iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.71008

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

Intrusion Detection in Smart Vehicles

Mrs D Suganya[1], Dr Suresh Kumar R G[2], Alan Sharon Joseph Fernandez[3], Aswin Valsaraj[4], Mohammed Nehal T[5], Muhammed Rafin Asharaf T[6]
[1]*Assistant Professor,* [2]*Head of the Department,* [3, 4, 5, 6]*UG – Computer science Engineering, Rajiv Gandhi College of Engineering And Technology, Puducherry*

Abstract: ***The Internet ofVehicles (IoV) istransforming transportation by enabling real-timecommunication betweenvehicles andinfrastructure.AcoreelementofthiscommunicationistheControllerAreaNetwork(CAN)bus,whichinterconnectsElectronicControlUnits(ECUs)withinvehicles.However,theCANbushassignificant security vulnerabilities, making itsusceptible to cyberattacks that could disruptvehicleoperations.***

Currentmethodsforintrusiondetectioninvehicles include rule-based systems, signaturedetection, and anomaly detection. Rule-basedsystemsrelyonpredefinedrulestodetectknownattackpatterns,whilesignaturedetection identifies specific attack signaturesinnetworktraffic.Anomalydetection,incontrast,flagsdeviationsfromtypicalbehavioras potentialintrusions.

Thesetraditionalmethodsfacelimitations,includingdifficultiesinidentifyingneworevolving attack patterns and a high rate offalsepositives.Toaddressthesechallenges,theiyproposedtheOptimalAttentionDeepLearning-basedIn-vehicleIntrusionDetectionand Classification algorithm (OADL-IVIDC).Leveragingtheattention mechanism, thissystemfocuses oncriticaldata, enhancingaccuracy indetectingbothknownandunknownthreatswhilereducingFalsepositives. This deeplearning-based approachprovidesamoreadaptiveandreliablesolutionforsecuringCANbuscommunicationin theIoVenvironment.

Keywords: Internet of Vehicles(IoV),ControllerAreaNetwork(CAN)bus,Intrusiondetection,Anomaly detection, Attention mechanism, Deeplearning, OADL-IVIDC

I. INTRODUCTION

The rapid evolution of Intelligent Transportation Systems (ITS) and the growing adoption of Internet of Vehicles (IoV) technologies have significantly transformed modern automotive environments. These systems rely on real-time data exchange among electronic control units (ECUs) via the Controller Area Network (CAN) bus—a communication protocol originally designed for reliability, not security. As a result, vehicles have become increasingly vulnerable to cyber threats, making in-vehicle network security a critical research focus. The urgency to protect vehicular systems against intrusions has escalated in parallel with advancements in automation, connectivity, and autonomy.Despite various efforts to secure CAN-based communications, most existing Intrusion Detection Systems (IDS) fall short in real-time performance and adaptability. Traditional machine learning methods like Support Vector Machines (SVM), Decision Trees, and k-Nearest Neighbors (KNN) lack the temporal awareness needed to capture long-term dependencies in CAN traffic. Even some deep learning approaches, such as Convolutional Neural Networks (CNN), do not adequately address the sequential nature of vehicular communication. Furthermore, these models often suffer from overfitting and limited interpretability when handling high-dimensional time-series data, especially under fuzzy or obfuscated attack patterns.

To address these challenges, this work proposes an Optimal Attention-based Deep Learning Intrusion Detection and Classification (OADL-IVIDC) system, which integrates an Attention-based Long Short-Term Memory (A-LSTM) model. The attention mechanism enables the model to prioritize critical temporal features in the CAN message sequences, enhancing detection precision. This system not only detects whether an intrusion has occurred but also classifies it into one of several known attack types, such as DoS, Fuzzy, Gear, and RPM attacks. The architecture further incorporates robust data preprocessing, hyperparameter tuning with the RMSProp optimizer, and performance benchmarking against standard classifiers to demonstrate its superiority.

