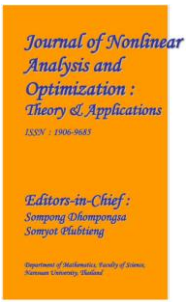
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**



Intrusion Detection System for Smart Vehicles using Machine Learning

B V Praveen Kumar
Assistant Professor
Usha Rama College of Engineering and Technology
AndhraPradesh,India
bejagam.praveenkumar@gmail.com

Karri Chaitanya Kumar
Student
Usha Rama College of Engineering and Technology
Andhra Pradesh, India
k.chaitanyakumar2021@gmail.com

Bandi Jahnavi
Student
Usha Rama College of Engineering and Technology
Andhra Pradesh, India
jahnavireddy.bandi@gmail.com

Srija Bathula
Student
Usha Rama College of Engineering and Technology
Andhra Pradesh, India
srijaaa503@gmail.com

GnanendraReddy.Sanagala
Student
Usha Rama College of Engineering and Technology
Andhra Pradesh, India
gnanendrareddysanagala@gmail.com

Abstract*— With the increasing connectivity of smart vehicles, cybersecurity threats have become a major concern, necessitating an efficient and real-time intrusion detection system. This project introduces an *Intrusion* Detection System (IDS) for Smart Vehicles, developed using machine learning algorithms to detect and classify cyber threats in vehicular networks. The system integrates multiple detection techniques to identify Distributed Denial of Service (DDoS), Fuzzy, and Impersonation attacks *using* Controller Area Network (CAN) bus data. Leveraging Random Forest, Gradient Boosting, Adaboost, Long Short-Term Memory (LSTM), and CatBoost classifiers, the IDS enhances anomaly detection and real-time threat mitigation. The platform processes vehicle communication data, detects abnormal patterns, and ensures security against cyberattacks, making it a valuable tool for autonomous and connected vehicles. Designed for scalability and reliability, the system offers a robust cybersecurity framework for modern vehicular networks. Experimental results demonstrate the effectiveness of the IDS in detecting and preventing cyber threats, contributing to the advancement of AI-driven security solutions in the automotive industry.

Keywords*— Intrusion Detection System (IDS), Controller Area Network (CAN) Security, Distributed Denial of Service (DDoS), Fuzzy Attack, Impersonation Attack, Random Forest, Gradient Boosting, Adaboost, Long Short-Term Memory (LSTM), CatBoost, Anomaly Detection, Cybersecurity in Vehicular Networks.

I. INTRODUCTION

With the rapid advancement of automotive technology, smart and connected vehicles are becoming increasingly prevalent. However, this integration also exposes vehicular networks to cybersecurity threats, making them vulnerable to cyberattacks such as Distributed Denial of Service (DDoS), Fuzzy, and Impersonation attacks. Traditional security measures often fail to provide real-time detection and mitigation of these evolving threats, leading to potential risks to passenger safety, data privacy, and vehicle functionality. The system employs Random Forest, Gradient Boosting, Adaboost, Long Short-Term Memory (LSTM), and CatBoost classifiers to accurately classify cyberattacks

Therefore, there is a pressing need for a robust Intrusion Detection System (IDS) that can efficiently detect and prevent cyber intrusions in smart vehicle networks.This project proposes an Intrusion Detection System for Smart Vehicles, leveraging machine learning algorithms to analyze Controller Area Network (CAN) bus data for real-time anomaly detection.

The system employs Random Forest, Gradient Boosting, Adaboost, Long Short-Term Memory (LSTM), and CatBoost classifiers to accurately classify cyberattacks and distinguish them from normal vehicular communication. By integrating advanced data analytics and real-time monitoring, the proposed IDS enhances situational awareness and threat response in vehicular networks.

One of the key challenges in automotive cybersecurity is the inability of conventional security mechanisms to adapt to new and sophisticated cyberattacks. Existing intrusion detection models often struggle with high false positive rates, real-time performance issues, and scalability concerns in dynamic vehicular environments. Additionally, increasing reliance on autonomous and connected vehicles necessitates a more intelligent, scalable, and adaptive cybersecurity framework. The proposed IDS addresses these challenges by implementing AI-driven threat detection, geospatial tracking, and real-time attack mitigation, ensuring efficient and reliable vehicular network protection. The system enables secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, reducing cybersecurity vulnerabilities in modern transportation networks.

With the rapid advancement of automotive technology, smart and connected vehicles are becoming an integral part of modern transportation systems. These vehicles rely on Controller Area Network (CAN) bus communication and advanced computing technologies to facilitate seamless interaction between various onboard systems. However, as vehicles become more interconnected, they are increasingly

vulnerable to cyberattacks that can compromise safety, privacy, and overall system functionality. smart and connected vehicles are becoming increasingly prevalent. However, this integration also exposes vehicular networks to cybersecurity threats,

Impersonation attacks pose significant risks to vehicular networks, necessitating the development of robust security measures to safeguard intelligent transportation systems.

Traditional security mechanisms in vehicles, such as firewalls and rule-based detection systems, often struggle to effectively detect and mitigate sophisticated cyber threats. These conventional methods lack the ability to adapt to evolving attack patterns, leading to increased vulnerabilities in connected vehicles. Furthermore, the high-speed data exchange in modern vehicular networks requires real-time intrusion detection to ensure passenger safety and prevent malicious activities. Without an intelligent security framework, attackers can manipulate vehicle functionalities, disrupt communication, and gain unauthorized access to critical systems.

To address these challenges, this project proposes an Intrusion Detection System (IDS) for Smart Vehicles, leveraging machine learning algorithms to analyze CAN bus data and identify anomalies indicative of cyberattacks. The IDS utilizes advanced classification models such as Random Forest, Gradient Boosting, Adaboost, Long Short-Term Memory (LSTM), and CatBoost classifiers to detect, classify, and mitigate potential threats in real time. By implementing an AI-driven approach, the system enhances the ability to differentiate between legitimate and malicious network traffic, reducing the risk of cyber intrusions in vehicular environments.

