Vol. 06, No. 1 (2024) 221-230, doi: 10.24874/PES.SI.24.02.005

Proceedings on Engineering Sciences

www.pesjournal.net

AN AI-POWERED SECURITY SYSTEM FOR CAN BUS ATTACKS IDENTIFICATION IN ELECTRIC AUTOMOBILES

S. B. Vinay Kumar[1]
B. P. Singh
Raman Batra
Akash Kumar Bhagat

Received 10.11.2023.
Received in revised form 17.01.2024.
Accepted 30.01.2024.
UDC – 004.056.5

Keywords:

Anomaly detection, CAN bus security, Attacks identification, AI-powered, Electric automobiles, Autonomous vehicles.

A B S T R A C T

The network connection within the car, the "Controller Area Network" (CAN) bus serves as an alternative protocol for electric automobiles. Tragically, the lack of a data authentication technique in the CAN bus protocol makes it susceptible to several types of assaults, making it easier for attackers to infiltrate the network. The CAN dataset is collected and the collected datasets attains for preprocessing stage using z-score normalization. For feature extraction, a restricted boltzmann machine (RBM) is used to extract the data. Next, our proposed method (MCFO-DANN) is used to identify and mitigate CAN Bus attacks in electric vehicles. Evaluation against other CAN bus anomaly detection methods demonstrates the superiority of MCFO-DANN, exhibiting higher accuracy. This proactive security solution fortifies electric vehicles against cyber-threats, ensuring real-time monitoring and response, thereby preserving the integrity and safety of the CAN Bus network in electric automobiles.

1. INTRODUCTION

Electric cars increasingly depend on interconnected electronic parts, therefore protecting Controller Area Network (CAN) buses is essential (Lee et al.,(2020)). Cyber-threats such as replay, injection, and spoofing attacks can affect the CAN bus, which connects electronic control units (ECUs). The automotive sector is depending on complex ECUs connected through the CAN bus protocol; therefore, it is critical to develop a security solution to detect CAN bus assaults in electric vehicles (Amiriet al.,(2023)). The system uses machine learning techniques to identify aberrant patterns in the CAN bus data, strengthening the security posture of electric vehicles and facilitating the early detection of potential attacks (Inyang et al.,(2023)). Real-time monitoring, quick threat detection, and prompt risk-reduction are made possible by the system's integration with the car's security architecture (Fan et al.,(2023)). This proactive strategy protects the CAN bus integrity, guaranteeing the dependability and safety of electric cars in a time when the fusion of automotive system. Because they are linked to the outside world, modern automobiles are a component of the Internet of Things (IoT) (Tange et al.,(2020)). Modern car has many sensors, actuators, and communication devices in addition to a high number of ECUs. By collecting and analyzing various types of data, these systems aim to

[1] Corresponding author: S. B. Vinay Kumar
Email: sb.vinaykumar@jainuniversity.ac.in

enhance automotive users' efficiency, speed and safety (Sulaiman et al.,(2023)).

Robust cyber-security measures, such as AI-powered systems for CAN bus attack verification, are essential to guarantee the resilience of electric vehicles against evolving cyber-attacks as the automotive industry keeps embracing connectivity and automation (Bathla et al.,(2023)). Malicious data modification on the CAN bus or attempts at unauthorized access can be detected using anomaly-based detection. Implementing secure authentication mechanisms and encryption techniques to protect communication channels are examples of intrusion prevention and strategies (Nagatyet al.,(2023)). Potential attacks to be avoided by limiting unwanted access to the CAN bus by the deployment of firewalls and access control systems. Patching and software updates on a regular basis are necessary to fix vulnerabilities and improve system resilience as a whole (Amato et al.,(2021)). Due to the absence of security mechanisms such as user authentication and message encryption, ECUs that are part of the CAN bus are susceptible to cyber-attacks. The gearbox, engine, speed, airbags, power train, and a great number of other subsystems of a vehicle can be controlled by ECUs (Kalutarageet al.,(2019)).

CAN Bus Security: It's a Significance in Electric Vehicles (EVs) that communicates between crucial components, including the power train control module, battery management system, and other ECUs, which is a primarily facilitated using the CAN bus in EVs (Ning et al.,(2019)). Attacks against electric cars CAN bus can have serious repercussions, including as illegal access, alteration of vital settings, and even the possibility of the vehicle being controlled remotely (Islam and Refat (2020)). If one is trying to figure out how long CAN bus frames take between packets or figure out specific time sequences, for abnormality identification, frequency-based intrusion detection systems have serious limitations (Bi et al.,(2022)). For instance, by progressively altering the periodicity or content of the data frames, certain complex attacks may render this ID invalid. (Duanet al., (2021)). To detect intrusions in the CAN bus transport, windows and doors are used and the intricacies of CAN bus attacks are potential ramifications for electric automobile (Qin et al.,(2021)). A typical CAN bus attack approach is depicted in Figure 1. The process has three stages: investigation, preparation, and attack stages. Attackers must identify a Forex interface at the intelligence stage in order to gain the access to the target vehicle network. CAN bus attack and On-Board Diagnostics II (OBD-II) port are two examples of these interfaces. Telematics systems also contain them. The selected interface can be used by attackers to create a malicious node. The malevolent entity may manifest as either an exterior device, such a laptop, or an external engine, or it may be an inside engine, including a hacked engine and malware-infected telemetry system(Hossainet al.,(2020)). Attackers use the rogue node to intercept and examine CAN communications sent across the bus during the preparation phase (Zhou et al.,(2019)). CAN is broadcast in nature, any transmission of CAN communications might be intercepted and recorded (ben Othmane et al.,(2020)). Attackers can generate harmful messages with specific goals by further analyzing historical CAN messages (Hou et al.,(2022)). Depending on how they are designed, enemies can perform various attacks during the attack phase, such as inserting malicious messages (D'Angelo et al.,(2020)). Based on their architecture, adversaries to carry out a variety of attacks during the attack phase, such as insertion malicious messages (Boumizaand Braham (2019)). Encrypt the data provided over the CAN bus to prevent unauthorized access to vital information and eavesdropping Establish a baseline of typical CAN bus performance in electric cars. Maintaining the security and dependability of electric vehicles requires CAN bus attack (Angeloet al.,(2020)).

