Intrusion Detection Systems for Automotive Networks: Implementing AI-Powered Solutions to Enhance Cybersecurity in In-Vehicle Communication Protocols

***Rajalakshmi Soundarapandiyan**, Elementalent Technologies, USA*

***Yeswanth Surampudi**, Beyond Finance, USA*

***Akila Selvaraj**, iQi Inc, USA*

Abstract

As the automotive industry evolves towards increased autonomy and connectivity, the cybersecurity of in-vehicle communication networks has become a critical concern. Modern vehicles incorporate multiple interconnected electronic control units (ECUs) that communicate through various protocols such as the Controller Area Network (CAN), FlexRay, and Ethernet, forming complex networks that are vulnerable to cyber-attacks. Intrusion Detection Systems (IDS) are pivotal in safeguarding these networks by identifying and mitigating malicious activities. This paper explores the implementation of Artificial Intelligence (AI)-powered IDS for automotive networks, specifically focusing on in-vehicle communication protocols like CAN and Automotive Ethernet. Traditional IDS methods have proven insufficient due to the evolving nature of attack vectors targeting vehicular networks, necessitating more advanced, adaptive, and scalable solutions. AI-powered IDS, leveraging machine learning (ML) and deep learning (DL) algorithms, have shown significant promise in detecting zero-day attacks and sophisticated intrusion attempts that bypass conventional rule-based detection systems.

This research provides a comprehensive analysis of the types of IDS applicable to automotive networks, including Signature-based, Anomaly-based, and Hybrid IDS, and emphasizes the growing preference for Anomaly-based IDS due to their adaptability and effectiveness against unknown threats. It discusses the architecture and operational principles of AI-based IDS, highlighting the role of supervised, unsupervised, and reinforcement learning algorithms in detecting anomalies within vehicular communication protocols. Techniques such as Support

Vector Machines (SVM), Random Forests, Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and Autoencoders are examined for their effectiveness in identifying deviations from normal traffic patterns, signaling potential intrusions. The paper evaluates these algorithms based on detection accuracy, false positive rates, computational overhead, and real-time processing capabilities, providing a critical assessment of their suitability for deployment in resource-constrained automotive environments.

Additionally, the study investigates the unique challenges associated with implementing AI-powered IDS in automotive networks, such as the high dimensionality of network data, latency constraints, limited processing power of ECUs, and the need for real-time detection and response mechanisms. The constraints posed by the bandwidth limitations of in-vehicle networks, particularly the CAN bus, are discussed, emphasizing the importance of lightweight and efficient algorithms. The potential of edge computing to complement AI-based IDS by providing distributed processing capabilities closer to the data source is explored, reducing latency and enabling real-time anomaly detection and response. Furthermore, the paper delves into the integration of AI-powered IDS with Vehicle-to-Everything (V2X) communication systems, ensuring the security of data exchanged between vehicles and other entities such as infrastructure, pedestrians, and cloud servers. This integration introduces additional challenges, including data privacy, synchronization, and scalability, which are addressed with proposed architectural modifications and hybrid IDS models that combine centralized and decentralized detection techniques.

Case studies involving real-world vehicular networks are presented to illustrate the practical applications and effectiveness of AI-powered IDS in detecting and mitigating diverse attack scenarios, such as Denial of Service (DoS) attacks, message spoofing, and replay attacks. These case studies highlight the performance benefits of ML and DL algorithms in dynamic and high-risk environments, underscoring their potential to significantly enhance the cybersecurity of modern and future vehicles. The paper also examines the use of Generative Adversarial Networks (GANs) to simulate realistic attack scenarios and train IDS models to recognize novel attack patterns, enhancing their robustness against adversarial machine learning techniques.

Finally, this research outlines the future directions and opportunities for AI-based IDS in automotive networks, including the integration of federated learning to facilitate collaborative model training across distributed vehicular nodes without compromising data privacy. The evolving regulatory landscape and standards for automotive cybersecurity, such as the ISO/SAE 21434, are also considered, emphasizing the need for IDS frameworks that comply with these standards while maintaining flexibility and scalability. The paper concludes with a discussion on the ethical considerations and potential risks associated with deploying AI-driven solutions in critical safety systems, advocating for a balanced approach that prioritizes both security and safety in the automotive domain.

Keywords:

automotive networks, intrusion detection systems, AI-powered solutions, in-vehicle communication protocols, CAN bus, Ethernet, machine learning, anomaly detection, cybersecurity, vehicle-to-everything (V2X).

1. Introduction

The advent of advanced automotive technologies has profoundly transformed vehicle architectures, leading to a marked increase in the complexity of in-vehicle networks. Initially, automotive networks were relatively simple, comprising a few electronic control units (ECUs) that managed basic vehicle functions. Over the past few decades, however, there has been a significant shift towards highly sophisticated, interconnected systems designed to support modern features such as advanced driver assistance systems (ADAS), infotainment systems, and vehicle-to-everything (V2X) communication. This evolution has been facilitated by the integration of high-speed communication protocols such as Controller Area Network (CAN) and Ethernet, which have become integral to the operation of contemporary vehicles.

The Controller Area Network (CAN), introduced in the early 1980s, was designed to provide robust and reliable communication between ECUs in vehicles, enabling real-time data exchange and coordination of critical functions. With the advent of more data-intensive applications, such as video streaming for cameras and sensors, automotive Ethernet has

emerged as a more scalable and higher-bandwidth alternative, supporting data rates up to 1 Gbps and beyond. The shift towards Ethernet and other high-speed protocols reflects the increasing demands for data processing and transmission in modern vehicles, driven by the proliferation of sensor-based technologies and complex vehicular networks.

Despite the advancements in automotive networking, this increased complexity introduces new vulnerabilities and challenges. The integration of numerous communication protocols, the proliferation of connected devices, and the rising sophistication of cyber threats necessitate robust security measures to protect against potential attacks. The automotive industry's transition towards greater connectivity and automation underscores the critical need for advanced security solutions that can effectively safeguard the integrity and confidentiality of vehicular networks.

The evolving landscape of automotive networks has brought to light several challenges and vulnerabilities associated with current communication protocols. The Controller Area Network (CAN), while reliable and widely used, was not originally designed with security in mind. Its broadcast nature, where messages are transmitted to all nodes on the network, makes it susceptible to various forms of attacks, including message spoofing, denial of service (DoS), and message injection. The lack of inherent authentication and encryption mechanisms in CAN further exacerbates its vulnerability to unauthorized access and manipulation.

Automotive Ethernet, although a significant advancement over CAN in terms of data transfer rates and bandwidth, presents its own set of security challenges. The Ethernet protocol's complexity and its widespread use in networked environments introduce potential attack vectors, such as network sniffing, man-in-the-middle attacks, and protocol exploitation. The increased data throughput and integration with external networks, including cloud services and V2X communication, further heighten the risk of exposure to cyber threats.

The challenge of securing in-vehicle communication protocols is compounded by the diverse and evolving nature of cyber threats. Attackers are continuously developing new techniques to exploit vulnerabilities, necessitating dynamic and adaptive security solutions. Traditional security measures, such as firewalls and intrusion prevention systems, are often inadequate in addressing the unique requirements of automotive networks, which demand real-time detection and response to sophisticated threats.

The primary objective of this study is to explore the implementation of AI-powered Intrusion Detection Systems (IDS) within automotive networks, with a specific focus on in-vehicle communication protocols such as CAN and Automotive Ethernet. The study aims to address the limitations of traditional security measures by leveraging advanced machine learning (ML) and deep learning (DL) techniques to enhance the detection and mitigation of cyber threats in real-time.

AI-powered IDS represent a promising solution for addressing the complex and dynamic nature of cybersecurity threats in automotive networks. By utilizing ML and DL algorithms, these systems can analyze vast amounts of network traffic data to identify anomalous patterns and potential intrusions that may be indicative of sophisticated attacks. The ability of AI-powered IDS to learn from historical data and adapt to emerging threats offers a significant advantage over conventional rule-based systems, which often struggle to keep pace with evolving attack techniques.

The significance of AI-powered IDS in enhancing vehicular cybersecurity lies in their potential to provide a higher level of protection for critical vehicular systems. By enabling real-time detection and response, these systems can help prevent unauthorized access, data breaches, and disruptions to vehicle operation. Furthermore, the integration of AI-powered IDS with existing automotive security frameworks can contribute to the development of a more resilient and adaptive cybersecurity posture, addressing the challenges posed by the increasing complexity of automotive networks.

This research focuses on the application of AI-powered IDS to automotive networks, with particular emphasis on in-vehicle communication protocols such as CAN and Automotive Ethernet. The study will examine the effectiveness of various machine learning and deep learning algorithms in detecting and mitigating cyber threats, considering factors such as detection accuracy, false positive rates, and computational overhead.

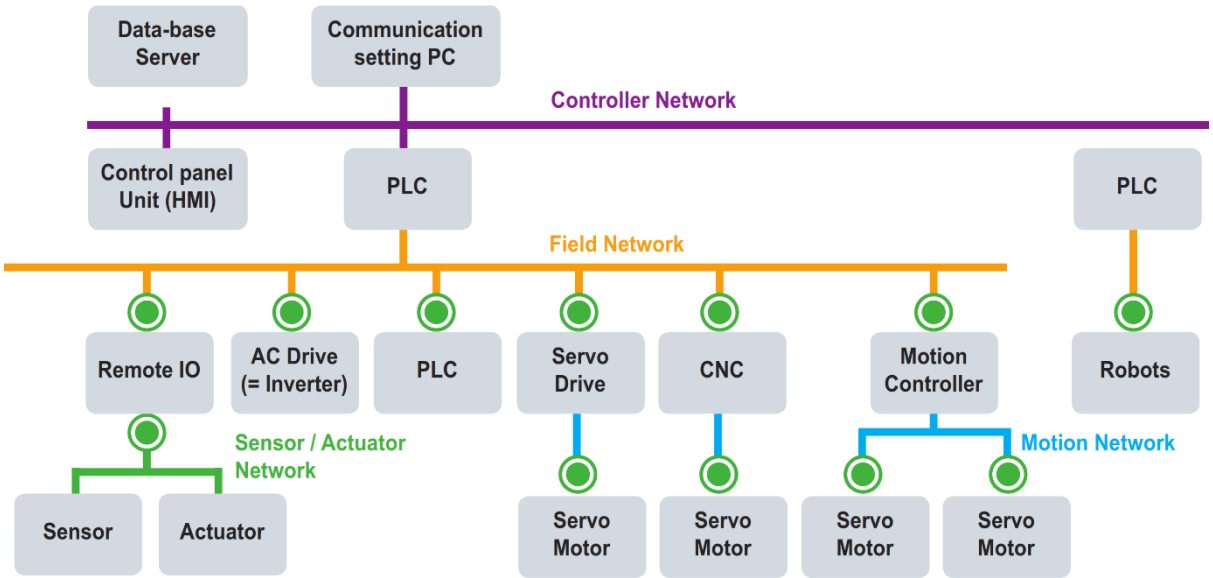
The scope of the research includes a detailed analysis of the architectural and operational principles of AI-based IDS, as well as an exploration of the unique challenges associated with deploying these systems in automotive environments. The study will also address the integration of AI-powered IDS with Vehicle-to-Everything (V2X) communication systems and evaluate real-world case studies to assess the practical applications and effectiveness of these solutions.