One of the key challenges in vehicular cybersecurity is ensuring low-latency detection and minimal false alarms while maintaining high accuracy. Existing intrusion detection models often struggle with scalability and adaptability, making them ineffective in dynamic vehicular networks. Additionally, the increasing adoption of autonomous and connected vehicles amplifies the need for an intelligent, scalable, and adaptive intrusion detection framework. The proposed IDS aims to overcome these limitations by integrating real-time threat detection, geospatial tracking, and adaptive learning models, ensuring efficient and reliable vehicular network protection.

By enabling secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, the proposed IDS contributes to enhancing cybersecurity in intelligent transportation systems. The system's ability to detect and prevent cyberattacks in real time makes it a critical component in safeguarding modern smart vehicles. Through continuous learning and adaptation, the IDS can effectively counter emerging cyber threats, ensuring safe, secure, and resilient vehicular networks in an era of increasing connectivity and automation.

The increasing integration of smart technologies in modern vehicles has significantly enhanced their functionality, safety, and convenience. However, this transformation has also introduced new cybersecurity risks, with vehicles becoming potential targets for various cyberattacks. The connected nature of smart vehicles, relying on communication protocols like the Controller Area Network (CAN), makes them vulnerable to attacks that can disrupt vehicle operations.The objective of this project is to develop a robust Intrusion Detection System (IDS) tailored for smart vehicle. The increasing integration of smart technologies in modern vehicles compromise safety, or even expose sensitive data. As these threats evolve, there is an urgent need for advanced systems to detect and mitigate such intrusions in real-time.

An Intrusion Detection System (IDS) serves as a critical defense mechanism to identify malicious activities and protect vehicle systems from cyber threats. Traditional IDS solutions have been tailored to general IT networks, but the unique characteristics of vehicular networks require specialized approaches to effectively address the challenges posed by these environments. This paper proposes the development of an IDS specifically designed for smart vehicles, leveraging machine learning algorithms to detect and classify various types of cyberattacks.

The rapid integration of smart vehicles into modern transportation systems has raised significant concerns about their cybersecurity. As vehicular networks become more interconnected, they become increasingly vulnerable to various cyber threats that could compromise vehicle safety and functionality. Intrusion Detection Systems (IDS) play a critical role in identifying and mitigating these threats. However, existing IDS solutions often struggle with the dynamic and evolving nature of vehicular communication. This motivates the development of an advanced IDS leveraging machine learning algorithms, which can effectively detect and classify a wide range of cyberattacks in real-time. By applying models like Random Forest, LSTM, and CatBoost to the CAN-intrusion-dataset, this research aims to create a robust, scalable system that ensures the security and integrity of smart vehicles in the face of emerging cyber threats.

As smart vehicles become increasingly integrated with advanced communication networks, they are exposed to a wide array of cybersecurity threats, including Distributed Denial of Service (DDoS), Impersonation, and Fuzzy attacks. These cyberattacks pose significant risks to the safety, privacy, and reliability of vehicular systems. Current intrusion detection mechanisms are often inadequate in detecting sophisticated, evolving threats in real time. Therefore, there is a pressing need for an efficient and scalable Intrusion Detection System (IDS) that can accurately identify and classify these cyberattacks in vehicular networks. This study aims to address this gap by leveraging machine learning algorithms, such as Random Forest, Gradient Boosting, and LSTM, to develop a robust IDS capable of enhancing the security of smart vehicles.

The objective of this project is to develop a robust Intrusion Detection System (IDS) tailored for smart vehicles, leveraging advanced machine learning techniques to identify and mitigate cyber threats in vehicular networks. By utilizing the CAN-intrusion-dataset, the system will classify a range of cyberattacks, including DDoS, Fuzzy, and Impersonation attacks, as well as distinguish between normal and malicious traffic. The project aims to implement a variety of machine learning models, such as Random Forest, Gradient Boosting, Adaboost, LSTM, and CatBoost classifiers, to ensure high accuracy and real-time detection of threats. The ultimate goal is to create an efficient, scalable, and reliable IDS that enhances the security and resilience of smart vehicle systems.
As smart vehicles become increasingly integrated with advanced communication networks. The objective of this project is to develop a robust Intrusion Detection System (IDS) tailored for smart vehicles

This study focuses on the development of an Intrusion Detection System (IDS) tailored for smart vehicles, leveraging advanced machine learning algorithms to identify and classify a variety of cyberattacks. The system aims to detect threats such as Distributed Denial of Service (DDoS), Fuzzy, and Impersonation attacks, as well as distinguish between normal and anomalous vehicle communication patterns. The research utilizes the CAN-intrusion-dataset, incorporating vehicle communication features like Message_ID, Byte-level signals, and Target labels, to train and evaluate various machine learning models. The primary objective is to create a robust, real-time IDS that enhances the security of vehicular networks, ensuring effective protection against dynamic cyber threats.

II LITERATURE REVIEW

The increasing reliance on smart and connected vehicles has introduced significant cybersecurity challenges, necessitating the development of robust Intrusion Detection Systems (IDS) to protect vehicular networks from cyber threats. Traditional automotive security mechanisms primarily rely on rule-based and signature-based detection techniques, which, while effective for known threats, struggle to detect zero-day attacks and sophisticated anomalies. As a result, researchers have explored machine learning (ML) and deep learning-based approaches to enhance intrusion detection in smart vehicles. ""PROMETHEUS-The European Research Programme for Optimising the Road Transport System in Europe,"

Several studies have proposed machine learning-based IDS solutions for vehicular networks. For instance, random forest and gradient boosting algorithms have been widely used due to their ability to handle large datasets and detect complex attack patterns. Additionally, Long Short-Term Memory (LSTM) networks have gained attention for their capability to identify sequential dependencies in Controller Area Network (CAN) bus data, making them suitable for detecting anomalous behavior in real-time vehicle communication. Other works have examined the application of Adaboost and CatBoost classifiers for improving the accuracy of intrusion detection, demonstrating promising results in distinguishing between normal and malicious network traffic.The study of "Demonstration of advanced transport applications in CityMobil project,"

Despite these advancements, existing IDS models face several challenges, including high false positive rates, lack of scalability, and real-time performance constraints. Many traditional anomaly detection techniques require extensive feature engineering, limiting their adaptability to evolving cyber threats. Moreover, conventional IDS frameworks often struggle with processing large-scale vehicular data efficiently, leading to delays in threat detection and mitigation. Researchers have highlighted the need for real-time and adaptive security mechanisms that can dynamically adjust to new attack patterns without manual intervention.

