



EagleEye - Secure Vehicle Communication and Data Integrity Using Blockchain and Machine Learning

Project ID: 24-25J-206

Project Proposal Report

Rizmaan M.F.M

Bachelor of Science Hons. In Information Technology
(Specialization in Data Science)

Department of Computer Science

Sri Lanka Institute of Information Technology

Sri Lanka

August 2024

EagleEye - Secure Vehicle Communication and Data Integrity Using Blockchain and Machine Learning

Project ID: 24-25J-206

Project Proposal Report

Rizmaan M.F.M

Supervisor: Mr. Samadhi Rathnayake

Co-Supervisor: Mr. Nelum Amarasinghe

Bachelor of Science Hons. In Information Technology
(Specialization in Data Science)

Department of Computer Science

Sri Lanka Institute of Information Technology

Sri Lanka


DECLARATION

I declare that this is my own work and this proposal does not incorporate without acknowledgement of any material previously submitted for a degree or diploma in any other

university or Institute of higher learning and to the best of my knowledge and belief it does not

contain any material previously published or written by another person except where the

acknowledgment is made in the text.

Name	Student ID	Signature
Rizmaan M.F.M	IT21295188	

The above candidate is carrying out research for the undergraduate dissertation under my supervision.



Signature of the Supervisor

23/08/2024

Date

Signature of the Co-Supervisor

Date

ACKNOWLEDGEMENT

I would like to extend my heartfelt gratitude to everyone who supported me throughout my 4th-year research project. First and foremost, I am deeply thankful to our Research Project supervisor, Mr. Samadhi Rathnayake, for his invaluable guidance and encouragement, which played a crucial role in completing this project. I also want to express my sincere appreciation to our co-supervisor, Mr. Nelum Amarasinghe, for his constructive suggestions during the planning phase of our research.

Additionally, I am grateful to the CDAP panel for their insightful advice, which greatly influenced our project. I would also like to acknowledge my Research Project leader, Dissanayake D.J.R, along with all my group members, for their unwavering support and collaboration in achieving our goals.

Lastly, I want to extend my deepest thanks to my parents and friends for their constant support and inspiration, which have been a source of motivation throughout this journey.

ABSTRACT

The integration of manned and autonomous vehicles poses substantial issues in maintaining the privacy and security of sensitive data in the fast-growing field of vehicular networks. The goal of this project is to create secure and reliable privacy solutions specifically for hybrid vehicle networks, where real-time information sharing is essential. This study uses novel approaches such as access control, encryption, and anonymization to protect data during transmission and storage. Furthermore, machine learning is employed to analyze system logs and network data, hence improving situational awareness and risk assessment. To reduce the risk of data loss, blockchain, cloud, and system storage strategies will be investigated. This study seeks to provide a comprehensive strategy for addressing the rising data security concerns.

Keywords: Manned and Unmanned Vehicles, autonomous vehicles, vehicular network, blockchain, Cyber threats, federated learning, encryption, machine learning, cloud

Table of Contents

DECLARATION.....	1
ACKNOWLEDGEMENT	2
ABSTRACT	3
LIST OF FIGURES	5
LIST OF ABBREVIATIONS.....	6
.1 INTRODUCTION	7
.2 Background and Literature Survey	8
.2.1 Privacy and Security in Vehicular Networks	9
.2.2 Advanced Techniques and Machine Learning	10
.2.3 Blockchain for Secure Data Storage	10
.3 RESEARCH GAP	11
.3.1 Real-Time Communication Security	11
.3.2 Advanced Privacy Techniques	11
.3.3 Integration of Machine Learning for Data Privacy	12
.3.4 Cyber threat prevention	12
.3.5 Data Storage Solutions	13
.4 RESEARCH PROBLEM	14
.5 OBJECTIVES.....	15
.5.1 Main Objectives.....	15
.5.2 Specific Objectives.....	16
.6 METHODOLOGY	18
.7 BUDGET AND BUDGET JUSTIFICATION	22
.8 REFERENCES.....	23
.9 APPENDICES	24
.9.1 Gantt Chart	24

LIST OF FIGURES

Figure 1 : Live Cyber Attacks Tracker	8
Figure 2 : Research Gap Diagram.....	13
Figure 3 : Overall System Diagram	19
Figure 4 : Individual System Diagram	21

