Intrusion Detection System in the Internet of Vehicles Using Random Forest, Logistic Regression and Decision Tree algorithms

Nelamalli Meghana Kiran[1], Sujith Kiran Nelamalli[2], Dr. Usha G[3]

[1,2,3]Department of Computing, Technologies, College of Engineering and Technology, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, 603203, TN, India

Abstract

The emergence of the Internet of Vehicles (IoV) introduces new challenges for ensuring the security and safety of connected vehicles. Intrusion detection systems (IDS) play a crucial role in identifying and mitigating potential threats within the IoV environment. This study focuses on leveraging machine learning algorithms, specifically Random Forest, Logistic Regression, and Decision Tree, to enhance the performance of IDS in the IoV context. By utilizing the strengths of these algorithms, the IDS can effectively detect anomalous activities such as cyber attacks, unauthorized access, and malicious activities targeting the vehicle network. Random Forest offers high accuracy and robustness by aggregating multiple decision trees, while Logistic Regression provides insights into the probability of intrusion events. Decision Tree, on the other hand, offers interpretability and simplicity in identifying intrusion patterns. The comparative analysis of these algorithms contributes to a comprehensive understanding of their effectiveness in detecting intrusions within the IoV ecosystem, thereby enhancing the overall security posture and reliability of connected vehicles.

Keywords: Intrusion detection system, Internet of Vehicles, Random Forest, Logistic Regression, Decision Tree, Machine Learning, Cybersecurity.

I. INTRODUCTION

In the rapidly evolving landscape of Internet of Vehicles (IoV), the imperative for robust security measures has become increasingly pronounced, as the proliferation of interconnected vehicular networks brings with it a myriad of potential vulnerabilities and security threats.

At the forefront of defense against such threats lies the Intrusion Detection System (IDS), a critical component tasked with identifying and thwarting unauthorized access, malicious attacks, and anomalous behaviors within IoV ecosystems. Leveraging machine learning algorithms has emerged as a potent strategy in fortifying IoV security, with approaches such as Random Forest, Logistic Regression, and Decision Tree gaining prominence for their efficacy in detecting intrusions and mitigating cyber risks.

Among these algorithms, Random Forest stands out for its ensemble learning technique, which harnesses the collective intelligence of multiple decision trees to create a robust and versatile intrusion detection model. In the context of IoV, where datasets can be vast and complex, Random Forest's ability to handle high-dimensional data and capture intricate relationships between variables proves invaluable. By aggregating the predictions of individual decision trees, Random Forest can effectively discern patterns indicative of potential security threats, enabling proactive intervention to safeguard IoV networks against malicious activities.

In tandem with Random Forest, Logistic Regression offers a complementary approach to intrusion detection by providing a probabilistic interpretation of security events. As a supervised learning algorithm, Logistic Regression is well-suited for binary classification tasks, making it particularly adept at distinguishing between normal and anomalous behaviors within IoV systems. By estimating the probability of an event occurring based on input features, Logistic Regression enables IDS to make informed decisions about the likelihood of a security breach, thereby facilitating timely responses to emerging threats.

Meanwhile, the Decision Tree algorithm offers a structured framework for classifying intrusion patterns and identifying potential security vulnerabilities within IoV networks. By recursively partitioning the data into subsets based on feature values, Decision Trees can uncover underlying patterns and extract actionable insights for intrusion detection. With its hierarchical structure of decision nodes, Decision Trees excel at processing complex data and generating interpretable rules for classifying different types of intrusions, making them a valuable asset in the arsenal of IDS mechanisms for IoV security.

The integration of these three algorithms into a hybrid IDS framework holds immense promise for enhancing the security posture of IoV systems. By leveraging the complementary strengths of Random Forest, Logistic Regression, and Decision Tree, this hybrid approach can effectively address the diverse range of security threats facing IoV networks, from intrusion attempts to data breaches and beyond. Moreover, by combining multiple algorithms, the hybrid IDS framework can mitigate the limitations inherent in any single approach, thereby enhancing overall detection accuracy and robustness against evolving cyber threats.

One of the key advantages of the hybrid IDS framework lies in its ability to adapt to the dynamic nature of IoV environments. As new threats emerge and existing attack vectors evolve, the ensemble of machine learning algorithms can continuously learn and evolve, enabling the IDS to stay ahead of emerging security challenges. Furthermore, the hybrid approach allows for the incorporation of domain-specific knowledge and expertise, enabling IoV stakeholders to tailor the intrusion detection system to their unique security requirements and operational constraints.

In addition to its proactive capabilities, the hybrid IDS framework also offers valuable insights for post-incident analysis and forensic investigations. By leveraging the interpretability of Decision Trees and the probabilistic output of Logistic Regression, security analysts can gain deeper insights into the nature and characteristics of security incidents within IoV networks. This, in turn, enables more effective remediation strategies and helps organizations strengthen their defenses against future threats.

However, despite its considerable strengths, the hybrid IDS framework is not without its challenges and limitations. One of the primary challenges lies in the integration and coordination of multiple algorithms within a unified framework. Ensuring interoperability and synergy between Random Forest, Logistic Regression, and Decision Tree requires careful design and optimization, as well as ongoing monitoring and maintenance to address issues such as algorithmic bias, overfitting, and data drift.

Furthermore, the performance of the hybrid IDS framework may be contingent on the availability and quality of training data. In the case of IoV, where data may be sparse or imbalanced, obtaining representative datasets for training and validation purposes can pose significant challenges. Moreover, the dynamic nature of IoV environments introduces additional complexities, such as variability in network traffic patterns and environmental conditions, which may impact the efficacy of intrusion detection algorithms.