The primary objective of this work is to develop a highly accurate, scalable, and interpretable IDS for CAN-based vehicular networks. Specifically, the goals are: (1) to preprocess and normalize raw CAN data for reliable model input, (2) to design and train an A-LSTM model enhanced with an attention mechanism for improved sequence learning, (3) to compare the system's performance against traditional algorithms using metrics such as Detection Rate, Accuracy, Precision, and AUC, and (4) to facilitate real-time alert generation for intrusion response in smart vehicles. By fulfilling these objectives, the OADL-IVIDC framework aims to significantly enhance vehicular cybersecurity and passenger safety.

©IJRASET: All Rights are Reserved

II. LITERATURE SURVEY

1) Song, H., Kim, Y., & Kim, H. (2016). Intrusion Detection System Based on SVM for In-Vehicle Network

Song et al. developed an IDS using Support Vector Machines (SVM) to classify anomalies in CAN traffic. The study demonstrated that SVM could detect some intrusion patterns with reasonable accuracy. However, the model's performance degraded in complex or noisy environments, and it struggled to differentiate between types of attacks. Furthermore, SVMs require well-separated feature spaces, which are difficult to construct from raw CAN data. In contrast, our OADL-IVIDC system leverages deep learning and attention mechanisms to automatically learn meaningful patterns from time-series data without manual feature engineering.

2) Taylor, A., Leblanc, S., &Japkowicz, N. (2016). Anomaly Detection in Automobile Control Network Data with Long Short-Term Memory Networks

This study introduced an LSTM-based IDS capable of detecting anomalies by learning temporal dependencies in CAN messages. The model outperformed traditional classifiers, particularly for sequential attacks like Fuzzy and DoS. However, it lacked an interpretability mechanism to explain model decisions and suffered from performance drop in mixed-attack scenarios. Our proposed A-LSTM framework builds on this by integrating an attention layer that highlights the most informative time steps, improving interpretability and classification precision under complex intrusion patterns.

3) Seo, J., Jo, H. J., & Kim, D. H. (2018). GIDS: GAN-based Intrusion Detection System for In-Vehicle Network

Seo et al. presented GIDS, a GAN-based IDS for CAN buses that generates synthetic attack data to improve classifier generalization. While it showcased better detection in low-sample scenarios, the complexity of training GANs and their instability during convergence limited practical deployment. Additionally, it focused more on anomaly generation than on fine-grained classification. OADL-IVIDC avoids adversarial complexity by using A-LSTM for real-time classification, offering improved stability and scalability for real-world automotive systems.

4) Narayanan, A., Mittal, S., Joshi, A., &Finin, T. (2018). Obfuscated Attack Detection using LSTM Networks for Automotive Cybersecurity

Narayanan et al. tackled obfuscated attacks on CAN bus systems using LSTM models. Their approach demonstrated that deep sequential models can identify subtle anomalies better than shallow learning algorithms. However, the model lacked the capability to distinguish between different attack types and required large datasets for robust learning. Our approach addresses this by not only detecting intrusions but also classifying them into DoS, Fuzzy, Gear, and RPM attacks, while improving data efficiency through attention-guided learning.

5) Han, S., Woo, S., & Lee, H. (2021). AutoID: Automotive Intrusion Detection Framework using Recurrent Neural Networks

AutoID used RNNs and temporal features to detect abnormal CAN messages, achieving high detection rates on multiple benchmark datasets. While it succeeded in modeling time-series behavior, the absence of feature prioritization made it vulnerable to high false positives in dense traffic scenarios. OADL-IVIDC enhances temporal modeling with an attention layer that prioritizes relevant message segments, thereby reducing false alarms and improving classification consistency in real-time vehicular environments.