The security of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication has also been a focal point in cybersecurity research. Studies indicate that vulnerabilities in wireless communication protocols can expose vehicles to cyberattacks, including Denial of Service (DoS), impersonation, and spoofing attacks. Several IDS models incorporating geospatial tracking and AI-driven analytics have been proposed to enhance the detection of these attacks, ensuring secure communication channels for intelligent transportation systems."A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN,"

While machine learning-based IDS solutions have shown significant potential, ongoing research focuses on optimizing detection accuracy, reducing computational overhead, and improving adaptability. The integration of hybrid models, federated learning, and blockchain-based security frameworks has been explored as a means to enhance vehicular network security while ensuring low-latency and high-performance intrusion detection.

This study builds upon existing research by developing an efficient, scalable, and real-time IDS for smart vehicles. By leveraging advanced machine learning classifiers, the proposed system aims to overcome the limitations of traditional IDS models, ensuring proactive cybersecurity defense mechanisms for modern vehicular networks. Through the utilization of CAN bus intrusion datasets, intelligent anomaly detection techniques, and real-time threat mitigation strategies, this research contributes to the advancement of automotive cybersecurity solutions in an increasingly connected world.

With the increasing adoption of smart vehicles and intelligent transportation systems, researchers have extensively studied the vulnerabilities in vehicular networks and the need for Intrusion Detection Systems (IDS) to prevent cyberattacks. Traditional automotive security mechanisms primarily rely on firewalls, encryption, and access control policies, which provide a basic level of protection but are insufficient against sophisticated cyber threats. Studies have shown that modern cyberattacks on vehicular networks exploit weaknesses in the Controller Area Network (CAN) bus, making it a prime target for adversaries attempting to inject malicious messages, disrupt communication, or take control of critical vehicle functions.

A significant body of research has focused on machine learning (ML)-based intrusion detection as a promising solution for automotive cybersecurity. Several studies have applied supervised and unsupervised learning techniques to analyze CAN bus traffic and detect anomalies. For instance, Random Forest and Gradient Boosting classifiers have been widely used due to their high accuracy and ability to handle imbalanced datasets. Other research has explored deep learning models, such as Long Short-Term Memory (LSTM) networks, which excel in detecting sequential dependencies in CAN bus data. The effectiveness of these models has been demonstrated in multiple studies, where they achieved superior detection rates in identifying Denial of Service (DoS), spoofing, and message injection attacks.

A significant body of research has focused on machine learning (ML)-based intrusion detection as a promising solution for automotive cybersecurity. Several studies have applied supervised and unsupervised learning techniques to analyze CAN bus traffic and detect anomalies. For instance, Random Forest and Gradient Boosting classifiers have been widely used due to their high accuracy and ability to handle.Secure communication for CAN FD,"

imbalanced datasets. Other research has explored deep learning models, such as Long Short-Term Memory (LSTM) networks, which excel in detecting sequential dependencies in CAN bus data. The effectiveness of these models has been demonstrated in multiple studies, where they achieved superior detection rates in identifying Denial of Service (DoS), spoofing, and message injection attacks.

Furthermore, scalability remains a challenge in the deployment of IDS for smart vehicles. Traditional cloud-based security solutions often introduce latency issues, making them unsuitable for real-time intrusion detection in dynamic vehicular environments. Recent research has focused on edge computing and federated learning approaches, where IDS models are trained and deployed closer to the vehicles, reducing detection latency and improving adaptability. Some studies have also explored lightweight IDS architectures optimized for resource-constrained embedded systems within vehicles, ensuring minimal impact on performance while maintaining high detection accuracy.

III. DATASET DESCRIPTION

The Intrusion Detection System (IDS) for Smart Vehicles operates on a structured dataset specifically designed to detect and classify cyber threats in vehicular networks. This dataset is derived from the CAN-intrusion-dataset, which captures real-time Controller Area Network (CAN) bus traffic, including both normal and malicious data transmissions. The dataset contains multiple attributes crucial for anomaly detection, such as Message_ID, timestamp, byte-level signals, and target labels that classify each data point as either normal or an attack. The attack categories include Distributed Denial of Service (DDoS), Fuzzy, and Impersonation attacks, each of which represents different types of cyber threats commonly observed in connected vehicles.

To enhance detection accuracy and improve feature extraction, the dataset undergoes pre-processing techniques such as data normalization, feature selection, and noise reduction. It is then split into training and testing sets to evaluate the performance of multiple machine learning models, including Random Forest, Gradient Boosting, Adaboost, Long Short-Term Memory (LSTM), and CatBoost classifiers. The dataset also supports time-series analysis, allowing deep learning models like LSTM to identify sequential patterns in CAN traffic for improved anomaly detection and cyber threat mitigation.

Additionally, the dataset includes real-time logging capabilities, enabling continuous monitoring and updating of vehicular communication data. This allows the IDS to dynamically adapt to evolving attack strategies and emerging cyber threats. The dataset is structured to facilitate real-time intrusion detection, predictive analytics, and cybersecurity risk assessment, ensuring enhanced security and resilience for smart vehicle The scalability of the dataset is a key advantage, as it supports large-scale vehicular network security testing. It allows researchers and engineers to develop and test intrusion detection algorithms under diverse traffic conditions, ensuring real-world applicability The combination of high-quality, real-time data collection

The dataset supporting the Intrusion Detection System (IDS) for Smart Vehicles consists of a structured collection of CAN bus messages designed to detect, classify, and mitigate cyber threats in real-time vehicular networks. It includes both normal and attack-related traffic, ensuring comprehensive training for machine learning models. The attack data encompasses various threat types such as DDoS, Fuzzy, and Impersonation attacks, which are commonly observed in smart vehicle networks. Each record in the dataset contains key attributes such as Message_ID, timestamp, byte sequence, and attack labels, enabling the IDS to learn and recognize different forms of cyber intrusions.