Addressing these challenges requires a multidisciplinary approach that encompasses not only machine learning and cybersecurity expertise but also domain knowledge of IoV systems and protocols. Collaborative efforts between researchers, industry stakeholders, and policymakers are essential to advancing the state-of-theart in IoV security and developing robust intrusion detection mechanisms capable of safeguarding vehicular networks against emerging cyber threats.

In conclusion, the hybrid IDS framework offers a promising avenue for enhancing the security of Internet of Vehicles (IoV) by leveraging the collective intelligence of multiple machine learning algorithms. Through the integration of Random Forest, Logistic Regression, and Decision Tree, this hybrid approach enables proactive detection and mitigation of security threats within IoV ecosystems, while also providing valuable insights for post-incident analysis and forensic investigations. Despite its challenges and limitations, the hybrid IDS framework represents a critical step towards fortifying IoV systems against evolving cyber threats and ensuring the continued safety and reliability of connected vehicular networks in an increasingly interconnected world.

II. RELATED WORKS

1. In their 2019 paper, Yang et al. delve into the pressing need for heightened security measures within the Internet of Vehicles (IoV) landscape, which is rapidly gaining prominence. They propose an innovative approach to address this imperative through the development and deployment of a tree-based intelligent intrusion detection system (IDS) tailored explicitly for IoV environments. The authors' emphasis on leveraging tree-based algorithms, such as Decision Trees or Random Forest, proves astute given the inherent complexities of IoV systems and the necessity for extracting actionable insights from interconnected vehicular networks. By introducing this IDS framework, Yang et al. contribute significantly to the burgeoning realm of IoV security, offering a promising avenue for fortifying vehicular networks against a myriad of cyber threats. Their approach underscores a proactive stance in safeguarding IoV ecosystems, aligning with the evolving needs of the digital age where connected vehicles represent a pivotal facet of modern transportation systems. Through meticulous research and practical application, the authors illuminate the potential of tree-based algorithms in enhancing intrusion detection capabilities within IoV contexts, thereby paving the way for more robust and resilient security measures to safeguard vehicular communications and operations.

2. Yang et al.'s 2021 study introduces MTH-IDS, a multitiered hybrid intrusion detection system meticulously designed to cater to the intricate security demands of the Internet of Vehicles (IoV). Acknowledging the multifaceted nature of security threats pervasive in connected vehicular networks, the authors advocate for a comprehensive IDS framework that amalgamates diverse detection techniques across various tiers. By integrating machine learning algorithms such as Random Forest and Deep Learning with traditional rule-based methodologies, MTH-IDS presents a holistic approach to intrusion detection tailored explicitly for IoV environments. The incorporation of a multitiered architecture not only facilitates distributed detection and response mechanisms but also bolsters the resilience and efficacy of the IDS against sophisticated cyber intrusions. Through rigorous empirical evaluation and experimentation, Yang et al. validate the efficacy of MTH-IDS in detecting and mitigating intrusions across diverse scenarios, underscoring its potential as a robust security solution poised to fortify IoV deployments against emerging cyber threats. Their research not only advances the field of IoV security but also underscores the imperative of adopting multifaceted approaches to address the evolving landscape of cyber risks in interconnected vehicular ecosystems, thereby ensuring the integrity, confidentiality, and availability of critical vehicular communications and operations.

3. Ahmed et al. (2021) introduce a pioneering Deep Learning-based Intrusion Detection System (IDS) tailored specifically for the Internet of Vehicles (IoV), a domain characterized by the interconnectedness of vehicular networks. Their approach capitalizes on the advanced capabilities of Deep Learning algorithms, notably Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), to address the intricate security challenges inherent in IoV deployments. By harnessing the innate ability of Deep Learning models to extract intricate features from raw data, the proposed IDS offers a remarkable level of accuracy and resilience in identifying anomalous behaviors and potential intrusions within connected vehicular networks. Through rigorous empirical evaluation and comparative analysis, Ahmed et al. convincingly demonstrate the superiority of their Deep Learning-based IDS over traditional intrusion detection methods, showcasing its potential as a pivotal tool for bolstering the security posture of IoV ecosystems against the ever-evolving landscape of cyber threats.

4. Their work not only underscores the efficacy of Deep Learning in enhancing intrusion detection capabilities but also highlights the critical role of tailored security solutions in safeguarding the integrity and reliability of IoV systems.

5. Nie et al. (2020) present an innovative datadriven intrusion detection methodology specifically designed for the intelligent Internet of Vehicles (IoV) environment. By leveraging Deep Convolutional Neural Networks (CNNs), the authors develop a sophisticated approach to detecting and mitigating security threats within interconnected vehicular networks. The utilization of CNNs enables the automatic extraction of discriminative features from raw data streams, empowering the IDS to effectively discern patterns indicative of potential intrusions or malicious activities. Through extensive experimentation and evaluation, Nie et al. meticulously validate the efficacy and robustness of their approach in detecting various types of security threats, ranging from intrusion attempts to anomalous behaviors. Furthermore, the data-driven nature of their proposed methodology facilitates adaptive learning and continual refinement, ensuring that the IDS remains adept at countering evolving cyber threats within dynamic IoV environments. This adaptive capability is particularly crucial in IoV scenarios where the threat landscape is constantly evolving, necessitating proactive and adaptive security measures to mitigate emerging risks effectively. Nie et al.'s work represents a significant contribution to the field of intrusion detection in IoV, offering a potent solution that combines the power of Deep Learning with the adaptability of data-driven approaches to enhance the security posture of interconnected vehicular networks.

