"Hybrid Intrusion Detection System for Enhanced Security in the Internet of Vehicles (IoV)"

A Project Report

Submitted By

EDUNOORI RAJESH-2203031260267

CH.SISINDHAR-2203031260029

LEELAPRASAD-2203031260274

SAI MADHAVA -2203031260129

in Partial Fulfillment For the Award

of the Degree of

BACHELOR OF TECHNOLOGY

COMPUTER SCIENCE &

ENGINEERING

Under the Guidance of

Prof. KRUPALI DEVI

Asst.Professor

VADODARA

April - 2026

PARUL UNIVERSITY

CERTIFICATE

This is to Certify that Project - 2 (303105300) of 7 Semester entitled “Hybrid Intrusion Detection System for Enhanced Security in the Internet of Vehicles (IoV)” of Group No. PU CSE-CS 16 has been successfully completed

by

EDUNOORI RAJESH-2203031260267

CH.SISINDHAR-2203031260029

LEELAPRASAD-2203031260274

SAI MADHAVA -2203031260129

under my guidance in partial fulfillment of the Bachelor of Technology (B.Tech) in Computer Science & Engineering of Parul University in Academic Year 2025- 2026.

Date of Submission :_ _ _ _ _ _ _ _ _

Prof. KRUPALI DEVI

Project Guide

Dr. AMIT BARVE
Head of Department,

CSE, PIET,

Parul University.

Project Coordinator:-

Acknowledgements

"The single greatest cause of happiness is gratitude."-Auliq-Ice

Certainly! In a more refined manner: "Throughout our significant endeavors, faced with numerous challenges and critical situations, this individual has been instrumental in bringing us closer to success. Working under the guidance of our esteemed mentor, Prof. KRUPALI DEVI mam, has been both an inspiration and a source of immense pride. Your ability to recognize potential in us that we hadn't seen in ourselves is truly an honor. Under Your mentorship, we have gained deeper insights into our capabilities."

student name-enrollment no:

EDUNOORI RAJESH-2203031260267
CH.SISINDHAR-2203031260029
LEELAPRASAD-2203031260274
SAI MADHAVA -2203031260129

PIET
Parul University,
Vadodara

Abstract

The use of autonomous vehicles (AVs) is a promising technology in Intelligent Transportation Systems (ITSs) to improve safety and driving efficiency. Vehicle-to-everything (V2X)technology enables communication among vehicles and other infrastructures.However, the rapid growth of IoV has also caused many security and privacy challenges that can lead to fatal accidents. To reduce smart vehicle accidents and detect malicious attacks in vehicular networks, several researchers have presented machine learning (ML)-based models for intrusion detection in IoT networks. However, a proficient and real-time faster algorithm is needed to detect malicious attacks in IoV. This article proposes a hybrid deep learning (DL) model for Cyber attack detection in IoV. The proposed model is based on long short-term memory (LSTM) and gated recurrent unit (GRU). The performance of the proposed model is analyzed by using two datasets—a combined D-DoS datasets that contains CIC DOS, CI-CIDS 2017, and CSE-CIC-IDS 2018, and a car-hacking Dataset. The experimental results demonstrate that the proposed algorithm achieves higher attack detection accuracy of 99.5% and 99.9% for D-DoS and car hacks, respectively. The other performance scores, precision, recall, and F1-score, also verify the superior performance of the proposed framework.

Keywords: deep learning; gated recurrent units; Internet of Things; Internet of Vehicles; long shortterm memory; machine learning

Table of Contents

Introduction

1.1 INTRODUCTION TO THE PROJECT

Internet of Things (IoT) is an advanced technology that connects smart devices to the internet, such as the Internet of Vehicles (IoV), wireless cameras, and other electronic devices. Due to the rapid increase of connected vehicles, several security and privacy challenges have been introduced . A basic framework for communications between vehicular networks is IoV . It establishes a dependable network transmission between vehicles. The IoV network consists of two sub-networks—intra-vehicle network and inter-vehicular network. The intra-vehicle network involves internal electronic devices and sensors of a vehicle, which are connected to a centralized controller for message transmission and performing a specific task . While an inter-vehicular network connects a vehicle to external devices using vehicle-to-everything (V2X) technology. V2X allows communication between vehicles and other communicative devices, such as signal antennas The security risks increase with the rapid growth in the connectivity of smart vehicles. An attack on the IoV network can affect stability, reliability, and cause accidents in vehicles. In June 2021, the World Health Organization (WHO) stated that every year 1.3 million deaths occur due to car accidents . In a real-life example, two hackers hacked a vehicle, took control of steering and brakes, and performed dangerous actions at high speed . During a cyber attack on a vehicle network, the attacker takes control of a vehicle, where he/she can perform dangerous stunts. A hacker has the ability to disable the brakes or jerk the steering wheel at a high speed, which may potentially lead to an accident. The attacker can also carry out a distributed denial of service (DDoS) attack, which engages the car controller area network (CAN) bus and prevents IoV-based vehicles from accessing the brakes at crucial times . DDoS attacks on inter-vehicle networks keep channels busy, such as not letting traffic signal lights turn red and keeping them green in dangerous places that may lead to accidents . An intrusion detection system (IDS) is needed to monitor