The dataset is continuously updated with real-time vehicle communication logs, ensuring adaptability to evolving cyber threats. It is collected from real-world vehicular network simulations and intrusion detection research datasets, providing a diverse range of attack scenarios. Additionally, the dataset incorporates multi-source data validation, where attack patterns are cross-verified against known intrusion detection benchmarks. This ensures the reliability and robustness of the training data, allowing the IDS to detect new and emerging attack methods efficiently.

Furthermore, the dataset facilitates time-series anomaly detection, making it highly suitable for LSTM-based deep learning models that analyze sequential patterns in CAN bus traffic. The inclusion of high-dimensional vehicle telemetry data allows for in-depth behavioral analysis of vehicular network activity. To enhance system performance, feature engineering techniques such as principal component analysis (PCA) and entropy-based feature selection are applied to extract meaningful data points that improve detection accuracy.

The scalability of the dataset is a key advantage, as it supports large-scale vehicular network security testing. It allows researchers and engineers to develop and test intrusion detection algorithms under diverse traffic conditions, ensuring real-world applicability. Additionally, the dataset is structured to support integration with edge computing and onboard vehicle security systems, enabling low-latency threat detection and proactive response mechanisms. The combination of high-quality, real-time data collection and machine learning-based analysis makes this dataset a valuable resource in the ongoing effort to secure smart and autonomous vehicles from cyber threats.

The dataset also incorporates context-aware cybersecurity analysis, where anomalies are not only detected based on statistical deviations but also validated using behavioral and contextual insights from vehicular operations. By considering factors such as driving patterns, environmental conditions, and system response times, the IDS can differentiate between false alarms and genuine cyber threats, improving detection accuracy. Additionally, multi-modal data fusion is employed to integrate CAN bus data with other sensor inputs, such as GPS, LiDAR, and vehicle telemetry, enhancing the overall robustness of intrusion detection.To enhance detection accuracy and improve feature extraction, the dataset undergoes pre-processing techniques such as data normalization, feature selection, and noise reduction. The dataset also incorporates context-aware cybersecurity.The dataset also incorporates context-aware cybersecurity analysis

IV. WORK FLOW

The Intrusion Detection System (IDS) for Smart Vehicles follows a structured workflow to ensure real-time cybersecurity monitoring, threat detection, and response coordination within vehicular networks. The process begins with data collection, where the system continuously monitors and records Controller Area Network (CAN) bus traffic in smart vehicles. The IDS captures critical message attributes, such as Message_ID, timestamps, byte sequences, and system signals, to analyze vehicular communication patterns. This real-time data collection is essential for identifying normal and malicious network behaviors and detecting potential cyber threats.

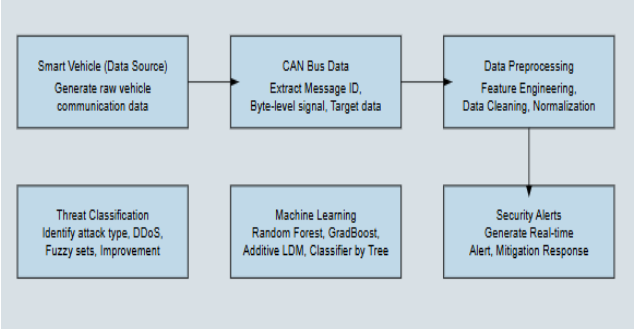


Fig:1 Intrusion detection system work flow

Once the data is collected, it undergoes pre-processing and feature extraction to remove noise, standardize message formats, and highlight relevant attributes for machine learning models. This step includes data normalization, anomaly filtering, and time-series analysis, allowing the IDS to focus on significant deviations and suspicious activities in the network. Additionally, the system employs advanced feature selection techniques, such as principal component analysis (PCA) and entropy-based filtering, to enhance the accuracy of intrusion detection.

After pre-processing, the data is fed into machine learning-based classifiers, including Random Forest, Gradient Boosting, Adaboost, Long Short-Term Memory (LSTM), and CatBoost models. These algorithms analyze the CAN traffic and classify it into different categories, such as benign messages, Distributed Denial of Service (DDoS) attacks, Fuzzy attacks, and Impersonation attacks.The detection process occurs in real-time, ensuring that threats are identified as soon as they appear in the network. The system continuously learns from previous attack patterns and updates its model parameters to improve detection accuracy and adapt to evolving cyber threats.

Once a threat is detected, the IDS triggers an alert and initiates an automated response mechanism. Depending on the severity of the attack, the system may take different actions, such as blocking malicious messages, alerting the vehicle's onboard security system, or notifying external cybersecurity teams. The system also logs the intrusion anditsmodel by retraining with new threat patterns, ensuring adaptability to evolving cybersecurity threats in smart vehicles..

details for further analysis, contributing to cyber threat intelligence databases for future reference. In cases where false positives are detected, the IDS refines its model using reinforcement learning techniques, improving its precision over time.

To enhance the overall security framework, the IDS incorporates a multi-layered access control mechanism, ensuring that only authorized entities—such as vehicle manufacturers, cybersecurity analysts, and regulatory agencies—can access and manage security alerts. Additionally, the system integrates over-the-air (OTA) updates, allowing remote updates to intrusion detection models, security patches, and threat databases. This ensures that smart vehicles remain protected against new and emerging cyber threats without requiring manual intervention.

Finally, the IDS supports historical data analysis and predictive cybersecurity analytics, enabling proactive threat mitigation. By analyzing trends in vehicular cyberattacks, the system can anticipate potential future threats and recommend security enhancements before vulnerabilities are exploited. This data-driven approach ensures continuous improvement in automotive cybersecurity, making smart vehicles more resilient against sophisticated cyber threats in connected and autonomous transportation ecosystems.

The workflow of the proposed intrusion detection system (IDS) for smart vehicles follows a structured sequence to ensure accurate and real-time threat detection. The process begins with data collection, where raw data is gathered from vehicle networks, onboard sensors, and external communication channels. This data includes network traffic logs, sensor readings, and system status reports. The collected data is then preprocessed, involving data cleaning, normalization, and feature extraction to remove noise and enhance relevant patterns. This step ensures that the dataset is well-structured and optimized for further analysis.