LIST OF ABBREVIATIONS

- ITS - Intelligent Transportation Systems
- V2V - Vehicle-to-Vehicle
- V2I - Vehicle-to-Infrastructure
- ML - Machine Learning
- ITS - Intelligent Transportation Systems
- V2X – Vehicles-to-Everything

.1 INTRODUCTION

The emergence of intelligent transportation systems has introduced a new era of connectivity in vehicular networks, where both manned and unmanned vehicles interact smoothly to improve road safety, traffic control, and overall effectiveness. Nevertheless, this enhanced interconnectivity also brings about substantial difficulties, namely with privacy and security. With the increasing complexity and integration of vehicle networks, safeguarding sensitive information has become a crucial need.

Hybrid vehicular networks, which rely on real-time data sharing and entail the coordination of autonomous and human-driven cars, are especially susceptible to cyber threats. The necessity for strong security measures is intensified by the potential ramifications of data breaches, which could jeopardize the safety of road users and the reliability of transportation systems. In order to tackle these difficulties, it is crucial to employ sophisticated privacy methods, such as encryption, access control, and anonymization, to protect data from unwanted access and cyber risks.

The objective of this research endeavor is to develop and apply a comprehensive privacy and security framework tailored for hybrid vehicle networks. The project will utilize machine learning techniques to examine network traffic and system logs in order to detect possible threats and improve the evaluation of risks. In addition, we will investigate the utilization of cloud, blockchain, and system storage technologies to guarantee the secure storage and transmission of data. The primary objective is to create a series of solutions that not only safeguard critical information but also improve the general endurance and trustworthiness of vehicle networks.

.2 Background and Literature Survey

The exponential growth of vehicular networks has significantly altered the domain of intelligent transportation systems (ITS), facilitating the emergence of interconnected cars that engage in real-time communication to augment safety, maximize efficiency, and improve customer satisfaction. Nevertheless, as the intricacy of these networks continues to grow, the significance of security and privacy issues has escalated, particularly in the context of handling confidential information exchanged between vehicles and supporting infrastructure. The present study examines the aforementioned difficulties by concentrating on the integration of privacy and security measures in hybrid vehicular networks, which amalgamate elements of both manned and unmanned vehicles.



Figure 1 : Live Cyber Attacks Tracker

Hybrid vehicular networks pose distinctive issues as a result of their dynamic and distributed characteristics. The amalgamation of diverse communication technologies, including Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I), in conjunction with the use of machine learning and blockchain technologies,

offers notable benefits while also presenting potential risk factors. The current body of research predominantly focuses on the examination of individual elements inside these networks, frequently overlooking the comprehensive approach necessary to ensure the security of the integrated system.

.2.1 Privacy and Security in Vehicular Networks

The significance of privacy and security in automobile networks has been underscored in numerous scholarly investigations. For example, conventional encryption techniques and access control mechanisms have been thoroughly investigated to safeguard the integrity and confidentiality of data. Nevertheless, the ever-changing structure of highway networks, combined with the frequent movement of nodes, presents considerable obstacles to the successful execution of these techniques. Furthermore, despite the existence of anonymization approaches aimed at safeguarding user identities, their utilization in the context of real-time vehicular communication has encountered limited investigation.

Contemporary breakthroughs in the field of machine learning present encouraging opportunities for augmenting security measures inside vehicle networks. The utilization of machine learning techniques enables the analysis of network traffic, identification of anomalies, and prediction of potential risks. Nevertheless, the majority of research has mostly concentrated on the identification of threats rather than their prevention, resulting in a dearth of proactive measures to mitigate such risks. Furthermore, the comprehensive implementation of machine learning in conjunction with conventional security techniques, such as encryption and access control, remains incomplete within the framework of hybrid vehicular networks.

In the realm of secure data storage, blockchain technology has emerged as a resilient

and effective option for safeguarding data within decentralized networks. The proposal suggests that implementation of this technology in automotive networks can serve as a mechanism to guarantee the integrity and transparency of data. Nevertheless, the integration of blockchain technology in hybrid vehicular networks, which involve the coexistence of both manned and unmanned vehicles, is now in its early developmental phase. The primary obstacle pertains to the development of a blockchain system that is both scalable and efficient, capable of effectively managing the substantial amount of data produced by these networks while maintaining optimal performance.

