INFORMATICS JOURNALS

43

SHRI-LEKH (Multi-disciplinary Research Journal) Vol 2(1), June 2026, p. 43-46

Online ISSN: 3139-5694
DOI:10.18311/SHRI-LEKH/2026/v2i1/53890

A Hybrid Deep Learning Framework for Intrusion Detection in Automotive Controller Area Networks

Winit Nilkanth Anandpawar[1]*, Shweta M. Barhate[1] and Mahendra P. Dhore[2]

[1]Department of Electronics and Computer Science, PGTD, R.T.M. Nagpur University, Nagpur - 440033, Maharashtra, India

[2]Pro-Vice-Chancellor, Sant Gadge Baba Amravati University, Amravati - 444602, Maharashtra, India

Abstract

The increasing connectivity of modern vehicles has made their internal networks, particularly the Controller Area Network (CAN), vulnerable to a wide range of cyber-attacks (Barnard *et al*., 2022). Traditional Intrusion Detection Systems (IDS) often struggle with the sophisticated, time-sensitive nature of these threats (Hariharan *et al*., 2022). This paper proposes a novel hybrid intrusion detection framework that leverages the complementary strengths of Machine Learning (ML) and Deep Learning (DL) to achieve high accuracy and real-time performance. Our methodology involves a multi-stage process: Acquiring the real-world Car-Hacking dataset, preprocessing and balancing data using SMOTE, and innovatively transforming tabular CAN data into a 2D image format. This transformation enables the application of pre-trained, lightweight Convolutional Neural Networks (CNNs) like EfficientNetB0 and InceptionV3 for spatial feature extraction. We further introduce a hybrid model that integrates EfficientNetB0 with a Long Short-Term Memory (LSTM) network to capture both spatial and temporal dependencies in the data, a critical capability for detecting multi-stage attacks (Arreche *et al*., 2024a). For comparative analysis, traditional ML models such as Logistic Regression, Random Forest, and a hybrid RF-SVM model are implemented. The proposed framework is designed to be computationally efficient, making it suitable for deployment in resource-constrained automotive systems (Musleh *et al*., 2023). This study outlines a complete, replicable methodology for developing a robust, hybrid IDS capable of defending next-generation intelligent vehicles (Awajan, 2023).

Keywords: Automotive Cybersecurity, CAN Bus, Deep Learning, EfficientNet, Hybrid Model, Intrusion Detection System, LSTM

INTRODUCTION

The automotive industry is undergoing a radical transformation with the advent of connected and autonomous vehicles. This connectivity, while enabling advanced features, exposes vehicles to critical cybersecurity threats. The Controller Area Network (CAN), the de facto standard for in-vehicle communication, lacks inherent security mechanisms, making it a prime target for attacks like Denial-of-Service (DoS), fuzzing, and spoofing. The dynamic and complex nature of these attacks renders conventional signature-based IDS and traditional ML models inadequate, as they often fail to capture high-level abstractions and temporal patterns (Roshan & Zafar, 2024).

To address these limitations, this research proposes a hybrid classification approach for IDS that synergistically combines ML and DL paradigms.

Email: *winit.anand@gmail.com, shwetab73@yahoo.com, mpdhore@rediffmail.com

The core contribution is a framework that is not only highly accurate but also efficient enough for real-time deployment. Key innovations include:

- The transformation of tabular CAN data into an image-like format to leverage powerful, pre-trained CNN architectures.
- The use of SMOTE to handle inherent class imbalance in intrusion datasets.
- The development of a novel hybrid EfficientNetB0 + LSTM model that captures both spatial features and temporal sequences in network traffic.
- A comprehensive comparative analysis including traditional ML classifiers and other DL models like InceptionV3.

This paper details the proposed methodology, model architectures, and implementation strategy, providing a pathway toward building intelligent and adaptive IDS for modern vehicles (Altulaihan *et al.*, 2024).

PROPOSED METHODOLOGY

The proposed methodology is structured into a sequential pipeline to ensure a systematic development and evaluation process.