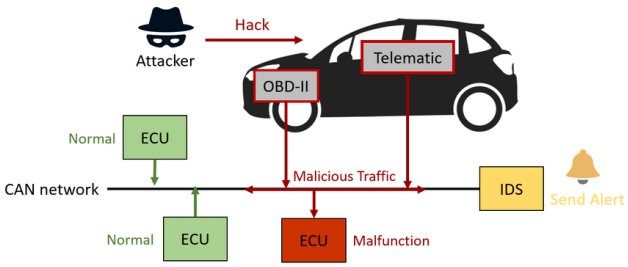

Figure 1. CAN bus-attack of automotive modules (https://www.researchgate.net/figure/Typical-CAN-bus-attack-scenario_fig2_363703690)

The aim of this research is to detect the CAN bus attack in electric vehicle technology and improve cyber-security utilizing the identification and mitigation of any threats to the CAN communication system, hence protecting the integrity and safety of vehicle operations.

Key contribution

- The key contribution of this research is the development of an AI-Powered Security System for CAN Bus Attacks Identification in Electric Automobiles.
- We gather the CAN dataset, and data preprocessing using Z-score normalization.
- We extract important features from preprocessed data using RBM. The EFNSO-DANN methodology provides techniques for real-time detection and response to any attacks on the CAN bus network, with the objective of enhancing the cyber-security of electric vehicles.
- To improve the security using hybrid EFNSO-DANN.

2. RELATED WORKS

Shi et al., (2022) proposed a Framework for the automobile CPS's CAN bus security testbed with the goal of improving researcher safety and CAN bus operating data enrichment. Additionally, a theoretical investigation focused on the testbed's latency in transmitting and getting periodic and aperiodic CAN signals. The results indicate that Algorithms 1 and 2 conduct the communication and gathering of time series data, and that there is a strong correlation between the generated timestamp in the database and the actual vehicle data timestamp. The stability of the security testbed was examined in the assessment process utilizing the two indicators of packet loss rate and latency. Kim et al., (2022) described a Vehicle E/E systems are controlled by ECUs.

For effective ECU communication, most automobile manufacturers employ the CAN protocol. Developing a system to avoid in-vehicle network assaults was crucial to driver safety. One of the greatest network security tools is the IDS. Dissimilar typical IDS for network security, in-vehicle IDS need a lightweight algorithm due to ECU processing power limitations. The purpose of this work is to offer a lightweight IDS method based on information frame modification for in-vehicle CAN. The proposed method uses the CAN data frame to compute the degree of change compressing technique that uses exclusive-OR procedures to lower ECU load. Ma et al., (2022) introduced a fast-deployable detection system for intrusions inside the car. In order to accomplish real time detection, a low complexity feature algorithm and fully utilized its benefits using a lightweight neural network based on GRU was employed. Using accessible datasets, the experiment was carried out in car embedded devices. The experiment's results revealed how rapidly, with high classification accuracy, and with immediate effectiveness, the ids might be set into effect. Furthermore, to talk about how IDS could by working with OTA services, you can strengthen the intelligence of vehicle operating systems and prevent potential assaults.

Huang et al., (2023) explained the reinforcement learning technique, was able to handle an inadvertent lateral assault and maintain the vehicle's position in the ego lane. The nation's highway development standard was used as a basis for selecting the discrete speed variations of 125 km/h, one hundred kilometers per hour, and eighty kilometers per hour as combinations of speed-curvature tests. Different curvatures every 50 meters, from 126 to 1200 meters, were also chosen. The tests were done in the Open.ai environment using an external racing wheel that was installed to mimic the inadvertent lateral attack. Empirical findings from the simulation indicate that the PPO was capable of managing an inadvertent lateral assault on a Chinese standard-designed roadway. Houet al., (2022) presented a dynamic attack graph generation mechanism for the IoV to discover and visualize security concerns from IoV system flaws. This study first models the IoV system's security aspects and interactions using its architecture and provides a network security ontology model. Second, they explained how to use Semantic Web Rule Language to build a causal reasoning rule basis for vulnerabilities. Finally, due to the frequent change in IoV network architecture, an ontology reasoning engine-based dynamic attack graph creation approach was developed to decrease attack graph overhead. Experimental findings demonstrate that the technique dynamically and correctly displays the IoV network attack graph.

3. METHODOLOGY

The purpose of EFNSO-DANN technique is used to improve the cyber-security of electric cars by offering methods for real-time detection and response to CAN bus network assaults. Here; first we have collected the dataset and then data pre-processing using z-score normalization is executed. The RBM method is employed to extract features from the pre-processed data. Features are taken out of the pre-processed data using the RBM technique.Our proposed method MCFO-DANN was executed. The proposed method's flow is depicted in Figure 2.