While the research aims to provide a comprehensive overview of AI-powered IDS for automotive networks, it is important to acknowledge certain limitations. The study will primarily focus on the technical aspects of IDS implementation and may not extensively cover broader topics such as regulatory compliance, ethical considerations, and industry-wide standardization efforts. Additionally, the research will be constrained by the availability of data and the specific contexts of the case studies reviewed.

2. Automotive Communication Protocols

Controller Area Network (CAN): Technical Details, Common Applications, and Vulnerabilities

The Controller Area Network (CAN), developed by Robert Bosch in the 1980s, is a robust, real-time, and fault-tolerant communication protocol widely utilized in automotive networks. Its design emphasizes reliability and efficiency, employing a multi-master, message-based architecture. CAN operates using a differential signal transmission scheme that provides noise immunity and robustness against electrical interference. The protocol supports a variety of data transmission speeds, ranging from 10 Kbps to 1 Mbps, accommodating various requirements for in-vehicle communication.



CAN's fundamental characteristic is its broadcast nature; messages are transmitted to all nodes on the network, which listen for messages relevant to their function. This approach simplifies network design and facilitates easy integration of new nodes. CAN messages are structured into data frames that include an identifier, control information, and data payload. The identifier is crucial, as it defines the message priority and determines the order in which messages are transmitted.

In automotive applications, CAN is instrumental in managing critical systems such as engine control units (ECUs), transmission control, and braking systems. It enables real-time data exchange between these units, ensuring coordinated operation and response to dynamic conditions. The protocol's fault-tolerant design includes features such as automatic retransmission of corrupted messages and error detection mechanisms, enhancing system reliability.

Despite its advantages, CAN is not without vulnerabilities. Its broadcast nature, while beneficial for network integration, poses significant security risks. Unauthorized nodes can potentially intercept and manipulate messages, leading to attacks such as message spoofing and injection. Additionally, the lack of built-in encryption and authentication mechanisms in CAN exposes the network to risks of data eavesdropping and unauthorized access. The simplicity of the CAN protocol, designed for efficiency rather than security, makes it susceptible to various types of cyber threats that traditional security measures may not adequately address.

Automotive Ethernet: Features, Advantages Over CAN, and Associated Security Concerns

Automotive Ethernet represents a significant advancement over traditional CAN, addressing the increasing demands for higher data throughput and bandwidth in modern vehicles. Ethernet technology, initially developed for general networking purposes, has been adapted for automotive applications to support high-speed data transfer and real-time communication. Automotive Ethernet supports data rates up to 1 Gbps and beyond, facilitating the transmission of large volumes of data generated by advanced sensors, cameras, and infotainment systems.

One of the primary advantages of Automotive Ethernet is its scalability. Unlike CAN, which operates on a fixed bandwidth and requires network segmentation for higher data rates,

Ethernet's flexible architecture allows for the deployment of various network topologies, such as star, daisy-chain, and hybrid configurations. This flexibility enhances network design and integration, accommodating a broader range of applications and requirements.

Automotive Ethernet also offers improved bandwidth and latency characteristics compared to CAN. Its support for high-speed data transfer and packet-based communication makes it suitable for applications requiring large data exchanges, such as high-definition video streaming and complex sensor fusion. Additionally, Ethernet's standardization and widespread use in other industries provide a mature ecosystem of tools and technologies for network management and troubleshooting.

However, the transition to Automotive Ethernet introduces new security challenges. The increased complexity and integration with external networks, including cloud services and Vehicle-to-Everything (V2X) communication, heighten the risk of exposure to cyber threats. Ethernet's susceptibility to network sniffing, man-in-the-middle attacks, and protocol exploitation necessitates the implementation of robust security measures. Unlike CAN, Ethernet does not inherently include security features, requiring additional layers of protection, such as encryption and authentication protocols, to safeguard against potential vulnerabilities.

Other Protocols: Brief Overview of Additional Communication Protocols Used in Automotive Networks

In addition to CAN and Automotive Ethernet, several other communication protocols play critical roles in automotive networks, each with its own unique features and applications.

FlexRay is a high-speed, time-triggered communication protocol designed to address the limitations of CAN in terms of data rate and real-time performance. FlexRay operates on a dual-channel architecture that provides redundancy and fault tolerance, making it suitable for safety-critical applications such as advanced driver assistance systems (ADAS) and autonomous driving. The protocol supports data rates up to 10 Mbps and employs a time-triggered protocol (TTP) to ensure deterministic communication, where messages are transmitted at predefined intervals. While FlexRay offers significant improvements in terms of speed and reliability, its complexity and cost are higher compared to CAN.

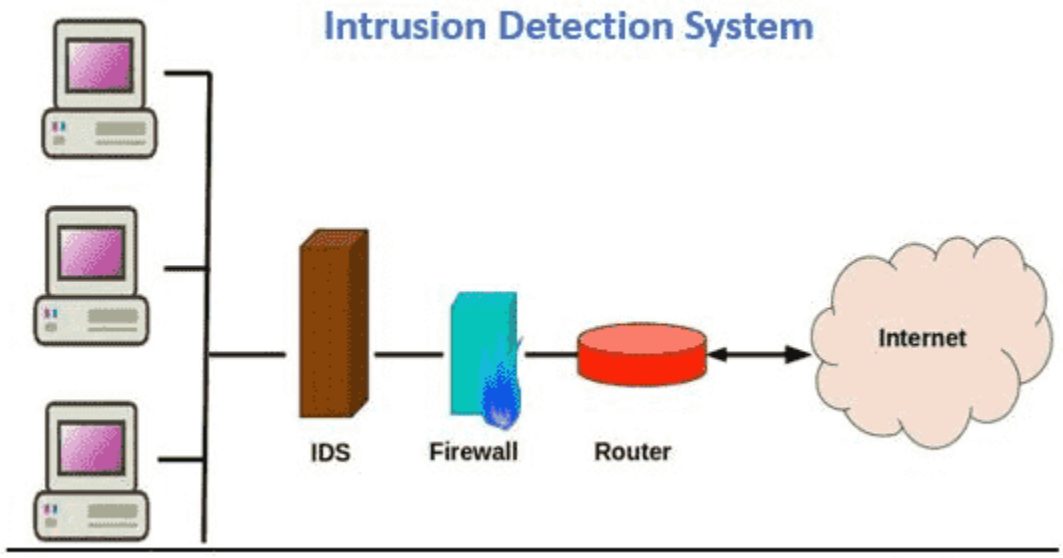
Local Interconnect Network (LIN) is another protocol used in automotive networks, designed for low-speed, low-cost applications. LIN is often employed for communication between lower-end ECUs and sensors, such as those managing interior lighting or window controls. It operates on a single-wire bus and supports data rates up to 20 Kbps. LIN's simplicity and cost-effectiveness make it an ideal choice for less critical functions where the performance requirements are lower.

Each of these protocols—CAN, Automotive Ethernet, FlexRay, and LIN—plays a distinct role in the automotive network ecosystem, addressing specific needs and requirements. As vehicles continue to evolve, the integration of these protocols and the development of new technologies will be crucial in managing the increasing complexity and ensuring the security and reliability of automotive networks.

3. Intrusion Detection Systems (IDS) Overview

Types of IDS: Signature-based, Anomaly-based, and Hybrid IDS

Intrusion Detection Systems (IDS) are critical components in the cybersecurity infrastructure of automotive networks, designed to detect and respond to potential threats by monitoring network traffic and identifying anomalous behavior. IDS can be broadly categorized into three primary types: signature-based, anomaly-based, and hybrid IDS, each with distinct characteristics and operational methodologies.



Signature-based IDS

Signature-based IDS is one of the most traditional and widely implemented forms of intrusion detection. This approach relies on predefined patterns, known as signatures, to identify malicious activities. These signatures are essentially patterns of known attack vectors or malicious payloads, derived from historical attack data and threat intelligence. The IDS system matches incoming network traffic or data packets against these signatures to detect and flag any occurrences of known threats.

The primary advantage of signature-based IDS lies in its accuracy and efficiency in detecting known threats. Since the system relies on specific signatures, it can achieve high detection rates for attacks that match these patterns. However, signature-based IDS has inherent limitations. It is ineffective against novel or zero-day attacks that do not have existing signatures. Additionally, the system's performance is heavily dependent on the timely and accurate updating of its signature database to ensure that it can detect emerging threats. The need for continuous updates and the inability to detect unknown threats are significant drawbacks of this approach.

Anomaly-based IDS

Anomaly-based IDS, in contrast to signature-based systems, focuses on identifying deviations from normal network behavior. This approach involves the establishment of a baseline of normal network activity, which includes patterns of traffic, user behavior, and system

operations. The IDS system continuously monitors network traffic and compares it to this baseline to detect any anomalies that may indicate potential intrusions or malicious activities.

The strength of anomaly-based IDS lies in its ability to detect previously unknown or zero-day attacks. By identifying deviations from established norms, it can potentially flag novel attack patterns that do not match any known signatures. This capability is crucial in environments where new and sophisticated threats are continuously evolving. However, anomaly-based IDS also has its challenges. The accuracy of this approach is highly dependent on the quality of the baseline model. False positives can occur if the baseline is not accurately established or if legitimate deviations are misinterpreted as threats. Additionally, the complexity of building and maintaining an accurate baseline can pose significant challenges.

Hybrid IDS

Hybrid IDS represents a convergence of the strengths of both signature-based and anomaly-based approaches. This system integrates the use of predefined signatures for known threats with anomaly detection techniques to identify unusual patterns that may indicate novel or sophisticated attacks. By combining these methodologies, hybrid IDS aims to leverage the strengths of both approaches while mitigating their individual limitations.

The hybrid IDS model benefits from the high accuracy of signature-based detection for known threats and the adaptability of anomaly-based detection for emerging or unknown threats. This dual approach enhances the overall effectiveness of the IDS, providing comprehensive coverage against a wide range of attack scenarios. However, the implementation of a hybrid IDS can be complex, requiring careful integration of the two detection mechanisms and effective management of their interactions. The system must balance the trade-offs between detection accuracy, false positives, and computational overhead to achieve optimal performance.

Traditional IDS Challenges: Limitations of Rule-based Systems in Detecting Advanced and Zero-day Attacks

Traditional Intrusion Detection Systems (IDS), particularly those employing rule-based approaches, face significant challenges in addressing the evolving landscape of cybersecurity threats. These systems rely heavily on predefined rules or signatures to identify malicious

activities, which can be effective for detecting known attack patterns. However, they exhibit notable limitations when confronted with advanced threats and zero-day attacks.