Dataset Acquisition

The Car-Hacking Dataset from OCSLab was used, containing real CAN bus traffic from a Hyundai Sonata. It includes normal driving data and labelled attack scenarios (DoS, Fuzzy, and Spoofing), providing a realistic testbed for IDS development (Saiyed & Al-Anbagi, 2024).

Data Preprocessing

A comprehensive preprocessing pipeline was applied:

- Feature and label separation: CAN message fields (ID, DLC, Data bytes) were extracted as features.
- Label encoding: Categorical labels were converted into numerical values.
- Scaling: Data was normalized using Standard Scaler to ensure zero mean and unit variance.

Handling Class Imbalance with SMOTE

The Synthetic Minority Over-sampling Technique (SMOTE) was applied to generate synthetic samples for the minority attack classes, mitigating model bias towards the predominant "Normal" class (Mishra *et al.*, 2023).

Text-to-image Transformation

A novel transformation was employed to convert pre-processed tabular data into image format. For every 27 data rows, a 3D array of shape 9x9x3 was created, simulating an RGB image. This allowed the utilization of transfer learning with CNN models like EfficientNetB0 and InceptionV3 (Yadav *et al.*, 2024).

Model Implementation and Evaluation

The dataset was split 80-20 for training and testing. The study implemented:

- Traditional ML models: Logistic regression, Stochastic gradient descent, Random forest, and MLP as baseline classifiers.
- Deep Learning Models: Lightweight versions of EfficientNetB0 and InceptionV3, fine-tuned on the image-transformed data.
- Hybrid model (RF+SVM): An ensemble model where random forest performs feature selection and an SVM with RBF kernel performs the final classification.
- Proposed hybrid model (EfficientNetB0 + LSTM): The core innovation, which extracts spatial features via EfficientNetB0 and models temporal dependencies *via* an LSTM network.

Performance was evaluated using accuracy, precision, recall, F1-score, AUC-ROC, and computational metrics like inference latency (Balega *et al.*, 2024).

MODEL ARCHITECTURES

Lightweight EfficientNetB0

EfficientNetB0, known for its compound scaling method, was used as a highly efficient spatial feature

extractor. The model, pre-trained on ImageNet, was fine-tuned by modifying its final classification head. Its MBConv blocks with depth wise separable convolutions and Swish activation make it ideal for resource-constrained environments (Javed *et al.*, 2024).

Lightweight Inception V3

InceptionV3 was adapted for its ability to capture multi-scale features through its inception modules and factorized convolutions. The pre-trained model was fine-tuned with early layers frozen, balancing accuracy and computational cost for real-time IDS (Yaras & Dener, 2024).

Hybrid Model: EfficientNetB0 + LSTM

This is the cornerstone of the proposed framework.

- Spatial feature extraction: The EfficientNetB0 backbone processes each 224x224x3 input image (resized from 9x9x3) and outputs a condensed feature vector via global average pooling (Li *et al.*, 2024).
- Temporal sequence modelling: These feature vectors are sequenced and fed into an LSTM layer (128/256 units), which learns the temporal dependencies across consecutive CAN messages (Krishnan & Shrinath, 2024).
- Classification: The LSTM's output is passed through dropout and dense layers before a final softmax layer classifies the sequence as normal or a specific attack type.

This architecture is uniquely suited to detect attacks that manifest over a sequence of packets, such as gradual spoofing or sustained flooding (Awotunde *et al.*, 2023).

EXPECTED OUTCOMES AND CONCLUSION

The proposed hybrid methodology is expected to significantly advance the state-of-the-art in automotive IDS. By fusing the spatial pattern recognition of CNNs with the temporal modelling of LSTMs, the EfficientNetB0+LSTM model is anticipated to achieve higher accuracy and a lower false-positive rate compared to standalone models. The use of transfer learning and lightweight architectures ensures the framework is deployable in real-world automotive Electronic Control Units (ECUs) (Alotaibi & Ilyas, 2023).