network traffic and detect malicious attacks. The performance of IDS depends on the accuracy of the detection algorithm. Improving the accuracy of IDS will reduce the false alarm rate. Existing IDS's have difficulty in improving performance and detecting unknown attacks. Machine learning (ML) techniques provide automated detection systems with impressive performance. Moreover, ML techniques have general capabilities to detect unknown attacks. Deep learning (DL) is a branch of ML, whose performance is remarkable. On the basis of performance, DL methods have become a research "hotspot" . The purpose of IDS is to identify different types of malicious network traffic and computer activities that a regular firewall might miss . From a trained set, ML can learn essential details. Moreover, ML algorithms handle nonlinear data and are easy to train .A generic cyber attack scenario on smart vehicles . Several researchers have suggested ML techniques for reducing issues related to smart vehicles. A proficient and fast algorithm is needed to detect malicious attacks in IoV. DL algorithms provide more efficient performances than traditional ML algorithms. For IDS, some commonly used DL algorithms are convolutional neural network (CNN), recurrent neural network (RNN), LSTM, and GRU. The CCN is more complex than other DL algorithms, because it requires data-like images in matrix form; the data must be normalized and converted into the form of an image matrix . The LSTM and GRU algorithms are effective at detecting malicious assaults over other ML and DL algorithms. Moreover, in IoV, some vehicles are connected for long time periods in which conventional ML models fail to convey long-term results. LSTM and GRU algorithms provide good accuracy in detecting malicious attacks

Chapter -2

Survey of Existing Literature

2.1 paper 1

* **Title**: ”Tree-based Intelligent Intrusion Detection System in Internet of Vehicles”

- **Author:** Li Yang

- **Abstract**: —The use of autonomous vehicles (AVs) is a promising technology in Intelligent Transportation Systems (ITSs) to improve safety and driving efficiency.Vehicle-to-everything (V2X) technology enables communication among vehicles and other infrastructures. However, AVs and Internet of Vehicles (IoV) are vulnerable to different types of cyber-attacks such as denial of service, spoofing, and sniffing attacks. In this paper, an intelligent intrusion detection system (IDS) is proposed based on tree-structure machine learning models. The results from the implementation of the proposed intrusion detection system on standard data sets indicate that the system has the ability to identify various cyber-attacks in the AV networks. Furthermore, the proposed ensemble learning and feature selection approaches enable the proposed system to achieve high detection rate and low computational cost simultaneously

- **Conclusion:** In conclusion, our research highlights This paper presents an Intrusion Detection System (IDS) using tree-based machine learning algorithms to secure vehicle networks against cyber-attacks. The approach improves accuracy, detection rate, and efficiency by addressing class imbalance and computational costs. Tested on CAN bus and external network datasets, the IDS outperforms existing methods, achieving up to 100% accuracy with significantly reduced computation time. Future improvements could involve hyper-parameter tuning through optimization techniques like particle swarm and Bayesian optimization.

2.2 paper 2

Title: ”MTH-IDS: A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles”

- Author: Abdallah Shami

Abstract: Modern vehicles, including connected vehicles and autonomous vehicles, nowadays involve many electronic control units connected through intra-vehicle networks to implement various functionalities and perform actions. Modern vehicles are also connected to external networks through vehicle-to-everything technologies, enabling their communications with other vehicles, infrastructures, and smart devices. However, the improving functionality and connectivity of modern vehicles also increase their vulnerabilities to Cyber-attacks targeting both intra-vehicle and external networks due to the large attack surfaces. To secure vehicular networks, many researchers have focused on developing intrusion detection systems (IDS’s) that capitalize on machine learning methods to detect malicious cyber- attacks. In this paper, the vulnerabilities of intra-vehicle and external networks are discussed, and a multi-tiered hybrid IDS that incorporates a signature-based IDS and an anomaly-based IDS is proposed to detect both known and unknown attacks on vehicular networks. Experimental results illustrate that the proposed system can detect various types of known attacks with 99.99% accuracy on the CAN-intrusion-dataset's representing the intra-vehicle network data and 99.88% accuracy on the CICIDS2017 Dataset's illustrating the external vehicular network data. For the zero-day attack detection, the proposed system achieves high F1-scores of 0.963 and 0.800 on the above two datasets, respectively. The average processing time of each data packet on a vehicle-level machine is less than 0.6 ms, which shows the feasibility of implementing the proposed system in real-time vehicle systems.

- **Conclusion:** This paper proposes a hybrid IDS combining signature-based and anomaly-based detection to secure vehicular networks from cyber-attacks. The system achieves high accuracy and efficiently detects both known and zero-day attacks in real-time environments.

