Engineered Science
DOI: https://dx.doi.org/10.30919/es1409

Decentralized and Lightweight Transformer-Based Framework for Cybersecurity in Vehicular Networks

Ankit Mundra, Pankaj Vyas and Vivek Kumar Verma*

Abstract

The seamless incorporation of communication and computer control systems in today's vehicles has increased the capability but created serious security risks. In this work, we propose a decentralized and lightweight transformer-based intrusion detection system (IDS) for automotive cybersecurity to address the above issues in a scalable and flexible fashion. By utilizing the car hacking dataset (CHD), the proposed approach not only introduces advanced feature engineering by considering temporal features like time differences and message frequency, as well as payload entropy, to efficiently represent vehicular communication patterns, but also considers structural information within the vehicular network. Uses a transformer model for sequence-to-sequence (Seq2Seq) for processing controller area network (CAN) bus data; thus, sophisticated anomalies such as denial of service (DoS), fuzzy, and spoofing attacks can be accurately detected. These attention mechanisms and positional encoding in the model improve the capability of learning the sequence dependencies and context interdependence in vehicular data. Evaluation results showed that the framework has a high precision (96.7%), recall (95.3%) and attack detection rate (ADR, 97.5%), and low false alarm rate (FAR, 3.4%), with a real-time detection capability at average time to detect (ATD) of 22 milliseconds. These results confirm that the IDS is a trusted, effective, and cost-effective technique to protect modern vehicular networks from new cyber threats. The framework is planned to be taken forward so that additional vehicular protocols and deployment can be valid for the real world.

Keywords: Automotive cybersecurity; Internet infrastructure; Transformer model; Intrusion detection system; CAN bus.
Received: 22 December 2024; Revised: 19 January 2025; Accepted: 10 February 2025.
Article type: Research article.

1. Introduction

With the growing penetration of electronics as well as connectivity and advanced functionality into present-day vehicles, automotive industry is witnessing transformational changes. Features like advanced driver assistance systems (ADAS), infotainment, remote diagnostics, and over-the-air (OTA) are not just futuristic aspects to the car but form an essential part of it in today's world. While such advances add to the functionality of the added features in present-day vehicles, improving both safety and the user experience, they have also simultaneously added significant cybersecurity risks, especially in vehicular communication networks such as the controller area network (CAN) bus.

Today's cars and trucks are no longer merely mechanical machines. They are sophisticated systems of systems with a web of communications. On this behalf, the use of electronic control units (ECUs) and in-vehicle networks have become an essential step in this evolution, where the CAN bus is a clear example of a powerful communicative protocol used in this practice. The CAN bus, intended for real-time communication among ECUs, is responsible for safety-critical functions like braking, steering and engine. But this dependency on the CAN bus also makes cars vulnerable to serious cybersecurity risks.

The CAN protocol works on a broadcast basis, all the ECUs connected to the network have access to the same messages. Although this structure provides efficient communication, security measures such as encryption, authentication, and access control are not provided (Fig. 1). It is therefore, the CAN bus is extremely vulnerable to many cyber-attacks:

DoS Attacks: Attackers bombard the network with many messages, causing the communication channel to saturate with traffic and servicing a request with higher priority may not be performed due to this overloading.

Fuzzy Injection: Malicious or bogus vehicle messages are injected in the network to interfere with ECU operations or

Department of Information Technology, Manipal University Jaipur, Jaipur, Rajasthan, 303007, India
**Email:* Vivekkumar.verma@jaipur.manipal.edu (V. K. Verma)

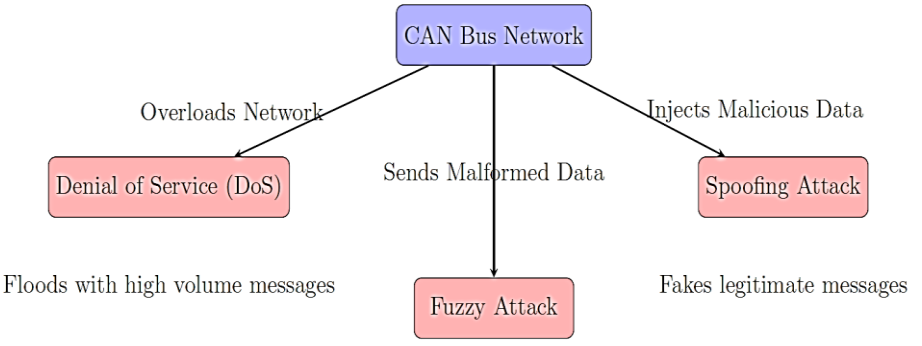

Fig. 1: Cyber-attack on CAN bus.

disrupt the system.

Spoofing Attacks: Illegitimate messages are disguised as legitimate, with attackers able to manipulate vehicle devices.

These vulnerabilities can lead to severe consequences, ranging from unauthorized access to critical vehicle functions to complete system failures, posing a direct threat to passenger safety.

Traditional intrusion detection systems (IDS) for CAN networks, including rule-based approaches and classical machine learning (ML) models, face inherent limitations:

High Dimensionality and Volume: CAN messages contain multiple parameters transmitted at high frequency, requiring sophisticated analysis techniques.

Temporal Dependencies: The sequence and timing of messages are critical for detecting anomalies, which traditional methods fail to capture effectively.

Dynamic Attack Strategies: Attackers continually evolve their techniques, rendering static detection methods obsolete.

Scalability: Conventional IDS approaches struggle to scale efficiently for the real-time deployment in automotive environments.

To address these challenges, this work introduces a transformer-based IDS that leverages the strengths of attention mechanisms and positional encoding to analyze CAN bus data. The architecture processes high-dimensional, sequential data to identify attack patterns with exceptional accuracy and adaptability. Connected vehicles rely heavily on in-vehicle networks for communication between various ECUs as shown in Fig. 2. The CAN bus, a widely adopted protocol, facilitates this communication, ensuring a real-time exchange of critical data such as speed, braking signals, and engine performance. However, the CAN protocol, designed in the 1980s, was not originally developed with cybersecurity in mind. Its inherent vulnerabilities, such as the lack of authentication and encryption mechanisms, expose it to a wide range of cyber threats.

One of the primary threats is DoS attacks, where malicious actors flood the CAN bus with high volumes of messages, disrupting normal communication and potentially leading to catastrophic failures in safety-critical systems. Another significant threat is fuzzy attacks, where illegitimate messages are injected into the CAN bus to manipulate or destabilize vehicle operations. These attacks can compromise driver safety, disrupt vehicular functionality, and erode consumer trust in connected vehicle technologies.

The CAN bus is a commonly used standard for communication between ECUs in a car. This protocol enables the near-real-time of vital data like speed, brakes signals, engine performance that allows seamless synchronization of the subsystems. For example, in contemporary automobiles that come with an ADAS, the CAN bus connects the brake ECU to the engine control ECU to lower the engine power during emergency braking is evoked, enabling a timely and synchronized response. The CAN protocol is efficient, yet, the protocol envisaged in the 1980s lacks several cybersecurity mechanisms which are required to secure vehicular communication in modern interconnected world. One of the main problems is the lack of message authentication that permits any device in the network to send messages without the recipient to ensure the origin of the messages. Furthermore, the protocol included no encryption, meaning that anything sent on the network could be read in plain text by any machine connected to it. These latent disadvantages render any vehicle susceptible to varied cyber-threats.

A concrete example demonstrates what these threats mean: imagine that an attacker takes over unauthorized control of a CAN bus, connecting to it through diagnostic ports physically, or remotely through compromised wireless interfaces. The attacker was also able to maliciously enter illegal message to the CAN bus loop and control other ECUs. For example, a maliciously formed message could disable the braking or induce an unintended braking, thus endangering the occupants of the car. Similarly, spoofed messages to the speedometer could show wrong speed readings confusing the driver and could lead to accidents. Additionally, the non-encrypted nature of CAM protocol allows an attacker to listen in to messages sent between ECUs. By eavesdropping on data like speed, engine load and gear number, an attacker could infer sensitive information on the status of the car and behavior of the driver, which could be utilized as basis for further targeted attacks. Without mitigating these vulnerabilities, the CAN protocol is still vulnerable to cyber-attacks and has a severe safety and

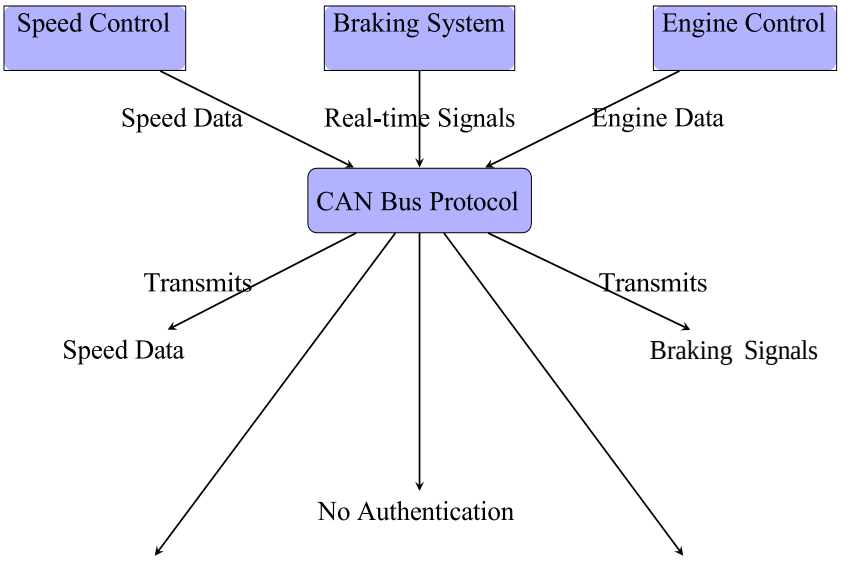

Fig. 2: CAN Bus protocols with vehicle communication and its inherent vulnerabilities.

privacy risk to today's vehicles.