Limitations in Detecting Advanced Attacks

Advanced persistent threats (APTs) and sophisticated cyber-attacks often involve highly complex and evasive tactics that challenge traditional rule-based IDS. These attacks are characterized by their ability to bypass conventional detection mechanisms through various techniques such as encryption, obfuscation, and multi-stage exploitation. Traditional IDS, with its reliance on static rules and signatures, may struggle to identify such sophisticated threats effectively.

APTs, for instance, are designed to remain undetected for extended periods, utilizing advanced techniques to evade traditional IDS mechanisms. They often employ custom-built malware or exploit previously unknown vulnerabilities, making it difficult for rule-based systems to recognize their activity. The static nature of rule-based detection means that any deviation from predefined patterns, which may indicate an advanced attack, might not be captured unless the attack pattern has been previously identified and incorporated into the rule set.

Additionally, advanced attacks may leverage polymorphic or metamorphic techniques to alter their code or behavior dynamically. This transformation can render existing signatures ineffective, as the attack's characteristics may no longer match the predefined rules. The inability of rule-based systems to adapt to these changes in real-time exacerbates their limitations in detecting advanced threats.

Challenges with Zero-day Attacks

Zero-day attacks, which exploit previously unknown vulnerabilities, present a particularly challenging scenario for rule-based IDS. The defining characteristic of zero-day attacks is their exploitation of vulnerabilities that are not yet documented or understood by the cybersecurity community. As such, there are no existing signatures or rules available to detect these attacks when they first emerge.

Traditional rule-based IDS systems, by their very nature, are unable to detect zero-day attacks until the attack vector is discovered and a corresponding signature or rule is developed. This

reactive approach to threat detection means that organizations are exposed to the risk of zero-day attacks until adequate detection mechanisms are implemented. The latency in updating signatures and rules further exacerbates the risk, leaving systems vulnerable during the interim period.

Moreover, the effectiveness of rule-based systems in identifying zero-day attacks is contingent upon the rapid dissemination of threat intelligence and the prompt updating of detection rules. The process of analyzing new attack vectors, developing appropriate signatures, and deploying them across systems is often time-consuming and may not keep pace with the rapid evolution of threats. Consequently, organizations may experience a window of vulnerability during which zero-day attacks can successfully compromise their systems.

The Need for Adaptive Solutions

Given the limitations of traditional rule-based IDS in addressing advanced and zero-day attacks, there is a pressing need for more adaptive and proactive solutions. Approaches that incorporate machine learning and artificial intelligence (AI) offer promising enhancements to traditional IDS by enabling dynamic and real-time analysis of network behavior. These advanced techniques can complement rule-based systems by providing the capability to detect anomalies and unknown threats based on patterns learned from historical data and ongoing network activity.

Machine learning-based IDS, for example, can analyze large volumes of data to identify patterns and deviations that may indicate advanced or zero-day attacks. By learning from both benign and malicious activities, these systems can adapt to emerging threats and provide a more comprehensive detection capability. Such adaptive solutions address the inherent limitations of rule-based systems, offering improved resilience against sophisticated and previously unknown attacks.

Role of IDS in Automotive Networks: Importance of IDS in Maintaining Vehicle Safety and Security

In the contemporary landscape of automotive engineering, where vehicles increasingly rely on complex electronic systems and interconnected networks, the role of Intrusion Detection Systems (IDS) in ensuring vehicle safety and security has become paramount. As modern vehicles integrate advanced technologies such as automated driving systems, infotainment

units, and vehicle-to-everything (V2X) communication, the security of in-vehicle networks is crucial to preventing potentially catastrophic consequences arising from cyber threats.

Significance of IDS in Ensuring Vehicle Safety

The safety of vehicular systems is profoundly dependent on the integrity and reliability of the communication networks that connect various electronic control units (ECUs). In modern vehicles, these networks—predominantly Controller Area Network (CAN) and Automotive Ethernet—manage critical functions such as braking, steering, and powertrain control. Any compromise in the security of these networks can have severe implications for vehicle operation, potentially leading to unsafe conditions or failures that endanger passengers and other road users.

An effective IDS plays a crucial role in maintaining vehicle safety by monitoring network traffic and identifying anomalies or unauthorized activities that could indicate a security breach. For instance, if an IDS detects abnormal communication patterns or unauthorized commands within the CAN bus that control braking or steering systems, it can generate alerts or initiate countermeasures to prevent the execution of potentially harmful actions. By providing real-time detection and response capabilities, IDS helps safeguard against attacks that could disrupt critical vehicle functions and compromise safety.

Furthermore, as vehicles adopt advanced driver assistance systems (ADAS) and autonomous driving technologies, the complexity of in-vehicle networks increases, amplifying the potential attack surface. IDS systems designed for automotive environments must therefore be capable of handling sophisticated threats and ensuring that the data integrity and communication reliability required for safe operation are upheld. The ability to detect and mitigate threats in real-time is essential for the safe deployment and functioning of these advanced systems, making IDS a fundamental component of modern automotive safety architectures.

Contribution of IDS to Vehicle Security

Beyond safety considerations, the security of automotive networks is essential for protecting vehicles from a wide range of cyber threats that could compromise both vehicle functionality and user privacy. In an era where vehicles are connected to external networks, including cloud services and other vehicles, the potential for cyber-attacks extends beyond the vehicle itself.

Threats such as remote hacking, unauthorized access to personal data, and manipulation of vehicle control systems pose significant risks.

An IDS contributes to vehicle security by providing continuous surveillance of network traffic and detecting potential threats that may originate from both internal and external sources. By identifying suspicious activities or deviations from established communication patterns, an IDS can prevent unauthorized access or tampering with sensitive vehicle systems. This capability is particularly important in the context of V2X communication, where vehicles interact with infrastructure, other vehicles, and cloud-based services. Ensuring the security of these interactions helps prevent malicious actors from exploiting vulnerabilities to compromise vehicle security or privacy.

Moreover, as the automotive industry increasingly incorporates over-the-air (OTA) updates for software and firmware, the security of these updates becomes critical. An IDS can help monitor and verify the integrity of OTA updates, ensuring that they are authentic and have not been tampered with. This is essential for maintaining the security and functionality of vehicle systems, as compromised updates could introduce vulnerabilities or disrupt operations.

Challenges and Considerations

Implementing IDS in automotive networks presents several challenges that must be addressed to ensure effective protection. The dynamic nature of automotive environments, characterized by frequent changes in network configurations and communication patterns, requires IDS systems to be adaptable and capable of learning from evolving threat landscapes. Additionally, the integration of IDS must be carefully managed to avoid introducing latency or disrupting the real-time performance of critical systems.

The complexity of modern automotive networks necessitates a comprehensive approach to IDS deployment, encompassing not only the detection of known threats but also the ability to identify novel and sophisticated attack vectors. Advances in machine learning and artificial intelligence offer promising enhancements to traditional IDS by enabling adaptive and proactive detection capabilities. However, the successful implementation of these technologies requires rigorous validation and integration into existing vehicle architectures.

4. AI-Powered IDS in Automotive Networks

Machine Learning Algorithms: Overview of Supervised, Unsupervised, and Reinforcement Learning Techniques

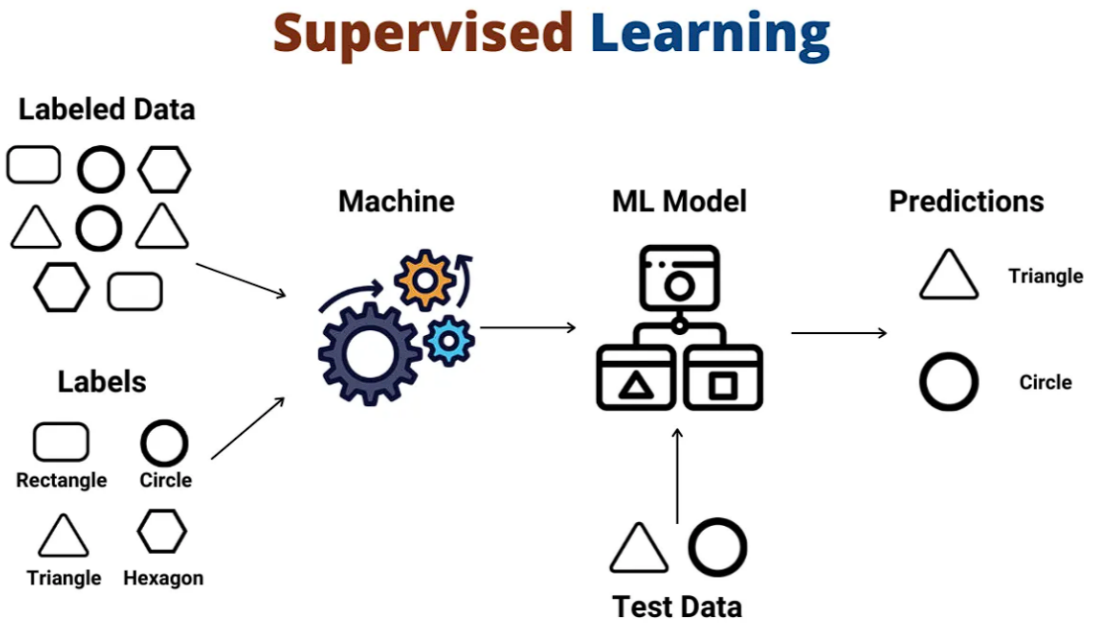
In the realm of automotive cybersecurity, the integration of artificial intelligence (AI) into Intrusion Detection Systems (IDS) represents a significant advancement over traditional rule-based methods. Machine learning (ML) algorithms, a core component of AI, offer sophisticated techniques for enhancing the detection and response capabilities of IDS. These techniques include supervised learning, unsupervised learning, and reinforcement learning, each contributing distinct advantages to the security of automotive networks.

Supervised Learning

Supervised learning is a machine learning approach wherein an algorithm is trained on a labeled dataset, which includes both input data and the corresponding output labels. The primary goal of supervised learning is to learn a mapping function from inputs to outputs, enabling the algorithm to predict labels for new, unseen data. In the context of IDS for automotive networks, supervised learning can be employed to classify network traffic as either normal or malicious based on historical data.

This technique involves training the model with a dataset containing known instances of both benign and malicious activities. During training, the algorithm learns to identify patterns and correlations within the data that differentiate normal traffic from potential threats. Once trained, the model can then be used to analyze real-time network traffic and detect deviations from learned patterns.

The strength of supervised learning lies in its ability to achieve high accuracy in classifying known threats, provided that the training data is representative of the threat landscape. However, its effectiveness is limited by its reliance on labeled data, which may not encompass all possible attack scenarios. Additionally, supervised learning models require regular updates to incorporate new threats, as the model's performance is contingent upon the relevance of the training data.