.2.2 Advanced Techniques and Machine Learning

Contemporary breakthroughs in the field of machine learning present encouraging opportunities for augmenting security measures inside vehicle networks. The utilization of machine learning techniques enables the analysis of network traffic, identification of anomalies, and prediction of potential risks. Nevertheless, the majority of research has mostly concentrated on the identification of threats rather than their prevention, resulting in a dearth of proactive measures to mitigate such risks. Furthermore, the comprehensive implementation of machine learning in conjunction with conventional security techniques, such as encryption and access control, remains incomplete within the framework of hybrid vehicular networks.

.2.3 Blockchain for Secure Data Storage

In the field of secure data storage, blockchain technology has emerged as a resilient and effective option for safeguarding data within decentralized networks. The proposal suggests that implementation of this technology in automotive networks can serve as a mechanism to guarantee the integrity and transparency of data. Nevertheless, the integration of blockchain technology in hybrid vehicular networks, which involve the coexistence of both manned and unmanned vehicles, is now in its early developmental

phase. The primary obstacle pertains to the development of a blockchain system that is both scalable and efficient, capable of effectively managing the substantial amount of data produced by these networks while maintaining optimal performance.

.3 RESEARCH GAP

Significant progress has been achieved in improving security and privacy in the ever-changing field of hybrid vehicle networks. Nevertheless, there are still significant deficiencies that must be resolved in order to provide a more secure and dependable setting for both manned and unmanned vehicles. This study finds and focuses on the following significant deficiencies:

.3.1 Real-Time Communication Security

Gap: Current research does not provide specific plans for ensuring the security of real-time communications in hybrid vehicle networks. The inherent dynamism of these networks, coupled with the imperative for immediate data interchange, gives rise to substantial risks that remain largely unexplored.

Solution: The objective of this research is to create and apply specialized encryption methods, access control mechanisms, and anonymization approaches that are designed to protect real-time communication. The project will improve the safeguarding of sensitive information throughout its transmission across the network by concentrating on federated learning.

.3.2 Advanced Privacy Techniques

Gap: Existing research lacks comprehensive exploration of sophisticated privacy methodologies, including hashing, encryption, and anonymization, specifically in the context of hybrid vehicle networks. These strategies are essential for preserving user privacy but are frequently not fully utilized or applied effectively in current frameworks.

Solution: This research aims to fill this gap by employing sophisticated privacy approaches that guarantee strong privacy protection for consumers. By incorporating these techniques into the hybrid vehicular network, the research will offer a more thorough approach to protecting personal information.

.3.3 Integration of Machine Learning for Data Privacy

Gap: The current studies does not comprehensively cover the application of machine learning (ML) in recognizing personal information and assuring data privacy in hybrid vehicular networks. Although machine learning (ML) has been used for numerous purposes, its ability to improve data privacy in this particular situation has not been fully studied.

Solution: This study aims to utilize machine learning techniques to examine network traffic and system logs, with the goal of enhancing risk evaluation and situational awareness. The research will showcase the effective utilization of machine learning in real-time to safeguard sensitive information by prioritizing data privacy.

.3.4 Cyber threat prevention

Gap: The majority of current research is centered around identifying and documenting cyber risks, rather than actively stopping them in real-time. The lack of proactive measures makes hybrid vehicular networks susceptible to attacks that cannot be addressed in a timely manner.

Solution: This research adopts a proactive approach to cybersecurity by prioritizing the prevention of cyber risks through the utilization of recommended methods and approaches. The study aims to enhance the security framework by utilizing blockchain technology to identify emerging vulnerabilities and regularly upgrade the centralized model in real-time.

.3.5 Data Storage Solutions

Gap: Existing strategies for data storage in hybrid vehicle networks lack complete solutions that effectively mitigate the risk of data loss. The incorporation of cloud, blockchain, and system storage solutions is frequently disregarded or inadequately dealt with.

Solution: This research suggests utilizing cloud, blockchain, and system storage technologies to ensure the security of data storage. By improving the ability of the vehicular network to withstand and recover from disruptions using these technologies, the study will provide a stronger and more dependable approach to reducing data loss.