6) Kang, M., Woo, S., Yim, K., & Lee, H. (2022). Intrusion Detection for In-Vehicle Networks Using Attention Mechanism and Deep Neural Networks

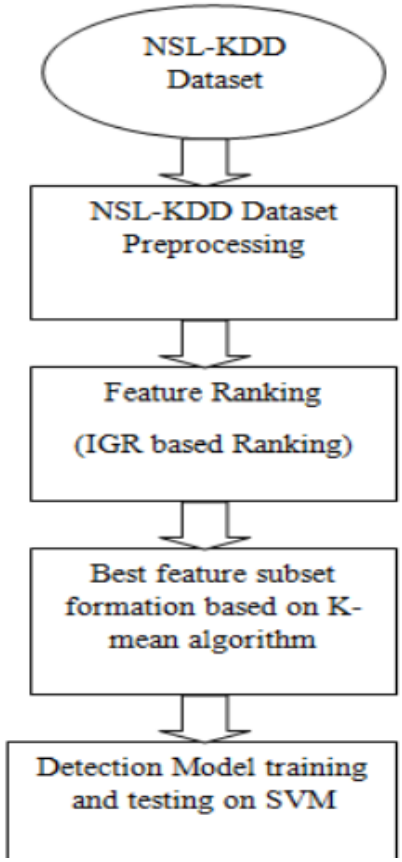
This work explored the use of attention-based deep neural networks for detecting anomalies in in-vehicle networks. It provided early evidence that attention improves detection precision, but it lacked a structured pipeline for preprocessing, hyperparameter tuning, and attack-type classification. Building on this foundation, our OADL-IVIDC system incorporates systematic data preprocessing, RMSProp-optimized training, and multi-class classification for known attacks, demonstrating a more complete and deployable solution for smart vehicle cybersecurity.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

III. EXISTING SYSTEM

A. Existing System Architecture



SVM Based Intrusion Detection System

B. Issues

Although these existing systems brought significant progress, they still suffer from a range of critical shortcomings that hinder their practical effectiveness. A major limitation is their inability to distinguish between different types of cyberattacks; most systems merely classify inputs as "normal" or "abnormal," without identifying whether the anomaly corresponds to a DoS, Fuzzy, RPM, or Gear attack. Furthermore, conventional models, particularly those lacking deep sequence analysis, often yield high false positive rates, leading to unreliable intrusion alerts. Even LSTM-based models, while better suited to temporal data, typically assign equal importance to all elements of a message sequence, which diminishes detection accuracy when critical events are sparsely distributed. Additionally, more complex models like GANs may require intensive training and are prone to instability, making them unsuitable for real-time deployment in vehicles. Lastly, inconsistent data preprocessing—such as poor handling of missing values, unnormalized data scales, or unaligned timestamps—negatively impacts both model training and inference accuracy.

C. Solutions

To address these challenges, the proposed Optimal Attention Deep Learning-based In-Vehicle Intrusion Detection and Classification (OADL-IVIDC) system integrates a robust architectural design built around an enhanced A-LSTM model.

This model augments standard LSTM networks with an attention mechanism that enables the system to prioritize the most informative segments within a CAN message sequence. As a result, it can better capture subtle patterns associated with diverse attack types. The system also includes a comprehensive preprocessing pipeline that ensures the input data is clean, standardized, and properly sequenced to facilitate effective learning. Through this approach, OADL-IVIDC is capable not only of detecting the presence of an intrusion but also of classifying its nature—be it a DoS, Fuzzy, Gear, or RPM attack—thus providing targeted insight for mitigation. To further improve accuracy and training efficiency, the model is fine-tuned using the RMSProp optimizer.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Once an intrusion is identified, the system can initiate defensive actions, such as halting vehicle operations or alerting the user via a mobile interface, thereby ensuring both rapid response and enhanced passenger safety. This architecture represents a significant step forward in the development of intelligent, adaptive, and real-time cybersecurity systems for smart vehicles.