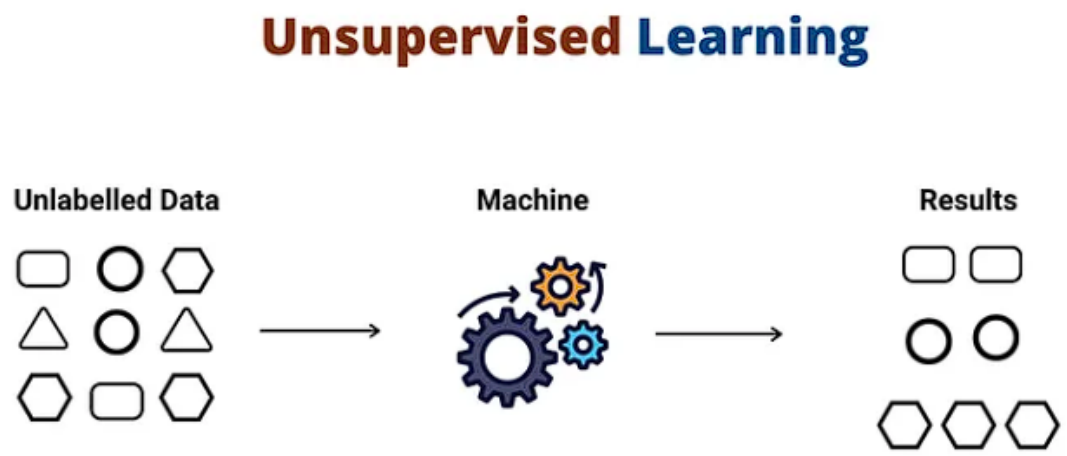


Unsupervised Learning

Unsupervised learning, in contrast, involves training algorithms on unlabeled data, where the goal is to uncover hidden patterns or structures within the dataset. This approach is particularly useful for identifying anomalies or deviations from normal behavior without prior knowledge of specific attack patterns.

In the context of automotive IDS, unsupervised learning techniques can be applied to detect novel or previously unknown threats by analyzing network traffic for unusual patterns that deviate from the established norms. For instance, clustering algorithms such as k-means or hierarchical clustering can group similar data points together, allowing the system to identify outliers that may indicate potential security breaches. Additionally, anomaly detection methods such as Isolation Forest or One-Class SVM can flag instances that significantly deviate from the learned normal behavior.

The advantage of unsupervised learning is its ability to identify previously unknown threats and adapt to new attack vectors without requiring labeled data. However, the challenge lies in accurately defining what constitutes "normal" behavior and minimizing false positives. The effectiveness of unsupervised learning depends on the quality of the feature extraction and the ability of the algorithm to generalize from the data.

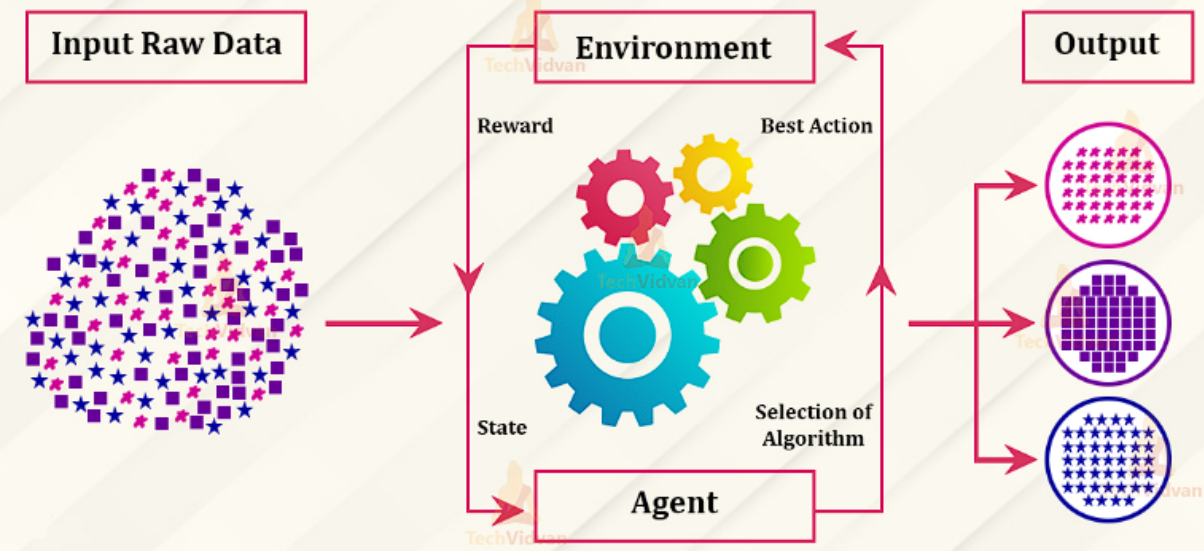


Reinforcement Learning

Reinforcement learning (RL) represents a different paradigm in machine learning, focusing on training algorithms to make decisions by interacting with an environment and learning from the consequences of their actions. In RL, an agent learns to maximize a cumulative reward by taking actions that lead to favorable outcomes while minimizing penalties for undesirable actions.

In the context of automotive IDS, reinforcement learning can be applied to enhance the system's ability to respond to detected threats dynamically. For example, an RL-based IDS can be trained to optimize its response strategies by evaluating the effectiveness of different mitigation actions based on their impact on system security and performance. The agent learns to balance exploration (trying new actions) with exploitation (using known effective actions) to improve its decision-making process over time.

The primary advantage of reinforcement learning is its adaptability and ability to optimize complex decision-making processes in real-time. It can continuously improve its performance by learning from interactions with the environment and adjusting its strategies accordingly. However, RL requires a well-defined reward structure and sufficient interaction with the environment to learn effectively. Additionally, the complexity of training RL agents and the need for significant computational resources can pose challenges in practical implementations.



Integration into Automotive Networks

Integrating AI-powered IDS into automotive networks involves leveraging these machine learning techniques to enhance the detection and response capabilities of traditional systems. By combining supervised, unsupervised, and reinforcement learning approaches, automotive IDS can achieve a comprehensive and adaptive security posture. Supervised learning can be used for accurate classification of known threats, unsupervised learning for detecting novel anomalies, and reinforcement learning for optimizing response strategies.

The successful implementation of AI-powered IDS in automotive networks requires careful consideration of various factors, including the quality of training data, the adaptability of learning algorithms, and the integration of AI models into existing network architectures. Continuous monitoring, evaluation, and updating of AI models are essential to ensure that they remain effective against evolving threats and maintain the security and integrity of automotive systems.

Deep Learning Approaches: Detailed Discussion on CNNs, LSTMs, and Autoencoders

The application of deep learning approaches in Intrusion Detection Systems (IDS) for automotive networks represents a significant leap forward in enhancing the detection and mitigation of cyber threats. Deep learning, a subset of machine learning characterized by its use of neural networks with multiple layers, has demonstrated substantial efficacy in various domains due to its ability to automatically learn features from raw data. Among the prominent deep learning techniques employed in automotive IDS are Convolutional Neural

Networks (CNNs), Long Short-Term Memory networks (LSTMs), and Autoencoders. Each of these approaches offers distinct advantages and is suited to specific aspects of intrusion detection and network security.

Convolutional Neural Networks (CNNs)

Convolutional Neural Networks (CNNs) are a class of deep learning models particularly effective for processing grid-like data, such as images and sequences. CNNs leverage convolutional layers to automatically and adaptively learn spatial hierarchies of features from input data. In the context of automotive networks, CNNs can be applied to analyze and interpret complex data structures, such as network traffic patterns, by detecting spatial relationships and patterns that may indicate security anomalies.

A CNN typically consists of several convolutional layers followed by pooling layers and fully connected layers. The convolutional layers apply filters to the input data, producing feature maps that highlight the presence of specific patterns or features. Pooling layers reduce the spatial dimensions of the feature maps, thereby decreasing computational complexity and enhancing feature abstraction. Finally, the fully connected layers integrate these features to perform classification or regression tasks.

In automotive IDS, CNNs can be used to detect anomalous patterns in network traffic by transforming raw packet data into a format that captures temporal and spatial dependencies. For example, CNNs can identify unusual patterns in traffic logs or intrusion signatures by learning from historical data. The ability of CNNs to automatically extract and learn relevant features from raw data makes them well-suited for identifying complex and subtle security threats that may be challenging to detect using traditional methods.

Long Short-Term Memory Networks (LSTMs)

Long Short-Term Memory networks (LSTMs) are a specialized type of Recurrent Neural Networks (RNNs) designed to address the limitations of conventional RNNs, particularly their difficulty in capturing long-term dependencies. LSTMs incorporate memory cells that store information over extended periods, enabling the model to learn and remember temporal sequences more effectively. This capability is crucial for analyzing sequential data where the context of past events influences the interpretation of current data.

In automotive IDS, LSTMs can be employed to monitor and analyze time-series data, such as network traffic over time. This temporal analysis is essential for detecting patterns or anomalies that evolve over extended periods. For instance, LSTMs can identify subtle variations in traffic patterns that may indicate a gradual or sophisticated attack, such as a slow data exfiltration or a distributed denial-of-service (DDoS) attack. By learning from historical sequences of network events, LSTMs can provide insights into evolving threats and enhance the ability of IDS to detect and respond to sophisticated cyber attacks.

Autoencoders

Autoencoders are a type of neural network used for unsupervised learning, primarily for dimensionality reduction and feature learning. An autoencoder consists of an encoder and a decoder. The encoder compresses the input data into a lower-dimensional latent representation, while the decoder reconstructs the original data from this compressed representation. The goal of training an autoencoder is to minimize the reconstruction error, which represents the difference between the original and reconstructed data.

In the realm of automotive IDS, autoencoders can be utilized for anomaly detection by learning a compact representation of normal network traffic and identifying deviations from this representation as potential anomalies. The reconstruction error serves as a measure of how well the model can represent normal behavior. A high reconstruction error indicates that the input data deviates significantly from the learned normal patterns, suggesting the presence of an anomaly or intrusion.

Autoencoders are particularly advantageous for anomaly detection in scenarios where labeled data is scarce or unavailable, as they do not require explicit labels for training. They can effectively learn the underlying structure of normal network traffic and identify deviations that may indicate security threats. Additionally, autoencoders can be combined with other techniques, such as supervised learning models, to enhance their performance and detection capabilities.

Integration and Practical Considerations

The integration of CNNs, LSTMs, and autoencoders into automotive IDS systems requires careful consideration of various factors, including data preprocessing, model training, and evaluation. Each deep learning approach brings unique strengths to the table, and their

effectiveness can be enhanced through hybrid models that combine the strengths of multiple techniques. For example, combining CNNs with LSTMs can leverage both spatial and temporal features of network traffic, while autoencoders can provide an additional layer of anomaly detection.

