SLIIT UNI
THE KNOWLEDGE UNIVERSITY

IT4010 – Research Project - 2024

Topic Assessment Form

Project ID: **24-25J-206**

1. Topic (12 words max)

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

2. Research group the project belongs to

Autonomous Intelligent Machines and Systems (AIMS)

3. Research area the project belongs to

Smart Systems (SS)

4. If a continuation of a previous project:

Project ID	-
Year	-

5. Brief description of the research problem including references (200 – 500 words max) – references not included in word count.

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 shows 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].

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.

6. Brief description of the nature of the solution including a conceptual diagram (250 words max)

To express the foundational pillars upon which our research (EagelEye) stands, we encapsulate its core within four key components:

Component 1: Secure Vehicle Communication with Hybrid Solutions

Utilizing advanced communication technologies and edge computing, this component aims to develop a hybrid communication protocol for real-time data exchange between vehicles and infrastructure. This protocol ensures low-latency and high-reliability communication essential for vehicular networks.

Component 2: Implement Privacy and Security Solutions in Hybrid Vehicular Networks

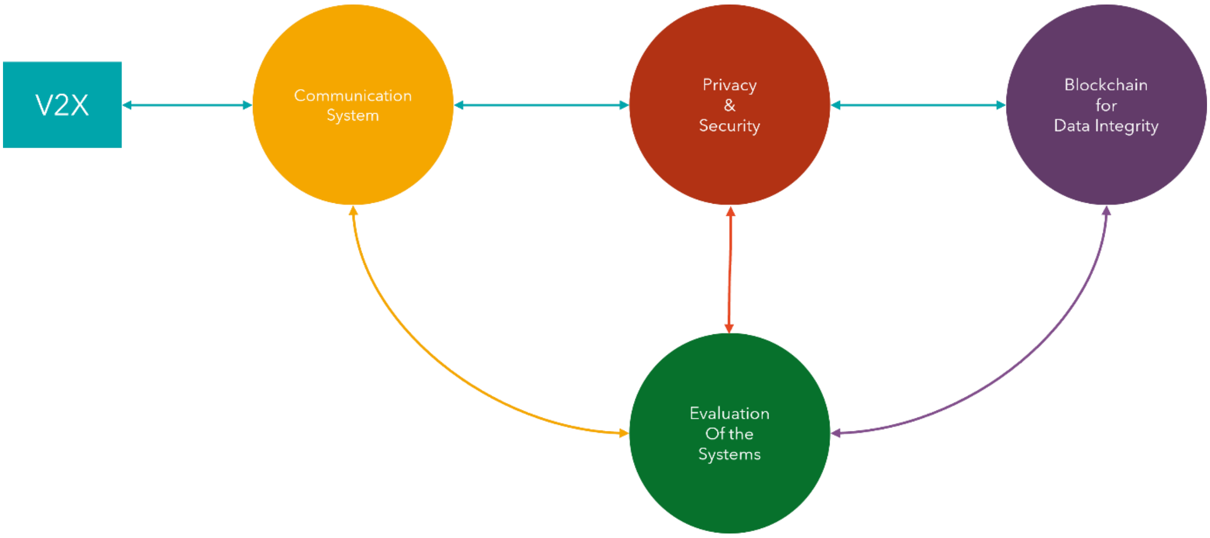
Addressing privacy and security concerns, this component develops encryption methods, access control mechanisms, and anonymization techniques to protect sensitive information during real-time communication and ensure data is secured. These measures safeguard the data against cyber threats and unauthorized access by using machine learning for ensure data privacy.