Research	01	02	03	04	05	Eagle Eye
Protect sensitive information during real-time communication in hybrid vehicular networks	✗	✗	✗	✓	✓	✓
enhance data privacy and security by leveraging advanced ML techniques for real-time analysis and threat detection.	✗	✓	✗	✗	✗	✓
identifying and mitigating potential cyber threats before they impact the network	✗	✗	✗	✓	✓	✓
decentralized and immutable storage technologies	✓	✓	✗	✓	✓	✓
advanced privacy techniques	✓	✓	✗	✓	✗	✓

Figure 2 : Research Gap Diagram

.4 RESEARCH PROBLEM

Hybrid vehicular networks encounter substantial obstacles with privacy and security as they incorporate increasingly sophisticated communication systems between manned and unmanned vehicles. The instantaneous pace of data flow inside these networks, along with the intricate interplay between different vehicles and equipment, renders them especially susceptible to cyber assaults. Although there have been improvements in vehicular communication technology, current methods frequently fail to offer complete security solutions that meet the specific requirements of these networks.

An essential concern is the absence of comprehensive implementation solutions for ensuring the security of real-time communications. Existing approaches lack comprehensive integration of advanced privacy measures, such as encryption, hashing, and anonymization, resulting in the vulnerability of sensitive information during transmission. Moreover, although machine learning has been employed in diverse cybersecurity applications, its capacity to improve data privacy and evaluate risks in hybrid vehicular networks has not been thoroughly investigated.

Another significant obstacle is the prioritization of detecting and documenting cyber threats rather than actively thwarting them. This reactive strategy is inadequate in a setting where the consequences of a breach might be exceedingly significant, possibly jeopardizing both vehicle safety and user privacy. Moreover, current data storage methods fail to adequately reduce the likelihood of data loss, especially in the context of hybrid vehicular networks where the secure handling of substantial amounts of data is of utmost importance.

The issue comes in the lack of a complete framework that combines advanced privacy approaches, real-time threat prevention, and secure data storage systems specifically tailored for hybrid vehicular networks. To tackle this issue, it is necessary to create and execute inventive measures that safeguard confidential data while also improving the general durability and dependability of communication systems in vehicles.

.5 OBJECTIVES

The overarching goal of this research is to develop and implement a comprehensive security and privacy framework for hybrid vehicular networks. The focus will be on addressing the unique challenges posed by these networks, which combine aspects of both manned and unmanned vehicles. The objectives of this research are divided into two categories: main objectives and specific objectives.

.5.1 Main Objectives

1. Enhance Privacy and Security in Hybrid Vehicular Networks:

- Develop and implement advanced encryption methods, access control mechanisms, and anonymization techniques to protect sensitive information during real-time communication in hybrid vehicular networks.
- Integrate machine learning models to analyze network traffic, detect anomalies, and predict potential cyber threats in real-time.

2. Develop a Proactive Cyber Threat Prevention Framework:

- Focus on preventing cyber threats through a proactive approach, leveraging preferred methods and techniques, including reinforcement learning, to enhance the situational awareness of both manned and unmanned vehicles.
- Design and implement a decentralized security management system using blockchain technology to ensure data integrity and transparency across the network.

3. Implement Secure Data Storage Solutions:

- Leverage cloud, blockchain, and system storage solutions to minimize the risk of data loss and ensure secure storage of critical data generated by hybrid vehicular networks.
- Develop a scalable blockchain architecture that can handle the high volume of data generated by hybrid vehicular networks without compromising performance.

.5.2 Specific Objectives

1. Develop Specific Encryption Methods for Real-Time Communication:

- Design and implement encryption methods tailored for securing real-time communications in hybrid vehicular networks, addressing the challenges posed by high mobility and dynamic topologies.

2. Implement Advanced Privacy Techniques:

- Develop and implement advanced privacy techniques, including hashing, encryption, and anonymization, to ensure robust protection of user data in hybrid vehicular networks.

3. Integrate Machine Learning for Data Privacy:

- Utilize machine learning models to analyze network traffic, identify personal information, and enhance risk assessment and situational awareness in hybrid vehicular networks.

4. Design a Proactive Cyber Threat Prevention Framework:

- Develop a framework for proactive cyber threat prevention using reinforcement learning and other preferred methods, focusing on real-time threat detection and mitigation.