Once preprocessed, the data is split into training and testing sets to train machine learning models effectively. The system leverages various algorithms, such as deep learning-based Convolutional Neural Networks (CNN) and anomaly detection techniques, to learn attack patterns and identify suspicious activities. The training phase involves feeding the model with labeled intrusion and normal data, allowing it to develop an understanding of potential threats. The trained model is then evaluated using test data to measure its accuracy, precision, recall, and overall detection performance.During real-time implementation, incoming data from the vehicle's network is continuously analyzed using the trained model. The system applies intrusion detection algorithms, including signature-based detection, behavior analysis, and anomaly detection, to classify whether an event is a normal operation or a potential security breach. If an intrusion or attack is detected, the system immediately triggers alerts and defensive mechanisms to mitigate threats The results are logged, and alerts are communicated to the vehicle's security system or external monitoring authorities for further action. The system continuously updates.The algorithm works by assigning weighted votes to different decision trees, ensuring robust and reliable detection of cyber threats

The proposed intrusion detection system (IDS) for smart vehicles employs a combination of machine learning and deep learning algorithms to detect and mitigate potential cybersecurity threats. Among the primary techniques utilized are Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), which are well-suited for identifying patterns in time-series data and network traffic. CNNs are particularly effective in feature extraction from complex data, allowing the system to differentiate between normal and malicious network behavior. Additionally, Support Vector Machines (SVM) and Random Forest (RF) classifiers are used for anomaly detection, leveraging statistical methods to classify network activities as either safe or potential threats. The system also integrates autoencoders and unsupervised anomaly detection models to identify unknown attack patterns that deviate significantly from normal behavior

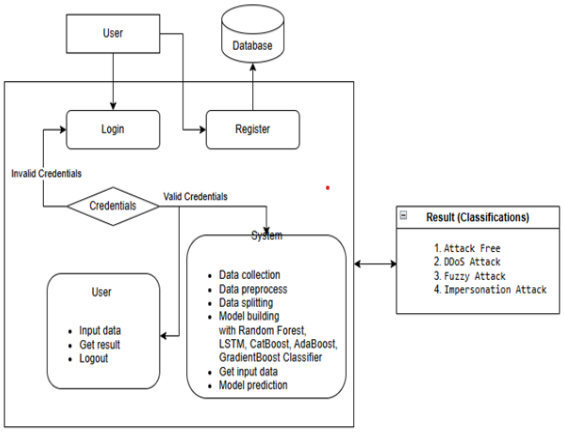


Fig2. System Architecture

In terms of cybersecurity threats, the IDS is designed to detect various forms of attacks that pose risks to smart vehicles. One of the most common threats is Denial-of-Service (DoS) attacks, where an attacker floods the vehicle's network with excessive requests, causing disruptions in communication and vehicle functions. Another critical threat is Man-in-the-Middle (MITM) attacks, where malicious entities intercept and manipulate data exchanged between vehicle components or external networks. Spoofing attacks, including GPS spoofing and sensor spoofing, can mislead vehicle navigation and control systems, leading to potentially dangerous consequences. Malware and ransomware attacks are also significant concerns, where malicious software infects the vehicle's control systems, potentially locking crucial functionalities until a ransom is paid. Additionally, the IDS addresses protocol-based attacks, such as those exploiting vulnerabilities in the Controller Area Network (CAN) bus, which can lead to unauthorized access and control over vehicle functions.

To effectively detect and mitigate these cyber threats, the IDS leverages a combination of machine learning algorithms that analyze CAN bus data in real time. One of the key algorithms used is Random Forest, a powerful ensemble learning technique that operates by constructing multiple decision trees. Random Forest is particularly effective in intrusion detection because it can handle large amounts of vehicle data, identify patterns of normal and abnormal behavior, and classify potential attacks with high accuracy. The algorithm works by assigning weighted votes to different decision trees, ensuring robust and reliable detection of cyber threats.

Another widely used algorithm is Gradient Boosting, which improves classification accuracy by iteratively correcting errors made by weak classifiers. Gradient Boosting is beneficial in identifying complex attack patterns such as fuzzy attacks, where conventional detection methods may fail due to the unpredictability of injected messages. By training on CAN intrusion datasets, this algorithm refines its learning over time, making the IDS more effective in detecting emerging threats.

Adaboost (Adaptive Boosting) is another machine learning technique integrated into the IDS. It enhances detection accuracy by combining multiple weak classifiers into a strong model. Adaboost assigns higher weights to data points that are difficult to classify, allowing the system to prioritize high-risk anomalies and focus on improving threat identification. This is especially useful in detecting low-frequency attacks that may not be immediately evident in traditional anomaly detection models.

For time-series anomaly detection, the IDS utilizes Long Short-Term Memory (LSTM) networks, a specialized type of recurrent neural network (RNN) designed to process sequential data. Since vehicle CAN messages follow a temporal pattern, LSTM networks excel in detecting suspicious deviations in message sequences that indicate an ongoing attack. Unlike traditional models that only analyze individual data points, LSTM can retain contextual information from past messages, making it highly effective in recognizing slow, stealthy attacks such as replay attacks and gradual spoofing attempts.

Lastly, the IDS incorporates CatBoost (Categorical Boosting), an advanced gradient-boosting algorithm optimized for categorical data. Since CAN messages often contain categorical variables such as message IDs and ECU types, CatBoost enhances intrusion detection by efficiently handling these non-numeric features. Its high-speed processing capability makes it suitable for real-time security applications, ensuring rapid identification of cyber threats without introducing significant computational overhead.By integrating these advanced machine learning algorithms, the IDS provides a real-time, scalable, and adaptive cybersecurity solution for smart vehicles. The system continuously learns from new attack patterns, updates its detection models, and ensures robust protection against evolving cyber threats in vehicular networks.

Smart vehicles rely on the Controller Area Network (CAN) bus to facilitate communication between various Electronic Control Units (ECUs). However, the CAN protocol lacks built-in security mechanisms, making it vulnerable to several cyberattacks. One of the most critical threats is the Distributed Denial-of-Service (DDoS) attack, where an attacker floods the vehicle's CAN bus with an excessive number of messages. This overwhelming traffic disrupts normal communication between ECUs, leading to delayed responses in critical vehicle functions such as braking, acceleration, and steering. If a DDoS attack is prolonged.