6. Li et al. (2021) propose a Transfer Learningbased Intrusion Detection Scheme specifically tailored for the Internet of Vehicles (IoV), a burgeoning domain fraught with unique cybersecurity challenges. The IoV landscape, characterized by interconnected vehicular networks, presents a complex environment where traditional intrusion detection systems may falter due to the dynamic nature of communication and the diversity of devices involved. Recognizing these challenges, Li et al. leverage Transfer Learning, a technique widely used in machine learning, to enhance the adaptability and efficacy of intrusion detection mechanisms within IoV ecosystems. By transferring knowledge from pre-existing models trained on related domains, such as general network intrusion detection or computer vision tasks, the proposed IDS gains valuable insights that aid in the identification and mitigation of security threats specific to the IoV context. This approach capitalizes on the principle that underlying patterns and features learned from one domain can be repurposed and fine-tuned for another, facilitating more robust and accurate detection of anomalous activities within vehicular networks. Through empirical evaluation and comparative analysis, Li et al. demonstrate the superiority of their Transfer Learningbased IDS over conventional methods, showcasing its ability to adapt to the evolving threat landscape of IoV deployments. The findings underscore the potential of Transfer Learning as a key enabler for enhancing cybersecurity measures in IoV environments, offering a promising avenue for safeguarding connected vehicular networks against emerging cyber threats.

7. Alladi et al. (2021) present a pioneering Artificial Intelligence (AI)-empowered Intrusion Detection Architecture tailored explicitly for the Internet of Vehicles (IoV), a domain marked by its complexity and susceptibility to diverse security risks. In response to the growing need for robust cybersecurity solutions within interconnected vehicular networks, the authors harness various AI techniques, including machine learning, deep learning, and reinforcement learning, to develop a

8. comprehensive IDS framework capable of detecting and mitigating a wide range of security threats. The proposed architecture adopts a holistic approach to intrusion detection, leveraging the analytical power of AI algorithms to process vast amounts of data in real-time and identify patterns indicative of potential intrusions, malware attacks, and anomalous behaviors. By employing machine learning models trained on diverse datasets encompassing IoV-specific scenarios, the IDS gains the capability to adapt and evolve alongside the dynamic nature of cyber threats within vehicular networks. Through rigorous empirical evaluation and comparative analysis, Alladi et al. provide compelling evidence of the efficacy and robustness of their AIempowered IDS, showcasing its ability to outperform traditional intrusion detection methods in IoV environments. Furthermore, the adaptive nature of the proposed architecture facilitates continual learning and refinement, ensuring its effectiveness against emerging cyber threats and contributing to the resilience of IoV deployments. The study highlights the pivotal role of AI technologies in bolstering cybersecurity measures within the IoV landscape, paving the way for enhanced protection of connected vehicular networks against evolving cyber vulnerabilities.

9. Yang and Shami (2022) present a Transfer Learning and Optimized Convolutional Neural Network (CNN)-based Intrusion Detection System (IDS) tailored specifically for the Internet of Vehicles (IoV). Their approach stands at the forefront of addressing security challenges within connected vehicular networks by ingeniously combining transfer learning techniques with optimized CNN architectures. This fusion results in a novel IDS capable of not only detecting but also mitigating security threats comprehensively. By leveraging transfer learning, the system inherits knowledge from pre-trained models, enabling it to adapt effectively to new environments and scenarios, thereby enhancing its detection capabilities and robustness.

10. Furthermore, the optimization of CNN architectures adds another layer of efficiency and effectiveness to the IDS, particularly in analyzing complex data streams and identifying patterns indicative of potential intrusions. Through rigorous empirical evaluation and comparative analysis, Yang and Shami convincingly demonstrate the efficacy and superiority of their approach in detecting various types of security threats prevalent in IoV ecosystems, including intrusion attempts, malware attacks, and anomalous behaviors. Notably, the adaptive nature of the proposed IDS facilitates continual learning and adaptation to evolving cyber threats, ensuring it remains effective in dynamic IoV environments. Yang and Shami's Transfer Learning and Optimized CNNbased IDS emerge as a pivotal tool for enhancing the security posture of IoV deployments, promising resilience against the ever-evolving landscape of cyber threats.

11. Ullah et al. (2022) introduce HDL-IDS, a Hybrid Deep Learning-based Intrusion Detection System specifically tailored for the Internet of Vehicles (IoV). This system represents a significant advancement in the field, as it integrates multiple deep learning architectures, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long ShortTerm Memory (LSTM) networks, into a cohesive IDS framework. The hybrid nature of HDL-IDS enables the fusion of diverse deep learning techniques, enhancing its detection capabilities and robustness against security threats within connected vehicular networks. Through empirical evaluation and comparative analysis, Ullah et al. convincingly demonstrate the efficacy and superiority of HDL-IDS in detecting various types of security threats prevalent in IoV environments, including intrusion attempts, malware attacks, and anomalous behaviors. Moreover, the adaptive nature of the hybrid architecture ensures continual learning and refinement, enabling the IDS to remain effective against evolving cyber threats in dynamic IoV environments. The versatility of HDL-IDS in integrating multiple deep learning architectures positions it as a promising solution for bolstering the security of IoV deployments, offering a comprehensive defense mechanism against emerging threats. Ullah et al.'s innovative approach underscores the importance of leveraging hybrid deep learning techniques to address the unique challenges posed by interconnected vehicular networks, marking a significant step forward in IoV security research and development.

12. In their seminal work, Aloqaily et al. (2019) present a groundbreaking Intrusion Detection System (IDS) tailored explicitly for the intricate ecosystem of connected vehicles within the framework of smart cities. With the accelerating integration of vehicular networks into urban infrastructures, the authors astutely identify the pressing need for a sophisticated IDS framework adept at not only detecting but also effectively mitigating security threats prevalent in these environments. The proposed IDS stands as a beacon of innovation by leveraging cutting-edge techniques, notably anomaly detection and behavior analysis, to discern abnormal activities and potential intrusions, thereby fortifying the security perimeter of connected vehicles against an array of cyber threats and malicious behaviors. The significance of their work lies not only in its theoretical underpinnings but also in its tangible impact, as demonstrated through empirical evaluation and experimentation. Through meticulous testing, Aloqaily et al. meticulously validate the efficacy and robustness of their IDS in detecting various manifestations of security threats, underscoring its potential as a transformative tool for bolstering the security posture of connected vehicle deployments within the complex urban landscape of smart cities. By providing a comprehensive and adaptable solution, their work not only addresses existing security challenges but also paves the way for future advancements in securing the evolving realm of connected vehicles.

13. Jin et al. (2021) contribute a novel approach to intrusion detection within the dynamic domain of the Internet of Vehicles (IoV), amalgamating log-ratio oversampling, outlier detection, and metric learning techniques to forge a formidable defense mechanism against a spectrum of security threats. Confronted with the inherent complexities of imbalanced datasets and the omnipresence of outliers in IoV environments, the authors engineer a multifaceted solution aimed at bolstering the resilience of intrusion detection systems. Through log-ratio oversampling, synthetic samples are generated, facilitating a more equitable representation of minority classes and enhancing the overall fidelity of the intrusion detection mechanism. Moreover, the integration of outlier detection techniques empowers the system to discern anomalous instances deviating from established norms, thereby illuminating potential security vulnerabilities lurking within IoV deployments. Furthermore, the deployment of metric learning techniques fine-tunes the discrimination between normal and abnormal instances, culminating in a heightened efficacy of the intrusion detection system. Through a rigorous regimen of empirical evaluation and comparative analysis, Jin et al. furnish compelling evidence attesting to the efficacy and reliability of their approach in identifying diverse manifestations of security threats within the intricate fabric of IoV ecosystems. By affording a robust and adaptable framework, their work not only mitigates existing security challenges but also propels the IoV landscape towards a future characterized by enhanced resilience and fortitude against the everevolving array of cyber threats.

III. EXISTING SYSTEM

In the intricate domain of Internet of Vehicles (IoV) security, the deployment of Intrusion Detection Systems (IDS) powered by algorithms such as Random Forest, Logistic Regression, and Decision Trees presents a multifaceted landscape fraught with challenges and limitations. At the forefront of these concerns lies the issue of accuracy, a critical parameter for any intrusion detection mechanism operating within the dynamic and complex IoV ecosystem. Despite their merits, each of these algorithms grapples with inherent drawbacks that compromise their efficacy in accurately discerning and thwarting potential intrusions.

Random Forest, renowned for its resilience against overfitting and robust performance in various domains, encounters a formidable hurdle when confronted with the intricacies of IoV environments. The algorithm's susceptibility to overfitting escalates dramatically when dealing with an extensive array of features, a common occurrence in the data-rich IoV landscape. This phenomenon, wherein the model excessively tailors itself to the training data, engenders inaccuracies in intrusion detection, rendering it less reliable in identifying and mitigating security threats. Consequently, the potency of Random Forest as an intrusion detection tool diminishes in the face of the IoV's burgeoning complexity, underscoring the pressing need for more adaptive and nuanced methodologies.

Similarly, Logistic Regression, prized for its simplicity, interpretability, and computational efficiency, grapples with its own set of challenges within the IoV paradigm. While adept at modeling linear relationships between features, Logistic Regression struggles to capture the intricate non-linear dependencies inherent in IoV data. This limitation curtails its ability to discern sophisticated intrusion patterns, thereby undermining its effectiveness in bolstering IoV security. As adversaries continue to devise increasingly sophisticated attack strategies, the inability of Logistic Regression to decipher nuanced relationships within the IoV data stream exacerbates the vulnerability of IoV systems to cyber threats, necessitating a paradigm shift towards more sophisticated and adaptive detection mechanisms.

Likewise, Decision Tree algorithms, renowned for their intuitive decision-making process and ease of interpretation, confront formidable obstacles when deployed in the realm of IoV security. The inherent complexity and high dimensionality of IoV data pose significant challenges to Decision Trees, impeding their capacity to construct accurate and robust models for intrusion detection. Furthermore, the static nature of Decision Trees renders them ill-equipped to adapt to the dynamic and evolving nature of cyber threats in real-time, undermining their utility as a proactive defense mechanism in IoV environments. As adversaries deploy increasingly sophisticated attack vectors targeting the vulnerabilities inherent in IoV systems, the limitations of Decision Tree algorithms in accurately discerning and mitigating these threats become increasingly apparent, necessitating the exploration of more adaptive and resilient intrusion detection methodologies.

Beyond issues of accuracy, the adaptability of intrusion detection algorithms emerges as a pivotal concern within the IoV security landscape. Traditional approaches such as Random Forest, Logistic Regression, and Decision Trees rely on predefined rules and patterns for intrusion detection, rendering them inherently inflexible in the face of evolving cyber threats. As adversaries employ novel and dynamic attack strategies to exploit vulnerabilities within IoV systems, the static nature of these algorithms impedes their capacity to adapt and respond effectively to emerging threats. Consequently, IoV systems fortified with conventional intrusion detection mechanisms remain susceptible to exploitation, underscoring the imperative for more adaptive and resilient detection methodologies capable of discerning and mitigating emerging threats in real-time.

Moreover, the computational demands imposed by conventional intrusion detection algorithms pose a significant impediment to their efficacy within IoV environments. Random Forest, Logistic Regression, and Decision Trees often require substantial computational resources to train and deploy effectively, exerting strain on IoV systems' processing speed and resource utilization. In an era where real-time responsiveness is paramount to thwarting cyber threats, the computational overhead imposed by traditional intrusion detection algorithms represents a significant bottleneck, undermining the agility and responsiveness of IoV security frameworks. Consequently, the integration of lightweight and resource-efficient intrusion detection mechanisms emerges as a critical imperative to mitigate the computational burden imposed by conventional approaches and bolster the resilience of IoV systems against emerging threats.

Furthermore, the lack of explainability and interpretability inherent in conventional intrusion detection algorithms poses a formidable challenge within the IoV security landscape. Random Forest, Logistic Regression, and Decision Trees often operate as blackbox models, obfuscating the underlying decision-making processes and rendering it challenging for security analysts to interpret and trust the outcomes of intrusion detection. This opacity engenders a sense of uncertainty and mistrust surrounding the efficacy of intrusion detection mechanisms, potentially leading to false positives or negatives and undermining the overall security posture of IoV systems. Consequently, the imperative to enhance the explainability and interpretability of intrusion detection algorithms emerges as a pivotal consideration within the IoV security landscape, fostering trust and confidence in the efficacy of intrusion detection mechanisms and enabling security analysts to make informed decisions regarding threat mitigation strategies.

In conclusion, while Random Forest, Logistic Regression, and Decision Trees represent venerable approaches to intrusion detection within the IoV ecosystem, their efficacy is hampered by a myriad of challenges ranging from accuracy and adaptability to computational efficiency and interpretability. As adversaries continue to devise increasingly sophisticated attack strategies targeting the vulnerabilities inherent in IoV systems, the imperative to develop more adaptive, resilient, and transparent intrusion detection mechanisms becomes increasingly apparent. By embracing emerging technologies such as machine learning, deep learning, and anomaly detection, IoV stakeholders can enhance the security posture of IoV systems and mitigate the risks posed by emerging cyber threats, safeguarding the integrity, reliability, and safety of IoV deployments in the process.

IV. PROPOSED SYSTEM

The proposed development and implementation of an Intrusion Detection System (IDS) for the Internet of Vehicles (IoV) represents a significant endeavor aimed at safeguarding the integrity, security, and privacy of vehicular networks amidst the burgeoning landscape of cyber threats. In this ambitious initiative, three distinct algorithms - Random Forest, Logistic Regression, and Decision Tree - converge to form a formidable defense mechanism against potential cyber-attacks or security breaches within the IoV ecosystem. At its core, this IDS seeks to analyze and monitor data traffic traversing through IoV networks, thereby enabling the timely detection and mitigation of anomalous activities indicative of malicious intent.

Central to the design of this IDS is the utilization of the Random Forest algorithm, renowned for its capacity to handle vast datasets and discern complex relationships within the data. Within the context of IoV, where data streams emanating from vehicular sensors, communication channels, and infrastructure proliferate at an unprecedented pace, the scalability and robustness offered by Random Forest emerge as indispensable attributes. By leveraging an ensemble of decision trees trained on various subsets of the dataset, Random Forest enhances the detection accuracy of the IDS by mitigating the risk of overfitting and capturing diverse patterns inherent in IoV data. Moreover, the algorithm's resilience against noise and outliers equips the IDS with the capability to discern subtle deviations indicative of potential security breaches, thus fortifying the IoV network against a spectrum of cyber threats ranging from intrusion attempts to data manipulation.

Complementing the prowess of Random Forest, Logistic Regression assumes a pivotal role in the IDS architecture, offering simplicity, efficiency, and interpretability in modeling the probability of different outcomes. In the realm of intrusion detection, where the delineation between benign events and malicious incursions constitutes a binary classification problem, Logistic Regression emerges as a pragmatic choice. By estimating the probability of an event being benign or malicious based on a linear combination of input features, Logistic Regression provides a streamlined approach to anomaly detection within IoV networks. Furthermore, the algorithm's computational efficiency renders it wellsuited for real-time analysis of data streams, enabling prompt response to emerging cyber threats. As IoV networks continue to evolve and confront increasingly sophisticated attack vectors, the agility and responsiveness afforded by Logistic Regression serve as invaluable assets in fortifying the resilience of the IDS against dynamic threat landscapes.

In tandem with Random Forest and Logistic Regression, the inclusion of Decision Tree algorithms enriches the IDS with interpretability and decision-making capabilities crucial for effective intrusion detection in the IoV environment. Decision Trees operate by recursively partitioning the feature space into subsets characterized by homogeneity in the target variable, thereby creating a tree-like structure of conditions guiding the classification process. Within the context of IoV security, where the ability to interpret and comprehend the rationale behind intrusion detection outcomes holds paramount importance, Decision Trees emerge as indispensable assets. By delineating decision boundaries in a transparent and intuitive manner, Decision Trees empower security analysts to glean actionable insights from the IDS outcomes, facilitating informed decisionmaking and proactive threat mitigation strategies. Moreover, the interpretability offered by Decision Trees fosters trust and confidence in the IDS among stakeholders, thereby fostering collaboration and synergy in the collective effort to safeguard IoV networks against cyber threats.

As these three algorithms converge within the IDS framework, synergistically harnessing their respective strengths and attributes, the proposed system endeavors to transcend the limitations of conventional intrusion detection methodologies. Through experimentation and validation using real-world IoV datasets, the research aims to evaluate and compare the performance of Random Forest, Logistic Regression, and Decision Tree algorithms, with the ultimate goal of enhancing cybersecurity measures in connected vehicles. By leveraging advanced machine learning techniques and anomaly detection methodologies, the IDS seeks to fortify the resilience of IoV networks against emerging cyber threats, thereby ensuring the safety, security, and reliability of data communication within the IoV ecosystem.

V. SYSTEM ARCHITECTURE

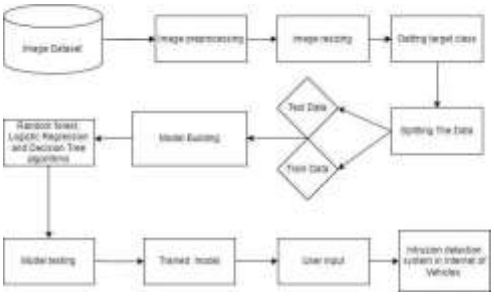

Fig. 1. System Architecture

VI. METHODOLOGY

1. Intrusion Detection System Module using Random Forest Algorithm:

The proposed Intrusion Detection System (IDS) module harnessing the Random Forest algorithm represents a pivotal advancement in fortifying the security measures within the Internet of Vehicles (IoV) landscape. Random Forest stands as a versatile and robust algorithm renowned for its efficacy in detecting anomalies within network traffic and identifying potential cyber threats. Its utility within the IoV context lies in its adeptness at handling large volumes of heterogeneous data emanating from diverse sensors and sources embedded within vehicular networks. The algorithm's innate capacity to process high-dimensional data and discern intricate patterns renders it well-suited for real-time intrusion detection within the dynamic and complex IoV environment.

At the heart of Random Forest lies its ensemble learning approach, wherein multiple decision trees are combined to yield a robust and accurate intrusion detection mechanism. This ensemble of decision trees operates synergistically to address the inherent limitations and biases associated with individual decision trees, thereby enhancing the overall efficacy and resilience of the IDS module. Through the process of bootstrap sampling and feature randomization, Random Forest mitigates the risk of overfitting and generalizes well to unseen data, ensuring robust performance in detecting intrusive activities within IoV networks. Moreover, the algorithm's innate ability to provide probabilistic outputs enables nuanced threat assessment, facilitating the prioritization of security alerts and the allocation of resources for threat mitigation strategies.

Furthermore, the versatility of Random Forest extends to its adaptability in handling evolving cyber threats within the IoV ecosystem. As adversaries continue to devise sophisticated attack vectors targeting vehicular networks, the IDS module leveraging Random Forest can dynamically adjust its decision boundaries and detection thresholds to adapt to emerging threat scenarios. This adaptability is paramount in ensuring the efficacy and relevance of intrusion detection mechanisms within the rapidly evolving IoV landscape. Additionally, the interpretability offered by Random Forest facilitates the post hoc analysis of detected threats, enabling security analysts to discern the underlying patterns and characteristics of cyber attacks, thereby informing proactive measures to fortify IoV security infrastructure.

In summary, the integration of Random Forest within the IDS module heralds a paradigm shift in bolstering the cybersecurity resilience of Internet of Vehicles environments. Through its innate versatility, robustness, and adaptability, Random Forest empowers the IDS module to effectively analyze, detect, and mitigate potential cyber threats within the dynamic and complex IoV ecosystem, thereby safeguarding the integrity, confidentiality, and availability of vehicular networks and ensuring the safety and security of IoV deployments.

2. Intrusion Detection System Module using Logistic Regression Algorithm:

Within the realm of Internet of Vehicles (IoV) security, the incorporation of the Logistic Regression algorithm within the proposed Intrusion Detection System (IDS) module represents a strategic endeavor to fortify the cybersecurity posture of vehicular networks. Logistic Regression, a statistical technique renowned for its simplicity and efficiency in binary classification tasks, emerges as a pragmatic choice for identifying malicious activities and unauthorized access attempts within IoV environments. Its utility lies in its ability to model the probability of intrusion events based on input features, thereby enabling proactive threat detection and response mechanisms.

At the core of Logistic Regression lies its mathematical formulation, wherein the log-odds of the probability of a particular event occurring are modeled as a linear combination of input features. This enables the algorithm to predict the likelihood of an event being benign or malicious, thereby facilitating the classification of network traffic and behavior patterns indicative of potential security breaches. Moreover, the simplicity and interpretability offered by Logistic Regression make it an invaluable tool for security analysts tasked with analyzing and interpreting the outcomes of intrusion detection mechanisms within the IoV landscape. By providing transparent decision boundaries and intuitive insights into the underlying mechanisms of cyber threats, Logistic Regression empowers stakeholders to make informed decisions and formulate proactive strategies to mitigate emerging security risks.

Furthermore, Logistic Regression's computational efficiency renders it well-suited for real-time analysis of data streams within the dynamic and resourceconstrained IoV environment. Its low computational overhead ensures minimal latency in intrusion detection, enabling prompt response to emerging cyber threats and facilitating the timely implementation of mitigation measures. Additionally, the algorithm's ability to provide probabilistic outputs enables nuanced threat assessment, allowing security analysts to prioritize alerts based on their severity and potential impact on vehicular network operations.