5. Leverage Blockchain for Secure Data Storage:

- Design and implement a decentralized blockchain-based storage solution to ensure data integrity and transparency, minimizing the risk of data loss in hybrid vehicular networks.

These objectives align with the overall goal of enhancing privacy and security in hybrid vehicular networks, addressing the gaps identified in the literature, and providing a robust solution for the challenges posed by these networks. By focusing on both the theoretical and practical aspects of privacy and security, this research aims to contribute to the development of secure and resilient vehicular networks.

.6 METHODOLOGY

The primary objective of this project is to improve privacy and security in hybrid vehicular networks, mitigating the increasing need for strong cybersecurity protocols in intelligent transportation systems. The present study is structured into multiple segments, each dedicated to examining distinct facets pertaining to security, privacy, and data management inside automotive networks. The primary objective is to establish a complete framework that guarantees secure, efficient, and dependable communication among vehicles, infrastructure, and users, hence reducing the likelihood of cyber threats.

Key Components:

1. **Real-Time Communication Security:** Focuses on securing real-time communications within the network through encryption methods, access control, and anonymization techniques, particularly using federated learning. This component aims to protect sensitive information during communication between vehicles and infrastructure.
2. **Advanced Privacy Techniques:** This component addresses the need for advanced privacy measures in vehicular networks. It implements hashing, encryption, and anonymization to safeguard user data. Machine learning algorithms are employed to analyze network traffic and system logs, enhancing situational awareness and improving risk assessment. The ultimate goal is to ensure data privacy while preventing cyber threats in real time.
3. **Cyber Threat Prevention:** This component emphasizes proactive cybersecurity, focusing on the prevention rather than just detection of threats. It leverages machine learning and blockchain technologies to continuously update and enhance security protocols, ensuring the system's resilience against emerging threats.
4. **Data Storage Solutions:** Addresses the challenge of secure data storage in vehicular networks. This component explores the use of cloud, blockchain, and

localized storage systems to minimize the risk of data loss and ensure data integrity across the network.

These components collectively form a robust system designed to secure hybrid vehicular networks, ensuring that data privacy, communication security, and threat prevention are effectively managed.

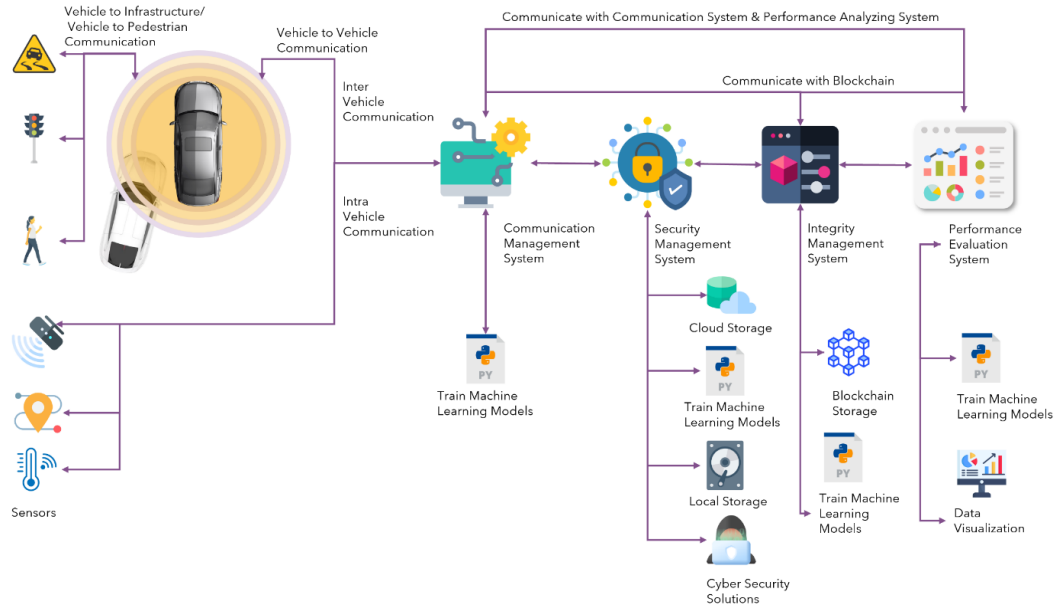


Figure 3 : Overall System Diagram

So if we focus on developing and implementing advanced privacy techniques to secure data in hybrid vehicular networks, the methodology is divided into several phases, each addressing a specific aspect of privacy and security.