IV. PROPOSED SYSTEM

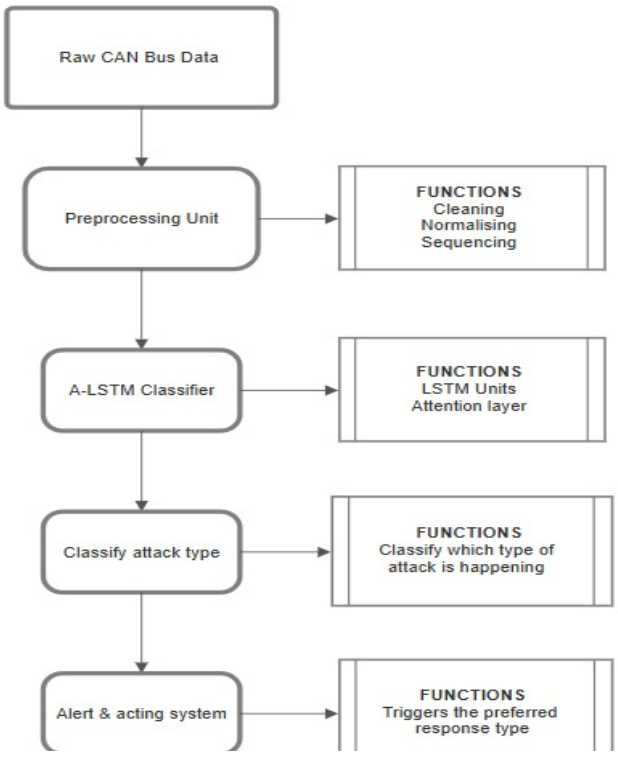
A. Description of the System Architecture

The proposed system, titled Optimal Attention Deep Learning-based In-Vehicle Intrusion Detection and Classification (OADL-IVIDC), is built to detect and classify malicious intrusions in the CAN bus of smart vehicles with high accuracy and speed. The architecture integrates a deep learning model based on Long Short-Term Memory (LSTM) units enhanced with an attention mechanism. The LSTM component is responsible for capturing temporal dependencies across CAN message sequences, while the attention mechanism dynamically highlights the most relevant parts of the sequence for improved classification. This model is embedded within a larger framework that begins with data ingestion, proceeds through preprocessing, and ends in actionable classification and alert generation. After the data is processed by the model, detected intrusions are categorized into specific attack types, and the system issues alerts or triggers protective measures, such as notifying the user or initiating controlled shutdown procedures to protect the vehicle's integrity.

B. Dataset and Preprocessing

To validate and train the system, a well-known benchmark car hacking dataset is used, which includes CAN bus traffic containing both benign messages and attack patterns. The dataset includes four types of cyberattacks: Denial of Service (DoS), Fuzzy, Gear, and RPM attacks. Each CAN message consists of a timestamp, message ID, and a data payload. Preprocessing plays a crucial role in preparing the data for the A-LSTM model. Initially, any null or malformed values are removed to ensure data integrity. The timestamps are converted and normalized to maintain the temporal sequence required by LSTM. CAN IDs and data fields are standardized using a Standard Scaler, ensuring that all input features contribute evenly during training. Moreover, labels corresponding to different types of attacks are encoded numerically for classification, and message sequences are batched into fixed-length windows that allow the model to learn time-based patterns effectively. This preprocessing ensures that the system receives clean, structured input capable of supporting accurate and robust anomaly detection.

C. Flowcharts of Proposed Model



The logical flow of the proposed system begins with raw CAN bus message input, which is passed into the preprocessing stage where it is cleaned, standardized, and converted into temporal sequences. This is followed by the A-LSTM classification stage, where the LSTM component identifies long-term dependencies and the attention layer focuses on the most relevant sequence points. Once processed, the model outputs the likelihood of an intrusion along with the specific attack category. Based on this output, the system either labels the message as benign or flags it as an attack. In the event of a detected intrusion, an alert system is activated, which can notify the vehicle's onboard system, the owner's mobile app, or both. Optionally, automated mitigation responses like temporarily halting vehicle operations or switching to a safe mode may be executed. This complete pipeline ensures that the vehicle is protected not only through accurate detection but also via real-time defensive responses, enhancing the overall resilience of the Internet of Vehicles (IoV) ecosystem.