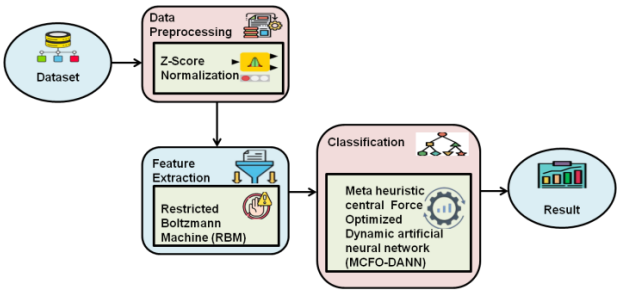

Figure 2. Flow graph

3.1 Dataset

The original dataset is utilized to evaluate the system was made available by (Javed et al., 2021). Attacks-free states, DoS attacks, impersonation attacks, and fuzzy assaults are featured in this dataset. The CAN traffic was classified using the datasets genuine vehicle's OBD-II port while message attacks were included. Assaults are among the kind of items listed below: DOS attack (a) and fuzzy attack (b)(c) A deceptive attack. The features of the CAN dataset for IDS are shown in Table 1. The timestamp charts display the data entry in a CAN graphically represented bus on a certain occasion.

Table 1. The CAN dataset elements for IDS (Javed et al., 2021).

Characteristic	Values
DLC	Number of data bytes, (from 0 to 8)
CAN IDS	Find CAN data in HEX (e.g., 043f)
Timestamp	Records time (s)
DLC	Range of data bytes is 0 to 8.

3.2 Data pre-processing using z- score normalization

In the context of CAN bus attacks, Z-score normalization is a statistical approach used to normalize data and find abnormalities. Z-score normalization known as statistical standardization is an analytical approach that is used to resolve Z-score abnormalities by dividing by the standard deviation and eliminating the mean from the result. The result sets the variables in CAN bus attacks on a same scale. By ensuring that data points have Z-score normalization to indicate 0, a standard deviation of 1, and the ability to facilitate the initial finding of anomalies and outliers. This approach improves the efficiency of potential security risk detection and facilitates data comparison and evaluation across multiple dimensions. Z-score normalization assists in enhancing data consistency and facilitates more efficient data analysis. To identify anomalous patterns in CAN bus data that signs of possible attacks or abnormalities. By using this normalization approach, IDS become more effective and the security of the CAN bus communication network is improved.

$$(Z - score)_T = \frac{(V_{th} - \mu)}{\sigma} \quad (1)$$

This formula shows that the discrepancy between the trait standard deviation and mean is used to get the greatest possible Z-score.

3.3 Feature extraction using Restricted Boltzmann machine (RBM)

The process of identifying patterns in network traffic, RBM in a bus attack discovers vulnerabilities. The RBM is a kind of neural network that helps with intrusion detection by identifying anomalies or malicious activities. To improve security and assist avoid or lessen cyber-risks in automotive systems is to detect deviations from the standard CAN bus behavior. The weighted vector W in equation seems to be used for the parameterization of the power spectral density E in RBM, with variables v and h denotes two transparent and hidden variables, respectively.

$$F(u, g) = -b^S u - a^S g - u^S Xg \quad (2)$$

The visible and hidden units' biased factors are denoted by u and g, respectively. Eq. (3), using v and h as the variables in E, is used to derive the density of probability P.

$$F(u, g) = \frac{1}{Y} f^{-F(u,g)} \quad (3)$$

Eq. (4) gives to normalize capricious y:

$$Y = \sum_{u',g'} f^{-F(u',g')} \quad (4)$$

Moreover, Eq. (5), which combines the aforementioned formulas, provides the probability of $v$across hidden neurons:

$$O(u) = \frac{1}{Y} \sum_g f^{-F(u,g)} \quad (5)$$

The variability in training data is evaluated using the log-similarity eq. (6) based on$m$:

$$\sum_{m=M}^{m=1} \frac{\partial log O\,(u^m)}{\partial X_{ji}} = \langle u_j g_i \rangle_{data} - \langle u_j g_i \rangle_{model} \quad (6)$$

$$\Delta X_{ji} = \varepsilon\,(\langle u_j g_i \rangle_{data} - \langle u_j g_i \rangle_{model} \quad (7)$$

Moreover, there is no association between the activation of hidden or transparent units for given g and j. Eq.(8) provides the conditional characteristic for a given u.

$$O(g|u) = \prod_i O(g_i|u) \quad (8)$$

Where $g_i \in \{0,1\}$ and the prospect of$X_{ji} = 1$ is given in Eq. (9):

$$O(g_i = 1\ |u) = \sigma\,(a_i + \sum_j u_j X_{ji}) \quad (9)$$

In this case, Eq. (10) specifies the logistic function σ as follows:

$$\sigma(w) = (1 + f^{-w})^{-1} \quad (10)$$

$$O\big(g_j = 1\ \big|u\big) = \sigma\,(a_j + \sum_i X_{ji}\, g_i) \quad (11)$$

In actuality, impartial evaluation by O challenging, but it may be used to replicate the first assessment of v from h. Gibbs sampling is used to change each part of the opaque and hidden layers simultaneously. Finally, the appropriate choice is computed using > by summing the expected and adjusted values of h and v. RBM parameters may be used to initiate recurrent neural networks.

