection laws and safety regulations.
- **Objective:** To ensure that the system operates within legal and ethical boundaries, meeting all necessary compliance requirements.

4. Performance Efficiency:

- **Description:** The system must optimize resource usage, including processing power, bandwidth, and storage, to achieve high performance without unnecessary overhead or resource consumption.
- **Objective:** To provide an efficient solution that minimizes operational costs and maximizes system effectiveness.

5. Usability:

- **Description:** The system must be user-friendly for all stakeholders, including automotive manufacturers, infrastructure providers, and end-users, with intuitive interfaces and clear documentation.
- **Objective:** To facilitate ease of adoption and operation, ensuring that users can effectively interact with and manage the communication protocol.

6. Security:

- **Description:** The system must incorporate robust security measures, including encryption, access controls, and intrusion detection, to protect against potential threats and vulnerabilities.
- **Objective:** To safeguard the integrity and confidentiality of data, ensuring the security of communication channels and protecting against unauthorized access.

7. Maintainability:

- **Description:** The solution must be designed for ease of maintenance and updates, allowing for straightforward troubleshooting, bug fixes, and enhancements.
- **Objective:** To ensure long-term sustainability and adaptability of the system, facilitating ongoing improvements and support.

EXPECTED TEST CASES

For a communication component in a vehicular communication system, relevant test cases should focus on verifying the effectiveness, security, and reliability of data transmission and reception. Here are the key test cases tailored to different aspects of the communication component:

1. Data Transmission and Reception

- **Test Case 1.1: Data Integrity**
 - **Objective:** Verify that data transmitted between vehicles and infrastructure remains intact and unaltered.
 - **Input:** Data packet sent from one vehicle to another or to infrastructure.
 - **Expected Result:** Data received matches the data sent, with no corruption or alteration.
- **Test Case 1.2: Data Latency**
 - **Objective:** Measure the time taken for data to travel from the sender to the receiver.
 - **Input:** Timestamped data packets sent and received.
 - **Expected Result:** Data is transmitted and received within the acceptable latency threshold (e.g., <100 milliseconds).
- **Test Case 1.3: Data Loss**
 - **Objective:** Ensure that no data packets are lost during transmission.
 - **Input:** A sequence of data packets sent under normal and high traffic conditions.
 - **Expected Result:** All data packets are received without loss.

2. Security and Authentication

- **Test Case 2.1: Encryption Verification**
 - **Objective:** Confirm that data is encrypted before transmission and can be decrypted by authorized recipients.
 - **Input:** Encrypted data packet sent and received.
 - **Expected Result:** Data is correctly encrypted and decrypted, ensuring data confidentiality.

- **Test Case 2.2: Authentication of Communication Entities**

- **Objective:** Ensure that only authenticated entities can participate in communication.
- **Input:** Communication attempts from authorized and unauthorized entities.
- **Expected Result:** Only authorized entities can successfully communicate, while unauthorized attempts are blocked.

- **Test Case 2.3: Anomaly Detection**

- **Objective:** Test the system's ability to detect and respond to anomalies in communication patterns.
- **Input:** Normal and anomalous data patterns.
- **Expected Result:** Anomalies are detected, and appropriate alerts or responses are triggered.

3. Interoperability

- **Test Case 3.1: Compatibility with Existing Systems**

- **Objective:** Verify that the communication protocol integrates seamlessly with existing vehicular communication systems.
- **Input:** Test data exchanged between new and legacy systems.
- **Expected Result:** Successful data exchange without compatibility issues.

- **Test Case 3.2: Integration with Various Technologies**

- **Objective:** Ensure the protocol works with different automotive and infrastructure technologies.
- **Input:** Data from various vehicle models and infrastructure components.
- **Expected Result:** Effective communication and integration across diverse technologies.

4. Performance and Scalability

- **Test Case 4.1: System Load Handling**

- **Objective:** Assess the system's performance under varying loads, including peak traffic conditions.

- **Input:** Simulated high traffic with numerous connected vehicles.
- **Expected Result:** The system maintains performance and stability under increased load.
- **Test Case 4.2: Scalability Testing**
 - **Objective:** Test the system's ability to scale with the addition of new vehicles and infrastructure components.
 - **Input:** Incremental addition of new communication entities.
 - **Expected Result:** The system scales efficiently, handling additional entities without performance degradation.

5. Reliability and Fault Tolerance

- **Test Case 5.1: System Uptime**
 - **Objective:** Ensure that the communication system remains operational over extended periods.
 - **Input:** Continuous system operation monitoring.
 - **Expected Result:** High system uptime with minimal or no downtime.
- **Test Case 5.2: Recovery from Failures**
 - **Objective:** Test the system's ability to recover from hardware or software failures.
 - **Input:** Simulated failure scenarios (e.g., network interruptions).
 - **Expected Result:** The system recovers and resumes normal operation within an acceptable time frame.

6. Compliance and Standards

- **Test Case 6.1: Adherence to Industry Standards**
 - **Objective:** Verify that the communication protocol complies with relevant industry standards and regulations.
 - **Input:** Compliance checklists and regulatory guidelines.
 - **Expected Result:** The system meets all applicable standards and regulatory requirements.

- **Test Case 6.2: Data Protection and Privacy**

- **Objective:** Ensure compliance with data protection laws and privacy regulations.
- **Input:** Data handling practices and privacy policies.
- **Expected Result:** The system adheres to data protection and privacy regulations, safeguarding user information.

These test cases are designed to ensure that the communication component meets the necessary requirements for secure, efficient, and reliable operation in a vehicular network. They cover various aspects, from data integrity and latency to security, interoperability, and scalability.