1. Privacy Techniques Implementation:

- **Encryption:** Develop and implement encryption protocols tailored to vehicular networks. These protocols will secure data transmissions between vehicles (V2V), vehicles and infrastructure (V2I), and vehicles to everything (V2X).
- **Anonymization:** Employ anonymization techniques to protect user identities and sensitive data. This involves masking identifiable information while maintaining data utility for necessary operations.

- **Hashing:** Integrate hashing mechanisms to ensure data integrity and prevent unauthorized access. Hash functions will be used to create unique data signatures, verifying the authenticity of information exchanged within the network.

2. Machine Learning for Data Privacy:

- **Traffic Analysis:** Use machine learning models to analyze network traffic in real-time. This analysis will help identify patterns indicative of potential threats or privacy breaches.
- **Risk Assessment:** Implement machine learning algorithms to assess the risk level of various network activities. This will involve training models on historical data to predict and mitigate possible security incidents.
- **Anomaly Detection:** Develop models that can detect anomalies in the system logs. These anomalies could indicate attempts to breach the system's privacy or other suspicious activities.

3. Federated Learning for Decentralized Security:

- **Distributed Learning Models:** Implement federated learning models where vehicles collaboratively train machine learning models without sharing raw data. This method ensures data privacy while improving the overall security model.
- **Reinforcement Learning:** Incorporate reinforcement learning techniques to adapt and update security protocols in real-time, based on the changing threat landscape and network conditions.

4. Cyber Threat Prevention:

- **Blockchain Integration:** Utilize blockchain technology to create a secure, decentralized ledger of network activities. This ledger will be used to verify and validate transactions, ensuring data integrity and traceability.
- **Proactive Threat Mitigation:** Focus on developing proactive measures to prevent cyber threats. This includes using blockchain to update machine learning models in real time, ensuring the system is always prepared for new and emerging threats.

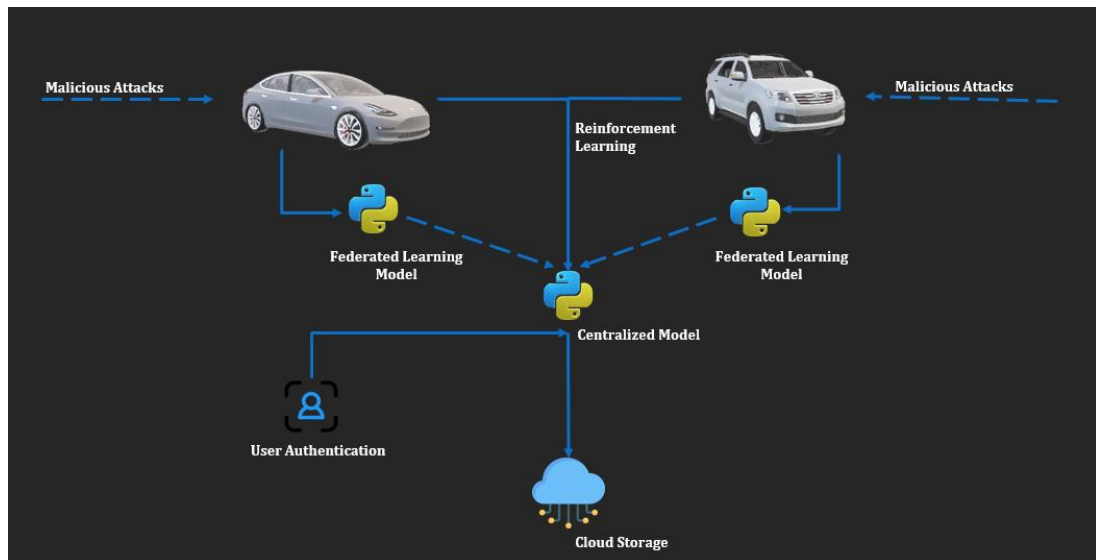


Figure 4 : Individual System Diagram

.7 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

.8 REFERENCES

- [1] G. Tewolde and B. Smith, "Small Scale Field Study of Vehicle-to-Vehicle (V2V) Communications for Safety Applications," 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.

.9 APPENDICES

.9.1 Gantt Chart