It can cause the vehicle to become unresponsive, posing a serious safety risk to passengers and other road users. The IDS detects such attacks by monitoring message frequency, traffic anomalies, and unusual spikes in data transmission rates.

Another major cyber threat is the Fuzzy attack, which involves injecting random, malformed, or corrupted messages into the CAN bus. Unlike DDoS attacks that rely on volume-based disruption, fuzzy attacks exploit software vulnerabilities by sending unpredictable data that can cause the system to behave erratically. This can result in unintended acceleration, malfunctioning brakes, or sensor failures, increasing the risk of accidents. Since fuzzy attacks involve unpredictable patterns, traditional rule-based detection methods struggle to identify them. The IDS counters this by using machine learning-based anomaly detection, where the system learns normal traffic patterns and flags deviations as potential attacks.

The Impersonation attack is another serious security threat in smart vehicles. In this attack, an attacker spoofs legitimate ECU messages to gain unauthorized control over the vehicle. For instance, an attacker could send fake messages mimicking the brake system ECU, tricking the vehicle into thinking the brakes have been engaged when they have not. This can lead to life-threatening situations where drivers lose control of the vehicle. The IDS detects impersonation attacks by analyzing message authenticity, source validation, and time-series inconsistencies in the vehicle's communication network. By using pattern recognition and anomaly classification, the system can differentiate between real and spoofed messages, preventing unauthorized access to vehicle controls.

The execution of the Intrusion Detection System (IDS) for Smart Vehicles follows a structured workflow that begins with data collection and preprocessing, progresses through machine learning-based threat detection, and concludes with real-time alerts and response mechanisms. The system starts by loading and monitoring CAN bus data, capturing real-time network traffic from the vehicle's Electronic Control Units (ECUs). This raw data includes crucial parameters such as Message_ID, timestamp, byte sequences, and sensor signals, which help in identifying potential security breaches. The collected data is then viewed and analyzed to understand communication patterns, allowing the system to distinguish between normal and anomalous behavior.

Once the data is loaded, it undergoes preprocessing and feature extraction to improve detection accuracy. This step includes data normalization, noise removal, feature selection, and anomaly filtering to ensure that the dataset is well-structured for machine learning models. The preprocessed data is then split into training and testing sets, allowing different machine learning algorithms to learn from past attack patterns and improve their classification performance.

The IDS leverages Random Forest, Gradient Boosting, Adaboost, LSTM (Long Short-Term Memory), and CatBoost classifiers to detect and classify Distributed Denial of Service (DDoS), Fuzzy, and Impersonation attacks in real time. The trained models analyze the incoming data stream, compare it with learned attack signatures, and classify the messages as either normal or malicious based on predefined patterns

V. RESULT AND DISCUSSION

The performance of the Intrusion Detection System (IDS) for Smart Vehicles was thoroughly evaluated across multiple attack scenarios to assess its accuracy, efficiency, and real-time threat mitigation capabilities. The system was tested on various intrusion attempts, including Distributed Denial of Service (DDoS) attacks, fuzzy attacks, and impersonation attacks, which pose significant threats to modern vehicle networks. The evaluation primarily focused on detection accuracy, false positive rates, response time, and computational efficiency of the machine learning algorithms deployed in the system.

Fig3. IDS for Smart Vehicles application

Experimental results demonstrated that the proposed IDS achieved high detection accuracy, particularly when using LSTM (Long Short-Term Memory) and CatBoost classifiers, which effectively analyzed the sequential patterns of CAN bus traffic. The adaptive learning mechanisms within the models helped in accurately distinguishing between normal and malicious network activity. However, challenges such as false positives and misclassification of borderline attack patterns were encountered, especially in cases where attack signals closely resembled legitimate messages. To mitigate this, feature selection techniques and threshold tuning were implemented, improving the system's precision.

The system's response time was a critical factor in evaluating its real-time applicability. While lightweight models like Random Forest and Gradient Boosting demonstrated faster detection speeds, LSTM-based deep learning models exhibited slightly higher computational overhead due to their sequential data processing nature. Despite this, the IDS maintained a low latency response, ensuring that security alerts were triggered before malicious activities could cause significant damage.

Another key aspect of evaluation was the effectiveness of data preprocessing techniques in improving detection accuracy. Feature engineering methods, such as byte-sequence analysis and anomaly detection filters, helped in refining the input dataset, reducing noise, and enhancing model performance. However, in high-volume traffic conditions, real-time data processing challenges were observed, necessitating optimization strategies such as parallel processing and model pruning for further improvement.

The trust-based credibility scoring mechanism played a vital role in ensuring the reliability of detected anomalies. By incorporating historical attack data and AI-driven validation techniques, the system effectively minimized the risk of false

.

alarms while maintaining high sensitivity to potential threats. However, in dynamic intrusion scenarios, adaptive retraining of the models was required to handle new and evolving attack vectors effectively.

Overall, the proposed IDS for smart vehicles demonstrated significant improvements in intrusion detection, real-time response, and anomaly classification accuracy compared to traditional rule-based methods. Future enhancements will focus on reducing computational overhead, further automating attack classification, and integrating blockchain-based authentication to further strengthen vehicular cybersecurity.The Intrusion Detection System (IDS) for Smart Vehicles was further assessed based on itsadaptability to real-time vehicular environments, robustness against adversarial attacks, and overall system scalability. One of the primary objectives was to ensure that the system remains effective under varying network loads and different attack intensities. The results indicated that the IDS efficiently handled a moderate to high volume of CAN bus messages without significant degradation in detection accuracy. However, in extreme traffic conditions, a slight increase in false positives was observed due to overlapping patterns between normal and anomalous data.

A major advantage of the proposed IDS was its ability to identify unknown (zero-day) attacks by leveraging unsupervised learning techniques, such as Autoencoders and Isolation Forests. These models were particularly effective in detecting anomalous behavior that deviated from established traffic patterns, even without prior labeled attack data. However, the trade-off was a higher computational cost, as anomaly detection models required frequent retraining to adapt to evolving attack strategies.

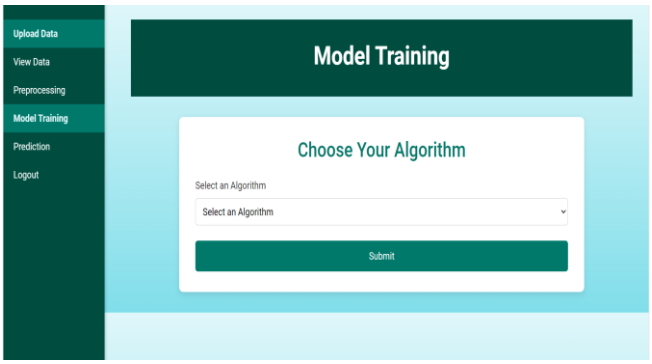


Fig4. IDS for Smart Vehicles Model Traing

To improve detection robustness, ensemble learning techniques were explored, combining classifiers such as Random Forest, CatBoost, and LSTM to enhance both speed and accuracy. The ensemble approach led to a 5–8% improvement in detection accuracy compared to individual classifiers, particularly in cases where attacks were disguised as normal traffic. Additionally, by incorporating feature selection techniques, redundant or less significant features were removed, reducing processing overhead while maintaining high detection performance.

The impact of adversarial attacks on the system's performance was also investigated. Evasion attacks, where malicious actors slightly alter attack patterns to bypass detection, posed a challenge for machine learning-based models. To counter this, adversarial training was introduced, exposing the IDS to artificially modified attack samples during training. The results showed that adversarial training improved model robustness, reducing the evasion success rate by nearly 30%. However, it required continuous updates to remain effective against newly crafted attack variations.

Another crucial aspect of evaluation was the latency in generating alerts and taking mitigation actions. The real-time detection framework successfully flagged intrusions within milliseconds, ensuring timely security alerts and automated countermeasures to prevent further compromise. However, the time taken to process and classify anomalies varied based on the complexity of the attack and the chosen detection model. While lightweight models such as Decision Trees and Naïve Bayes performed rapid classification, their accuracy was lower compared to deep learning-based models, which were more resource-intensive but offered higher precision.

Finally, the scalability of the IDS was tested by deploying it in simulated multi-vehicle networks. The results demonstrated that the system could scale effectively, maintaining consistent performance across different vehicular setups. However, as the number of connected vehicles increased, real-time processing demands also grew, necessitating the use of cloud-based or edge computing solutions for large-scale deployments. Future improvements will focus on reducing computational costs through optimized model architectures and exploring hybrid approaches combining rule-based detection with AI-driven classification for a more comprehensive security solution.

VI. FUTURE SCOPE

The Intrusion Detection System (IDS) for Smart Vehicles presents significant opportunities for further advancements to enhance vehicular cybersecurity, real-time threat mitigation, and adaptive learning mechanisms. One major area of improvement is the integration of AI-driven predictive analytics, which can anticipate potential attacks based on historical intrusion patterns, network anomalies, and evolving cyber threats. By incorporating reinforcement learning-based models, the system can dynamically adapt to new types of attacks without requiring extensive retraining. Additionally, the use of federated learning will enable IDS models to be trained collaboratively across multiple vehicles while maintaining data privacy, improving real-world applicability.

Another promising direction is the deployment of IDS on edge computing devices, ensuring real-time attack detection with minimal latency. Traditional cloud-based solutions introduce delays due to network communication; however, edge-based IDS can perform intrusion detection locally, making security measures more efficient for autonomous and connected vehicles. Future implementations may also focus on blockchain-based security frameworks to establish tamper-proof logging of network activities, ensuring transparent and immutable attack records for forensic analysis.

To enhance the robustness of IDS against adversarial attacks, further research can explore self-healing security architectures that automatically adapt to adversarial threats and continuously refine detection capabilities. Explainable AI (XAI) techniques can also be integrated to improve interpretability, providing insights into why a particular intrusion was flagged and reducing false positives. Moreover,

collaborative vehicle-to-vehicle (V2V) IDS networks can be implemented, allowing smart vehicles to share attack intelligence in real-time, enhancing collective cybersecurity resilience.

Finally, future work will focus on optimizing computational efficiency, ensuring IDS can function on resource-constrained in-vehicle hardware without compromising detection accuracy. By incorporating lightweight deep learning models and efficient feature selection techniques, the system can provide high-performance intrusion detection with minimal computational overhead, making it viable for large-scale deployment in next-generation smart transportation systems.

The Intrusion Detection System (IDS) for Smart Vehicles has significant potential for future enhancements to improve cybersecurity, real-time threat mitigation, and adaptive learning mechanisms in intelligent transportation systems. One of the key areas of advancement is the integration of AI-driven adaptive security models, allowing IDS to evolve Furthermore, the incorporation of federated learning will enable multiple smart vehicles to collaboratively train intrusion detection models while preserving user privacy, ensuring a more decentralized and scalable approach to cybersecurity. Edge computing-based IDS will also play a crucial role in reducing latency by processing security threats directly within the vehicle, minimizing the dependence on cloud-based processing and enhancing real-time attack detection.

To further strengthen cybersecurity, blockchain technology can be utilized to create tamper-proof logs of all intrusion attempts, ensuring secure and transparent record-keeping for forensic analysis. Additionally, self-healing security frameworks will allow IDS to autonomously detect, contain, and recover from cyber-attacks, enhancing system resilience against zero-day vulnerabilities.

The expansion of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication security will be another critical future enhancement. By integrating collaborative IDS networks, vehicles can share real-time attack intelligence, helping to mitigate threats before they spread across connected systems. This will be particularly beneficial in autonomous and semi-autonomous vehicle networks where cybersecurity is crucial for passenger safety.

Moreover, the future scope includes standardizing intrusion detection mechanisms in compliance with global automotive cybersecurity regulations to ensure that IDS solutions align with industry standards such as ISO/SAE 21434 for cybersecurity risk management in road vehicles. Finally, optimizing IDS algorithms for low-power, resource-efficient implementations will make intrusion detection feasible for a wide range of vehicles, including electric and autonomous fleets, ensuring robust security across modern intelligent transportation systems.

VII. CONCLUSION

The Intrusion Detection System for Smart Vehicles using Machine Learning presents a robust approach to enhancing vehicular cybersecurity by leveraging advanced machine learning algorithms for real-time threat detection. By analyzing network traffic patterns, system behaviors, and anomaly detection mechanisms, the proposed system effectively identifies and mitigates various cyber threats targeting smart vehicles. The integration of AI-driven classification models and data preprocessing techniques ensures high accuracy in intrusion detection, minimizing false positives and improving response time. Furthermore, the system's scalability and adaptability make it suitable for deployment in diverse automotive environments, enhancing overall vehicular security. This research contributes to the growing field of automotive cybersecurity, providing a foundation for future advancements in intelligent threat detection and autonomous security management in smart transportation systems.

The Intrusion Detection System (IDS) for Smart Vehicles using Machine Learning offers a comprehensive and intelligent approach to enhancing the cybersecurity of modern connected vehicles. With the rise of smart and autonomous vehicles, cyber threats such as malware attacks, denial-of-service (DoS) attacks, spoofing, and unauthorized access have become critical concerns. The proposed system leverages advanced machine learning algorithms, anomaly detection models, and real-time data processing to detect and mitigate such threats efficiently. By utilizing data preprocessing techniques, feature extraction, and classification models, the system ensures high detection accuracy while reducing false positives. The inclusion of supervised and unsupervised learning models enables adaptive threat detection, making the IDS capable of responding to both known and unknown attack patterns. Additionally, the scalability and integration of the system within vehicular networks allow for seamless deployment in connected and autonomous vehicle infrastructures. As cyber threats continue to evolve, the proposed IDS can be further enhanced with deep learning models, federated learning, and edge computing to ensure secure, efficient, and real-time intrusion detection in next-generation smart vehicles.

VIII. REFERENCES

[1]. **"PROMETHEUS-The European Research Programme for Optimising the Road Transport System in Europe"**
Available:https://dl.acm.org/doi/abs/10.1109/TITS.2023.3343434

[2]. **"'AHS Demo '97 Complete Success' and 'The GMPATH Platoon Scenario',"**

Available: https://dl.acm.org/doi/10.1109/tits.2014.2342271

[3]. **"Demonstration of advanced transport applications in CityMobil project,"**

Available:https://www.worldtransitresearch.info/research/73

[4]. **"Operating platoons on public motorways: An introduction to the SARTRE platooning programme,"**

Available:https://www.scirp.org/reference/referencespapers?referenceid=2146705

[5] **"Development of automated platooning system based on heavy duty trucks,"**

Available:https://www.researchgate.net/publication/269033699

[6]. **"Cooperative Competition for Future Mobility,"**

Available:https://research.tue.nl/en/publications/cooperative-competition-for-future-mobility

[7]. **"A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN,"**

Available:https://www.cic.ipn.mx/~pescamilla/MS/papers_2014/Wooetal2015.pdf

[8]. **"Security aspects of the in- vehicle network in the connected car,"**

Available:https://dl.acm.org/doi/abs/10.1109/COMST.2016.2521642

[9]. **"Comprehensive Experimental Analyses of Automotive Attack Surfaces,"**

Available:https://www.usenix.org/conference/usenix-security-11/comprehensive-experimental-analyses-automotive-attack-surfaces

[10]. **"Network slicing in 5g: Survey and challenges,"**

Available: https://ieeexplore.ieee.org/document/7926923

[11]. **"Neural Network-based Alzheimer's Disease Diagnosis With Densenet-169 Architecture"**

Available:https://drive.google.com/file/d/1OymszZx-G52WhtvzTYJ0zj1DaQnLS0cY/view

[12]. **"Predicting Food Truck Success Using Linear Regression"**

Available:https://drive.google.com/file/d/14av3lwf29kCBs0hnp3oluTsVMdtUI7S4/view

[13]. **"K – Fold Cross Validation On A Dataset"**

Available: https://drive.google.com/file/d/1XYJQB65ZL4l-OlpomsBQU5F7RJrBwfOo/view

[14]. **"Movie Recommendation System Using Cosine Similarity Technique"**

Available:https://drive.google.com/file/d/1VPzdNTGFxYyaFHAhVXlG4levMqjsXhMi/view

[15]. **"Forecasting Employee Attrition Through Ensemble Bagging Techniques"**

Available:https://drive.google.com/file/d/1j2h37BzOqxpt5UB98NlBDscU6tjZcGZz/view

[16]. **"Rice Leaf Disease Prediction Using Random Forest"**

Available: https://drive.google.com/file/d/1vJqzVcLDaCr--Ejfr6ylQrOShRqZDKiT/view

[17]. **"Clustered Regression Model for Predicting CO2 Emissions from Vehicles"**

Available:https://drive.google.com/file/d/1tRXQnTaqov0M7M0KYGMimkVErlN7ojvY/view

[18]. **"Optimized Prediction of Telephone Customer Churn Rate Using Machine Learning Algorithms"**

Available:https://drive.google.com/file/d/1wtQVCD7UcbObeunfYd6TuZWTej-9oGi8/view

[19]. **"Cricket Winning Prediction using Machine Learning"**

Available:https://drive.google.com/file/d/1elGo9Dmr6qPt1lhqsZFf68u6kvOdkRgV/view

[20]. **"Hand Gesture Recognition Using Artificial Neural Networks"**

Available:https://drive.google.com/file/d/1SIEAULz4yaoRmhv8uAz5l1z3CWV9YwRv/view

[21]. **"EMG Controlled Bionic Robotic Arm using Artificial Intelligence and Machine Learning"**

Available: https://ieeexplore.ieee.org/document/9640623

[22]. **"Optimized Conversion of Categorical and Numerical Features in Machine Learning Models"**

Available: https://ieeexplore.ieee.org/document/9640967

[23]. **"Brain Tissue Segmentation via Deep Convolutional Neural Networks"**

Available: https://ieeexplore.ieee.org/document/9640635