Practical implementation also involves addressing challenges such as computational resource requirements, model interpretability, and real-time performance. Deep learning models, especially those with complex architectures, often require significant computational resources and may introduce latency in detection and response. Balancing the trade-off between detection accuracy and system performance is crucial for ensuring the effective deployment of deep learning-based IDS in automotive networks.

Algorithm Selection Criteria: Factors Influencing the Choice of Algorithms for Automotive IDS

The selection of appropriate algorithms for Intrusion Detection Systems (IDS) in automotive networks is a critical decision that impacts the effectiveness, efficiency, and reliability of the security solution. Given the complexity and dynamic nature of automotive networks, which include various communication protocols such as CAN, Ethernet, and FlexRay, selecting the right algorithm involves careful consideration of several factors. These factors include the nature of the data, real-time performance requirements, the ability to handle evolving threats, and the overall system constraints.

Nature of Data

The type and quality of data available for training and evaluation significantly influence algorithm selection. Automotive networks generate a diverse range of data, including network traffic logs, communication protocol messages, and sensor data. Algorithms must be capable of handling this data efficiently, extracting meaningful features, and distinguishing between normal and anomalous patterns.

For instance, Convolutional Neural Networks (CNNs) are particularly adept at processing spatial data and are well-suited for tasks involving structured data representations such as network packet headers or traffic patterns. Conversely, Long Short-Term Memory networks (LSTMs) excel in analyzing sequential and temporal data, making them ideal for detecting anomalies in time-series data from continuous network monitoring. Autoencoders, with their

ability to learn compact representations of normal behavior, are useful for unsupervised anomaly detection when labeled data is limited or unavailable.

Real-Time Performance Requirements

Automotive IDS systems often need to operate in real-time or near-real-time to provide timely detection and response to potential threats. Consequently, the computational efficiency and latency of the chosen algorithms are paramount. Algorithms that require extensive processing power or have high latency may not be suitable for real-time applications, where swift detection and mitigation are essential.

For real-time performance, simpler models or those with efficient implementations may be preferred. For example, traditional machine learning algorithms such as decision trees or random forests, when properly optimized, can offer fast inference times compared to more complex deep learning models. However, deep learning approaches such as CNNs and LSTMs, while potentially more computationally intensive, can be optimized through techniques such as model pruning, quantization, and hardware acceleration to meet real-time constraints.

Ability to Handle Evolving Threats

Automotive networks are subject to an evolving threat landscape, where new attack vectors and techniques continually emerge. Algorithms must possess the capability to adapt to these evolving threats effectively. This adaptability can be achieved through continuous learning, model updates, and integration of feedback mechanisms.

Supervised learning algorithms require frequent retraining with updated labeled data to remain effective against new threats. In contrast, unsupervised learning methods such as autoencoders and clustering algorithms can adapt more readily to novel anomalies, as they do not rely on predefined threat signatures. Reinforcement learning approaches can also be employed to dynamically adjust response strategies based on ongoing interactions with the network environment.

Scalability and Complexity

The scalability of an algorithm refers to its ability to handle increasing volumes of data and complexity without a significant degradation in performance. Automotive networks can

generate vast amounts of data, particularly in modern vehicles with numerous sensors and communication channels. Therefore, the selected algorithms must be scalable and capable of managing large-scale data while maintaining accuracy and efficiency.

Complexity also plays a role in the selection process. More complex models may provide higher accuracy but at the cost of increased computational requirements and longer training times. Simpler models may offer faster processing but might not capture intricate patterns in the data. A balance must be struck between model complexity and practical constraints such as computational resources and deployment environments.

Integration and Compatibility

The integration of IDS algorithms into existing automotive network architectures is another crucial consideration. The chosen algorithms must be compatible with the current network infrastructure and capable of interacting with other components of the security system. This includes considerations for data formats, communication protocols, and system interfaces.

For example, algorithms must be able to process data in real-time from various sources such as CAN or Ethernet without significant modification. Additionally, the integration process should ensure that the IDS does not introduce vulnerabilities or performance bottlenecks into the network.

Interpretability and Explainability

In the context of automotive cybersecurity, interpretability and explainability of the algorithms are important for understanding and validating detection results. Stakeholders need to comprehend how and why certain decisions are made by the IDS to ensure trust and facilitate incident response.

While traditional machine learning models often provide greater interpretability compared to deep learning models, advanced techniques such as attention mechanisms in CNNs or feature importance measures in ensemble methods can offer insights into model decisions. However, the trade-off between model complexity and interpretability must be carefully managed to ensure effective deployment and operation.

Data Privacy and Security

Finally, data privacy and security considerations are essential when selecting IDS algorithms. Automotive networks handle sensitive information, and the chosen algorithms must ensure that data is processed and stored securely. This includes considerations for data anonymization, secure data transmission, and protection against potential data breaches.

5. Implementation and Architecture

System Architecture: Design of AI-powered IDS for In-Vehicle Networks

The design of an AI-powered Intrusion Detection System (IDS) for in-vehicle networks necessitates a comprehensive system architecture that integrates seamlessly with automotive communication protocols while ensuring effective real-time threat detection and mitigation. This architecture encompasses several critical components: data acquisition, preprocessing, model inference, and response mechanisms.

At the core of the architecture is the data acquisition layer, responsible for capturing and aggregating network traffic from various in-vehicle communication channels, such as Controller Area Network (CAN), Automotive Ethernet, and other relevant protocols. This layer utilizes sensors, network taps, or embedded monitoring tools to continuously collect data. Given the diverse nature of the data sources, the architecture must support multiple data formats and protocols to ensure comprehensive coverage of the vehicular network environment.

The preprocessing layer follows, where raw data is cleaned, normalized, and transformed into a format suitable for analysis. This step involves removing noise, handling missing values, and standardizing data to ensure consistency. Feature extraction techniques are employed to identify relevant attributes from the raw data, which may include network packet headers, payload information, and temporal sequences. Effective preprocessing is crucial for enhancing the accuracy and efficiency of subsequent model training and inference.

The AI model inference layer is where machine learning and deep learning algorithms are applied to detect anomalies and potential threats. The choice of algorithms—such as Convolutional Neural Networks (CNNs), Long Short-Term Memory networks (LSTMs), or Autoencoders—depends on the specific requirements of the application, including the nature

of the data and the real-time performance constraints. This layer operates in real-time or near-real-time, continuously analyzing incoming data and generating alerts for suspicious activities.

Finally, the response mechanism layer is responsible for taking appropriate actions based on the detections made by the AI model. This can include logging the incident, alerting operators, or triggering automated responses to mitigate identified threats. Integration with vehicle control systems is essential to ensure that the IDS can act effectively without disrupting normal operations or compromising vehicle safety.

Data Collection and Preprocessing: Methods for Acquiring and Preparing Network Data for Analysis

The efficacy of an AI-powered IDS is heavily dependent on the quality and comprehensiveness of the data used for training and evaluation. Data collection and preprocessing are therefore fundamental to developing a robust and effective IDS.

Data collection involves capturing network traffic and communication logs from various in-vehicle systems. Techniques for data collection include network sniffing, which uses tools to monitor and record network traffic; data loggers, which capture specific communication events; and embedded monitoring solutions integrated directly into the vehicle's communication hardware. For effective monitoring, the collection process must ensure minimal impact on network performance and be capable of handling high-speed data streams typical in modern automotive environments.

Preprocessing is a multi-step process aimed at transforming raw data into a structured format suitable for analysis. This process begins with data cleaning, which addresses issues such as corrupted packets, incomplete records, and erroneous entries. Data normalization is then applied to standardize numerical values and ensure consistency across different data sources. Feature extraction is a critical step where relevant characteristics are derived from raw data. This may include statistical features such as packet sizes, inter-arrival times, and communication frequencies, as well as more complex features derived through techniques like Principal Component Analysis (PCA) or feature selection algorithms.

Handling temporal data, particularly for protocols such as CAN, requires specific preprocessing methods to account for the sequential nature of the data. Techniques such as

windowing, where data is segmented into fixed-size windows, and time-series feature extraction are employed to capture temporal dependencies and patterns relevant to anomaly detection.

Model Training and Validation: Techniques for Training and Validating AI Models on Vehicular Data

Training and validating AI models for IDS in automotive networks involves several critical steps to ensure that the models are effective in detecting anomalies and resilient to evolving threats.

Model training begins with selecting appropriate algorithms based on the characteristics of the data and the specific requirements of the IDS. Supervised learning approaches, such as CNNs and LSTMs, require labeled datasets where normal and anomalous behaviors are explicitly defined. These models are trained to learn the distinguishing features of each class, iteratively adjusting their parameters to minimize classification errors.

Unsupervised learning methods, such as Autoencoders, do not rely on labeled data but instead learn to reconstruct normal patterns of behavior. The reconstruction error is then used to identify deviations that may indicate anomalous activity. This approach is particularly useful in scenarios where labeled data is scarce or unavailable.

During training, models are exposed to a representative subset of the data, allowing them to learn and generalize patterns of normal and anomalous behavior. This process involves partitioning the data into training, validation, and test sets to evaluate model performance and prevent overfitting. Cross-validation techniques, such as k-fold cross-validation, are employed to assess the model's ability to generalize to unseen data.

Model validation involves assessing the trained models on separate validation datasets to fine-tune hyperparameters and improve performance. Metrics such as accuracy, precision, recall, and F1-score are used to evaluate the effectiveness of the models. Additionally, techniques such as Receiver Operating Characteristic (ROC) curves and Area Under the Curve (AUC) are employed to analyze the trade-offs between true positive rates and false positive rates.

Post-training, models are subjected to testing with real-world or simulated data to assess their performance under realistic conditions. This phase is crucial for identifying any potential issues related to real-time deployment, such as latency, false positives, and false negatives. Continuous monitoring and periodic retraining are necessary to adapt the models to new threats and changes in the network environment.

6. Challenges in AI-Powered IDS Deployment

Data Dimensionality: Handling High-Dimensional Data from Automotive Networks

In the context of automotive networks, data dimensionality poses a significant challenge for the deployment of AI-powered Intrusion Detection Systems (IDS). Automotive networks generate high-dimensional data, where each network packet or message may contain numerous attributes, such as packet length, source and destination addresses, and various protocol-specific fields. The high-dimensional nature of this data can lead to several issues:

Firstly, high-dimensional data often suffers from the "curse of dimensionality," where the volume of the feature space increases exponentially with the number of dimensions. This phenomenon can lead to sparse data distributions, making it difficult for machine learning models to generalize effectively. Sparse data can adversely affect the performance of models, leading to overfitting or underfitting, as the algorithms may struggle to identify meaningful patterns amidst the noise.

Additionally, high-dimensional data increases the computational complexity of model training and inference. Algorithms that operate in high-dimensional spaces require significant computational resources and time to process and analyze data. This complexity can lead to longer training times and increased latency during real-time analysis, which is critical for automotive systems where timely detection and response are essential.