3.4 Metaheuristic central Force-Optimized Dynamic artificial neural network (MCFO-DANN)

3.4.1 Metaheuristic central Force-Optimized (MCFO)

A naturalistic technique for solving optimization issues is called MCFO. It used to initiate assaults inside the framework of a CAN bus. An attacker could compromise security by interfering with the CAN bus's communication channels via manipulation of the optimization process. This highlights the need of strong security measures in place to protect CAN bus networks from possible dangers and illegal access. MCFO resolves issue (1) based on the probes' passage across the decision space (DS) following computed paths the DS defined by $\partial = y_1, y_2, \ldots . y_n$ a collection of probes are shown in MCFO as possible fixes, A variable initial probe distribution created by deploying sensors set the beginning location of each sensor$Nj$the total number of first probes, where is the starting vectors of acceleration are zero. Iterations must reach their acceptable maximum in order to finish, therefore during the inspection process; the probe location and acceleration are adjusted. If the contemporary best fitness is less than the differential between the average best performance over steps (including the present step) and the CFO process is terminated premature. The CFO technique is following eq. (12),

$$B_j^o(s) = H\sum_{\substack{l=1 \\ l\neq o}}^{M_o} v\,(N^l(s) - N^o(s))\,(N^l(l) - N^o(s))^{\propto} \quad (12)$$

$$Q_j^o(s+1) = Q_j^o(s) + \frac{1}{2}B_j^o(s)\Delta s^2 \quad (13)$$

$$V(y) = \begin{cases} 1\ y \geq 0 \\ 0\ else; \end{cases} \quad (14)$$

The eq. (16) to calculate accelerated;

$$Q_j^o(s+1) = Q_j^{min} + E_{rep}\,[Q_j^o(s-1) - Q_j^{min} \quad (15)$$

Time-stamped, impenetrable validated and real-time metrics are obtained by the CFO.

$$Q_j^o(s+1) = Q_j^{max} + E_{rep}\,[Q_j^{min} - Q_j^o(s-1)] \quad (16)$$

$$\bar{Q}_j^{min} = Q_j^{min} + \frac{1}{2}\,[Q_{best} - Q_j^{min}] \quad (17)$$

Eq. (19) determined the initial performance matrix and the optimal explore fitness;

$$\bar{Q}_j^{max} = Q_j^{max} - \frac{1}{2}\,[Q_j^{max} - Q_{best}] \quad (18)$$

Iterations must reach their maximum limit to terminate. CFO algorithm terminates early if a discrepancy between current best fitness and average best fitness throughout all steps, including immediate step.

3.4.2 Dynamic artificial neural network (DANN)

DANNs are statistical models that indicate an apparent dependence on an individual's cognitive ability. DANN is built in layers, with many neurons at each level. In order to predict the output vectors $[V]$, [D], and $[A]$ in this research, a number of experiments were conducted. Standardized mean square error (MSE) and linear correlation coefficient (R) are two of the most reliable metrics to assess a DANN's effectiveness.

$$\mathrm{MSE} = \frac{\mathrm{J}\times\mathrm{I}\times\mathrm{MS}}{\sum_{\mathrm{i}=1}^{\mathrm{I}}\frac{\mathrm{J}\sum_{\mathrm{j}=1}^{\mathrm{J}}\mathrm{t}_{\mathrm{ji}}^2 - \left(\sum_{\mathrm{j}=1}^{\mathrm{J}}\mathrm{t}_{\mathrm{ji}}\right)^2}{\mathrm{J}}} \quad (19)$$

$$\mathrm{MS} = \frac{1}{\mathrm{J}}\sum_{\mathrm{j}=1}^{\mathrm{J}}\sum_{\mathrm{i}=1}^{\mathrm{I}}\left(\mathrm{t}_{\mathrm{ji}} - \mathrm{x}_{\mathrm{ji}}\right)^2, \quad (20)$$

$$K = \frac{\frac{\sum_{j=1}^{J}(t_j - t)(x_j - \bar{x})}{J}}{\left(\sqrt{\frac{\sum_{j=1}^{J}(t_j - \bar{t})^2}{J}} \times \sqrt{\frac{\sum_{j=1}^{J}(x_j - \bar{x})^2}{J}}\right)} \quad (21)$$

The variables of J and I represent the total experimental data and the performance layer neurons, respectively. The expected and objective solutions for thet_j, sequence of data in thex_{ji} layer of the output neuron are $j$and$t_j - \bar{t}$ their instructions are y and$d$. The closer of K is 1 and 0. Visually appealing DANNs have quicker MSE approaches 0. Algorithm 1 shows that DANN. Another tool to show the variations between the target and expected value after training is error histogram (EH). Figure 3 shows that DANN process.

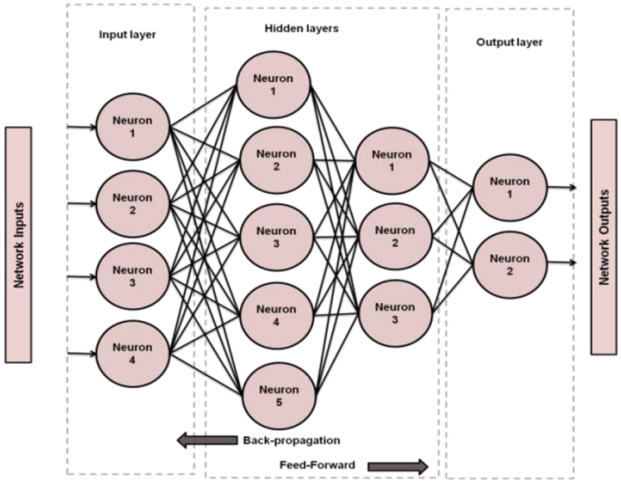

Figure 3. DANN process

3.4.3 Hybrid of MCFO-DANN

The MCFO-DANN hybrid uses centralized force-driven metaheuristic approaches to improve optimization and learning in dynamic contexts and provide efficient and adaptable performance. A complex hybrid model, the MCFO-DANN effectively combines DANN with metaheuristic optimization methods. Using the power of central force optimization a metaheuristic derived from celestial mechanics, this novel method improves the way of dynamic neural networks are trained. MCFO-DANN enhances model performance across different datasets and changing patterns by dynamically adjusting network parameters during training. By overcoming conventional optimization obstacles, this hybridization makes efficient convergence possible. Because MCFO and dynamic neural networks function well together, MCFO-DANN is a flexible and effective way to solve dynamic and challenging problems in Artificial intelligence (AI) and machine learning (ML), as demonstrated by Algorithm 1.