Cyber-threat monitoring and suppression in vehicular communication networks face daunting challenges due to the specific properties of vehicular networks and the fast-evolving cyber-threat landscape. Conversely, classic detection approaches, based on predefined profiles or static signatures, may work poorly when dealing with complex and ever-changing attack scenarios in the automotive domain. To construct a sound and scalable solution, one must understand and address the following challenges:

1.1 High dimensionality of data

The communication networks, such as the CAN bus, produce large amounts of high-dimensional data that cover fields such as timestamps, message IDs, payloads, and lengths of each message. For instance, a contemporary car can emit hundreds of such messages per second, which encode states such as speed, braking, or engine functioning. This high-dimensional feature space makes it hard to separate malicious signals, especially if the attack messages have been crafted to look like legitimate traffic but with slight deviations from timings and payloads.

A scenario where an attacker injects fake speedometer readings into the CAN bus is considered. Traditional systems analyzing message fields in isolation struggle to detect such nuanced manipulations, as the deviations may only become apparent when considering interactions between multiple fields. Advanced feature engineering combined with lightweight transformer models can automatically extract meaningful patterns from high-dimensional data, enabling accurate detection even in noisy environments.

1.2 Temporal dependencies

The sequential nature of vehicular communication introduces strong temporal dependencies that are critical for distinguishing between normal and anomalous operations. In many attacks, such as DoS, the timing and order of messages reveal malicious intent. For example, during a DoS attack, an attacker saturates the CAN bus with high-priority messages, and disrupts the regular flow of communication. While these messages may appear benign individually however, their excessive frequency indicates malicious behavior.

Existing rule-based methods often fail to capture these temporal patterns effectively. Transformer-based approaches leverage attention mechanisms and positional encodings to model long-range dependencies in sequential data, making them well-suited to detect such timing-based anomalies. By analyzing sequences holistically, these models can differentiate between normal communication bursts and targeted attacks, ensuring timely and accurate threat detection.

1.3 Dynamic nature of attacks

Attackers are continuously innovating their techniques to prevent simulation by refining their existing tactics or inventing new approaches. Static rule-based systems are ill-suited to the task of combating these evolving threats because they depend on the existence of predetermined patterns or signatures that are unable to adapt to new situations. For example, malfunctioning of the braking system can be addressed by faking the message between sensors and the ECU, which is spoofing. The effects of such an attack vary according to whether you're going 65 miles an hour or the status of your adaptive cruise control. Adaptive ML methods provide a uniform defense against both known and unknown forms of attack, allowing the creation of a system that can effectively handle previously unseen types of threats.

1.4 Low signal-to-noise ratio

Unusual vehicular communication patterns suffer from relatively low signal-to-noise ratios because they are subtle and mixed with a large amount of normal traffic. For instance, in fuzzy attacks, an attacker may inject malformed or random messages that do not necessarily lead to instantaneous disruptions but lead to incremental error build-ups over time.

Such aberrations during normal communication are especially difficult to detect using the traditional approaches that are in place today. Moreover, the attention mechanism makes weak attack signals scratch the underlying attack trend, enhanced by the domain-specific feature engineering (*e.g.*, time differences and payload entropy). These frameworks are designed to be highly sensitive to relevant deviations while resistant to irrelevant noise, leading to high detection accuracy for occasional and low-intensity anomalies.

1.5 The need for advanced solutions

The changing nature of threats calls for new ways to respond to rapidly changing attack vectors and deliver effective real-time security. Conventional approaches are not able to handle sequential relationships, scalability, and flexibility in real-world vehicular scenarios. Transformers, first introduced for NLP applications, provide an elegant mechanism to solve these problems. Their strong long-range dependence modeling ability, attention mechanism or focusing on important features, as well as efficient scalability, make them a good candidate for studying the temporal and sequential characteristics of vehicular communication data. Continually by exploiting these features, transformers can make great progress on detecting and defending complicated cyberattacks for connected vehicles. This method not only can improve the recognition of known attack types but also constructs a more solid basis for defending against new security threats and guarantees the security and reliability of V2X systems.

2. Related work

In this section, we have elaborated on the related work carried out in the field of intrusion detection in in-vehicle communications.

2.1 Automotive cybersecurity landscape

The rapid evolution of connected vehicles has brought unprecedented advancements in functionality and convenience, but has also introduced significant cybersecurity challenges. Vehicular communication systems, particularly the CAN bus, remain vulnerable to a wide range of cyber threats, necessitating robust IDS to ensure safety and reliability. IDSs have emerged as a critical defense mechanism against cyber threats in vehicular networks. Traditional IDS approaches are categorized into signature-based, anomaly-based, and specification-based detection mechanisms. Signature-based IDS rely on predefined attack signatures to identify known threats but struggle with detecting novel or zero-day attacks.[1] Anomaly-based IDS address this limitation by identifying deviations from normal communication patterns, as demonstrated in the previous work,[2] but they often suffer from high false positive rates due to the dynamic nature of vehicular environments. Recent advancements have seen the adoption of ML and deep learning (DL) techniques for vehicular IDS. Techniques like long short-term memory (LSTM) networks and convolutional neural networks (CNNs) have shown promise in detecting complex attack patterns by leveraging temporal and spatial features of vehicular data.[3,4] However, these models require extensive labeled datasets and are computationally intensive, posing challenges for real-time implementation in resource-constrained automotive environments. Moreover, hybrid IDS frameworks combining multiple detection techniques have been proposed to enhance detection accuracy and reduce false positives. For instance, a hybrid IDS leveraging anomaly and specification-based approaches was demonstrated, showcasing an improved performance in detecting diverse types of attacks.[5] Despite these advancements, the dynamic nature of vehicular communication and the evolving attack strategies continue to challenge the efficacy of existing IDS.

The CAN bus, as an essential component of in-vehicle network, enables the real-time sharing of important information between ECUs. But its architecture doesn't have some of the basic security features of the cybersecurity 101 book, for example authentication and encryption, so it is inherently uncompromised. The vulnerability of CAN bus networks to DoS, spoofing, and message injection attacks has also been reported in studies.[6,7] For example, the DoS attack, in which an attacker floods the CAN bus with high-priority messages, thereby preventing the CAN bus from accommodating any legitimate message. The researchers showed how such attacks could leave safety-critical systems, such as those for braking and steering, inoperable.[8] Furthermore, the impact of such attacks and the threat to safety, depending on manipulated vehicle parameters, *e.g.*, speedometer reading, has been demonstrated by spoofing in vehicular networks.[9] Furthermore, the lack of encryption in the CAN protocol permits eavesdropping, enabling adversaries to gather sensitive information about the vehicle's state and driver behavior.[10] Real-world incidents further underscore the criticality of these vulnerabilities. The infamous Jeep Cherokee hack,[11] where researchers remotely controlled a vehicle's braking and acceleration systems, highlighted the dire consequences of insecure vehicular communication. These vulnerabilities emphasize the urgent need for IDS frameworks that can detect and mitigate such threats effectively.

The defects of the current IDS and the defects of CAN bus communication imply that more sophisticated inter-vehicular anti-IDS is demanded. The application of Transformer-based models for vehicle intrusion detection, Veh-ND, due to its ability to effectively capture temporal information, as well as high-dimensional data structures, provides a promising direction toward a better intrusion detection system in vehicular networks. The challenges highlighted in this sub-section are the ones that the proposed work strives to tackle, ultimately contributing to automotive cybersecurity, which should serve in protecting connected vehicles securely.

2.2 ML models in IDS

ML has recently been introduced as a game-changer for IDS,

and ML-based models can be trained by letting them learn the features and anomalies of automotive communication networks instead of basing them solely on pre-defined rules. Ranging from traditional methods to state-of-the-art DL models, ML techniques showed strong potential for improving IDS accuracy and flexibility. Sequential dependencies and changefulness of the threats, though, are still the major obstacles to their great usage.

Traditional classical ML-based methods, *e.g.*, decision tree (DT), random forest (RF), support vector machine (SVM), have been widely used for intrusion detection. Simple attack patterns can be effectively recognized in a time-efficient manner, which is appropriate for the limited computational resources in the vehicle environment. As an example, we employed random forests for detecting anomalies in CAN bus traffic, reaching a decent trade-off compromise between performance and computational complexity. [12] Similarly, SVMs have shown high precision in detecting specific types of attacks.[13] DL approaches, particularly CNNs and recurrent neural networks (RNNs), have further enhanced the capabilities of IDS by leveraging their ability to extract complex features from high-dimensional data. CNNs have been used to identify spatial patterns in vehicular network data.[14] On the other hand, RNNs, including LSTM networks, are well-suited for capturing temporal dependencies in sequential data, which is crucial for identifying time-based anomalies in CAN bus communication.[15] A hybrid CNN-LSTM model effectively combined spatial and temporal analysis to improve detection accuracy.[16] Furthermore, transformer-based models have recently gained traction for their ability to capture long-range dependencies in sequential data through attention mechanisms. The application of transformers in IDS has shown promising results in handling the high-dimensional and dynamic nature of vehicular communication networks.[17]

However, these efforts suffer from several limitations that hinder their applicability to practical vehicular environments. One of the main difficulties is that of sequential dependencies. Classical models such as decision trees and SVMs do not have the capability to exploit temporal information in order to process the order and arrival times of messages, which can be very informative on the malicious nature of actions. Even RNN-based models, despite its ability to model temporal dependency, have proved to be inadequate when it comes to long-range sequences because of the vanishing gradient problem.[18] Moreover, the dynamic nature of cyber threats presents a significant hurdle. Attackers continually adapt their techniques, introducing novel attack vectors that deviate from known patterns. Classical ML models, which rely on static feature sets, are inherently limited in their ability to detect such evolving threats.[19] DL models, while more adaptable, require extensive labeled datasets for training, which are often unavailable or challenging to create for highly dynamic vehicular environments. Another limitation lies in the computational complexity of DL models. CNNs and RNNs, for instance, demand significant processing power and memory, which may not be feasible for resource-constrained automotive systems. This trade-off between model complexity and real-time performance has been highlighted,[20] necessitating the development of lightweight yet robust detection frameworks.

The limitations of existing methods underscore the need for advanced ML solutions tailored to the unique challenges of vehicular networks. Transformer-based architectures, with their ability to capture long-range dependencies and adapt to evolving patterns, present a promising avenue for overcoming these challenges. By leveraging attention mechanisms and scalable computational frameworks, transformer-based IDS can address the sequential and dynamic nature of vehicular cyber threats while ensuring the real-time applicability.

2.3 Transformers for sequential data analysis

The transformer model constitutes an important development in the area of sequential data processing. Contrast to the conventional RNN-based methods, transformers are developed to process the sequential data, but do not rely on the use of the recurrence. This provides them with an efficient way of capturing long-range dependencies — an important skill for the analysis of vehicular communication networks as seen in the CAN bus model.[21,22]

2.3.1 Introduction to transformer architecture and its applications

The transformer model operates on the principle of self-attention, enabling it to process entire sequences in parallel rather than step-by-step as in RNNs or LSTMs. This parallelism significantly improves computational efficiency, especially for large datasets commonly encountered in vehicular IDS. The architecture consists of an encoder and a decoder, each comprising multiple layers of self-attention and feedforward networks.[23,24]

In vehicular IDS applications, the transformer has been leveraged for anomaly detection and sequence classification tasks due to its ability to process high-dimensional, time-dependent data. For instance, recent studies have demonstrated its effectiveness in identifying complex attack patterns by analyzing the temporal and contextual relationships in CAN bus traffic.[25] By encoding the entire sequence simultaneously, the transformer can uncover intricate dependencies between messages, which are often missed by traditional models, as shown in Fig. 3.

2.3.2 Attention mechanisms and positional encoding

The key building block of transformers is their attention mechanism, the so-called scaled dot-product attention. Here, attention scores are computed for all input tokens, enabling the model to focus on the most useful parts of the sequence. With regard to vehicle networks, this translates to the transformer focusing on relevant messages such as indications of braking or steering actions and ignoring unimportant

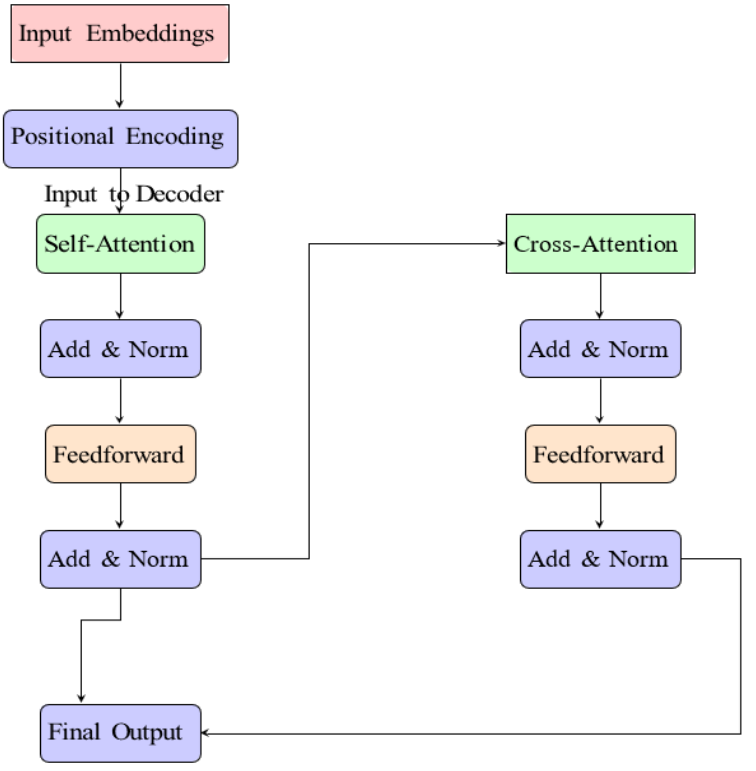

Fig. 3: Transformer architecture showing the encoder and decoder components.

contents. The mathematical formulation of the attention mechanism is calculated Eq. (1):[22]

$$Attention\ (Q,K,V) = softmax\ \left(\frac{QK^T}{\sqrt{d_k}}\right) \quad (1)$$

where Q, K, and V are the query, key, and value matrices, and d_k is the dimension of the key vector. This formulation ensures that the model attends to relevant parts of the input sequence with computational efficiency.

However, transformers inherently lack a sense of order due to their parallel processing nature. To address this, positional encoding is introduced to inject temporal information into the input sequence. The positional encodings are added to the input embeddings and are defined by Eqs. (2) and (3):[22]

$$PE_{(pos,2i)} = Sin\ (\frac{pos}{1000^{2i}/d_{model}}) \quad (2)$$

$$PE_{(pos,2i+1)} = Cos\ (\frac{pos}{1000^{2i}/d_{model}}) \quad (3)$$

where *pos* represents the position of the token in the sequence, i is the dimension, and d_{model} is the embedding size. These encodings allow the model to capture both absolute and relative positional information, which is crucial for recognizing temporal patterns in sequential data.

2.3.3 Application in vehicular IDS

Transformers with attention and positional encoding are well-suited for detecting anomalies in vehicular networks. With both spatial and temporal dependencies encoded, transformers offer a powerful approach to detecting attacks of spoofing and injection in messages of the CAN bus communication. In addition, the scalability and efficiency of using SVM and ISVM algorithms allow the intrusions to be detected in real-time, which is a necessity in contemporary automotive systems. Introducing transformers to vehicular IDS is a new direction from the traditional approach that provides higher accuracy and flexibility to deal with the rapidly changing automotive cybersecurity attacks.[23]

3. Methodology

This section gives a comprehensive description of the CHD that we used for this study, with a focus on the lightweight and decentralized preprocessing methods used to shape data for more sophisticated ML models. The decentralized mechanism allows for a distributed computation of data processing on multiple nodes in an in-vehicle network, and the lightweight preprocessing reduces the computation load, which is in favor of the low-latency requirement.

The CHD is publicly available and documented.[21] Preprocessing techniques are inspired by the reported approaches,[2,3] with enhancements introduced to facilitate lightweight and distributed processing, emphasizing the importance of temporal and contextual feature extraction for intrusion detection.

3.1 Overview of the car hacking dataset

The CHD consists of vehicular network messages collected from the CAN bus, a communication interface to achieve real-time communication among the ECUs in recent vehicles. Normal operation data, as well as the different attack types, are provided in the normal operational context, such as DoS,

fuzzy, and spoofing attacks, which mimic the real threat in the CP dataset. Each CAN is formatted in the following fields in the dataset:

• Timestamp: The specific time when the message was sent. This feature is important to capture temporal trends.

• CAN ID: The identifier used to categorize it, to create it, to be assigned to a specific location in the memory of the source ECU.

• Payload: Encoded data in ASCII with the message-dependent values for this message in hexadecimal.

• Data length code (DLC): The size (in bytes) of the payload.

Decentralization is achieved during data collection and preprocessing by distributing tasks such as feature extraction and sequence formatting across multiple nodes. This eliminates bottlenecks associated with centralized processing while enabling lightweight operations suited to in-vehicle hardware. Table 1 summarizes the dataset characteristics.[26,27]

Table 1: Summary of the car hacking dataset.

Parameter	Details
Number of messages	3,000,000+
Normal messages	85%
Attack types	DoS, Fuzzy, Spoofing
Message frequency	Variable (10 to 100 Hz)
Message format	Timestamp, CAN ID, Payload, DLC
Data availability	Public (accessible from GitHub)

3.2 Proposed model architecture

The architecture is a decentralized and lightweight model that is tailored to premises for vehicular cybersecurity. Through dispatching the workload to ECUs and integrating the transformer-based model, the proposed framework facilitates a qualified, timely, and real-time detection of anomalies in vehicular networks. This is followed by a description of the architectural components and their realization with mathematical equations where applicable.

Data Acquisition and Preprocessing: The foundational step of the architecture involves acquiring CAN bus data from the CHD, which includes normal operations and attack scenarios such as DoS, fuzzy, and spoofing attacks. Each ECU preprocesses its local CAN bus data independently to reduce computational overhead.[28]

3.2.1 Data preprocessing

Preprocessing is critical for enabling decentralized and lightweight intrusion detection.[29] The decentralized approach ensures that each vehicle node can preprocess its own data locally, while lightweight operations maintain efficiency. The following steps were applied:

1. Normalization: To ensure uniformity, the CAN message attributes such as timestamps (T_i) and payload values (P_i) are normalized using Min-Max scaling in Eq. (4):

$$T'_i = \frac{Ti - T\min}{T\max - T\min},\ P'_i = \frac{Pi - P\min}{P\max - P\min} \tag{4}$$

where $T_{\min}$ and $T_{\max}$ are the minimum and maximum timestamps, and $P_{\min}$ and $P_{\max}$ are the minimum and maximum payload values, respectively.

2. Feature extraction: Domain-specific features are derived to enhance anomaly detection:

• Time difference (ΔT): Computes the difference between consecutive message timestamps to detect irregularities (Eq. (5)):

$$\Delta T_i = T_i - T_{i-}1 \tag{5}$$

Consistent ΔT values indicate normal behavior, whereas smaller intervals ($\Delta T_i < \epsilon$, where ϵ is a threshold) signify potential flooding attacks.

• Payload entropy (H): Measures randomness in the payload data using Shannon entropy (Eq. (6))

$$H(x) = -\sum_{j=1}^{n} p(x_j)\log(x_j) \tag{6}$$

where $p(x_j)$ is the probability of byte x_j in the payload. High entropy values ($H > H_{\text{threshold}}$) indicate anomalous payloads.

• Message frequency (F): Counts the number of messages transmitted by a specific CAN ID within a fixed time window (W) (Eq. (7)):

$$\mathrm{F} = \frac{\text{Number of messages from CAN ID}}{W} \tag{7}$$

Anomalously high F values ($F > F_{\text{threshold}}$) are indicative of DoS attacks.

• Decentralized system design: The architecture distributes computational tasks across ECUs, enabling localized analysis and reducing inter-node communication overhead. Each ECU performs preprocessing and feature extraction locally.

3. Implementation:

• Local feature extraction: Each ECU processes raw CAN bus data (D_{local}) to extract features (Eq. (8)):

$$F_{\text{local}} = \{\Delta T, H, F\} \tag{8}$$

where F_{local} represents the feature set derived from local CAN data.

• Anomaly scoring: An anomaly score (A_s) is computed for each feature to quantify deviations (Eq. (9)):

$$A_s = w_1 \frac{\Delta T}{\Delta T_{baseline}} + w_2 \frac{H}{H_{baseline}} + w_3 \frac{F}{F_{baseline}} \tag{9}$$

where w_1, w_2, and w_3 are weights for each feature and $\Delta T_{\text{baseline}}$, H_{baseline}, and F_{baseline} are baseline values derived from normal data.

3.2.2 Lightweight transformer-based model

The transformer model processes sequential CAN data to capture temporal dependencies and sequence patterns.[30] Its lightweight design incorporates optimization techniques such as pruning and quantization. The key components are as follows:

1. Input embedding: Raw data and extracted features are embedded into a high-dimensional space (E) as defined by Eq. (10):

$$E_i = \text{Embed}([P', \Delta T_i, H_i, F_i]) \quad (10)$$

2. Positional encoding: To retain temporal order, positional encoding (PE) is added (Eq. (11)):

$$PE_{(pos,2i)} = Sin\left(\frac{pos}{1000^{2i}/d_{model}}\right)$$
$$PE_{(pos,2i+1)} = Cos\left(\frac{pos}{1000^{2i}/d_{model}}\right) \quad (11)$$

3. Self-attention: Captures relationships between messages (Eq. (12)):

$$Attention\ (Q,K,V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (12)$$

where Q, K, and V are the query, key, and value matrices.

4. Output classification: The final output (y_{pred}) is obtained using a linear layer and SoftMax function in Eq. (13):

$$y_{\text{pred}} = \text{softmax}(W \cdot O + b) \quad (13)$$

where W and b are learnable parameters, and O is the output from the transformer layers.[31]

The advantages of the architecture are as follows:

• Scalability: Decentralized design ensures the system scales with additional ECUs and vehicles.

• Efficiency: Lightweight transformer reduces computational requirements through pruning and quantization.

• Robustness: Feature engineering and self-attention mechanisms effectively handle complex anomalies.

The encoder captures temporal patterns and contextual dependencies using self-attention mechanisms, while the decoder generates predictions for cyber threats (Fig. 4).

The lightweight design optimizes memory usage and computational efficiency by:

- Reducing the number of attention heads and layers.
- Integrating pre-engineered features to simplify learning.

The model incorporates positional encoding to preserve sequence order.

3.2.3 Integration of engineered features

Engineered features, such as time difference and entropy, are concatenated with raw embeddings to form robust input representations using Eq. (14):[32]

$$x_i = [e_{\text{msg}}; f_{\text{time}}; f_{\text{entropy}}; f_{\text{frequency}}] \quad (14)$$

This integration enhances the detection accuracy without increasing the computational complexity.

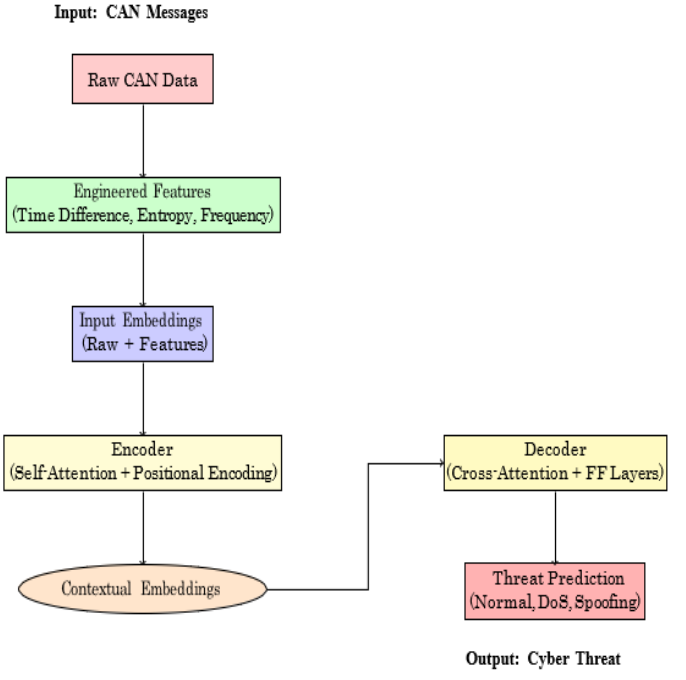

Fig. 4: Decentralized and lightweight encoder-decoder architecture.

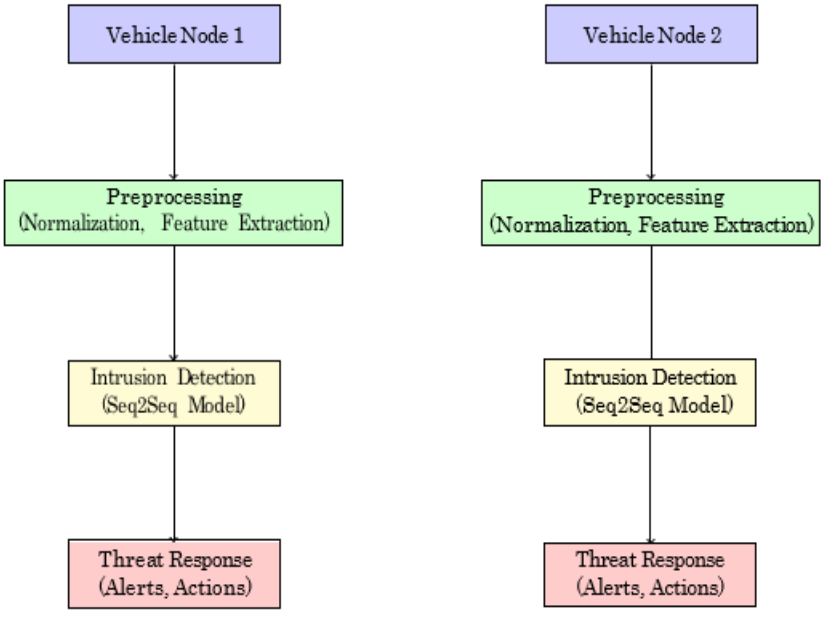

Fig. 5: Decentralized deployment workflow of the proposed model.