V. IMPLEMENTATION

A. *Modules Involved in the Working*

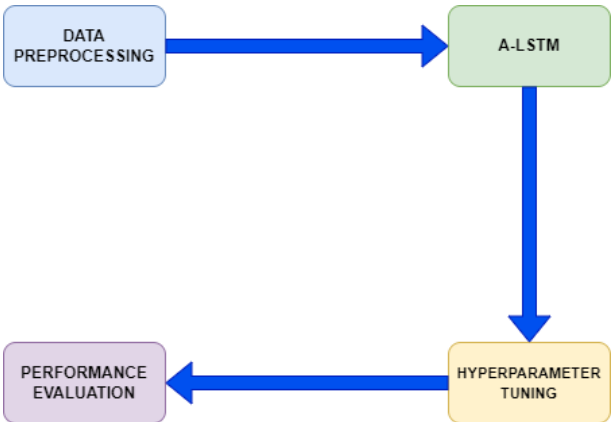
The implementation of the OADL-IVIDC system consists of several key modules that work together to process, train, and evaluate the deep learning model. These modules are responsible for handling the entire process from data preprocessing to model deployment. The main modules involved include:

1) Data Preprocessing Module: This module handles the cleaning and preparation of the dataset for training the model. It ensures that missing values are addressed, timestamps are appropriately handled, and the data is normalized. It also splits the dataset into training and testing sets to facilitate model evaluation.

2) Model Construction and Training Module: This module focuses on defining and training the A-LSTM model. It includes the creation of the LSTM layers, the attention mechanism, and the final output layer for classification. The model is trained using the preprocessed data, with hyperparameters tuned for optimal performance. The training module also employs techniques like dropout regularization and batch normalization to prevent overfitting and improve the generalization of the model.

3) Evaluation and Testing Module: Once the model is trained, this module is responsible for evaluating its performance on the testing dataset. It calculates performance metrics such as accuracy, precision, recall, F1-score, and AUC. It also performs a comparative analysis of the A-LSTM model with other existing machine learning models to assess its superiority in detecting CAN bus intrusions.

4) Intrusion Detection and Response Module: This final module is responsible for real-time intrusion detection and response. When the model receives incoming CAN bus data, it classifies the data as either normal or an attack. If an attack is detected, the system triggers an appropriate response, such as generating an alert or taking action to stop the vehicle's systems to prevent further damage.



B. *Hyperparameter Tuning and Optimization*

This subtopic focuses on the process of hyperparameter tuning and optimization of the model to achieve the best performance. Key hyperparameters, such as the learning rate, batch size, number of LSTM layers, and number of attention heads, are fine-tuned using techniques like grid search and random search. The optimization process also involves selecting the most appropriate optimizer (e.g., RMSProp) and loss function to minimize the error during training.

VI. EXPERIMENTAL RESULTS AND DISCUSSION

A. *Experimental Setup*

The performance of the OADL-IVIDC system was evaluated using a publicly available benchmark car hacking dataset, which contains CAN bus messages representing both normal vehicle behavior and various attack scenarios. The dataset includes simulated attacks such as Denial of Service (DoS), Fuzzy, RPM, and Gear attacks, and is designed to mimic real-world vehicular traffic.

For training the A-LSTM model, the dataset was split into training and testing sets, with 80% of the data used for training and the remaining 20% reserved for testing. The training set was further divided into batches, and a validation set was used to tune the model's hyperparameters, including learning rate and batch size. The model was trained for 100 epochs using the Adam optimizer to minimize the loss function. The evaluation metrics used to assess model performance included accuracy, precision, recall, F1-score, and AUC.