Algorithm 1: Dynamic artificial neural network

```
def __init__(self, input size, hidden layers, output size):
    # Initialize neural network architecture
self.input size = input size
self.hidden layers = hidden layers
self.output_size = output size
self. weights = initialize weights ()
def train(self, training data, labels):
    # Train the neural network using backpropagation
    # Update weights based on the training data and
labels

def predict(self, input_data):
    # Forward pass through the network to make
predictions
    # Adjust the network structure dynamically if
needed
return output
# Example Usage:
```

```
input_size = 5
hidden_layers = [10, 8]
output_size = 3
dynamic_nn = DynamicANN(input_size, hidden_layers, output_size)
# Train the network
training_data
dynamic_nn.train(training_data, labels)
# Make predictions
input_data = output_prediction = dynamic_nn.predict(input_data)
```

4. RESULT

To analyze the performance of the proposed method in terms of precision, accuracy, F1-score, recall and the existing methods such asGenerative Adversarial Nets based Intrusion Detection System(GIDS) (Gundu and Maleki (2022)), "Support Vector Machine" (SVM) ,(Anggoro and Kurnia(2020)), "k-nearest neighbors algorithm" (KNN),(Anggoro and Kurnia(2020)) and Wavelet-based Intrusion Detection System (WINDS)(Chen X et al.,(2021)), that is explained in detail. Authentication and authorization procedures are taken into consideration when the CAN bus evolved as a dependable, secure, and adaptable proprietary network.

Table 2 shows that 27% of these attacks included taking over the vehicle.

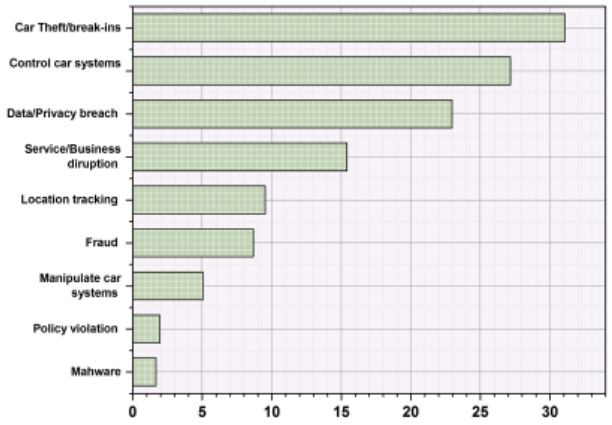

Figure 4. Impact of cyber-attacks (https://arxiv.org/pdf/2104.03763.pdf)

Table 2. Variables of cyber-attack (https://arxiv.org/pdf/2104.03763.pdf)

Malware	1.68
Policy violation	1.96
Manipulate car systems	5.04
Fraud	8.68
Location tracking	9.52
Service/Business disruption	15.41
Data/Privacy breach	22.97
Control car systems	27.17
Car Theft/break-ins	31.09

4.1 Accuracy

In order to identify CAN bus attacks in electric vehicles, network traffic must be observed for illegal messages or strange data rates. Accurate execution of such attacks can compromise vehicle functionality, safety, and security. Staying informed of new cyber-risks in the automobile sector requires continuous research and upgrades.

Figure 5 displays a comparison of accuracy between the suggested and current methods, and Table 3 shows the accuracy's numerical results. The suggested approach accomplishes 98%, whereas current approaches such as GIDS (82%), WINDS (89%) KNN (85%), SVM (87%). It demonstrates that our suggested solution is more effective than the existing method.

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \quad (22)$$

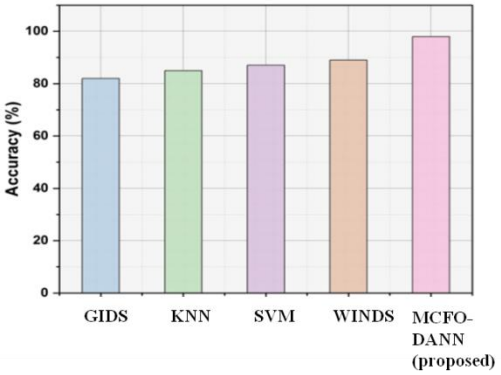

Figure 5. Comparison of accuracy

Table 3. Numerical outcomes of accuracy

Methods	Accuracy (%)
GIDS (Gunduand Maleki(2022))	82
KNN (Anggoro and Kurnia (2020))	85
SVM (Anggoro and Kurnia (2020))	87
WINDS (Chen et al., (2021))	89
MCFO - DANN (Proposed)	98

4.2 Precision

Advanced IDS are necessary to identify CAN bus attacks in electric cars. Network traffic anomaly analysis, abnormal message rates, and unexpected data patterns might be used to identify potential threats. Precision algorithm used to improve intrusion detection of accuracy and guarantees quick reaction to any cyber-security threats in electric vehicle technologies.

The comparative analysis of the precision with proposed and existing method is shown in Figure 6 and Table 4 Numerical outcomes of precision. When compared with other existing methods, the proposed method achieves 95 % and existing methods such as GIDS attains 80.1%, WINDS achieves 90.2%, KNN achieves 84.7%, SVM achieves 87.3%. It demonstrates that our suggested solution is more effective than the existing method.

$$\text{precision} = \frac{\text{TP}}{\text{TP+FP}} \quad (23)$$

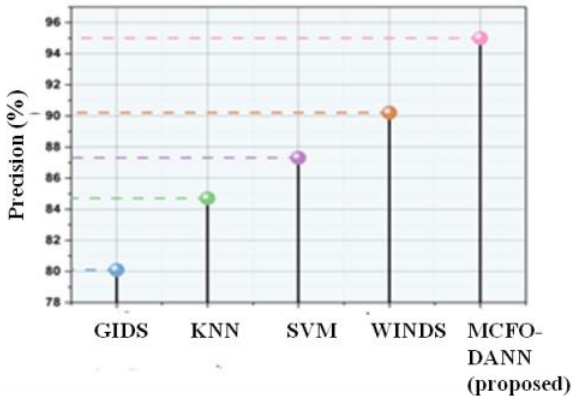

Figure 6. Comparison of precision

Table 4. Numerical outcome of precision

Methods	Precision (%)
GIDS (Gundu and Maleki(2022))	80.1
KNN (Anggoro and Kurnia (2020))	84.7
SVM (Anggoro and Kurnia (2020))	87.3
WINDS (Chen et al., (2021))	90.2
MCFO - DANN (Proposed)	95

4.3 Recall

In order to identify CAN bus attacks in electric cars, network traffic must be observed for abnormalities. An attack may be indicated by anomalous patterns, unexpected messages, or abrupt changes in the data. The identification and mitigation of possible risks need the use of IDS and regular software updates for vehicles. Recalls for impacted automobiles may be issued by manufacturers. Figure 7 compares the recall using the proposed and current methods, while Table 5 shows the recall's numerical results.When compared the proposed method achieves 93 % and existing methods such as GIDS (78%), WINDS (88%) KNN (82%), SVM (84%). It demonstrates that our suggested solution is more effective than the existing method.

$$\text{Recall} = \frac{\text{FN}}{\text{FN+TP}} \quad (24)$$

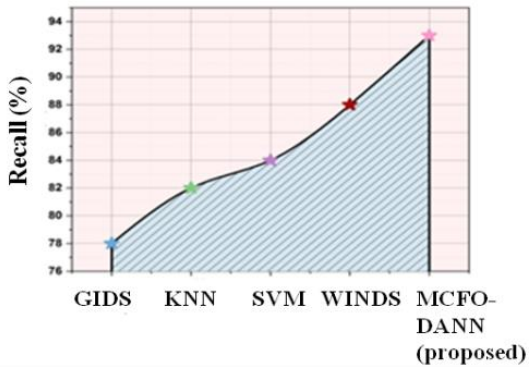

Figure 7. Comparison of recall

Table 5. Numerical outcome of recall

Methods	Recall (%)
GIDS (Gundu and Maleki (2022))	78
KNN (Anggoro and Kurnia (2020))	82
SVM (Anggoroand Kurnia(2020))	84
WINDS (Chen et al., (2021))	88
MCFO - DANN (Proposed)	93

4.4 F1-score

Cybersecurity requires the ability to recognize CAN bus threats in electric vehicle technology. The accuracy of detection is improved by using anomaly detection techniques, such as machine learning algorithms. In order to provide an appropriate assessment of detection system effectiveness in minimizing possible threats to the vehicle's CAN bus network, evaluation measures such as the F1-score that offer a balanced measure of accuracy and recall. Figure 8 compares the F1 score using the suggested and current methods, while Table 6 shows the F1-score's numerical results. When compared with other existing methods, our proposed method achieves 96% and existing methods such as GIDS (84%), WINDS (91%) KNN (86%), SVM (88%). It demonstrates that our suggested solution is more effective than the existing method.

$$\text{F1} - \text{score} = \frac{(\text{precision}) \times (\text{recall}) \times 2}{\text{precision+recall}} \quad (25)$$

Search mode, the definition of probability is as follows:

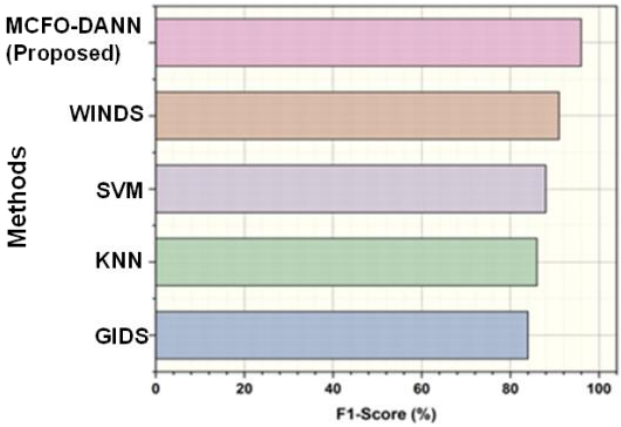

Figure 8. Comparison of F1-score

Table 6. Numerical outcome of F1-score.

Methods	F1-Score (%)
GIDS (Gundu and Maleki (2022))	84
KNN (Anggoro and Kurnia (2020))	86
SVM (Anggoroand Kurnia (2020))	88
WINDS (Chen et al., (2021))	91
MCFO - DANN (Proposed)	96

5. DISCUSSION

IDS based on GANs include drawbacks such as susceptible to adversarial assaults, in which attackers influence the GANs to produce fake samples, resulting in false negatives. Further, GANs might have trouble identifying intricate and dynamic infiltration patterns, which would reduce their usefulness in dynamic cyber security scenarios (GunduandMaleki (2022)). The KNN technique includes its high processing cost during prediction, particularly for big datasets. Furthermore, class distributions are not uniform, KNN's inability to handle unbalanced datasets might negatively affect classification accuracy (Anggoro and Kurnia(2020)) (SVM) is sensitive to the selection of the kernel and hyper parameters, which is a drawback. Inappropriate kernel selection or incorrect parameter configuration might result in less than ideal performance. Considerable datasets may be problematic for SVMs because of the considerable increase in training time. Furthermore, SVM model interpretation might be difficult in high-dimensional domains (Anggoro and Kurnia (2020)). The sensitivity of the WINDS to parameter choices and the possibilities of large false positive rates are its drawbacks. It is necessary to fine-tune settings to achieve optimum performance, which leaves it vulnerable to changes in network circumstances. Enhancing WINDS efficacy requires robustness enhancements and parameter optimization techniques (Chen et al., (2021)). By analyzing these drawbacks, our suggested method MCFO-DANN tends to overcome this issue and provide more efficient results.

6. CONCLUSION

An important development in protecting the integrity and operation of contemporary automotive networks is the implementation of an AI-powered security solution for CAN bus attack recognition in electric vehicles. The system's capacity to identify and react to any attacks on its own improves the cyber-security posture of electric cars as a whole, protecting both the people in vehicle and the larger transportation network. Among the possible downsides include false positives, changing assault tactics, avoiding discovery, costly implementation, and reliance on continual modifications to AI models for effectiveness. To overcome this problem, we proposed MCFO-DANN method to ensure the integrity and safety of vehicle communication networks in electric automobiles. Our experiment results for accuracy attain98%, precision attains (95%), recall attains (93%), and F1-score attains (96%), which shows that our proposed MCFO-DANN approaches produce outstanding results.

6.1. Future scope

Future studies will concentrate on detecting and preventing CAN bus threats to create an AI-powered security solution for electric vehicles. The technology will improve the cyber-security of electric cars and guarantee their safe and secure operation by using cutting edge machine learning algorithms to identify abnormalities and patterns indicating of cyber-attacks.

References:

Amato, F., Coppolino, L., Mercaldo, F., Moscato, F., Nardone, R., &Santone, A. (2021).CAN-bus attack detection with deep learning. IEEE Transactions on Intelligent Transportation Systems, 22(8), 5081-5090. https://doi.org/10.1109/TITS.2020.3046974

Amiri, Z., Heidari, A., Darbandi, M., Yazdani, Y., JafariNavimipour, N., Esmaeilpour, M. ...&Unal, M. (2023).The personal health applications of machine learning techniques in the internet of behaviors. Sustainability, 15(16), 12406. https://doi.org/10.3390/su151612406

Anggoro, D. A., &Kurnia, N. D. (2020). Comparison of accuracy level of support vector machine (SVM) and K-nearest neighbors (KNN) algorithms in predicting heart disease. International Journal, 8(5), 1689- 1694. https://doi.org/10.30534/ijeter/2020/32852020

Bathla, G., Bhadane, K., Singh, R. K., Kumar, R., Aluvalu, R., Krishnamurthi, R., ...&Basheer, S. (2022). Autonomous vehicles and intelligent automation: Applications, challenges, and opportunities. Mobile Information Systems, 2022. https://doi.org/10.1155/2022/7632892

Ben othmane, L., Dhulipala, L., Abdelkhalek, M., Multari, N., &Govindarasu, M. (2020). On the performance of detecting injection of fabricated messages into the can bus. IEEE Transactions on Dependable and Secure Computing, 19(1), 468-481. https://doi.org/10.1109/TDSC.2020.2990192

Bi, Z., Xu, G., Xu, G., Tian, M., Jiang, R., & Zhang, S. (2022). Intrusion detection method for in-vehicle can bus based on message and time transfer matrix. Security and Communication Networks, 2022. https://doi.org/10.1155/2022/2554280

Boumiza, S., & Braham, R. (2019, October). An anomaly detector for CAN bus networks in autonomous cars based on neural networks. In 2019 international conference on wireless and mobile computing, networking and communications(WiMob) (pp. 1-6), IEEE. https://doi.org/10.1109/WiMOB.2019.8923315

Chen, X., Li, Y., Zhang, Y., Ye, X., Xiong, X., & Zhang, F. (2021). WINDS: A wavelet-based intrusion detection system for Controller Area Network (CAN). IEEE Access 2021, 9, 58621–58633. https://doi.org/10.3380/pr9010367

D'Angelo, G., Castiglione, A., &Palmieri, F. (2020).A cluster-based multidimensional approach for detecting attacks on connected vehicles. IEEE Internet of Things Journal, 8(16), 12518-12527. https://doi.org/10.1109/JIOT.2020.3032935

Duan, X., Yan, H., Tian, D., Zhou, J., Su, J., &Hao, W. (2021). In-vehicle CAN bus tampering attacks detection for connected and autonomous vehicles using an improved isolation forest method. IEEE Transactions on Intelligent Transportation Systems. https://doi.org/10.1109/TITS.2021.3128634

Fan, Z., Yan, Z., & Wen, S. (2023). Deep Learning and Artificial Intelligence in Sustainability: A Review of SDGs, Renewable Energy, and Environmental Health. Sustainability, 15(18), 13493. https://doi.org/10.3390/su151813493

Fyhr, P., Hjelm, R., & Wahlström, J. (2022). An experimental study of forced vibration influence on disc brake drag torque in heavy commercial road vehicles. *Tribology in Industry*, *44*(1), 123–131. https://doi.org/10.24874/ti.1132.06.21.09