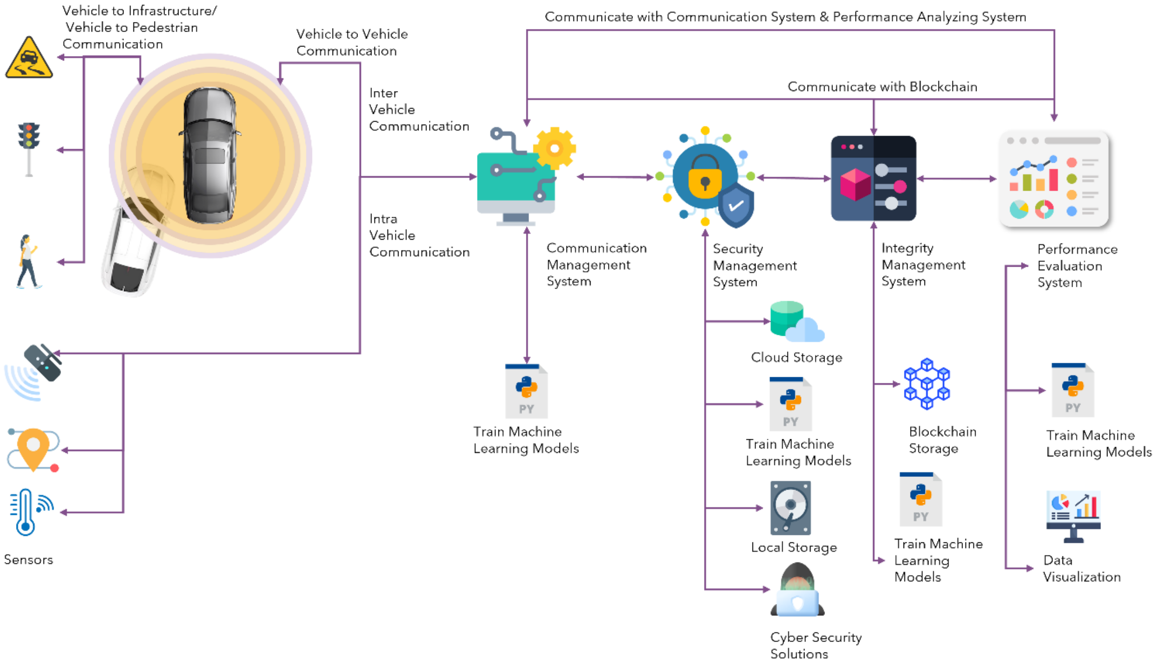
Component 3: Implement Data Integrity Solutions for Hybrid System

This component focuses on implementing blockchain technology to securely store and audit critical vehicular events. The blockchain's decentralized and immutable ledger ensures data integrity, providing a reliable audit trail for crucial events in vehicular networks and use machine learning strategies for reducing verification time of the blockchain.

Component 4: Evaluation of Performance in Hybrid Systems

This component evaluates the effectiveness of the hybrid approach combining advanced communication technologies and blockchain for secure data storage. It focuses on performance metrics such as data integrity, security, scalability, and resource efficiency. Optimization strategies are developed to enhance the performance of the blockchain system, ensuring it meets the demands of vehicular networks.


V2X
Communication System
Privacy & Security
Blockchain for Data Integrity
Evaluation Of the Systems


Vehicle to Infrastructure/ Vehicle to Pedestrian Communication
Vehicle to Vehicle Communication
Inter Vehicle Communication
Intra Vehicle Communication
Sensors
Communicate with Communication System & Performance Analyzing System
Communicate with Blockchain
Communication Management System
Train Machine Learning Models
Security Management System
Cloud Storage
Train Machine Learning Models
Local Storage
Cyber Security Solutions
Integrity Management System
Blockchain Storage
Train Machine Learning Models
Performance Evaluation System
Train Machine Learning Models
Data Visualization

7. Brief description of specialized domain expertise, knowledge, and data requirements (300 words max)

This research project explores the integration of blockchain technology in vehicular networks to securely store and audit critical events. To address the real-time communication limitations of blockchain, a hybrid approach is proposed, combining advanced communication technologies for immediate data exchange with blockchain for secure event logging. This approach enhances the security and reliability of vehicular networks, contributing to safer and more efficient transportation systems. Identifying cybersecurity solutions is another crucial aspect of the project aimed at enhancing security.

Blockchain Technology

Expertise in blockchain technology is essential for developing a secure and immutable data storage system. This includes understanding the principles of distributed ledgers, consensus mechanisms (e.g., Proof of Work (POW), Proof of Stake (POS)), and smart contracts. Also, the knowledge of blockchain platforms and implementing and customizing blockchain solutions tailored to vehicular networks is important.

Machine Learning and Artificial Intelligence

Proficiency in machine learning (ML) and artificial intelligence (AI) is vital for processing and analyzing large volumes of vehicular data. This includes expertise in supervised and unsupervised learning, neural networks, and predictive analytics. Skills in programming languages like Python and frameworks such as TensorFlow or PyTorch are necessary for developing and training ML models.

Vehicular Networks and Communication Protocols

In-depth knowledge of vehicular networks, including Vehicle-to-Everything (V2X) communication, is crucial. Understanding protocols like Dedicated Short-Range Communications (DSRC) and Cellular V2X (C-V2X) is necessary for designing real-time communication systems. Familiarity with Software-Defined Networking (SDN) and Edge Computing will also support the development of a dynamic and efficient vehicular communication network.

Cybersecurity and Data Privacy

Expertise in cybersecurity principles and data privacy regulations is required to ensure the secure handling of sensitive vehicular data. This includes knowledge of encryption techniques, secure access control mechanisms, and privacy-preserving data analytics.