PROJECT PLAN

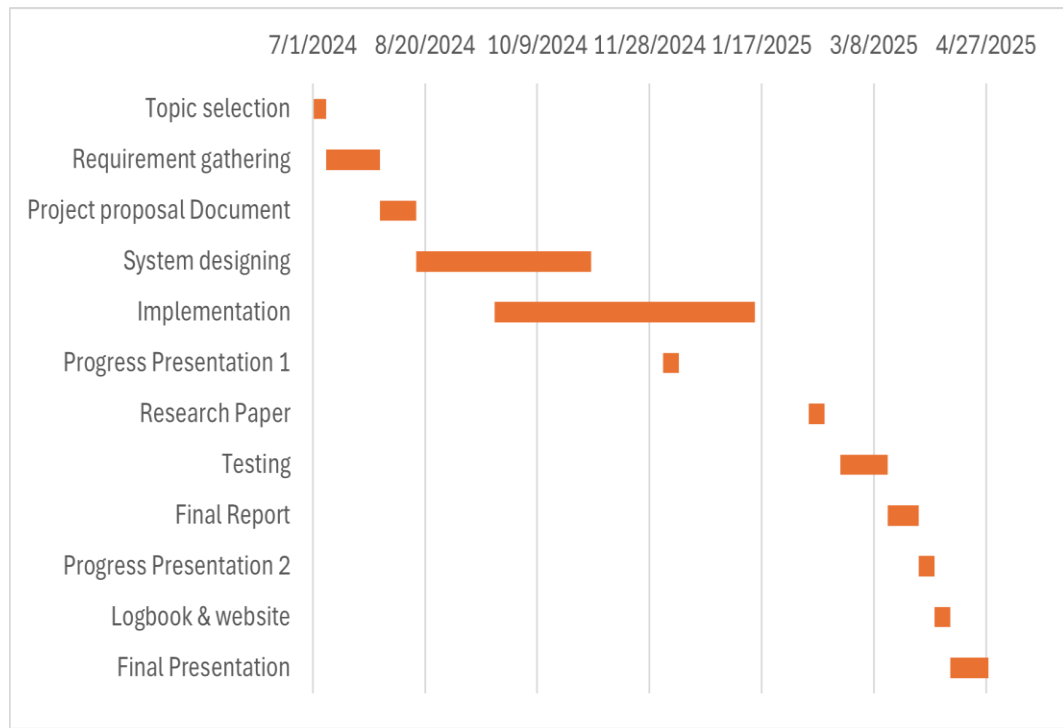


Figure 9. Gantt Chart

BUDGET AND BUDGET JUSTIFICATION

Item	Description	Estimated Cost
CAN Shield	Hardware component interfacing with the CAN bus and ESP32 microcontroller	LKR2,376.69
DB9 Adapter cable	Connector for accessing the OBD2 port in the vehicle; includes four pins for CAN bus and power	LKR3,911.02
USB extension cable	Cable for extending the USB connection to the microcontroller or other components	LKR424.20
Dash CAM	Camera mounted on the dashboard to record video footage of the vehicle's surroundings.	LKR4,060.14
Total		LKR 10,772.05

Table 2. Overall Budget

CONCLUSION

The research on securing vehicle communication through hybrid solutions has demonstrated the critical importance of integrating advanced technologies, such as blockchain and machine learning, to address the evolving challenges of vehicular networks. As the automotive industry continues to advance towards fully autonomous and connected vehicles, the need for robust, secure, and scalable communication protocols has become more urgent than ever.

By implementing a hybrid approach that combines the immutable and decentralized nature of blockchain with the predictive and analytical power of machine learning, this research offers a pioneering framework for ensuring secure vehicle-to-everything (V2X) communication. The development of a secure communication protocol not only protects vehicles from cyber threats but also enhances overall traffic safety by enabling real-time data exchange and anomaly detection across vehicular networks.

The research has also emphasized the importance of stakeholder engagement, compliance with regulatory standards, and the need for continuous monitoring and adaptation to technological advancements and potential risks. The functional and non-functional requirements outlined provide a comprehensive roadmap for developing a communication system that is not only effective in the current landscape but is also future proof against emerging challenges.

In conclusion, this research contributes to the foundational work necessary for the next generation of intelligent transportation systems. The hybrid solution proposed serves as a robust blueprint for securing vehicular communication, ensuring that as vehicles become more interconnected, they do so in a manner that prioritizes security, reliability, and scalability. This research sets the stage for further innovation, paving the way for safer and more efficient transportation networks worldwide.

REFERENCES

- [1] G. Tewolde and B. Smith, "Small Scale Field Study of Vehicle-to-Vehicle (V2V)," *2019 IEEE 16th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT and AI (HONET-ICT)*, pp. 059-063, 2019.
- [2] A. Chougule, I. Kulkarni, T. Alladi, V. Chamola and F. R. Yu, "HybridSecNet: In-Vehicle Security on Controller Area Networks Through a Hybrid Two-Step LSTM-CNN Model," *IEEE Transactions on Vehicular Technology*, pp. 1-11, 2024.
- [3] C. Wen-Jing and H. Qing-Tian, "Requirements Analysis for Vehicle-to-Vehicle Safety Communication," *2012 International Conference on Industrial Control and Electronics Engineering*, pp. 216-218, 2012.
- [4] J. Huang, D. Fang, Y. Qian and R. Q. Hu, "Recent Advances and Challenges in Security and Privacy for V2X Communications," *IEEE Open Journal of Vehicular Technology*, vol. 1, pp. 244-266, 2020.
- [5] J. Ahmad, M. U. Zia, I. H. Naqvi, J. N. Chattha, F. A. Butt, T. Huang and W. Xiang, "Machine learning and blockchain technologies for cybersecurity in connected vehicles," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 14(1), p. e1515, 2024.