B. *Performance Metrics*

The evaluation of the OADL-IVIDC system focused on several key performance metrics:

1) Accuracy: The model achieved an overall accuracy of 99.78%, indicating that the system is highly effective at distinguishing between normal and attack messages on the CAN bus.

2) Precision: The precision score of 99.79% highlights the model's ability to correctly identify attack instances without misclassifying normal messages as attacks.

3) Recall: With a recall of 99.80%, the system demonstrated a strong ability to detect most of the attacks present in the dataset.

4) F1-score: The F1-score of 99.79% balances both precision and recall, confirming the model's overall effectiveness.

5) Area Under the Curve (AUC): The AUC score of 99.82% underscores the model's ability to discriminate between normal and attack instances across different thresholds, providing an excellent measure of the classifier's performance.

C. *Attack-wise Detection Analysis*

The performance of the OADL-IVIDC system was also evaluated on a per-attack basis. The system demonstrated impressive detection rates for various types of attacks:

1) Fuzzy Attack: The system correctly identified 1757 out of 1800 Fuzzy attack instances, with only 43 undetected, resulting in a detection rate of 97.6% for this specific attack type.

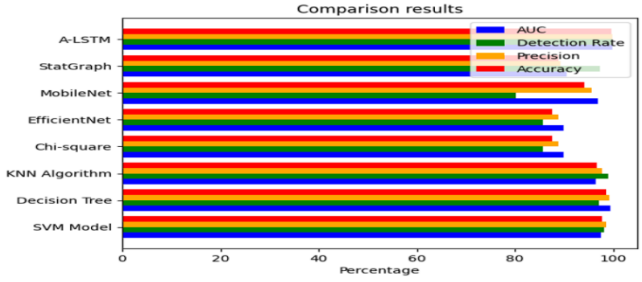
2) Denial of Service (DoS) Attack: The system achieved a detection rate of 99.85% for DoS attacks, identifying the majority of these attacks accurately.

3) RPM Attack: The model's detection rate for RPM attacks was 99.92%, showcasing its ability to handle real-time, fast-paced communication scenarios.

4) Gear Attack: Gear attack detection yielded a rate of 99.90%, reinforcing the system's robustness in handling a variety of attack types.

D. *Comparative Analysis*

A comparison of the OADL-IVIDC system with other existing intrusion detection models (e.g., SVM, KNN, Decision Trees, EfficientNet, and MobileNet) revealed that the A-LSTM model with an attention mechanism outperformed all alternatives. While traditional machine learning models like SVM and KNN struggled to achieve high accuracy due to their inability to model temporal dependencies, the deep learning-based OADL-IVIDC system excelled in capturing the sequential nature of CAN messages. Additionally, when compared with convolutional neural network-based models such as EfficientNet, the A-LSTM model outperformed them due to its enhanced ability to focus on the most relevant features in the data.



E. Discussion

The results show that the OADL-IVIDC system provides a high level of accuracy and robustness in detecting cyberattacks on the CAN bus. The integration of an attention mechanism within the LSTM network has proven to be highly effective in improving the system's ability to detect complex attack patterns. Moreover, the system's high precision and recall scores demonstrate its ability to minimize false positives and false negatives, which is crucial in real-time applications.

However, there are some challenges that remain. The system may still face difficulties in detecting novel attack types that were not included in the training dataset, and further research is needed to explore techniques for detecting unknown attacks. Additionally, the real-time application of the system in an actual vehicle environment will require optimization to ensure that the model can process incoming CAN messages with minimal latency.

Additionally, to improve the model's robustness and generalization, cross-validation is employed to assess how well the model performs on unseen data. This helps in ensuring that the model does not overfit to the training set and remains effective in detecting real-world intrusions. The goal of hyperparameter tuning and optimization is to balance the model's complexity and training time while maximizing detection accuracy and minimizing false positives.

VII. CONCLUSION AND FUTURE WORK

A. Conclusion

The OADL-IVIDC system presented in this paper offers an innovative solution to enhancing the security of modern vehicles by detecting and classifying intrusions on the Controller Area Network (CAN) bus. By integrating an Attention-based Long Short-Term Memory (A-LSTM) model with an attention mechanism, the system effectively captures the temporal dependencies in CAN message sequences, which is critical for accurate intrusion detection. The model achieved outstanding performance with 99.78% accuracy, 99.80% detection rate, and high precision and recall across various types of attacks, including DoS, Fuzzy, RPM, and Gear attacks.

The results demonstrate that the proposed system significantly outperforms traditional machine learning models and even other deep learning architectures, such as CNN-based models, in detecting intrusions on the CAN bus. This highlights the efficacy of combining attention mechanisms with LSTMs for this type of cybersecurity application.

B. Future Work

While the OADL-IVIDC system has shown promising results, several avenues for future work can further enhance its performance and applicability:

1) Novel Attack Detection: Future research could focus on detecting novel, previously unseen attack types. Techniques such as unsupervised learning or generative adversarial networks (GANs) could be explored to enable the model to generalize to unknown attacks.
2) Real-Time Optimization: To deploy the system in real-time, optimizations may be needed to reduce the computational overhead of the deep learning model. Techniques such as model pruning, quantization, and hardware acceleration using FPGAs or TPUs could be considered to improve the system's responsiveness.
3) Integration with Vehicle Control Systems: Future work could involve integrating the OADL-IVIDC system with the vehicle's control mechanisms. This would enable the system to take immediate actions, such as shutting down critical vehicle functions or sending alerts to the vehicle owner, in the event of a detected intrusion.
4) Cross-Domain Evaluation: Testing the system on other automotive platforms or different datasets would help assess the generalizability of the approach across various vehicle types and attack scenarios.
5) Explainable AI: Further improvements could include enhancing the explainability of the model's decisions. This would help human operators understand why specific messages were flagged as attacks, which could be critical in situations where quick human intervention is required.