Data Requirements

This project requires real-time vehicular data (speed, location, sensor readings), historical event data (collision records, traffic incidents), and simulation data from tools like SUMO and Veins. Additionally, blockchain transaction data (timestamps, cryptographic hashes, smart contract logs) is essential for monitoring and analyzing the blockchains system’s performance.

8. Objectives and Novelty

Main Objective

In vehicular communication systems, ensuring data integrity and secure communication is critical to safety and efficiency. Our project aims to leverage blockchain technology, cyber security strategies and machine learning to enhance the integrity and security of vehicular data. By creating a hybrid system that detects and records audit critical vehicular events. The novelty of our approach is integrating real-time event detection with secure data logging, offering a comprehensive solution for vehicular data management and security, even though there are research and applications for improvements of vehicular data security, there is no such application for identifying audit critical events for improving safety of the passengers using blockchain and hybrid strategies for secured vehicular communication.

Member Name	Sub Objective	Tasks	Novelty
Dissanayake D.J.R	Secure Vehicle Communication with Hybrid Solutions	In this preliminary step, data will be collected from intra vehicle communication (Sensors) and inter vehicle communication such as V2V, V2I, V2P using visible light, GPS, LiDAR systems and use machine learning for analyses and predict behavior and the critical events of the vehicles. Use blockchain critical event models for predictions of vehicle communication.	Hybrid Protocol: This protocol integrates traditional and modern communication methods, enabling real-time data exchange with secure logging via blockchain for train and enhance the efficiency of the models that used for object detection which used to vehicle to vehicle (V2V) communication and vehicle to pedestrian (V2P) communication and vehicle to infrastructure (V2I) communication.

Rizmaan M.F.M	Implement Privacy and Security Solutions in Hybrid Vehicular Networks	Use privacy techniques such as hashing, encryption and identify personal information using ML and use prevent cyber threats using preferred methods, use cloud, blockchain and system storage for minimizing the risk of data loss.	Advanced Privacy Techniques: Implementing encryption, access control, and anonymization and data storing strategies ensures robust privacy protection for users. By using machine learning, analyze network traffic, system logs and improve risk assessment and enhance situational awareness in manned and unmanned vehicles.
Kuhananth C	Implement Data Integrity Solutions	Implement smart contract, blockchain and use machine Learning for reducing verification time of the blocks, checking the data integrity through inter component communication and machine learning analyses.	Machine Learning Integration with blockchain data: ML algorithms analyze real-time vehicular data to detect anomalies and verify integrity before blockchain logging, enhancing security and using machine learning for reducing verification time of the blockchain.
Sulakkana H.D.S.R	Evaluation of Performance in Hybrid Systems	Conduct a performance analysis of the blockchain-based secure vehicle communication system by simulating a vehicular network. Measure key performance metrics such as latency, throughput,	we propose a novel approach to enhance security and reliability in blockchain-based systems through advanced anomaly detection and mitigation strategies. This component addresses three distinct challenges: detecting anomalies in electronic

		scalability, security, and data integrity. Optimize the system based on the findings and re-test to ensure improved performance. Use blockchain critical events logs for building accurate models.	transactions of cryptocurrencies, identifying fraudulent activities that compromise blockchain integrity, and analyzing the performance of Distributed Denial-of-Service (DDoS) attacks using blockchain-based blacklists. Leveraging machine learning algorithms such as One Class Support Vector Machines (OCSVM), K-Means, Support Vector Machines, Random Forest, and Decision Trees, we achieved high accuracy in detecting anomalies and classifying malicious activities.

9. Supervisor checklist

a) Does the chosen research topic possess a comprehensive scope suitable for a final-year project?

Yes	✓	No	

b) Does the proposed topic exhibit novelty?

Yes	✓	No	

c) Do you believe they have the capability to successfully execute the proposed project?

Yes	✓	No	

d) Do the proposed sub-objectives reflect the students' areas of specialization?

Yes	✓	No	

e) Supervisor's Evaluation and Recommendation for the Research topic:

The suggestions given by the TAF evaluation panel, have beed addressed by the students.

10. Supervisor details

	Title	First Name	Last Name	Signature
Supervisor	Mrs	Samadhi	Rathnayake	
Co-Supervisor	Mr.	Nelum	Amarasena	
External Supervisor				
Summary of external supervisor's (if any) experience and expertise				

***Important**:

1. According to the comments given by the panel, make the necessary modifications and get the approval by the **Supervisor** or the **Same Panel**.
2. If the project topic is rejected, identify a new topic, and follow the same procedure until the topic is approved by the assessment panel.