The inclusion of traditional ML and other DL models provides a robust comparative baseline, highlighting the trade-offs between model complexity and performance. The innovative text-to-image transformation opens a new paradigm for applying computer vision techniques to network security (Arreche *et al.*, 2024b).

In conclusion, this paper presents a comprehensive, novel, and practical pathway for building intelligent intrusion detection systems. The outlined methodology is not only tailored for the automotive domain but is also generalisable to other IoT and cyber-physical systems, contributing a scalable and effective solution to the evolving challenges of cybersecurity.

REFERENCES

Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2024). Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms. *Sensors*, *24*(3), 713. https://doi.org/10.3390/s24030713

Alotaibi, Y., & Ilyas, M. (2023). Ensemble-learning framework for intrusion detection to enhance internet of things devices security. *Sensors*, *23*(12), 5568. https://doi.org/10.3390/s23125568

Arreche, O., Guntur, T. R., Roberts, J. W., & Abdallah, M. (2024). E-XAI: Evaluating black-box explainable AI frameworks for network intrusion detection. *IEEE Access*, *12*, 23954-23988. https://doi.org/10.1109/ACCESS.2024.3365140 \

Arreche, O., Guntur, T., & Abdallah, M. (2024). XAI-IDS: Toward proposing an explainable artificial intelligence framework for enhancing network intrusion detection systems. *Applied Sciences*, *14*(10), 4170. https://doi.org/10.3390/app14104170

Awajan, A. (2023). A novel deep learning-based intrusion detection system for IoT networks. *Computers*, 12(2), 34. https://doi.org/10.3390/computers12020034

Awotunde, J. B., Folorunso, S. O., Imoize, A. L., Odunuga, J. O., Lee, C. C., Li, C. T., & Do, D. T. (2023). An ensemble

tree-based model for intrusion detection in industrial internet of things networks. *Applied Sciences*, *13*(4), 2479. https://doi.org/10.3390/app13042479

Balega, M., Farag, W., Wu, X. W., Ezekiel, S., & Good, Z. (2024). Enhancing IoT security: Optimizing anomaly detection through machine learning. *Electronics*, *13*(11), 2148. https://doi.org/10.3390/electronics13112148

Barnard, P., Marchetti, N., & DaSilva, L. A. (2022). Robust network intrusion detection through explainable artificial intelligence (XAI). *IEEE Network Letters*, *4*(3), 167-171. https://doi.org/10.1109/LNET.2022.3186589

Hariharan, S., Robinson, R. R. R., Prasad, R. R., Thomas, C., & Balakrishnan, N. (2022). XAI for intrusion detection system: Comparing explanations based on global and local scope. *Journal of Computer Virology and Hacking Techniques*, *19*(2), 217-239. https://doi.org/10.1007/s11416-022-00441-2

Javed, A., Ehtsham, A., Jawad, M., Awais, M. N., Qureshi, A.H., & Larijani, H. (2024). Implementation of lightweight machine learning-based intrusion detection system on IoT devices of smart homes. *Future Internet*, *16*(6), 200. https://doi.org/10.3390/fi16060200

Krishnan, D., & Shrinath, P. (2024). Robust botnet detection approach for known and unknown attacks in IoT networks using stacked multi-classifier and adaptive thresholding. *Arabian Journal for Science and Engineering*, *49*(9), 12561-12577. https://doi.org/10.1007/s13369-024-08742-y

Li, J., Othman, M. S., Chen, H., & Yusuf, L. M. (2024). Optimizing IoT intrusion detection system: Feature selection versus feature extraction in machine learning. *Journal of Big Data*, *11*(1), 36. https://doi.org/10.2139/ssrn.4636793

Mishra, A. K., Paliwal, S., & Srivastava, G. (2023). Anomaly detection using deep convolutional generative adversarial networks in the internet of things. *ISA Transactions*, 145, 493-504. https://doi.org/10.1016/j.isatra.2023.12.005

Musleh, D., Alotaibi, M., Alhaidari, F., