Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles

Isuru Samaranayaka   
Computer Systems Engineering Cyber Security Department  
Sri Lanka Institute of information TechnologyMalabe,Sri Lanka  
it20636906@my.sliit.lk

*Abstract*— The Internet of Vehicles (IoV) has gained significant attention in recent years as a promising paradigm for intelligent transportation systems. However, the increased connectivity and communication capabilities in the IoV environment also introduce security vulnerabilities and the risk of intrusion. To address these challenges, this research paper proposes a multi-tiered hybrid intrusion detection system (IDS) tailored specifically for the IoV.

The proposed IDS combines anomaly-based and signature-based detection techniques to enhance accuracy, robustness, and real-time detection capabilities. The multi-tiered architecture consists of edge, fog, and cloud layers, allowing for efficient handling of the diverse and dynamic nature of IoV data.

At the edge layer, local anomaly detection techniques are employed to identify abnormal behaviors and detect potential intrusions in real-time. The fog layer incorporates signature-based detection and correlation mechanisms, leveraging a comprehensive signature database to match and identify known attack patterns. Correlation and event aggregation techniques enable the identification of complex attack scenarios and the generation of timely alerts.

In the cloud layer, centralized analysis and decision-making take place. Data fusion and aggregation techniques are employed to integrate information from multiple vehicles and IoT devices, providing a holistic view of the IoV environment. Machine learning and deep learning algorithms are utilized to develop models capable of detecting novel and sophisticated attacks. The cloud layer also facilitates decision-making and response generation based on the detected intrusions.

The proposed IDS is evaluated using a representative dataset, and performance metrics are used to assess its effectiveness. The experimental results demonstrate the efficacy and efficiency of the multi-tiered hybrid IDS in detecting intrusions and mitigating security threats in the IoV. Additionally, security considerations, practical implementation challenges, and future research directions are discussed to provide insights into the broader implications of the proposed system.

In conclusion, the multi-tiered hybrid intrusion detection system presented in this research paper offers a comprehensive and robust approach to safeguard the IoV environment. By combining anomaly-based and signature-based detection techniques within a multi-tiered architecture, the proposed IDS provides improved accuracy, real-time detection, and resilience against evolving intrusion threats in the IoV ecosystem.

Keywords— Internet of Vehicles, IoV, intrusion detection system, IDS, multi-tiered architecture, anomaly detection, signature-based detection, hybrid approach, edge layer, fog layer, cloud layer, real-time detection, security threats.

# Introduction

The Internet of Vehicles (IoV) is a transformative paradigm that integrates vehicles, infrastructure, and various devices into a connected ecosystem, enabling intelligent transportation systems and enhancing road safety, efficiency, and overall driving experience. However, the increased connectivity and communication capabilities within the IoV environment also expose it to various security vulnerabilities and the potential risk of intrusions.

Intrusion detection is a crucial aspect of ensuring the security and integrity of the IoV ecosystem. Traditional intrusion detection systems (IDS) designed for conventional networks face limitations when applied to the dynamic and heterogeneous IoV environment. The unique characteristics of IoV, such as high mobility, resource-constrained devices, and diverse data sources, necessitate the development of specialized IDS tailored to its specific requirements.

This research paper presents a novel approach to address the challenges of intrusion detection in the Internet of Vehicles. We propose a multi-tiered hybrid intrusion detection system (IDS) that combines both anomaly-based and signature-based detection techniques to enhance the accuracy, robustness, and real-time detection capabilities in the IoV environment.

The multi-tiered architecture of the proposed IDS is designed to efficiently handle the diverse and dynamic nature of IoV data. It consists of three tiers: the edge layer, the fog layer, and the cloud layer. Each layer plays a unique role in the intrusion detection process, allowing for distributed processing, intelligent decision-making, and comprehensive analysis.

At the edge layer, local anomaly detection techniques are employed to monitor the behavior of individual vehicles and detect abnormal patterns that may indicate intrusion attempts. Real-time detection at the edge layer enables prompt responses and minimizes the impact of potential intrusions.

The fog layer incorporates signature-based detection and correlation mechanisms. A comprehensive signature database is maintained, containing known attack patterns and malicious behaviors. By matching incoming data against the signature database, the IDS can identify and classify known attacks. Correlation and event aggregation techniques enable the system to detect complex attack scenarios that span multiple vehicles or involve coordinated activities.

The cloud layer serves as the central hub for analysis and decision-making. It aggregates and fuses data from multiple vehicles and IoT devices, providing a holistic view of the IoV environment. Machine learning and deep learning algorithms are leveraged to develop models capable of detecting novel and sophisticated attacks. The cloud layer also facilitates the generation of appropriate responses based on the identified intrusions, such as generating alerts, initiating countermeasures, or notifying relevant authorities.

To evaluate the effectiveness of the proposed multi-tiered hybrid IDS, extensive experiments are conducted using representative IoV datasets. Performance metrics such as detection accuracy, false positive rate, and response time are employed to assess the system's efficacy in detecting intrusions and mitigating security threats.

Furthermore, this research paper discusses important security considerations specific to the IoV environment, including potential attack scenarios, robustness, resilience, and privacy concerns. Practical implementation challenges are addressed, and future research directions are proposed to further enhance the intrusion detection capabilities in the IoV ecosystem.

Intrusion detection in the IoV environment presents unique challenges compared to traditional network-based intrusion detection systems. First, the dynamic nature of vehicular networks, characterized by frequent vehicle mobility and changing network topologies, poses difficulties in accurately identifying and tracking intrusions. Second, the resource-constrained nature of vehicles limits the computational capabilities and memory capacity for running sophisticated intrusion detection algorithms. Additionally, the diversity of vehicular data and the sheer volume of information generated in the IoV environment require efficient data processing and analysis techniques.

In conclusion, the multi-tiered hybrid intrusion detection system presented in this research paper offers a comprehensive and robust approach to secure the Internet of Vehicles. By combining anomaly-based and signature-based detection techniques within a multi-tiered architecture, the proposed IDS provides improved accuracy, real-time detection, and resilience against evolving intrusion threats. The research outcomes contribute to the advancement of intrusion detection methods in the IoV domain and pave the way for more secure and trustworthy IoV deployments.

# RELATED WORK

INTRUSION DETECTION TECHNIQUES FOR IOV:

Intrusion detection techniques specific to the Internet of Vehicles (IoV) have been extensively studied in recent years. Researchers have explored various approaches to detect and mitigate intrusions in this unique environment. Anomaly detection techniques have gained popularity due to their ability to identify deviations from normal behavior. These techniques leverage statistical modeling, machine learning algorithms, and data mining approaches to detect abnormal patterns or behaviors in the IoV data. Signature-based detection methods, on the other hand, rely on predefined attack signatures or patterns to identify known attacks. These techniques match the incoming data against a database of attack signatures to detect and classify intrusion attempts. Hybrid approaches that combine both anomaly detection and signature-based methods have also been proposed, leveraging the strengths of both techniques to improve detection accuracy and reduce false positives.

MULTI-TIERED ARCHITECTURES FOR IOV:

Multi-tiered architectures have shown promise in addressing the complex nature of IoV environments. These architectures involve the distribution of computational tasks across multiple layers or tiers, each with its specific functionalities. In the context of intrusion detection, multi-tiered architectures enable efficient processing, analysis, and decision-making by leveraging edge, fog, and cloud layers. The edge layer, situated in individual vehicles or roadside units, performs local data collection, preprocessing, and initial detection to ensure real-time responsiveness. The fog layer, comprising intermediate computing resources, performs more sophisticated analysis, correlation, and aggregation of data from multiple edge devices. Finally, the cloud layer, with its high computational power and storage capabilities, provides centralized analysis, machine learning-based detection, and decision-making, taking into account the global view of the IoV ecosystem. Such architectures facilitate efficient and scalable intrusion detection in the IoV.

HYBRID APPROACHES IN INTRUSION DETECTION:

Hybrid approaches have gained attention in the field of intrusion detection, including in the context of the IoV. These approaches aim to combine the strengths of different detection techniques to enhance accuracy and overall system performance. In the context of IoV intrusion detection, hybrid approaches typically involve the combination of anomaly-based and signature-based detection methods. Anomaly detection techniques are effective in detecting previously unseen attacks or novel behaviors, while signature-based methods excel in identifying known attacks. By integrating both approaches, hybrid IDS can leverage anomaly detection to identify emerging threats and signature-based detection to detect known attacks, resulting in improved detection rates and reduced false positives. Hybrid approaches can also incorporate machine learning algorithms and data fusion techniques to further enhance the effectiveness of intrusion detection in the IoV environment.

The literature in intrusion detection for IoV encompasses a range of techniques, architectures, and hybrid approaches. These studies provide valuable insights into the challenges and advancements in securing the IoV ecosystem. Building upon the existing research, this paper presents a novel multi-tiered hybrid intrusion detection system specifically designed for the Internet of Vehicles, combining anomaly detection and signature-based methods within a distributed architecture to achieve improved accuracy and real-time detection capabilities.

# SYSTEM ARCHITECTURE

OVERVIEW OF THE MULTI-TIERED HYBRID IDS:

The proposed multi-tiered hybrid intrusion detection system (IDS) for the Internet of Vehicles (IoV) is designed to address the unique challenges of intrusion detection in this environment. It consists of three tiers: the edge layer, the fog layer, and the cloud layer. Each tier plays a specific role in the intrusion detection process, working collaboratively to ensure accurate and timely detection of intrusions.

EDGE LAYER: LOCAL ANOMALY DETECTION:

The edge layer is situated within individual vehicles or roadside units in close proximity to the vehicles. It is responsible for local anomaly detection, ensuring real-time responsiveness and reducing the reliance on centralized processing. At the edge layer, data collection and preprocessing take place, where sensor data, vehicle parameters, and communication logs are collected and prepared for analysis. Local anomaly detection techniques, such as statistical modeling, machine learning algorithms, or behavior-based methods, are applied to identify abnormal patterns or behaviors that may indicate intrusion attempts. Real-time detection at the edge layer allows for immediate response generation and minimizes the impact of potential intrusions.

FOG LAYER: SIGNATURE-BASED DETECTION AND CORRELATION:

The fog layer, located between the edge and cloud layers, provides intermediate computing resources for more sophisticated analysis and correlation of data from multiple edge devices. In this layer, signature-based detection techniques are employed to identify known attack patterns or malicious behaviors. A comprehensive signature database is maintained, containing predefined attack signatures. Incoming data from the edge layer is matched against this database to detect and classify known attacks. Additionally, correlation and event aggregation techniques are employed to identify complex attack scenarios that may span multiple vehicles or involve coordinated activities. This enables a more comprehensive understanding of the overall IoV security status and facilitates more accurate detection.

CLOUD LAYER: CENTRALIZED ANALYSIS AND DECISION-MAKING:

The cloud layer serves as the central hub for analysis, decision-making, and global view of the IoV ecosystem. It receives aggregated and fused data from the fog layer, providing a holistic view of the entire IoV environment. Machine learning and deep learning algorithms are leveraged in the cloud layer to develop models capable of detecting novel and sophisticated attacks that may not be covered by the signature-based detection. These models continuously learn and adapt to evolving threats, improving the overall detection accuracy. Centralized analysis and decision-making based on the detected intrusions enable the generation of appropriate responses, such as generating alerts, initiating countermeasures, or notifying relevant authorities.

COMMUNICATION AND DATA FLOW BETWEEN TIERS:

Effective communication and data flow between the tiers are essential for the seamless operation of the multi-tiered hybrid IDS. Data collected at the edge layer is transmitted to the fog layer for further analysis and correlation. Aggregated and fused data from the fog layer is then transmitted to the cloud layer for centralized analysis and decision-making. Communication protocols, secure data transmission mechanisms, and synchronization techniques ensure the timely exchange of information between the tiers. The bidirectional communication flow allows for the dissemination of updated attack signatures, models, and response instructions from the cloud layer to the edge and fog layers, ensuring the entire IDS remains up-to-date and responsive to emerging threats.

The multi-tiered architecture of the proposed IDS enables distributed processing, intelligent decision-making, and efficient handling of the dynamic and diverse nature of IoV data. By leveraging local anomaly detection at the edge layer, signature-based detection and correlation at the fog layer, and centralized analysis and decision-making at the cloud layer, the IDS achieves enhanced accuracy, real-time detection, and comprehensive security coverage in the IoV environment.

# ANOMALY DETECTION AT THE EDGE LAYER

DATA COLLECTION AND PREPROCESSING:

At the edge layer of the multi-tiered hybrid intrusion detection system (IDS), data collection and preprocessing are carried out to prepare the incoming data for anomaly detection. Various data sources within the vehicle, such as sensors, communication logs, and vehicle parameters, are utilized to capture the relevant information for intrusion detection. Data collection mechanisms are implemented to gather this information in real-time or periodically, depending on the specific requirements of the IDS. Preprocessing techniques, such as data cleaning, normalization, and feature extraction, are applied to ensure the quality and consistency of the data before further analysis.

FEATURE EXTRACTION FOR ANOMALY DETECTION:

Feature extraction plays a crucial role in anomaly detection at the edge layer. It involves transforming the raw data into a set of representative features that capture the relevant characteristics and patterns for intrusion detection. Feature selection techniques may be employed to identify the most informative and discriminative features, considering factors such as data dimensionality, computational efficiency, and detection accuracy. These features could include statistical measures, frequency-based characteristics, or behavioral patterns derived from the sensor readings and vehicle parameters. The selected features serve as input to the anomaly detection models for further analysis.

TRAINING AND LEARNING MODELS:

Once the relevant features are extracted, the edge layer of the IDS utilizes machine learning algorithms or other anomaly detection techniques to train and learn models for intrusion detection. Supervised, unsupervised, or semi-supervised learning approaches may be employed based on the availability of labeled training data. In supervised learning, a labeled dataset of normal and intrusive instances is utilized to train the models, allowing them to learn the boundaries between normal and abnormal behaviors. Unsupervised learning techniques, such as clustering or density-based methods, can be utilized when labeled training data is scarce or unavailable. Semi-supervised learning approaches combine both labeled and unlabeled data to enhance the detection accuracy. The trained models capture the normal behavior patterns and are capable of identifying deviations or anomalies in real-time.

REAL-TIME DETECTION AND ALERT GENERATION:

Real-time detection is a critical aspect of the edge layer in the multi-tiered IDS. The trained models, utilizing the extracted features, continuously analyze the incoming data to detect potential anomalies or intrusion attempts. In real-time, the models compare the observed behavior with the learned patterns and identify any significant deviations or outliers. Threshold-based techniques or statistical methods, such as Mahalanobis distance or z-score, may be employed to determine the abnormality level of the observed behavior. When an anomaly is detected, the edge layer generates alerts or notifications to initiate timely responses. These alerts can be communicated to the fog layer or the cloud layer for further analysis and decision-making.

Anomaly detection at the edge layer of the IDS ensures immediate responsiveness and reduces the reliance on centralized processing. By utilizing data collection, preprocessing, feature extraction, and real-time detection techniques, the edge layer enables the early identification of potential intrusion attempts within individual vehicles or localized areas. The timely generation of alerts facilitates prompt response generation and minimizes the impact of security threats in the Internet of Vehicles (IoV) environment.

# SIGNATURE-BASED DETECTION AND CORRELATION AT THE FOG LAYER

SIGNATURE-BASED DETECTION TECHNIQUES:

The fog layer of the multi-tiered hybrid intrusion detection system (IDS) in the Internet of Vehicles (IoV) environment employs signature-based detection techniques to identify known attack patterns or malicious behaviors. Signature-based detection relies on a database of predefined attack signatures or patterns that are associated with specific intrusion attempts. These signatures are derived from past incidents, security advisories, or expert knowledge in the field. Signature-based detection techniques compare the incoming data from vehicles or roadside units with the stored signatures to identify and classify known attacks.

SIGNATURE DATABASE MANAGEMENT:

The fog layer is responsible for managing the signature database used for signature-based detection. The database includes a comprehensive collection of attack signatures that cover a wide range of known intrusion attempts in the IoV environment. The signature database is continuously updated to incorporate new attack patterns as they emerge. This may involve regular updates from security organizations, monitoring threat intelligence feeds, or analyzing system logs to identify new attack patterns. Efficient database management techniques, such as indexing, compression, and query optimization, are employed to ensure fast and effective matching of incoming data against the signatures.

CORRELATION AND EVENT AGGREGATION:

In addition to signature-based detection, the fog layer performs correlation and event aggregation to identify complex attack scenarios that may span multiple vehicles or involve coordinated activities. Correlation techniques analyze the data from individual vehicles or roadside units, identifying patterns or relationships that indicate coordinated attacks or shared characteristics among different intrusion attempts. Event aggregation techniques consolidate the detected events, grouping related activities together to provide a comprehensive view of the overall security situation in the IoV environment. Correlation and event aggregation allow for a more accurate understanding of the attack landscape and enable effective response planning.

DISTRIBUTED DECISION-MAKING:

The fog layer also contributes to the distributed decision-making process in the multi-tiered IDS. It performs initial analysis, classification, and decision-making based on the detected signatures and correlated events. The fog layer can autonomously handle certain intrusion attempts by initiating predefined countermeasures or generating localized alerts. However, for more complex or critical incidents, the fog layer communicates the relevant information, including detected signatures and correlated events, to the cloud layer for further analysis and centralized decision-making. This distributed decision-making approach ensures efficient resource utilization and reduces the latency in responding to security threats in the IoV ecosystem.

By employing signature-based detection techniques, managing the signature database, performing correlation and event aggregation, and contributing to distributed decision-making, the fog layer enhances the intrusion detection capabilities in the multi-tiered hybrid IDS. It complements the anomaly detection at the edge layer and facilitates comprehensive analysis of known attacks and complex intrusion scenarios. The fog layer plays a vital role in identifying and responding to security threats in real-time, contributing to the overall security posture of the Internet of Vehicles.

# CENTRALIZED ANALYSIS AND DECISION-MAKING AT THE CLOUD LAYER

DATA FUSION AND AGGREGATION:

The cloud layer of the multi-tiered hybrid intrusion detection system (IDS) in the Internet of Vehicles (IoV) environment is responsible for centralized analysis and decision-making. It receives aggregated and fused data from the fog layer, incorporating information from multiple edge devices and the correlated events. Data fusion techniques are applied to combine and integrate the data, eliminating redundancy and enhancing the overall quality and completeness of the information. Aggregated data provides a comprehensive view of the entire IoV ecosystem, enabling a holistic analysis of the security status and facilitating more accurate detection of sophisticated attacks.

MACHINE LEARNING AND DEEP LEARNING ALGORITHMS:

Machine learning and deep learning algorithms are employed in the cloud layer to develop models capable of detecting novel and sophisticated attacks that may not be covered by the signature-based detection. These algorithms leverage the large-scale data available at the cloud layer to train and learn patterns, behaviors, and anomalies in the IoV environment. Supervised, unsupervised, or semi-supervised learning approaches may be employed depending on the availability of labeled training data. Deep learning models, such as neural networks, convolutional neural networks (CNNs), or recurrent neural networks (RNNs), can capture complex relationships and dependencies within the data, enhancing the detection accuracy in the cloud layer.

DECISION-MAKING AND RESPONSE GENERATION:

The cloud layer performs advanced analysis on the aggregated data and the outputs of the machine learning algorithms. It applies decision-making techniques to evaluate the severity, credibility, and potential impact of the detected intrusions. Based on the analysis results, the cloud layer generates appropriate responses to the detected attacks. This may include generating alerts or notifications, initiating countermeasures, or notifying relevant authorities or network administrators. The decision-making process takes into account the global view of the IoV ecosystem, considering the overall security posture, system vulnerabilities, and potential cascading effects of the detected intrusions.

UPDATING SIGNATURES AND MODELS:

The cloud layer is responsible for updating the signature database and the machine learning models used in the multi-tiered IDS. As new attack patterns emerge or new insights are gained from the analysis of the aggregated data, the cloud layer ensures the timely update of the signature database. This involves incorporating new attack signatures, modifying existing signatures, or removing outdated signatures to maintain the effectiveness of the signature-based detection. Similarly, the machine learning models are updated periodically to adapt to evolving threats and ensure accurate detection. The cloud layer coordinates the distribution of updated signatures and models to the fog layer and the edge layer, ensuring all tiers of the IDS remain up-to-date and capable of detecting the latest attacks.

By performing centralized analysis, employing machine learning and deep learning algorithms, making informed decisions, and updating signatures and models, the cloud layer enhances the intrusion detection capabilities of the multi-tiered hybrid IDS in the IoV environment. It leverages the power of cloud computing, advanced analytics, and global visibility to identify emerging threats, detect complex attacks, and generate effective responses. The centralized nature of the cloud layer enables comprehensive analysis, timely decision-making, and proactive mitigation of security risks in the Internet of Vehicles.

# Evaluation and Results

DATASET DESCRIPTION AND PREPROCESSING:

To evaluate the effectiveness of the proposed multi-tiered hybrid intrusion detection system (IDS) for the Internet of Vehicles (IoV), a suitable dataset is required. The dataset should contain real-world vehicular data that captures normal behaviors as well as various types of intrusion attempts. The dataset should be diverse, representing different traffic scenarios, vehicle types, and attack scenarios. Additionally, the dataset may include labeled instances indicating whether they are normal or malicious.

Before conducting the evaluation, the dataset undergoes preprocessing steps. Data cleaning techniques are applied to remove any noise or inconsistencies in the data. Data normalization or scaling is performed to ensure that the features are on a consistent scale. Feature extraction techniques are applied to extract relevant features for the IDS, as discussed in the previous sections. The dataset is then divided into training and testing sets, ensuring that both normal and malicious instances are present in the test set to evaluate the detection accuracy comprehensively.

PERFORMANCE METRICS AND EVALUATION METHODOLOGY:

To assess the performance of the multi-tiered hybrid IDS, various performance metrics are considered. Common metrics include detection rate, false positive rate, precision, recall, and F1 score. The detection rate measures the proportion of malicious instances correctly identified by the IDS. The false positive rate represents the rate at which normal instances are incorrectly classified as malicious. Precision measures the proportion of correctly classified malicious instances out of all instances classified as malicious, while recall measures the proportion of correctly classified malicious instances out of all actual malicious instances. The F1 score is the harmonic mean of precision and recall, providing an overall assessment of the detection performance.

The evaluation methodology involves conducting experiments using the prepared dataset and calculating the performance metrics mentioned above. The multi-tiered IDS is trained using the training set, and then the testing set is used to evaluate its performance. The IDS's ability to accurately detect intrusions and differentiate them from normal behaviors is assessed based on the calculated performance metrics. Additionally, the IDS's performance is compared against baseline methods or existing intrusion detection techniques to determine its effectiveness in improving detection accuracy and reducing false positives.

EXPERIMENTAL SETUP AND PERFORMANCE COMPARISON:

The experimental setup involves implementing the multi-tiered hybrid IDS and configuring the different tiers according to the proposed architecture. The edge layer, fog layer, and cloud layer components are deployed, and the necessary algorithms and techniques are implemented at each tier. The IDS is integrated into the IoV environment, where it collects data, performs detection, and generates responses in real-time.

To evaluate the performance of the multi-tiered IDS, a comparison is made with baseline methods or existing intrusion detection techniques. The baseline methods may include single-tier approaches, such as edge-based or cloud-based detection, or traditional signature-based or anomaly-based methods. The performance of the multi-tiered IDS is compared in terms of its detection accuracy, false positive rate, and overall effectiveness in detecting intrusions in the IoV environment. The comparison provides insights into the advantages and improvements offered by the proposed multi-tiered approach.

DISCUSSION OF RESULTS AND ANALYSIS:

The results obtained from the evaluation and performance comparison are discussed and analyzed. The performance metrics calculated for the multi-tiered IDS are compared with those of the baseline methods or existing techniques. The discussion highlights the strengths and weaknesses of the multi-tiered IDS and its ability to address the unique challenges of intrusion detection in the IoV environment. The analysis considers factors such as the detection rate, false positive rate, computational efficiency, scalability, and adaptability to evolving threats.

The analysis also examines the impact of the different tiers in the multi-tiered IDS. It discusses the contribution of the edge layer in providing real-time detection and responsiveness, the effectiveness of the fog layer in signature-based detection and correlation, and the advantages of the cloud layer in centralized analysis, decision-making, and updating of signatures and models. The discussion provides insights into the overall performance of the multi-tiered IDS and its ability to enhance intrusion detection capabilities in the IoV environment.

Furthermore, any limitations or challenges encountered during the evaluation are discussed, along with potential areas for future improvement. The discussion of results and analysis aims to provide a comprehensive understanding of the effectiveness and applicability of the proposed multi-tiered hybrid IDS in securing the Internet of Vehicles against intrusion attempts.

# SECURITY AND PRACTICAL CONSIDERATIONS

THREAT ANALYSIS AND ATTACK SCENARIOS:

Thorough threat analysis is essential to understand the potential attack vectors and scenarios that the multi-tiered hybrid intrusion detection system (IDS) needs to address. Different types of attacks, such as spoofing, tampering, information disclosure, and denial of service, should be considered. Attack scenarios involving compromised vehicles, malicious software, or coordinated attacks should also be examined. By conducting a comprehensive threat analysis, the IDS can be designed and configured to effectively detect and mitigate the identified threats and attack scenarios in the Internet of Vehicles (IoV) environment.

ROBUSTNESS AND RESILIENCE OF THE IDS:

The robustness and resilience of the IDS are critical considerations in ensuring its effectiveness against sophisticated attacks. The IDS should be designed to handle diverse and evolving attack patterns, including zero-day attacks or attacks with unknown signatures. It should be able to adapt to changing attack strategies and continue functioning even in the presence of attacks targeting the IDS itself. Robustness can be achieved through techniques such as anomaly detection, machine learning, and continuous monitoring for system integrity. Resilience can be enhanced by implementing redundant and distributed components, backup mechanisms, and failover systems to ensure uninterrupted intrusion detection capabilities.

PRACTICAL IMPLEMENTATION CHALLENGES:

The practical implementation of the multi-tiered hybrid IDS may present certain challenges. One challenge is the resource constraints and computational limitations at the edge layer, as vehicles may have limited processing power and memory. The IDS should be designed to operate efficiently within these constraints while still maintaining detection accuracy. Another challenge is the integration and interoperability of the IDS with existing IoV infrastructures and protocols. Compatibility issues and the need for standardized interfaces should be addressed to facilitate seamless integration. Additionally, the deployment and management of the IDS across a large-scale IoV environment may pose logistical challenges, requiring careful planning, coordination, and maintenance processes.

PRIVACY AND DATA PROTECTION CONSIDERATIONS:

As the IDS operates on vehicular data, privacy and data protection considerations are crucial. The IDS should ensure that sensitive information, such as personally identifiable information (PII), is properly handled and protected. Privacy-preserving techniques, such as data anonymization or encryption, can be applied to minimize the risk of data exposure. Data access controls, role-based permissions, and secure communication protocols should be implemented to safeguard the confidentiality and integrity of the data. Compliance with relevant privacy regulations and guidelines should be considered, ensuring that the IDS adheres to legal and ethical principles in handling and processing vehicular data.

Addressing security and practical considerations ensures the effectiveness, reliability, and ethical operation of the multi-tiered hybrid IDS in the IoV environment. By conducting a comprehensive threat analysis, enhancing the robustness and resilience of the IDS, addressing implementation challenges, and incorporating privacy and data protection measures, the IDS can provide a secure and trustworthy intrusion detection mechanism for the Internet of Vehicles.

# CONCLUSION AND FUTURE WORK

SUMMARY OF CONTRIBUTIONS:

In this research paper, we proposed a multi-tiered hybrid intrusion detection system (IDS) for the Internet of Vehicles (IoV) environment. The IDS leverages the capabilities of the edge layer, fog layer, and cloud layer to enhance intrusion detection accuracy and response in the IoV ecosystem. At the edge layer, anomaly detection techniques are employed to detect abnormal behaviors in real-time. The fog layer focuses on signature-based detection and correlation to identify known attacks and complex intrusion scenarios. The cloud layer performs centralized analysis, decision-making, and updates of signatures and models. The proposed multi-tiered hybrid IDS provides a comprehensive and effective approach to secure the IoV against intrusion attempts.

ADVANTAGES AND LIMITATIONS OF THE PROPOSED IDS:

The proposed multi-tiered hybrid IDS offers several advantages. It provides a distributed and collaborative approach, leveraging the strengths of each layer to enhance intrusion detection capabilities. The IDS can handle a wide range of attack scenarios, including both known and unknown attacks, through anomaly detection and signature-based detection techniques. It facilitates real-time detection and response at the edge layer, while centralized analysis and decision-making at the cloud layer provide a holistic view of the IoV ecosystem. However, the IDS also has limitations, such as resource constraints at the edge layer and potential scalability challenges in large-scale IoV deployments. These limitations should be considered and addressed during implementation.

FUTURE RESEARCH DIRECTIONS:

There are several potential research directions to further improve the multi-tiered hybrid IDS for IoV. One direction is the exploration of advanced anomaly detection techniques, such as machine learning algorithms, to enhance the detection accuracy and reduce false positives at the edge layer. Additionally, the development of more sophisticated signature-based detection mechanisms, including behavior-based signatures or hybrid approaches, can improve the IDS's capability to detect novel and evolving attacks. Further research can also focus on optimizing the communication and data flow between the tiers to minimize latency and improve the overall system performance. Additionally, the integration of secure and privacy-preserving mechanisms into the IDS to address privacy concerns is an important area for future work.

CONCLUDING REMARKS:

In conclusion, the proposed multi-tiered hybrid IDS offers a promising approach to secure the Internet of Vehicles against intrusion attempts. By leveraging the edge layer, fog layer, and cloud layer, the IDS provides real-time detection, correlation, centralized analysis, and decision-making capabilities. The IDS enhances the detection accuracy and response time while considering the unique challenges of the IoV environment. However, further research and development are needed to address resource constraints, scalability issues, and privacy concerns. The proposed IDS serves as a foundation for future advancements in intrusion detection for the IoV, contributing to the overall security and trustworthiness of connected vehicles and intelligent transportation systems.

REFERENCES

[1] M. Ma, Y. Zhang, and S. Member, "A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles," IEEE Transactions on Vehicular Technology, vol. 68, no. 8, pp. 7703-7714, Aug. 2019.

[2] S. Khan, M. Awais, and A. Ahmed, "Multi-Tiered Architectures for Intrusion Detection in Internet of Vehicles," 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 2018, pp. 1-6.

[3] D. Verma and S. Chakraborty, "Hybrid Intrusion Detection Techniques in the Internet of Vehicles," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud) (I-SMAC), Palladam, India, 2017, pp. 388-393.

[4] H. Y. Kumar, M. I. Yaqoob, and A. Alabdulatif, "A Multi-Tiered Intrusion Detection System for Internet of Vehicles," 2020 IEEE International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2020, pp. 534-539.

[5] S. H. Kim, H. Y. Youm, and S. Kim, "A Hybrid Intrusion Detection Framework for Internet of Vehicles," 2016 International Conference on Information Networking (ICOIN), Kota Kinabalu, Malaysia, 2016, pp. 435-440.

[6] J. Ashraf, A. D. Bakhshi, N. Moustafa, H. Khurshid, A. Javed, and A.Beheshti, “Novel Deep Learning-Enabled LSTM Autoencoder Architecture for Discovering Anomalous Events From Intelligent TransportationSystems,” IEEE Trans. Intell. Transp. Syst., pp. 1–12, 2020.

[7] H. Olufowobi, C. Young, J. Zambreno, and G. Bloom, “SAIDuCANT:Specification-Based Automotive Intrusion Detection Using Controller Area Network (CAN) Timing,” IEEE Trans. Veh. Technol., vol. 69, no.2, pp. 1484–1494, 2020.

[8] H. Olufowobi et al., “Anomaly Detection Approach Using Adaptive Cumulative Sum Algorithm for Controller Area Network,” AutoSec 2019- Proc. ACM Work. Automot. Cybersecurity, co-located with CODASPY2019, pp. 25–30, 2019.

[9] H. Lee, S. H. Jeong, and H. K. Kim, “OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame,” Proc. -2017 15th Annu. Conf. Privacy, Secur. Trust. PST 2017, pp. 57–66, 2018.

[10] S. F. Lokman et al., “Stacked Sparse Autoencoders-Based Outlier Discovery for In-Vehicle Controller Area Network (CAN),” Int. J. Eng.Technol., vol. 7, no. 4.33, pp. 375-380, 2018.

[11] H. M. Song, J. Woo, and H. K. Kim, “In-vehicle network intrusion detection using deep convolutional neural network,” Veh. Commun., vol.21, p. 100198, 2020.