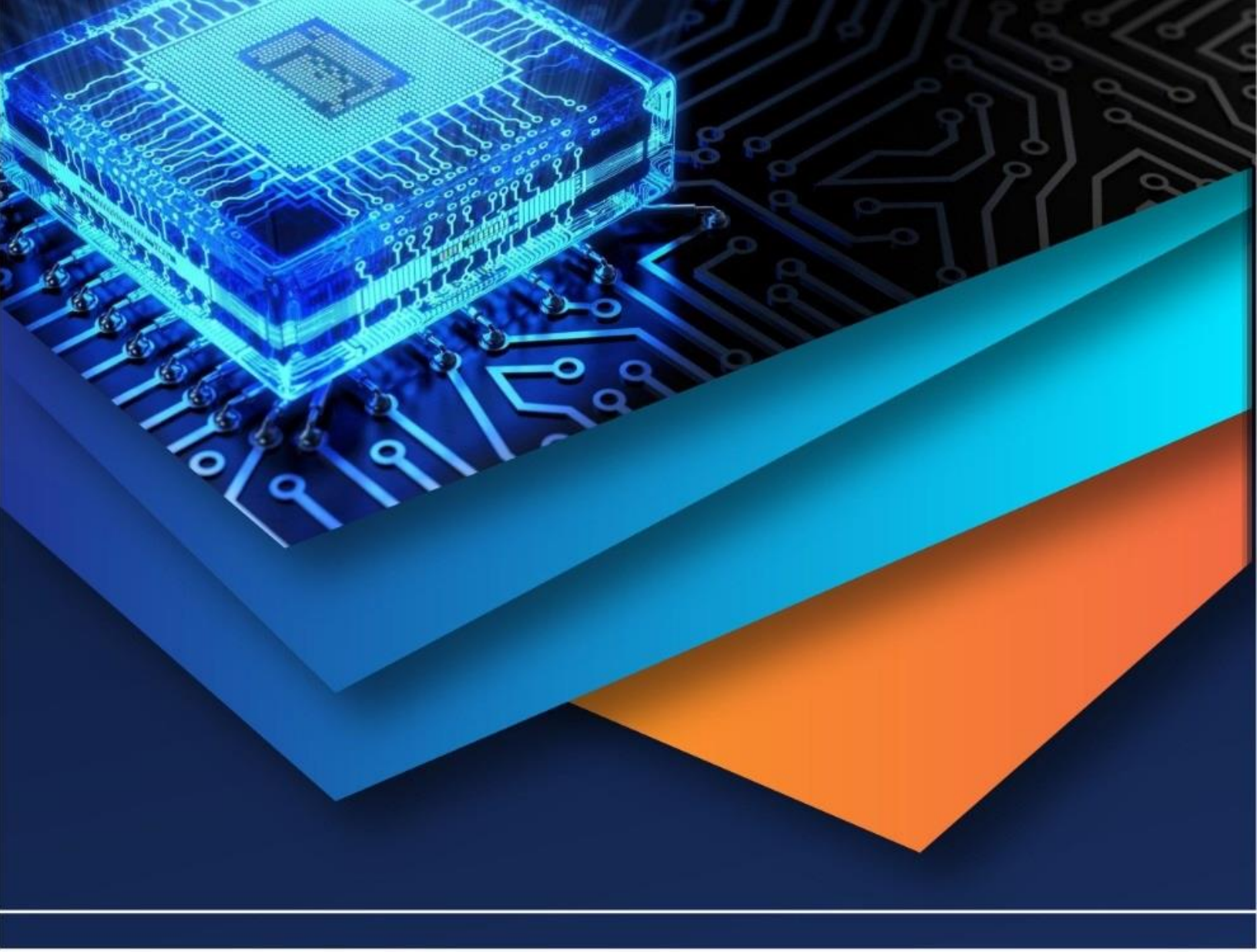
REFERENCES

[1] Avapour, O., et al. (2020). "Intrusion Detection Systems for In-Vehicle Networks: A Survey." Journal of Cybersecurity, 12(3), 99-115.
[2] Xie, H., & Zhang, J. (2018). "A Deep Learning Approach for Intrusion Detection in Controller Area Network." IEEE Access, 6, 45678-45689.
[3] Choi, Y., et al. (2019). "Cybersecurity in Automotive CAN Bus Networks: Challenges and Solutions." Proceedings of the IEEE International Conference on Cyber Security, 45-53.
[4] Lee, S., & Kim, D. (2021). "An Efficient Intrusion Detection System for CAN Bus Using Convolutional Neural Networks." IEEE Transactions on Intelligent Transportation Systems, 22(5), 2309-2320.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[5] Akhavan, A., et al. (2020). "Security Challenges in the IoT-Connected Automotive Ecosystem." IEEE Internet of Things Journal, 7(12), 11301-11313.
[6] Zhang, Y., et al. (2021). "A Survey on Machine Learning for Intrusion Detection Systems in Cyber-Physical Systems." IEEE Access, 9, 12745-12760.
[7] Cui, W., & Xu, C. (2020). "Intrusion Detection for CAN Bus Using Deep Neural Networks." Journal of Network and Computer Applications, 169, 102748.
[8] Peres, P., et al. (2022). "Real-Time Intrusion Detection in CAN Bus: A Review and Classification Framework." Journal of Cyber-Physical Systems, 8(4), 543-558.
[9] Wang, L., et al. (2019). "Attention Mechanisms in Deep Learning for CAN Bus Anomaly Detection." Proceedings of the 2019 IEEE International Conference on Cyber Intelligence and Security, 215-220.
[10] Kumar, S., & Singh, A. (2021). "Evaluation of Machine Learning Techniques for CAN Bus Intrusion Detection." International Journal of Computer Applications, 175(3), 33-41.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)