Gundu, R., &Maleki, M. (2022, May). Securing CAN bus in connected and autonomous vehicles using supervised machine learning approaches. In 2022 IEEE International Conference on Electro Information Technology (eIT) (pp. 042-046).IEEE. https://doi.org/10.1109/eIT53891.2022.9813985

Hossain, M. D., Inoue, H., Ochiai, H., Fall, D., &Kadobayashi, Y. (2020). LSTM-based intrusion detection system for in-vehicle can bus communications. IEEE Access, 8, 185489-185502. https://doi.org/10.1109/ACCESS.2020.3029307

Hou, S., Chen, X., Ma, J., Zhou, Z., & Yu, H. (2022). An ontology-based dynamic attack graph generation approach for the internet of vehicles. Frontiers in Energy Research, 10, 928919. https://doi.org/10.3389/fenrg.2022.928919

Huang, L., Ma, W., Wang, L., &An, K. (2023). Using Reinforcement Learning to Handle the Unintended Lateral Attack in the Intelligent Connected Vehicle Environment. Journal of Advanced Transportation, 2023. https://doi.org/10.1155/2023/3187944

Inyang, V., Kanakana, G. M., &Laseinde, O. T. (2023).Application of sustainable smart manufacturing technologies and toolkits in the automotive industry. International Journal of Low-Carbon Technologies, 18, 412-422. https://doi.org/10.1093/ijlct/ctad023

Islam, R., &Refat, R. U. D. (2020). Improving CAN bus security by assigning dynamic arbitration IDs. Journal of Transportation Security, 13(1-2), 19-31. https://doi.org/10.1007/s12198-020-00208-0

Javed, A. R., Ur Rehman, S., Khan, M. U., Alazab, M., & Reddy, T. (2021). CANintelliIDS: Detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU. IEEE transactions on network science and engineering, 8(2), 1456-1466. https://doi.org/10.1109/TNSE.2021.3059881

Kalutarage, H. K., Al-Kadri, M. O., Cheah, M., &Madzudzo, G. (2019, October).Context-aware anomaly detector for monitoring cyber attacks on automotive CAN bus. In Proceedings of the 3rd ACM Computer Science in Cars Symposium (pp. 1-8). https://doi.org/10.1145/3359999.3360496

Kim, W., Lee, J., Lee, Y., Kim, Y., Chung, J., & Woo, S. (2022). Vehicular Multilevel Data Arrangement-Based Intrusion Detection System for In-Vehicle CAN. Security and Communication Networks, 2022, 1-11. https://doi.org/10.1155/2022/4322148

Lee, J., Singh, J., Azamfar, M., &Pandhare, V. (2020).Industrial AI and predictive analytics for smart manufacturing systems.In Smart Manufacturing (pp. 213-244).Elsevier. https://doi.org/10.1016/B978-0-12-820027-8.00008-3

Ma, H., Cao, J., Mi, B., Huang, D., Liu, Y., & Li, S. (2022). A GRU-based lightweight system for CAN intrusion detection in real time. Security and Communication Networks, 2022.doi:https://doi.org/10.1155/2022/5827056

Nagaty, K. A. (2023). IoT Commercial and Industrial Applications and AI-Powered IoT.In Frontiers of Quality Electronic Design (QED) AI, IoT and Hardware Security (pp. 465-500). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-16344-9_12

Ning, J., Wang, J., Liu, J., & Kato, N. (2019).Attacker identification and intrusion detection for in-vehicle networks. IEEE communications letters, 23(11), 1927-1930. https://doi.org/10.1109/LCOMM.2019.2937097

Qin, H., Yan, M., &Ji, H. (2021). Application of controller area network (CAN) bus anomaly detection based on time series prediction. Vehicular Communications, 27, 100291. https://doi.org/10.1016/j.vehcom.2020.100291

Shi, D., Kou, L., Huo, C., & Wu, T. (2022).A CAN Bus Security Testbed Framework for Automotive Cyber-Physical Systems. Wireless Communications and Mobile Computing, 2022. https://doi.org/10.1155/2022/7176194

Sulaiman, A., Nagu, B., Kaur, G., Karuppaiah, P., Alshahrani, H., Reshan, M. S. A., ...&Shaikh, A. (2023). Artificial Intelligence-Based Secured Power Grid Protocol for Smart City. Sensors, 23(19), 8016. https://doi.org/10.3390/s23198016

Tange, K., De Donno, M., Fafoutis, X., &Dragoni, N. (2020). A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities. IEEE Communications Surveys & Tutorials, 22(4), 24892520. https://doi.org/10.1109/COMST.2020.3011208

Zhou, A., Li, Z., &Shen, Y. (2019).Anomaly detection of CAN bus messages using a deep neural network for autonomous vehicles. Applied Sciences, 9(15), 3174. https://doi.org/10.3390/app9153174

S. B. Vinay Kumar
JAIN (Deemed-to-be University), Ramanagara District, Karnataka, India
sb.vinaykumar@jainuniversity.ac.in
ORCID 0000-0001-7349-1697

B. P. Singh
Maharishi University of Information Technology, Uttar Pradesh, India
bhanupratapmit@gmail.com
ORCID 0000-0001-5346-4309

Raman Batra
Noida Institute of Engineering & Technology, Greater Noida, Uttar Pradesh, India
ramanbatra@niet.co.in
ORCID 0009-0006-7359-7313

Akash Kumar Bhagat
Arka Jain University, Jamshedpur, Jharkhand, India
akash.b@arkajainuniversity.ac.in
ORCID 0000-0001-8717-764X