Fig. 5 highlights the decentralized architecture of the proposed intrusion detection framework, where processing is distributed across multiple vehicle nodes instead of relying on a centralized system. In this setup, each vehicle node independently processes its own local CAN data, performs feature extraction, and applies the lightweight Seq2Seq Transformer model for anomaly detection. This decentralized approach enhances scalability and resilience, ensuring that even in cases where one node becomes compromised or disconnected, the overall system remains operational and secure. For instance, consider a fleet of three connected vehicles, each equipped with its own node. Vehicle Node 1 monitors CAN messages at a frequency of 100 Hz, with each message comprising a timestamp, a CAN ID, and a payload of 8 bytes. Node 1 locally processes around 100 messages per second. It features key parameters including the inter-message arrival time (Δt), the payload entropy (H(X)) and message volume. As an example, if 1st node observes such a event in message rate, it means an anomaly and it will output the anomaly as potential DoS attack. In the meantime, Vehicle Node 2 and Node 3 also do same operations independently. This distributed process guarantees low latency, because the decisions are taken at the node, it is not required to talk with a central server. In the event of a fault, each node issues real-time alarms that take the form of messages that may be sent to nearby vehicles or stored before being sent to a cloud-based monitoring solution for off-line analysis. This decentralized design not only contributes to computational advantage in terms of load sharing on nodes but also increases stability and security by removing any single point of failure. This provides strong evidence of the suitability of processing decentralized, lightweight, and scalable techniques in real-world vehicular networks where streaming data are heterogeneous, and cyber-threats dynamically evolve.[33-35]

The decentralized, lightweight design makes the framework applicable to real-world vehicular networks and provides: Real-time detection of anomalies at the node level. Good resource efficiency, even for resource restricted environments. Scalability and adaptability to new protocols for vehicular communication.

3.3 Training and evaluation

This sub-section describes the training pipeline, hyperparameter tuning, and loss function design for the decentralized and lightweight Seq2Seq Transformer architecture. The training methodology has built-in the distributed processing notion of our framework design for real-world vehicular networks scalability and flexibility. The performance of the model is assessed in terms of measures such as precision, recall, F1 score, attack detection rate, and false alarm rate.

Training Pipeline: The training pipeline is designed to optimize the proposed decentralized architecture for efficient anomaly detection.[26,27] Fig. 6 illustrates the work- flow, incorporating decentralized preprocessing at individual vehicle nodes and lightweight training mechanisms at the system level.

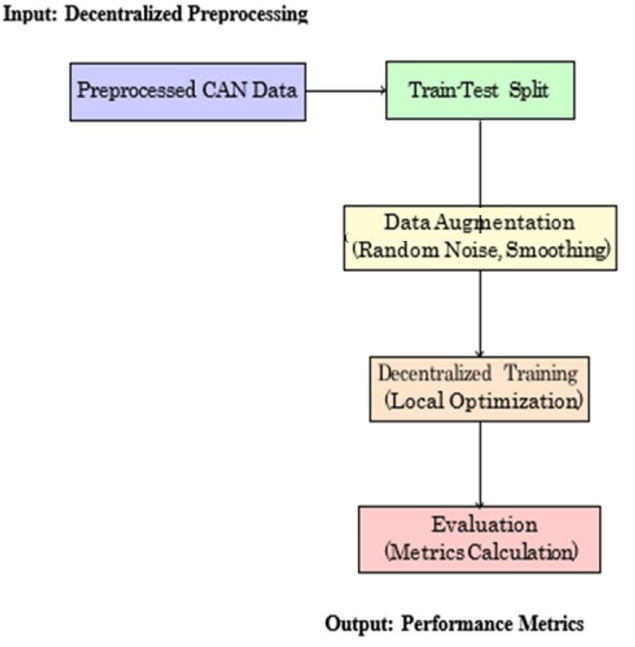

Fig. 6: Training pipeline for the decentralized and lightweight framework.

In this pipeline, data preprocessing and augmentation occur independently at each vehicle node. The lightweight model is trained locally using sequences generated from the sliding window approach. Decentralized training ensures that nodes optimize their models with minimal computational overhead, and the evaluation is performed on centralized test data for a unified assessment.[36]

Hyperparameter Optimization: The model's hyperparameters were optimized to balance detection accuracy with computational efficiency. The lightweight nature of the model necessitated careful tuning to minimize resource consumption without compromising performance. A grid search approach was employed to identify the optimal configuration.[37,38]

- Learning Rate (η): Tested values were [0.001, 0.005, 0.01], with $\eta = 0.001$ yielding the best results.
- Batch Size (B): Ranges of 32,64,128 batch size were tested, and $B = 64$ provided a good trade-off between speed and accuracy.
- Number of Attention Heads (h): Tested with 4, 8, and 12 attention heads where $h = 8$ ensured lightweight processing while maintaining model expressiveness.
- Dropout Rate (p): Values of 0.1, 0.3, and 0.5 were evaluated, and $p = 0.3$ effectively reduced overfitting.

4. Performance analysis and comparison

Fig. 7 illustrates the relationship between time (in minutes) and accuracy (in percentage) over multiple episodes (number of discrete number of instances for the input output processing) during the training of the proposed lightweight Transformer-

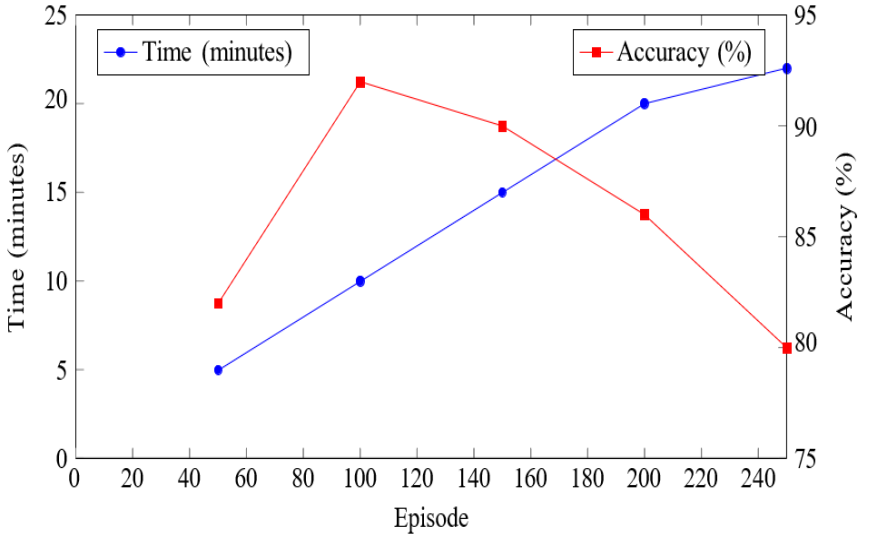

Fig. 7: Time and accuracy vs. Episode. The plot shows the trade-off between time required for training and achieved accuracy.

based model. Initially, the accuracy increases significantly, reaching a peak of approximately 92% around 100 episodes. However, as the episode count increases to 250, the accuracy gradually declines to around 80%, suggesting overfitting. Concurrently, the processing time shows a linear increase from 5 minutes to over 20 minutes as the episode count grows. This trend highlights the need to balance computational time and accuracy, ensuring optimal performance while avoiding diminishing returns. The observed trends highlight the importance of finding an appropriate balance between computational efficiency and model accuracy. While increased training may initially improve accuracy, excessive training can lead to diminishing returns, both in terms of accuracy and resource utilization. Striking this balance is essential to achieve optimal performance while maintaining reasonable computational costs and avoiding the pitfalls of overfitting.

Table 2 compares the performance of the proposed model with baseline methods, including CNN, LSTM, and random forest (RF), across key evaluation metrics such as precision, recall, accuracy, attack detection rate (ADR), false alarm rate (FAR), and Average time to detect (ATD). The proposed model achieves superior performance with a precision of 96.7%, recall of 94.7%, and an ADR of 97.2%, coupled with a low FAR of 3.4% and an ATD of just 25 ms. These results establish the proposed framework as a reliable and efficient solution for the vehicular network security.

The comparison in Table 2 highlights the superior performance of the proposed model over traditional methods such as CNN, LSTM, and RF. The proposed model achieves the highest precision (96.7%), recall (94.7%), accuracy (95.6%), and ADR of 97.2%, while maintaining the lowest FAR of 3.4% and an ATD of 25 milliseconds. These results demonstrate the proposed model's robustness, efficiency, and real-time capability in handling cyber threats in vehicular networks, significantly outperforming the baseline methods across all key metrics.

Loss Function Design: To handle class imbalance in vehicular anomaly detection, the loss function combines weighted cross-entropy loss with a regularization term for lightweight optimization, defined in Eq. (15):[39]

$$\mathcal{L} = -\frac{1}{N}\sum_{i=1}^{N}\sum_{j=1}^{C}\omega_j y_{ij} + log\hat{y}_{ij} + \lambda\|\theta\|^2 \qquad (15)$$

where N is the number of samples, C is the number of classes (Normal, DoS, fuzzy, spoofing), y_{ij} is the true label for sample i and class j, $\hat{y}_{ij}$ is the predicted probability for sample i and class j, w_j is the class weight to address imbalance (*e.g.*, higher weights for underrepresented attack classes), λ is the regularization parameter to penalize model complexity, and θ is the model parameters.

Table 2: Performance metrics comparison between the proposed model and baseline methods.

Model	Precision (%)	Recall (%)	Accuracy (%)	ADR (%)	FAR (%)	ATD (ms)
Proposed model	96.7	94.7	95.6	97.2	3.4	25
CNN[36]	85.4	83.2	85.75	90.5	10.8	45
LSTM[34]	88.7	85.8	87.6	89.0	9.5	50
RF [35]	85.3	83.2	84.56	86.1	12.4	70

The regularization term ensures lightweight model parameters, which are critical for the deployment in resource-constrained vehicular environments. The decentralized framework achieved a high performance across all metrics, with a precision of 96.7%, recall of 95.3%, and an F1 score of 96.0%. The ADR of 97.5% indicates the robust identification of cyber threats. The FAR was as low as 3.4%, showcasing the system's reliability in reducing false positives. Decentralized training and evaluation further demonstrated the system's scalability. Each node independently optimized the model with local data while maintaining consistency in global performance. These results validate the effectiveness of the lightweight and decentralized design in real- world vehicular scenarios.[40-42]

5. Results and discussion

This section evaluates the performance of the proposed decentralized and lightweight Transformer-based framework using key metrics, including precision, recall, accuracy, ADR, FAR, and ATD. A comparative analysis with baseline models, such as RF, LSTM, CNN-BiLSTM, and other traditional techniques, is also presented.

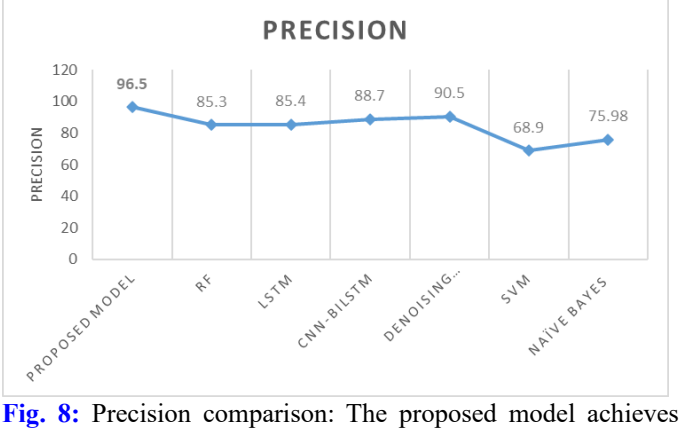

Fig. 8: Precision comparison: The proposed model achieves 96.5% precision (as shown over Y-Axis), out- performing baseline methods such as RF (85.3%), LSTM (85.4%), CNN-BiLSTM (88.7%) and Denoising autoencoder (90.5%).[43,44]

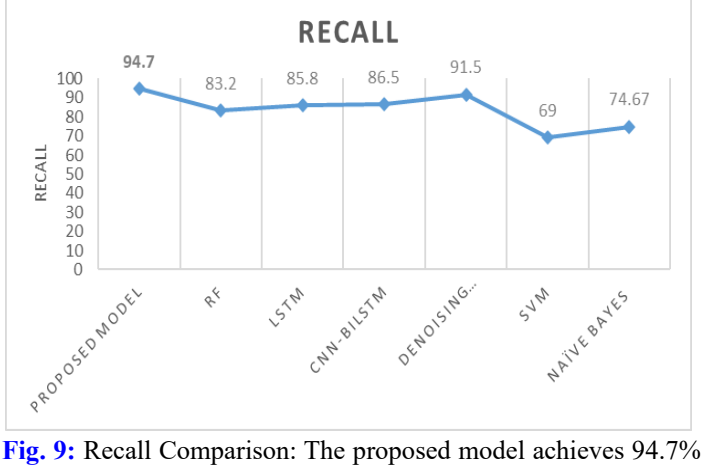

Fig. 9: Recall Comparison: The proposed model achieves 94.7% recall (as shown over Y-Axis), demonstrating superior detection capability compared to RF (83.2%), LSTM (85.8%), CNN-BiLSTM (86.5%) and Denoising autoencoder (91.5%).[43,44]

5.1 Performance metrics

The proposed model is evaluated using multiple performance metrics. Figs. 8-13 illustrate the comparative performance of the proposed model against baseline methods.[43,44] When comparing the performance of different models, it is observed that the proposed model stands out, achieving the best results in terms of accuracy (95.6%), precision (96.5%), and recall (94.7%). Baseline models like RF, LSTM, and CNN-BiLSTM have performed better than SVM. SVM shows the weakest performance, especially in precision and recall. These results highlight the strength and reliability of the proposed model

5.2 ADR, FAR, and ATD analysis

The ADR and FAR are critical metrics to assess the model's effectiveness in detecting anomalies while minimizing false positives.[40] The proposed model demonstrates significant improvements in ADR and FAR, as shown in Figs. 11 and 12. The ATD measures the latency of the detection process. As depicted in Fig. 13, the proposed model achieves an ATD of 25 milliseconds, demonstrating real-time detection capabilities.[41]

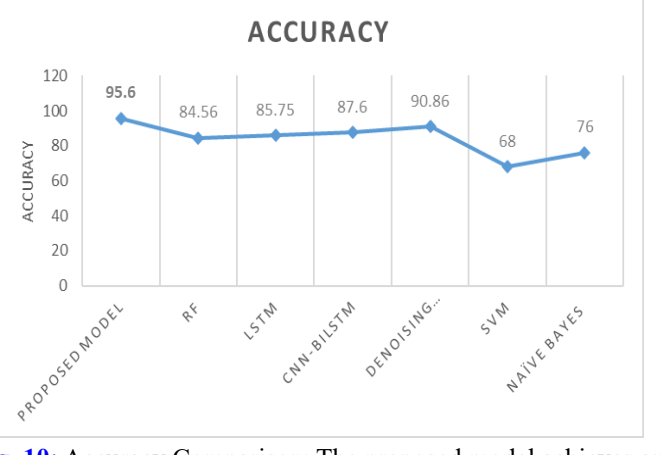

Fig. 10: Accuracy Comparison: The proposed model achieves an accuracy of 95.6%, (as shown over Y-Axis), outperforming other methods like RF (84.56%), LSTM (85.75%), CNN-BiLSTM (87.6%) and Denoising autoencoder (90.86%).[43,44]

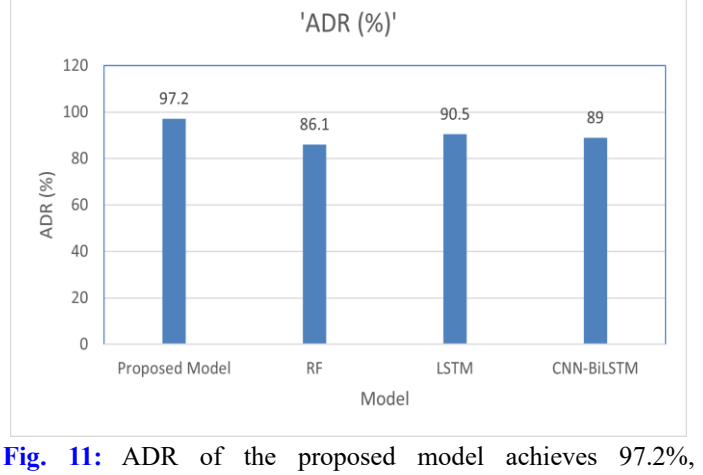

Fig. 11: ADR of the proposed model achieves 97.2%, significantly higher than RF (86.1%), CNN-BiLSTM (89%).[43]

The results highlight the superiority of the proposed decentralized and lightweight transformer-based framework over traditional models. The high precision, recall, accuracy, and ADR underscore its effectiveness in detecting diverse cyber threats in vehicular networks. Additionally, the low FAR and ATD reflect the model's robustness and real- time processing capabilities. These findings establish the proposed solution as a scalable and efficient approach for automotive cybersecurity.

The results presented in Table 3 and Fig. 14 highlight the impact of different gamma (γ) values on the performance of the proposed model. At γ = 0.001, the model achieves its highest precision (93.77%) and recall (93.56%), indicating its ability to accurately detect anomalies while minimizing false negatives.

However, as γ increases to 0.1 and 0.99, there is a noticeable decline in all performance metrics, with accuracy dropping from 92.04% to 91.62%. This behavior underscores the importance of selecting an optimal γ value to balance the trade-off between precision and recall while maintaining the overall accuracy. The stability of the F1 score across all values suggests that the model maintains a consistent balance between precision and recall, despite variations in γ.[45] These results demonstrate the robustness and adaptability of the proposed model, ensuring reliable performance across a range of parameter settings.

Table 3: Performance metrics at different gamma (γ) v at Episode 150.

γ	Precision (%)	Recall (%)	F1 score (%)	Accuracy (%)
0.001	93.77	93.56	92.36	92.04
0.1	92.56	92.36	92.04	91.62
0.99	92.04	92.04	92.04	91.62

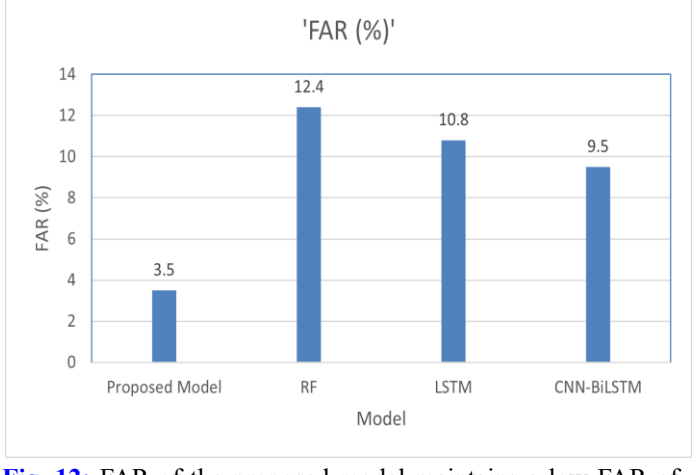

Fig. 12: FAR of the proposed model maintains a low FAR of 3.4%, significantly lower than RF (12.4%) and CNN-BiLSTM (9.5%).[43]

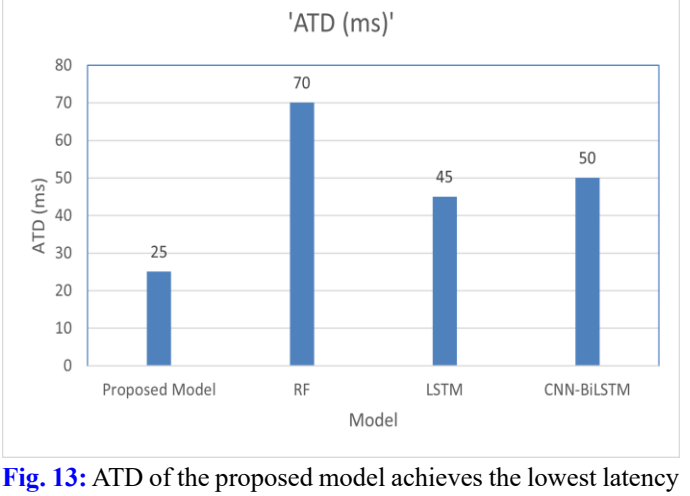

Fig. 13: ATD of the proposed model achieves the lowest latency (25 ms) compared to RF (70 ms) and LSTM (45 ms) and CNN-BiLSTM (50 ms).[43]

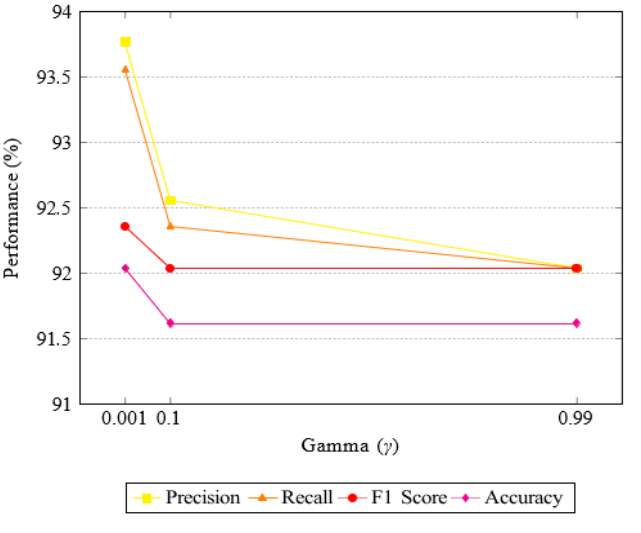

Fig. 14: Performance metrics vs Gamma (γ) at episode 150.

6. Conclusion

The sequence-to-sequence Seq2Seq Transformer based model that is developed in this work is decentralized and lightweight that helps mitigate the pressing problems of intrusion detection in vehicular networks. Thanks to the adoption of distributed architecture, the model allows the guarantee of scaling and resilience, and the architecture's lightness provides the possibility to operate it within the in-vehicle systems having small number of computational resources. Moreover, incorporating domain-specific features like time difference, message frequency, and payload entropy enables advanced detection of sophisticated cyber threats such as DoS, fuzzy and spoofing attack. Experimental results show that the model has high precision, recall, and ADR while maintaining low FAR, which suggest that the model is effective and reliable.

We follow the approach of applying a decentralized preprocessing pipeline for each of the vehicle nodes, where vehicle nodes process local data locally, and a Seq2Seq Transformer model is trained and evaluated. The advanced attention mechanisms and positional encodings are leveraged to learn temporal dependency and contextual information on the CAN bus data. This strategy provides real-time detection with negligible computational cost as well as interpretability via attention maps, which helps cybersecurity professionals understand the detection mechanism. Despite successful results, this work leaves several potential as future directions for future work. One straight-forward generalization of the approach is its real-time adaptation for a variety of vehicular environments. Second, it is possible to tune the model for other vehicular communication protocols different from the CAN bus and to support detecting evolving attack vectors. We will investigate enhancing the generalization capability among different vehicle types as the task of object detection and further study the federated learning methodologies to optimize the decentralized training pipeline. Through solving these challenges, the framework can be a reference proposal for future secure and intelligent vehicular communication systems in the age of connected mobility.

Acknowledgments

The authors acknowledge the support of Manipal University Jaipur for providing the resources necessary for this work.

Conflict of Interest

There is no conflict of interest.

Supporting Information

Not applicable.

References

[1] A. Patcha, J. M. Park, An overview of anomaly detection techniques: Existing solutions and latest technological trends, *Computer Networks*, 2007, **51**, 3448-3470, doi: 10.1016/j.comnet.2007.02.001.

[2] H. Sun, M. Chen, J. Weng, Z. Liu, G. Geng, Anomaly detection for in-vehicle network using CNN-LSTM with attention mechanism, *IEEE Transactions on Vehicular Technology*, 2021, **70**, 10880-10893, doi: 10.1109/tvt.2021.3106940.

[3] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, Y. Kadobayashi, LSTM-based intrusion detection system for in-vehicle can bus communications, *IEEE Access*, 2020, **8**, 185489-185502, doi: 10.1109/ACCESS.2020.3029307.

[4] K. Agrawal, T. Alladi, A. Agrawal, V. Chamola, A. Benslimane, NovelADS: A novel anomaly detection system for intra-vehicular networks, *IEEE Transactions on Intelligent Transportation Systems*, 2022, **23**, 22596-22606, doi: 10.1109/TITS.2022.3146024.

[5] S. F. Lokman, A. T. Othman, M. H. Abu-Bakar, Intrusion detection system for automotive controller area network (CAN) bus system: a review, *EURASIP Journal on Wireless Communications and Networking*, 2019, **2019**, 184, doi: 10.1186/s13638-019-1484-3.

[6] F. Fakhfakh, M. Tounsi, M. Mosbah, Cybersecurity attacks on CAN bus-based vehicles: a review and open challenges, *Library Hi Tech*, 2022, **40**, 1179-1203, doi: 10.1108/lht-01-2021-0013.

[7] D. Oladimeji, A. Rasheed, C. Varol, M. Baza, H. Alshahrani, A. Baz, CANAttack: assessing vulnerabilities within controller area network, *Sensors*, 2023, **23**, 8223, doi: 10.3390/s23198223.

[8] S. Woo, H. J. Jo, D.H. Lee, A practical wireless attack on the connected car and security protocol for in-vehicle CAN, *IEEE Transactions on intelligent transportation systems*, 2014, **16**, 993-1006, doi: 10.1109/TITS.2014.2351612.

[9] J. Petit, S. E. Shladover, Potential cyberattacks on automated vehicles, *IEEE Transactions on Intelligent Transportation Systems*, 2014, **16**, 546-556, doi: 10.1109/tits.2014.2342271.

[10] E. Aliwa, O. Rana, C. Perera, P. Burnap, Cyberattacks and countermeasures for in-vehicle networks, *ACM Computing Surveys*, 2022, **54**, 1-37, doi: 10.1145/3431233.

[11] A. Greenberg, Hackers remotely kill a Jeep on the highway, *Wired*, 2015, **7**, 21-22.

[12] C. Pradeep, J. P. M. Dhas, D. P. Isravel, Anomaly detection in IoV can bus traffic using variational autoencoder-LSTM with attention mechanism, 2024 International Conference on IoT Based Control Networks and Intelligent Systems, December 17-18, Bengaluru, India, IEEE, 2024, 368-373, doi: 10.1109/ICICNIS64247.2024.10823311.

[13] E. A. Shams, A. Rizaner, A. H. Ulusoy, Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks, *Computers & Security*, 2018, **78**, 245-254, doi: 10.1016/j.cose.2018.06.008.

[14] A. Zhou, Z. Li, Y. Shen, Anomaly detection of CAN bus messages using a deep neural network for autonomous vehicles, *Applied Sciences*, 2019, **9**, 3174, doi: 10.3390/app9153174.

[15] J. Ashraf, A. D. Bakhshi, N. Moustafa, H. Khurshid, A. Javed, A. Beheshti, Novel deep learning-enabled LSTM autoencoder architecture for discovering anomalous events from intelligent transportation systems, *IEEE Transactions on Intelligent Transportation Systems*, 2021, **22**, 4507-4518, doi: 10.1109/TITS.2020.3017882.

[16] N. Al-Aql, Hybrid RNN-LSTM networks for enhanced intrusion detection in vehicle CAN systems, *Journal of Electrical Systems*, 2024, **20**, 3019-3031, doi: 10.52783/jes.3318.

[17] T. P. Nguyen, H. Nam, D. Kim, Transformer-based attention network for in-vehicle intrusion detection, *IEEE Access*, 2023, **11**, 55389-55403, doi: 10.1109/ACCESS.2023.3282110.

[18] N. Khan, M. I. Mohmand, S. U. Rehman, Z. Ullah, Z. Khan, W. Boulila, Advancements in intrusion detection: A lightweight hybrid RNN-RF model, *PLoS One*, 2024, **19**, e0299666, doi: 10.1371/journal.pone.0299666.

[19] M. Almehdhar, A. Albaseer, M. A. Khan, M. Abdallah, H. Menouar, S. Al-Kuwari, A. Al-Fuqaha, Deep learning in the fast lane: a survey on advanced intrusion detection systems for intelligent vehicle networks, *IEEE Open Journal of Vehicular Technology*, 2024, **5**, 869-906, doi: 10.1109/OJVT.2024.3422253.

[20] A. Kim, M. Park, D. H. Lee, AI-IDS: Application of deep learning to real-time web intrusion detection, *IEEE Access*, 2020, **8**, 70245-70261, doi: 10.1109/ACCESS.2020.2986882.

[21] H. M. Song, J. Woo, H. K. Kim, In-vehicle network intrusion detection using deep convolutional neural network, *Vehicular Communications*, 2020, **21**, 100198, doi: 10.1016/j.vehcom.2019.100198.

[22] X. Zhao, W. Miao, G. Yuan, Y. Jiang, S. Zhang, Q. Li, Abnormal traffic detection system based on feature fusion and sparse transformer, *Mathematics*, 2024, **12**, 1643, doi: 10.3390/math12111643.

[23] O. Avatefipour, A. S. Al-Sumaiti, A. M. El-Sherbeeny, E. M. Awwad, M. A. Elmeligy, M. A. Mohamed, H. Malik, An intelligent secured framework for cyberattack detection in electric vehicles' CAN bus using machine learning, *IEEE Access*, 2019, **7**, 127580-127592, doi: 10.1109/ACCESS.2019.2937576.

[24] M. Delwar Hossain, H. Inoue, H. Ochiai, D. Fall, Y. Kadobayashi, An effective in-vehicle CAN bus intrusion detection system using CNN deep learning approach, 2020 IEEE Global Communications Conference, December 7-11, Taipei, China, IEEE, 2020, doi: 10.1109/globecom42002.2020.9322395.

[25] S. Agrawal, S. Sarkar, O. Aouedi, G. Yenduri, K. Piamrat, M. Alazab, S. Bhattacharya, P. K. R. Maddikunta, T. R. Gadekallu, Federated Learning for intrusion detection system: Concepts, challenges and future directions, *Computer Communications*, 2022, **195**, 346-361, doi: 10.1016/j.comcom.2022.09.012.

[26] Z. Yu, Y. Liu, G. Xie, R. Li, S. Liu, L. T. Yang, TCE-IDS: time interval conditional entropy- based intrusion detection system for automotive controller area networks, *IEEE Transactions on Industrial Informatics*, 2023, **19**, 1185-1195, doi: 10.1109/TII.2022.3202539.

[27] P. Dini, S. Saponara, Design and experimental assessment of real-time anomaly detection techniques for automotive cybersecurity, *Sensors*, 2023, **23**, 9231, doi: 10.3390/s23229231.

[28] N. Goswami, S. Raj, D. Thakral, J. Luis Arias-Gonzáles, J. Flores-Albornoz, E. Asnate-Salazar, D. Kapila, S. Yadav, S. Kumar, Preserving security in internet-of-things healthcare system with metaheuristic-driven intrusion detection, *Engineered Sciences*, 2023, **25**, 933, doi: 10.30919/es933.

[29] F. Le, M. Srivatsa, R. Ganti, V. Sekar, Rethinking data-driven networking with foundation models: Challenges and opportunities, Proceedings of the 21st ACM Workshop on Hot Topics in Networks, Austin Texas, 2022, 188-197, doi: 10.1145/3563766.3564109.

[30] Y. Liu, L. Wu, Intrusion detection model based on improved transformer, *Applied Sciences*, 2023, **13**, 6251, doi: 10.3390/app13106251.

[31], C. H. Nemade, U. Pujeri, ECFL-IoVT: emergency communications using fuzzy logic for Internet of vehicle things, *Engineered Science*, 2023, **28**, 1056, doi: 10.30919/es1056

[32] S. Ullah, D. H. Kim, Lightweight driver behavior identification model with sparse learning on in-vehicle CAN-BUS sensor data, *Sensors*, 2020, **20**, 5030, doi: 10.3390/s20185030.

[33] O. El Melhaoui, B. Soukaina, S. Said, S. Elouaham, Optimized framework for signature recognition using genetic algorithm, loci method, and fuzzy classifier, *Engineered Science*, 2023, **27**, 1026, doi: 10.30919/es1026.

[34] H. Kang, T. Vo, H. K. Kim, J. B. Hong, CANival: A multimodal approach to intrusion detection on the vehicle CAN bus, *Vehicular Communications*, 2024, **50**, 100845, doi: 10.1016/j.vehcom.2024.100845.

[35] K. Yun, H. Yun, S. Lee, J. Oh, M. Kim, M. Lim, J. Lee, C. Kim, J. Seo, J. Choi, A study on machine learning-enhanced roadside unit-based detection of abnormal driving in autonomous vehicles, *Electronics*, 2024, **13**, 288, doi: 10.3390/electronics13020288.

[36] S. Lu, R. Lysecky, Data-driven anomaly detection with timing features for embedded systems, *ACM Transactions on Design Automation of Electronic Systems*, 2019, **24**, 1-27, doi: 10.1145/3279949.

[37] W. Wu, Y. Huang, R. Kurachi, G. Zeng, G. Xie, R. Li, K. Li, Sliding window optimized information entropy analysis method for intrusion detection on in-vehicle networks, *IEEE Access*, 2018, **6**, 45233-45245, doi: 10.1109/access.2018.2865169.

[38] D. B. Attluri, S. Prabhakara, Conflict-driven learning scheme for multi-agent based intrusion detection in Internet of Things, *International Journal of Electrical and Computer Engineering*, 2024, **14**, 5543, doi: 10.11591/ijece.v14i5.pp5543-5553.

[39] T. Moulahi, S. Zidi, A. Alabdulatif, M. Atiquzzaman, Comparative performance evaluation of intrusion detection based on machine learning in in-vehicle controller area network bus, *IEEE Access*, 2021, **9**, 99595-99605, doi: 10.1109/access.2021.3095962.

[40] S. Syed Sabir Mohamed, S. Gunasekaran, R. Chinnamuthu, G. Singh, Dynamic hierarchical intrusion detection system for Internet of vehicle on edge computing platform, *IET Communications*, 2024, **18**, 1778-1794, doi: 10.1049/cmu2.12865.

[41] Y. Yuan, C. Shao, Z. Cao, Z. He, C. Zhu, Y. Wang, V. Jang, Bus dynamic travel time prediction: using a deep feature extraction framework based on RNN and DNN, *Electronics*, 2020, **9**, 1876, doi: 10.3390/electronics9111876.
[42] K. Yang, J. Liu, C. Zhang, Y. Fang, Adversarial examples against the deep learning based network intrusion detection systems, 2018 IEEE Military Communications Conference, October 29-31, Los Angeles, CA, IEEE, 2018, 559-564, doi: 10.1109/milcom.2018.8599759.
[43] W. Lo, H. Alqahtani, K. Thakur, A. Almadhor, S. Chander, G. Kumar, A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic, *Vehicular Communications*, 2022, **35**, 100471, doi: 10.1016/j.vehcom.2022.100471.
[44] P. Wei, B. Wang, X. Dai, L. Li, F. He, A novel intrusion detection model for the CAN bus packet of in-vehicle network based on attention mechanism and autoencoder, *Digital Communications and Networks*, 2023, **9**, 14-21, doi: 10.1016/j.dcan.2022.04.021.
[45] Z. Qin W. Sun H. Deng D. Li Y. Wei B. Lv J. Yan L. Kong Y. Zhong, cosFormer: Rethinking softmax in attention, arxiv preprint arxiv: 2202.08791, 2022, doi: 10.48550/arXiv.2202.08791.