Dimensionality reduction techniques, such as Principal Component Analysis (PCA), t-Distributed Stochastic Neighbor Embedding (t-SNE), or feature selection methods, can be employed to mitigate these issues. These techniques aim to reduce the number of features while preserving the essential characteristics of the data. However, dimensionality reduction

must be performed carefully to ensure that important information is not lost, which could potentially impact the accuracy of the IDS.

Real-Time Constraints: Addressing Latency and Computational Limitations of Automotive ECUs

Automotive Electronic Control Units (ECUs) are embedded systems that manage various functions within a vehicle, including communication protocols and safety systems. These ECUs often have stringent real-time constraints, requiring timely processing and response to ensure vehicle safety and operational efficiency. The deployment of AI-powered IDS in such environments presents several challenges related to latency and computational limitations:

The latency associated with data processing and anomaly detection is a critical concern. In-vehicle networks must handle high-speed data streams, and any delay in processing can result in missed or delayed threat detection. Real-time IDS must therefore be optimized to minimize processing time while maintaining accuracy. This involves designing algorithms and models that can operate efficiently within the constrained computational resources of ECUs.

Computational limitations further compound the challenge. ECUs have finite processing power, memory, and storage, which restrict the complexity of algorithms that can be deployed. Advanced machine learning and deep learning models, such as Convolutional Neural Networks (CNNs) or Long Short-Term Memory networks (LSTMs), often require substantial computational resources, which may exceed the capabilities of standard automotive ECUs. Optimizing these models for embedded systems involves techniques such as model compression, quantization, and efficient inference frameworks to reduce their computational footprint without sacrificing performance.

Additionally, the integration of AI models into ECUs must consider the trade-offs between accuracy and computational efficiency. While complex models may offer higher accuracy, they also demand more processing power and memory. Striking a balance between these factors is crucial to ensuring that the IDS remains effective without overwhelming the ECUs.

Bandwidth and Resource Limitations: Impact on the Efficiency of IDS Algorithms

Bandwidth and resource limitations in automotive networks can significantly impact the efficiency of AI-powered IDS algorithms. Automotive networks are typically designed with

bandwidth constraints to manage the high volume of data generated by various sensors and communication channels. These constraints can affect the performance of IDS systems in several ways:

Bandwidth limitations restrict the amount of data that can be transmitted and processed within a given time frame. This can lead to challenges in real-time data analysis, as the IDS must process incoming data streams rapidly while adhering to bandwidth constraints. In scenarios where the network is congested or data traffic is high, the IDS may experience delays in data processing or encounter difficulties in maintaining real-time detection capabilities.

Resource limitations, including processing power, memory, and storage, also impact the deployment of IDS algorithms. Automotive ECUs often operate with limited resources, which can restrict the complexity of the algorithms that can be implemented. Efficient use of available resources is essential to ensure that the IDS can perform effectively without degrading overall system performance.

To address these challenges, strategies such as data sampling, aggregation, and preprocessing can be employed to manage bandwidth and resource utilization. Data sampling involves selecting representative subsets of data for analysis, which can reduce the volume of data that needs to be processed. Aggregation techniques combine multiple data points into summary statistics, minimizing the amount of data transmitted while retaining key information. Preprocessing methods, such as feature extraction and dimensionality reduction, help to reduce the data volume and complexity, making it more manageable for the IDS.

7. Integration with Vehicle-to-Everything (V2X) Communication

Overview of V2X: Importance and Functionality of V2X Communications

Vehicle-to-Everything (V2X) communication represents a transformative paradigm in automotive technology, facilitating seamless interaction between vehicles and their surrounding environment. V2X encompasses various communication modalities, including Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), and Vehicle-to-Network (V2N), which together enable vehicles to communicate with each other, with traffic infrastructure such as traffic lights and road signs, with pedestrians carrying smart

devices, and with broader network services, respectively. This communication is essential for enhancing road safety, optimizing traffic flow, and enabling autonomous driving functionalities.

The core functionality of V2X communication lies in its ability to provide low-latency, high-reliability data exchange, crucial for safety-critical applications. Through Dedicated Short-Range Communication (DSRC) or Cellular Vehicle-to-Everything (C-V2X) technology, V2X systems support real-time data sharing, allowing vehicles to broadcast their location, speed, and direction to surrounding entities. Such capabilities enable the implementation of cooperative awareness messages (CAMs) and decentralized environmental notification messages (DENMs), which are vital for applications like collision avoidance, lane-change assistance, and emergency braking systems.

The importance of V2X communication is underscored by its potential to significantly reduce traffic accidents, enhance driving comfort, and improve fuel efficiency. By leveraging information from other vehicles and infrastructure, V2X enables anticipatory driving, where vehicles can preemptively adjust their behavior in response to predicted traffic conditions or potential hazards. This paradigm shift not only enhances safety but also paves the way for a more efficient and sustainable transportation ecosystem.

Security Considerations: Integration Challenges and Security Implications

While V2X communication offers substantial benefits for automotive safety and efficiency, it also introduces significant security challenges. The integration of V2X systems with in-vehicle networks necessitates a robust security framework to protect against various cyber threats. Given that V2X communications rely on the exchange of critical safety information over wireless networks, they are inherently vulnerable to several attack vectors, including spoofing, eavesdropping, denial-of-service (DoS) attacks, and man-in-the-middle (MitM) attacks.

One of the primary security considerations in V2X integration is ensuring the authenticity and integrity of messages exchanged between vehicles and infrastructure. Attackers could potentially inject false messages, disrupt communication channels, or replay legitimate messages to manipulate vehicle behavior, leading to hazardous situations on the road. Consequently, secure communication protocols such as the IEEE 1609.2 standard for V2X

security are employed to provide message authentication, confidentiality, and integrity using Public Key Infrastructure (PKI) and digital certificates.

Another integration challenge pertains to the dynamic and distributed nature of V2X environments, where vehicles frequently enter and leave the network. This high mobility poses difficulties in managing cryptographic keys, establishing secure communication channels, and maintaining trust among entities. In addition, the need for low-latency communication conflicts with the computational overhead required for cryptographic operations, necessitating a delicate balance between security and performance.

Furthermore, the integration of V2X systems with in-vehicle networks requires addressing privacy concerns, as the continuous broadcasting of location and other sensitive data can potentially be exploited for tracking or profiling purposes. To mitigate these risks, privacy-preserving techniques such as pseudonym-based authentication and group signatures are being explored to protect user identities while maintaining the ability to verify message authenticity.

Enhanced IDS Models: Approaches for Integrating IDS with V2X Systems

Given the security implications of V2X communication, the integration of Intrusion Detection Systems (IDS) into V2X-enabled vehicles is of paramount importance to enhance the overall security posture of automotive networks. Enhanced IDS models tailored for V2X environments must address unique challenges such as high mobility, dynamic network topology, and real-time processing requirements.

One approach to integrating IDS with V2X systems involves the development of distributed IDS architectures that leverage the cooperative nature of V2X communication. In such architectures, each vehicle or infrastructure node is equipped with a lightweight IDS that monitors local network traffic for potential anomalies. These distributed IDS instances communicate and share anomaly reports with neighboring nodes to achieve a collective situational awareness. By employing consensus-based mechanisms, these systems can validate the legitimacy of reported anomalies and reduce the likelihood of false positives or negatives.

Another promising approach is the use of federated learning to enhance IDS models in V2X environments. Federated learning allows multiple entities (vehicles, infrastructure nodes) to

collaboratively train a global IDS model without sharing raw data, thereby preserving data privacy. Each entity trains the IDS model locally using its own data and shares only the model updates with a central server, which aggregates the updates to improve the global model. This approach enables IDS models to continuously learn from diverse data sources in a V2X environment, enhancing their ability to detect novel and evolving threats.

Machine learning-based IDS models, specifically designed for V2X systems, can also leverage the spatio-temporal characteristics of V2X data. By analyzing patterns in both space and time, these models can effectively identify anomalies that may indicate cyber-attacks or abnormal behavior. For instance, Graph Neural Networks (GNNs) and Recurrent Neural Networks (RNNs) can be employed to model the dynamic interactions between vehicles and infrastructure over time, allowing for the detection of coordinated attacks that span multiple nodes in the V2X network.

Additionally, integrating IDS with V2X systems requires addressing the challenges of real-time detection and response. Given the stringent latency requirements of V2X communication, IDS models must be optimized for low-latency operation. Techniques such as model pruning, quantization, and hardware acceleration using specialized processors (e.g., GPUs, TPUs) can be employed to achieve fast and efficient anomaly detection without compromising accuracy.

8. Case Studies and Practical Applications

Real-World Implementations: Case Studies Illustrating the Application of AI-Powered IDS in Automotive Settings

The deployment of AI-powered Intrusion Detection Systems (IDS) in automotive networks has been increasingly explored in recent years as a means to bolster vehicular cybersecurity. Several real-world implementations have demonstrated the potential of these systems to detect and mitigate a variety of cyber threats in automotive settings. One notable case study is the integration of machine learning-based IDS in a fleet of connected vehicles by a leading automotive manufacturer. In this implementation, the IDS utilized a combination of supervised learning algorithms and deep neural networks to identify anomalies in Controller Area Network (CAN) traffic, which is a common protocol in vehicular communication

networks. By leveraging both in-vehicle and cloud-based computing resources, the IDS was able to process high-dimensional data streams from multiple Electronic Control Units (ECUs) in real-time, providing a comprehensive defense mechanism against cyber threats.

In another instance, an academic-industry collaboration developed an IDS tailored for Electric Vehicle (EV) charging infrastructure, which represents a critical component of smart grid integration. This IDS was designed to detect anomalies in the communication between EVs and charging stations, which could indicate potential attacks such as unauthorized access or data manipulation. The system utilized a combination of clustering techniques and autoencoders to identify deviations from normal charging patterns, enabling the early detection of both known and unknown threats. The implementation demonstrated that AI-powered IDS could effectively safeguard EV charging systems from cyber-attacks while maintaining operational efficiency.

Furthermore, a European consortium focused on autonomous driving research implemented a deep learning-based IDS in a fully autonomous vehicle prototype. The IDS employed Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks to analyze sensor data and inter-vehicular communication messages in real-time. The system was capable of detecting a wide range of cyber-attacks, including data injection, spoofing, and signal jamming, which are known to compromise the functionality and safety of autonomous driving systems. This implementation showcased the potential of AI-driven IDS to enhance the resilience of autonomous vehicles against sophisticated cyber threats.

Attack Scenarios: Analysis of Specific Attack Scenarios (e.g., DoS, Spoofing) and How AI-Powered IDS Responded

The effectiveness of AI-powered IDS in automotive networks is largely determined by their ability to respond to specific attack scenarios that threaten vehicular safety and security. Denial-of-Service (DoS) attacks, for instance, represent a significant threat to connected vehicles, as they can overwhelm the vehicular network and disrupt critical communication between ECUs. In a practical deployment involving a simulated vehicular network environment, an AI-powered IDS was evaluated for its capability to detect and mitigate DoS attacks. The system employed a combination of decision trees and recurrent neural networks to analyze traffic patterns and identify abnormal traffic spikes indicative of a DoS attack. Upon detection, the IDS triggered a mitigation strategy that involved isolating the compromised

nodes and rerouting traffic through alternative pathways, thereby maintaining network integrity and functionality.

Another prevalent attack scenario is spoofing, where an attacker sends falsified messages to ECUs or other vehicles to manipulate vehicle behavior. In a controlled experiment conducted on a vehicle testbed, an AI-powered IDS based on support vector machines (SVM) and autoencoders was implemented to detect GPS spoofing attacks. The IDS analyzed time-series data from multiple sensors, including GPS, accelerometer, and gyroscope, to identify inconsistencies in the reported location and motion of the vehicle. When a spoofing attack was detected, the IDS alerted the vehicle control system and switched to an alternative localization method, such as dead reckoning or sensor fusion, to maintain accurate positioning information. The results demonstrated that the AI-powered IDS could effectively detect and respond to spoofing attacks with a high degree of accuracy and minimal false positives.

Moreover, the deployment of AI-powered IDS has been tested against sophisticated multi-vector attacks that combine different attack types, such as message injection and signal jamming. In one such case study, a hybrid IDS utilizing both deep learning and reinforcement learning was implemented in a connected vehicle environment to detect and respond to these complex attack scenarios. The IDS was able to learn from the evolving attack patterns and adapt its detection strategy accordingly. The system's response mechanism involved dynamic adjustment of communication parameters and the activation of redundant communication channels to ensure continued operation of safety-critical functions. This approach highlighted the ability of AI-driven IDS to provide robust and adaptive defense against advanced cyber-attacks in automotive networks.

Performance Evaluation: Assessment of Effectiveness, Accuracy, and Efficiency in Real-World Applications

The performance of AI-powered IDS in real-world automotive applications is typically evaluated based on several key metrics, including detection accuracy, false positive rate, computational efficiency, and real-time responsiveness. In the case studies discussed above, the effectiveness of the IDS in detecting various cyber threats was measured through a combination of offline and online testing using realistic vehicular datasets and testbed environments. The IDS models demonstrated high detection accuracy, often exceeding 95% for well-known attack types such as DoS and spoofing. This high accuracy was achieved by

employing advanced machine learning techniques that could capture the intricate patterns and correlations in network traffic data.

However, a critical challenge in IDS performance is minimizing the false positive rate, which refers to the incorrect classification of legitimate traffic as malicious. A high false positive rate can lead to unnecessary alerts and degrade the overall user experience. The AI-powered IDS implemented in the connected vehicle fleet case study utilized ensemble learning techniques and feature selection methods to reduce the false positive rate to below 2%. This low rate was achieved by carefully balancing the sensitivity and specificity of the detection models, ensuring that legitimate variations in network traffic were not misclassified as anomalies.

Computational efficiency is another vital consideration for the deployment of IDS in resource-constrained automotive environments. The IDS models in the autonomous vehicle prototype case study were optimized for execution on embedded systems with limited processing power and memory. Techniques such as model pruning, quantization, and edge computing were employed to reduce the computational overhead and enable real-time detection with minimal latency. The system achieved a processing time of less than 50 milliseconds per inference, meeting the stringent latency requirements for autonomous driving applications.

In terms of real-time responsiveness, the ability of the IDS to quickly detect and respond to cyber threats is crucial for maintaining vehicular safety. The federated learning-based IDS deployed in the V2X-enabled vehicles demonstrated a response time of under 100 milliseconds for detecting and mitigating attacks, such as signal jamming and data injection. This rapid response was made possible by leveraging distributed computing resources and edge AI techniques, which enabled decentralized decision-making and reduced the need for centralized processing.

Overall, the performance evaluation of AI-powered IDS in real-world automotive settings indicates that these systems are capable of providing high accuracy, low false positive rates, and efficient real-time detection and response. However, further research is needed to enhance the scalability, adaptability, and robustness of these systems in the face of evolving cyber threats and increasingly complex vehicular networks. Future advancements in AI algorithms, hardware acceleration, and collaborative threat intelligence will be instrumental in realizing the full potential of AI-powered IDS for automotive cybersecurity.

9. Future Directions and Opportunities

Federated Learning: Potential for Collaborative Model Training Across Distributed Vehicular Nodes

The advent of federated learning (FL) presents a transformative opportunity for enhancing the performance and adaptability of Intrusion Detection Systems (IDS) in automotive networks. In contrast to traditional centralized machine learning paradigms, where data is aggregated and processed in a centralized server, federated learning facilitates collaborative model training directly on distributed vehicular nodes, such as Electronic Control Units (ECUs) and embedded devices. This decentralized approach aligns well with the data privacy and bandwidth limitations inherent in vehicular networks, as it enables each node to train models locally on its data while only sharing model updates with a central aggregator.

The application of federated learning to automotive IDS offers several advantages. Firstly, it enhances privacy preservation by ensuring that raw data, which could include sensitive information related to driver behavior, location, and vehicle diagnostics, remains localized and is not transmitted to external servers. Secondly, federated learning enables real-time adaptation of IDS models to local environments. Since vehicular networks can exhibit significant variability due to differences in road conditions, traffic patterns, and regional cybersecurity threats, federated learning allows each vehicle to develop models that are optimized for its specific context. Moreover, this approach fosters collaborative cybersecurity defense across an entire fleet of vehicles. By aggregating model updates from multiple vehicles, federated learning allows for the development of robust, generalized IDS models that can detect emerging threats more effectively.

However, implementing federated learning for automotive IDS also poses several challenges that need to be addressed. Communication overhead and model synchronization between distributed nodes must be optimized to minimize latency and energy consumption, which are critical constraints in vehicular environments. Furthermore, techniques to handle non-IID (independently and identically distributed) data, which is typical in heterogeneous vehicular networks, are necessary to prevent model bias and ensure fair and balanced model performance across different vehicles. Future research should focus on developing

lightweight federated learning algorithms, model aggregation methods that account for node heterogeneity, and secure communication protocols to protect model updates from adversarial manipulation. The integration of these advancements into automotive IDS architectures could significantly bolster their effectiveness in detecting and mitigating a wide range of cyber threats.

Regulatory and Standards Compliance: Integration of IDS with Evolving Automotive Cybersecurity Standards (e.g., ISO/SAE 21434)

As the automotive industry increasingly recognizes the importance of cybersecurity, regulatory bodies and standardization organizations have introduced comprehensive guidelines to address cybersecurity risks in vehicular networks. The ISO/SAE 21434 standard, which provides a framework for managing cybersecurity risks throughout the lifecycle of road vehicles, represents a critical step toward standardizing automotive cybersecurity practices. This standard emphasizes a risk-based approach to identify, assess, and mitigate cybersecurity threats, ensuring that vehicles are designed and maintained with robust cybersecurity protections.

The integration of AI-powered IDS into automotive cybersecurity frameworks necessitates alignment with evolving standards such as ISO/SAE 21434. This integration involves ensuring that IDS architectures, algorithms, and processes conform to the guidelines for risk assessment, threat analysis, and incident response outlined in these standards. For instance, IDS must be designed to support continuous monitoring and threat detection, aligned with the cybersecurity management system (CSMS) requirements of ISO/SAE 21434. Additionally, IDS should provide capabilities for real-time risk assessment and incident response, which are essential components of a proactive cybersecurity posture as mandated by the standard.

Moreover, as new cybersecurity standards emerge, IDS models must be continually updated to comply with the latest regulatory requirements. This necessitates the development of modular and scalable IDS architectures that can accommodate changes in regulatory guidelines without necessitating complete system redesigns. Furthermore, the integration of IDS with other cybersecurity controls, such as secure boot, authentication, and encryption mechanisms, is essential to ensure comprehensive compliance with standards. Future research should focus on developing IDS frameworks that facilitate seamless integration with

standardized cybersecurity architectures, enhancing both regulatory compliance and overall vehicular cybersecurity resilience.

Ethical and Safety Considerations: Balancing Cybersecurity with Vehicle Safety and Ethical Implications

While the deployment of AI-powered IDS significantly enhances vehicular cybersecurity, it also introduces several ethical and safety considerations that must be carefully addressed. One primary concern is the potential for IDS to impact the safety and operational reliability of vehicles. For example, false positives generated by an IDS could inadvertently trigger protective measures that disrupt normal vehicle functions, potentially compromising vehicle safety. To mitigate such risks, it is essential to develop IDS models that are not only highly accurate in detecting cyber threats but also exhibit a low false positive rate to minimize unintended consequences. Techniques such as adversarial training, uncertainty quantification, and hybrid detection models can be employed to enhance the reliability and robustness of IDS models in operational environments.

Another ethical consideration involves the balance between privacy and security. While the detection and mitigation of cyber threats are paramount, IDS must also respect the privacy of vehicle occupants. The implementation of privacy-preserving AI techniques, such as federated learning and differential privacy, can help ensure that sensitive data is protected during IDS operations. However, the trade-off between data utility and privacy must be carefully managed to ensure that privacy protections do not undermine the effectiveness of threat detection.

Furthermore, the deployment of AI-powered IDS in autonomous vehicles raises ethical questions related to decision-making in the event of cyber-attacks. In scenarios where an attack compromises critical vehicle functions, such as braking or steering, the IDS must make real-time decisions that balance the safety of vehicle occupants with that of other road users. The development of ethical frameworks for IDS decision-making, potentially incorporating principles from autonomous driving ethics, is crucial to ensuring that these systems operate in a manner that is both safe and ethically sound.

Looking forward, it is evident that the future of AI-powered IDS in automotive networks will be shaped by a confluence of technological advancements, regulatory developments, and

ethical considerations. Federated learning represents a promising avenue for collaborative and privacy-preserving model training, while adherence to evolving automotive cybersecurity standards will ensure regulatory compliance and system robustness. Concurrently, addressing the ethical and safety implications of IDS deployment will be critical to achieving a balanced and sustainable approach to automotive cybersecurity. Future research should explore interdisciplinary approaches that combine advances in machine learning, cybersecurity, automotive engineering, and ethics to create comprehensive and resilient IDS solutions that are capable of meeting the complex demands of modern vehicular networks.

10. Conclusion

This research has provided a comprehensive exploration of the integration of Artificial Intelligence (AI)-powered Intrusion Detection Systems (IDS) in automotive networks, particularly within the context of in-vehicle communication systems and emerging Vehicle-to-Everything (V2X) paradigms. The study underscored the pressing need for advanced IDS solutions that can effectively address the growing landscape of cybersecurity threats targeting modern vehicles, which are increasingly characterized by sophisticated electronic control units (ECUs), complex software stacks, and ubiquitous connectivity features. Through a detailed discussion on the various machine learning algorithms such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and Autoencoders, the paper demonstrated how these techniques can be leveraged to enhance the detection accuracy and efficiency of IDS in vehicular environments.

The discussion on algorithm selection criteria illuminated the multifaceted considerations that influence the choice of algorithms for automotive IDS, including computational constraints, real-time processing needs, and robustness against evolving threats. The system architecture for AI-powered IDS was meticulously elaborated, highlighting key components such as data collection, preprocessing methodologies, model training, and validation strategies. These architectural components provide a blueprint for developing IDS systems that are capable of handling the unique challenges of vehicular networks, such as high-dimensional data and real-time constraints. The study further explored integration challenges and opportunities

with V2X communication systems, proposing enhanced IDS models that can operate seamlessly within this rapidly evolving landscape.

Practical applications were illustrated through real-world case studies that demonstrated the effectiveness of AI-powered IDS in detecting specific attack scenarios, such as Denial-of-Service (DoS) and spoofing attacks. These case studies provided empirical evidence of the performance, accuracy, and efficiency of the proposed IDS models, highlighting both their strengths and areas that require further refinement. The research also identified critical challenges in the deployment of AI-powered IDS, such as handling high-dimensional data, addressing latency and computational limitations of automotive ECUs, and managing bandwidth and resource constraints. Each of these challenges was discussed in detail, and potential solutions were proposed, contributing to the body of knowledge on automotive cybersecurity.

The findings of this research have significant implications for the future of automotive cybersecurity. The integration of AI-powered IDS represents a paradigm shift in the way cybersecurity threats are detected and mitigated in vehicular environments. Traditional IDS techniques, which rely heavily on signature-based or rule-based approaches, are increasingly becoming inadequate in the face of sophisticated and adaptive cyber threats. In contrast, AI-powered IDS, with their ability to learn from data, identify anomalies, and adapt to evolving attack patterns, provide a more dynamic and robust defense mechanism. The deployment of these systems can lead to a substantial enhancement in the security posture of modern vehicles, especially as they become more connected and autonomous.

Moreover, the incorporation of federated learning techniques into IDS models offers a promising approach to addressing privacy and scalability concerns. Federated learning enables collaborative model training across distributed vehicular nodes without compromising data privacy, thereby supporting a decentralized cybersecurity defense strategy. This is particularly pertinent in the context of V2X communications, where vehicles must not only defend against direct attacks but also ensure secure communication with other vehicles and infrastructure. AI-powered IDS that are integrated with V2X systems could play a critical role in creating a secure ecosystem for future intelligent transportation systems (ITS), where real-time data sharing and decision-making are paramount.

From a regulatory perspective, the research also highlights the importance of aligning IDS development with evolving automotive cybersecurity standards, such as ISO/SAE 21434. Compliance with these standards not only ensures the technical robustness of IDS solutions but also facilitates their acceptance and deployment in the automotive industry. This alignment is critical as regulatory bodies increasingly emphasize the need for comprehensive cybersecurity risk management throughout the lifecycle of road vehicles. The ability of AI-powered IDS to provide continuous monitoring, threat detection, and real-time response aligns well with these regulatory expectations, further solidifying their role in future automotive cybersecurity frameworks.

While the research provides a strong foundation for understanding the potential and challenges of AI-powered IDS in automotive networks, several areas require further investigation to fully realize their capabilities. First, future research should focus on the development of lightweight and efficient AI models that can operate under the stringent computational and energy constraints of vehicular ECUs. Techniques such as model pruning, quantization, and knowledge distillation could be explored to optimize deep learning models for resource-constrained environments.

Second, the integration of AI-powered IDS with V2X systems presents numerous opportunities for enhancing collaborative cybersecurity defense but also raises challenges related to secure and reliable communication. Future research should explore advanced cryptographic protocols and secure multi-party computation techniques to safeguard data integrity and privacy in V2X-enabled IDS architectures. Additionally, the development of hybrid IDS models that combine anomaly detection with predictive analytics could offer a more proactive approach to threat detection and mitigation.

Third, there is a need for large-scale, real-world datasets that reflect the diversity and complexity of vehicular network environments. Such datasets are critical for training and validating IDS models, ensuring that they are robust against a wide range of attack scenarios and environmental conditions. Collaborative efforts between academia, industry, and government agencies could facilitate the creation of standardized, publicly available datasets that support the development of more effective and generalizable IDS solutions.

Finally, as AI-powered IDS become more integrated into critical automotive systems, it is imperative to establish ethical guidelines and safety standards that govern their deployment

and operation. Future research should examine the ethical implications of autonomous IDS decision-making, particularly in scenarios where safety and cybersecurity objectives may conflict. The development of ethical frameworks that prioritize both cybersecurity and vehicle safety will be essential to ensure the responsible deployment of AI technologies in the automotive sector.

The integration of AI into automotive cybersecurity, particularly through the deployment of AI-powered IDS, represents a significant advancement in the protection of modern vehicles against an increasingly sophisticated cyber threat landscape. As vehicles become more connected and autonomous, the need for intelligent, adaptive, and scalable cybersecurity solutions has never been more critical. AI-powered IDS offer a promising approach to meeting this need, providing robust defenses that can detect, adapt to, and mitigate evolving threats in real time. However, the successful implementation of these systems will require a holistic approach that addresses technical, regulatory, ethical, and safety considerations.

References

1. A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in *Proc. 9th EAI Int. Conf. Bio-inspired Inf. Commun. Technol.* (BICT), New York, NY, USA, 2016, pp. 21–26.
2. M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO–simulation of urban mobility: An overview," in *Proc. 3rd Int. Conf. Adv. Syst. Simul.* (SIMUL), Barcelona, Spain, 2011, pp. 55-60.
3. S. Khan, A. Gumaei, A. Anwar, and H. Daudpota, "A hybrid intelligent approach for effective intrusion detection in connected vehicles," *Future Gener. Comput. Syst.*, vol. 105, pp. 403–412, 2020.
4. Potla, Ravi Teja. "Enhancing Customer Relationship Management (CRM) through AI-Powered Chatbots and Machine Learning." Distributed Learning and Broad Applications in Scientific Research 9 (2023): 364-383.
5. Machireddy, Jeshwanth Reddy, Sareen Kumar Rachakatla, and Prabu Ravichandran. "AI-Driven Business Analytics for Financial Forecasting: Integrating Data

Warehousing with Predictive Models." Journal of Machine Learning in Pharmaceutical Research 1.2 (2021): 1-24.

6. Singh, Puneet. "Revolutionizing Telecom Customer Support: The Impact of AI on Troubleshooting and Service Efficiency." Asian Journal of Multidisciplinary Research & Review 3.1 (2022): 320-359.
7. Pelluru, Karthik. "Enhancing Cyber Security: Strategies, Challenges, and Future Directions." Journal of Engineering and Technology 1.2 (2019): 1-11.
8. Rachakatla, Sareen Kumar, Prabu Ravichandran, and Jeshwanth Reddy Machireddy. "Scalable Machine Learning Workflows in Data Warehousing: Automating Model Training and Deployment with AI." Australian Journal of Machine Learning Research & Applications 2.2 (2022): 262-286.
9. K. Xiao, D. Freeman, and A. Datta, "Leveraging side channels for automotive intrusion detection: A case study," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security* (CCS), London, UK, 2018, pp. 1-14.
10. Y. Duan, X. Li, L. Ding, and Z. Gao, "A machine learning-based multi-layer intrusion detection system for VANETs," *IEEE Access*, vol. 8, pp. 12131-12143, 2020.
11. G. Loukas, "Machine Learning and Anomaly Detection for Automotive Cybersecurity," in *Cybersecurity for Connected Vehicles: Security, Privacy and Safety*, 1st ed., B. Suraj and P. Anwar, Eds. Cham, Switzerland: Springer, 2021, ch. 5, pp. 123-146.
12. R. Bhatia, S. Malik, and A. Kaul, "Machine learning techniques for cyber attack detection in vehicular ad-hoc networks," *Int. J. Commun. Syst.*, vol. 34, no. 6, p. e4753, 2021.
13. C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, Las Vegas, NV, USA, 2015, pp. 1–91.
14. T. Tong, X. Cheng, X. Yang, J. Wang, and W. Liu, "Automotive intrusion detection using deep neural networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2115–2143, 2021.
15. Machireddy, Jeshwanth Reddy, and Harini Devapatla. "Leveraging Robotic Process Automation (RPA) with AI and Machine Learning for Scalable Data Science

Workflows in Cloud-Based Data Warehousing Environments." Australian Journal of Machine Learning Research & Applications 2.2 (2022): 234-261.

16. Potla, Ravi Teja. "AI in Fraud Detection: Leveraging Real-Time Machine Learning for Financial Security." Journal of Artificial Intelligence Research and Applications 3.2 (2023): 534-549.
17. S. Song, S. Yoo, and B. Kang, "A hybrid anomaly detection approach combining deep learning with expert knowledge for industrial control systems," *IEEE Trans. Ind. Informat.*, vol. 16, no. 4, pp. 2651-2661, 2020.
18. B. Subba, S. Biswas, and S. Karmakar, "A neural network-based system for intrusion detection and attack classification in autonomous vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 1, pp. 123-133, 2022.
19. R. Mitchell and I. R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surv.*, vol. 46, no. 4, pp. 1–29, 2014.
20. M. Habler and H. Hadeli, "Integrating anomaly detection systems for smart car cybersecurity," in *Proc. IEEE 7th Int. Conf. Inf. Syst. Security Privacy* (ICISSP), Prague, Czech Republic, 2021, pp. 99–106.
21. M. T. Rahman, K. J. Bowers, N. Saxena, and N. Memon, "Detecting anomalous CAN bus messages using a neural network-based intrusion detection system," *IEEE Trans. Veh. Technol.*, vol. 71, no. 3, pp. 2567-2578, 2022.
22. A. W. Doosti, S. Srivastava, and A. Choudhary, "A federated learning-based intrusion detection system for vehicular networks," in *Proc. IEEE Int. Conf. Smart Infrastruct. Technol.* (ICSIT), 2023, pp. 95-101.
23. H. Abie and I. Balasingham, "Risk-based adaptive security for smart IoT in eHealth," in *Proc. Int. Conf. Wireless Mobile Comput. Netw. Commun.* (WiMob), Barcelona, Spain, 2012, pp. 597–604.
24. E. Yaghini, M. H. Manshaei, and A. Barati, "Intrusion detection system for in-vehicle networks using ensemble learning methods," *Veh. Commun.*, vol. 29, p. 100351, 2021.

25. Z. Durumeric, M. Bailey, and J. A. Halderman, "An internet-wide view of Internet-wide scanning," in *Proc. 23rd USENIX Secur. Symp.* (USENIX Security), San Diego, CA, USA, 2014, pp. 65–78.

26. X. Cao, Z. Hu, and Y. Zhang, "Securing V2X communication systems in connected and automated vehicles: A survey," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 8823–8836, 2021.

27. M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," in *Proc. 9th Workshop Cryptogr. Hardware Embedded Syst.* (CHES), Vienna, Austria, 2007, pp. 7–22.