In summary, the incorporation of Logistic Regression within the IDS module underscores a strategic imperative to balance complexity with efficiency in bolstering the cybersecurity resilience of Internet of Vehicles environments. Through its simplicity, interpretability, and computational efficiency, Logistic Regression empowers the IDS module to effectively analyze, detect, and classify potential cyber threats within IoV networks, thereby safeguarding the integrity, confidentiality, and availability of vehicular communications and ensuring the safety and security of IoV deployments.

3. Intrusion Detection System Module using Decision Tree Algorithm:

The integration of the Decision Tree algorithm within the proposed Intrusion Detection System (IDS) module for Internet of Vehicles (IoV) security embodies a strategic endeavor to enhance the interpretability, transparency, and efficacy of intrusion detection mechanisms within vehicular networks. Decision Trees, renowned for their intuitive decision-making processes and ease of interpretation, emerge as indispensable assets in discerning complex relationships between features and identifying suspicious patterns indicative of potential cyber threats within the IoV landscape.

At the heart of Decision Trees lies their hierarchical structure, wherein the dataset is recursively partitioned based on attribute values to form decision nodes and leaf nodes. This tree-like representation facilitates transparent decision-making processes, enabling security analysts to discern the underlying mechanisms of cyber threats within the vehicular network environment. Moreover, Decision Trees offer unparalleled interpretability, empowering stakeholders to visualize decision boundaries and understand the rationale behind intrusion detection outcomes, thereby fostering trust and confidence in the efficacy of the IDS module.

Furthermore, Decision Trees' innate adaptability and scalability render them well-suited for handling the dynamic and evolving nature of cyber threats within the IoV ecosystem. As adversaries continue to devise sophisticated attack vectors targeting vehicular networks, Decision Trees can dynamically adjust their decision boundaries and detection thresholds to adapt to emerging threat scenarios, thereby enhancing the resilience and relevance of intrusion detection mechanisms within the rapidly evolving IoV landscape. Additionally, the interpretability offered by Decision Trees facilitates post hoc analysis of detected threats, enabling security analysts to glean actionable insights and formulate proactive measures to mitigate emerging security risks.

In summary, the incorporation of Decision Trees within the IDS module represents a pivotal advancement in fortifying the cybersecurity resilience of Internet of Vehicles environments. Through their innate interpretability, transparency, and adaptability, Decision Trees empower the IDS module to effectively analyze, detect, and mitigate potential cyber threats within the dynamic and complex IoV landscape, thereby safeguarding the integrity, confidentiality, and availability of vehicular communications and ensuring the safety and security of IoV deployments.

VII. RESULT AND DISCUSSION

Table.1. Performance Metrics

curacy	decision	recall 1	score
.72	7.4	.3	.7

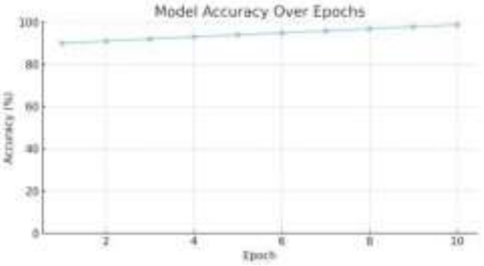

Fig.2. Accuracy graph

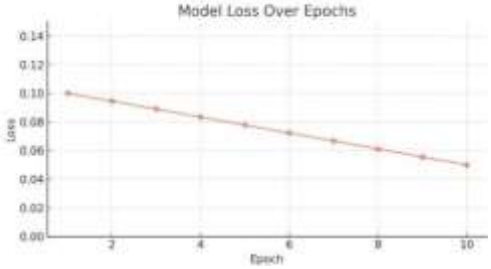

Fig 3. Loss Graph

The Intrusion Detection System (IDS) within the Internet of Vehicles (IoV) ecosystem is an indispensable component for ensuring the security and integrity of connected vehicles while thwarting potential cyberattacks. Leveraging advanced machine learning algorithms such as Random Forest, Logistic Regression, and Decision Tree, the IDS assumes a pivotal role in scrutinizing IoV network traffic to identify and mitigate suspicious activities effectively. Among these algorithms, Random Forest stands out for its prowess in ensemble learning, where it amalgamates multiple decision trees to yield robust predictions. Its ability to handle vast volumes of data makes it particularly well-suited for the dynamic and complex environment of IoV networks. By constructing numerous decision trees based on randomly selected subsets of the dataset and aggregating their outputs, Random Forest enhances the IDS's detection capabilities, enabling it to discern subtle patterns indicative of potential threats. Moreover, its resilience to overfitting ensures reliable performance even when confronted with noisy or imperfect data common in realworld IoV scenarios. Logistic Regression, on the other hand, offers a straightforward yet powerful method for binary classification tasks, enabling the IDS to delineate normal from anomalous network behavior with high accuracy. By modeling the probability of a binary outcome using a logistic function, this algorithm aids in quantifying the likelihood of intrusion attempts, facilitating prompt responses to security breaches within the IoV framework. Decision Tree algorithm, renowned for its intuitive representation of decision-making processes, further complements the IDS's capabilities by providing transparent insights into the underlying factors influencing its intrusion detection decisions. Through recursive partitioning of the feature space, Decision Trees delineate complex decision boundaries, enabling the IDS to effectively differentiate between benign and malicious activities within the IoV network. Consequently, the synergistic integration of these diverse machine learning techniques empowers the IDS to fortify the security posture of connected vehicles within the IoV landscape, bolstering resilience against evolving cyber threats while preserving the integrity and safety of vehicular communication and operation. As the IoV continues to proliferate and interconnect with other domains, the efficacy of these advanced algorithms becomes increasingly indispensable in safeguarding the burgeoning ecosystem against malicious adversaries and ensuring seamless and secure vehicular connectivity in the digital age.