2.3 paper 3

Title: ”Dynamic hierarchical intrusion detection system for internet of vehicle on edge computing platform”

- **Author:** Syed Sabir Mohamed S
- **Abstract:** In recent days, the Internet of Vehicles (IoV) and its network of connected automobiles have revealed several new security risks. Classical intrusion detection systems face challenges in identifying intrusions due to the growing number of vehicles, the dynamic nature of IoV, and limited resources. A hierarchical clustering method allows dividing the IoV network into clusters. The elements that determine the outcome are the geographical proximity and the traffic density. It is called the Dynamic Hierarchical Intrusion Detection Framework (DHIDF) for the IoV. To protect infrastructure and passengers, an IoV-specific DHIDF using edge computing has been proposed. Because of this, anomaly detection and localised assessment of danger will become less required. The application of DHIDF on a large scale inside the ecosystem of IoV is not entirely out of the question. The term encompasses several subfields, including intelligent transportation networks (ITNs), smart city infrastructure, fleet management, transportation, and autonomous vehicle systems. The efficacy of DHIDF is assessed through simulations that replicate current and potential future threats, including those related to the Internet of Things. Analysis of key performance parameters, including response time, detection accuracy, asset utilization, and scalability, has been conducted to assess the system's feasibility and durability. dataset.
- **Conclusion:** The DHIDF framework presents a promising solution for addressing security challenges in the IoV ecosystem. By leveraging clustering hierarchy, edge computing, and adaptive algorithms, it enhances detection accuracy, response speed, and overall network security. Its applications extend to fleet management, autonomous vehicles, smart cities, and IoT-based infrastructures. Future research should focus on improving its adaptability, integrating AI-driven detection mechanisms, and strengthening security with block-chain and privacy-preserving techniques to keep pace with evolving Cyber threats. abuse.

2.4 paper 4

Title: ”A hybrid deep learning based intrusion detection system using spatial-temporal representation in-vehicle network traffic”

- **Author:** Lo, Wei

  Abstract:A significant increase in the use of electronics control units (ECUs) in modern vehicles has made controller area network (CAN) a de facto standard in the automotive industry. CAN standard has been designed as a reliable and straightforward broadcast-based protocol for providing serial communication between ECUs without considering security aspects like authentication and encryption. Cyber attackers have exploited these vulnerabilities to mount a variety of attacks against CAN-based in-vehicle network. In this work, we proposed a hybrid deep learning-based intrusion detection system (HyDL-IDS) based upon spatial-temporal representation for characterizing in-vehicle network traffic accurately. For this purpose, we use convolutional neural network (CNN) and long short term memory (LSTM) in sequence for extracting spatial and temporal features automatically from in-vehicle network traffic. The proposed HyDL-IDS have been validated using a benchmark car-hacking data set. The reported results demonstrate approximately 100% detection accuracy with a low false alarm rate for different cyber-attacks, including denial-of-service (DoS) attacks, fuzzy attacks and spoofing (Gear and revolutions per minute (RPM)) attacks based on the identified dataset. The HyDL-IDS have significantly improved detection accuracy and false alarm rate for detecting intrusions in-vehicle network compared to other methods, namely Naive Bayes, Decision tree, Multi-layer perceptron, CNN, and LSTM based on spatial-temporal representation of in-vehicle network traffic.

- **Conclusion:** Technological advancements in the automotive industry have brought significant improvements in-vehicle systems and comfort. Electronic Control Units (ECUs) enhance safety and convenient driving in vehicles by sharing control data using in-vehicle networks with external services and internal communication over controller area network (CAN). CAN protocol was designed initially without considering security aspects as de facto standard in the automotive industry, leading to several cyber-attacks

2.5 paper 5

Title: ”Intrusion detection system for cyber attacks in the Internet of Vehicles environment”

- **Author:** Mohamed Selim Korium

- **Abstract:** This paper presents a novel framework for intrusion detection specially designed for cyberattacks, such as Denial-of-Service, Distributed Denial-of-Service, Distributed Reflection Denial-of-Service, Brute Force, Botnets, and Sniffing, on vehicles that are situated in the Internet of Vehicles environment. We propose an intrusion detection system based on machine learning that is capable of detecting abnormal behavior by examining network traffic to find unusual data flows. In this paper, we have presented a strategy for intrusion detection through a careful evaluation and selection of the most effective techniques for the following steps of the machine learning process: (i) data preprocessing by using Z-score normalization that preserves the data distribution for the proposed method and handles outliers; (ii) feature selection by using a regression model that simplifies the model complexity and reduces the execution time; and (iii) model selection and training – Random Forest, Extreme Gradient Boosting, Categorical Boosting, Light Gradient Boosting Machine – with hyperparameter optimization to control the behavior in the training phase and to prevent overfitting. The effectiveness of the proposed solution is demonstrated by extensive numerical experiments carried out using the well-known standard datasets CIC-IDS-2017, CSE-CIC-IDS-2018, and CIC-DDoS-2019, both separately and merged. We achieved a high accuracy above 99.8% within a running time of 46.9 s and 0.24 s detection time for the three combined intrusion detection system datasets, thereby showing that the proposed intrusion detection system outperforms the previous methods introduced in the literature.

- **Conclusion:** Vehicles in the Internet of Vehicles environment are vulnerable to various types of cyberattacks, which may cause a serious threat to human lives. Therefore, we need an efficient IDS to guarantee safe operations against cyberattacks. In this paper, we developed IDS models to detect cyberattacks in well-known imbalanced datasets that are related to the Internet of Vehicles environment