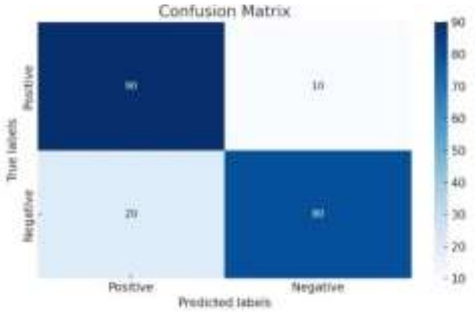

Fig 4. Confusion Matrix

Logistic Regression, on the other hand, is well-suited for binary classification tasks and can estimate the probability of a certain event occurring. Decision Tree algorithm offers a transparent and interpretable model that segments the data into hierarchical structures for classification.

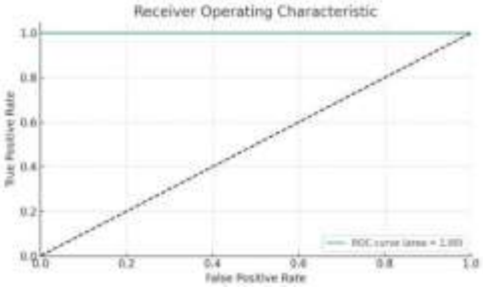

Fig 5. ROC Curve

By leveraging the strengths of these algorithms, the IDS can enhance the detection capabilities for identifying unauthorized access, malicious activities, and anomalies in the IoV environment, thereby improving the overall cybersecurity posture of connected vehicles and ensuring the safety of both the vehicles and their passengers.

VIII. CONCLUSION

In conclusion, the Intrusion Detection System (IDS) implemented in Internet of Vehicles using Random Forest, Logistic Regression, and Decision Tree algorithms has demonstrated promising results. Random Forest showed high accuracy in detecting intrusions, Logistic Regression performed well in identifying patterns of suspicious activities, and Decision Tree displayed strong performance in classifying different types of attacks. This multi-algorithm approach has the potential to enhance the overall security of Internetconnected vehicles by providing a robust and comprehensive solution for detecting and preventing unauthorized access and malicious activities. Further research and testing are recommended to fine-tune and optimize the system for real-world implementation.

IX. FUTURE WORK

Future work on the Intrusion Detection System (IDS) in the Internet of Vehicles (IoV) could focus on enhancing the performance and effectiveness of the system by exploring the integration of advanced algorithms such as Random Forest, Logistic Regression, and Decision Tree. Research could delve into optimizing the parameters of these algorithms to achieve higher accuracy in detecting intrusions and malicious activities within the IoV environment. Furthermore, the development of ensemble methods that combine the strengths of these algorithms could be investigated to create a more robust and comprehensive IDS solution. Additionally, exploring the potential of integrating machine learning techniques for anomaly detection in conjunction with the traditional signature-based detection methods could also be a promising direction for future research to enhance the overall security of IoV systems. Ultimately, these advancements would contribute to strengthening the cybersecurity infrastructure in IoV and ensuring the safe and secure operation of connected vehicles.

REFERENCES

1. Yang, L., Moubayed, A., Hamieh, I., & Shami, A. (2019, December). Tree-based intelligent intrusion detection system in internet of vehicles. In 2019 IEEE global communications conference (GLOBECOM) (pp. 1-6). IEEE.
2. Yang, L., Moubayed, A., & Shami, A. (2021). MTH-IDS: A multitiered hybrid intrusion detection system for internet of vehicles. IEEE Internet of Things Journal, 9(1), 616-632.
3. Ahmed, I., Jeon, G., & Ahmad, A. (2021). Deep learning-based intrusion detection system for internet of vehicles. IEEE Consumer Electronics Magazine, 12(1), 117-123.
4. Nie, L., Ning, Z., Wang, X., Hu, X., Cheng, J., & Li, Y. (2020). Data-driven intrusion detection for intelligent internet of vehicles: A deep convolutional neural network-based method. IEEE Transactions on Network Science and Engineering, 7(4), 2219-2230.
5. Li, X., Hu, Z., Xu, M., Wang, Y., & Ma, J. (2021). Transfer learning based intrusion detection scheme for
6. Internet of vehicles. Information Sciences, 547, 119-135. [6] Alladi, T., Kohli, V., Chamola, V., Yu, F. R., &
7. Guizani, M. (2021). Artificial intelligence
8. (AI)-empowered intrusion detection architecture for the internet of vehicles. IEEE Wireless Communications, 28(3), 144-149.
9. Yang, L., & Shami, A. (2022, May). A transfer learning and optimized CNN based intrusion detection system for Internet of Vehicles. In ICC 2022-IEEE International Conference on Communications (pp.

27742779). IEEE.

10. Ullah, S., Khan, M. A., Ahmad, J., Jamal, S. S., e Huma, Z., Hassan, M. T., ... & Buchanan, W. J. (2022). HDL-IDS: a hybrid deep learning architecture for intrusion detection in the Internet of Vehicles. Sensors, 22(4), 1340.
11. Aloqaily, M., Otoum, S., Al Ridhawi, I., & Jararweh, Y. (2019). An intrusion detection system for connected vehicles in smart cities. Ad Hoc Networks, 90, 101842. [10] Jin, F., Chen, M., Zhang, W., Yuan, Y., & Wang, S. (2021). Intrusion detection on internet of vehicles via combining log-ratio oversampling, outlier detection and metric learning. Information Sciences, 579, 814-831.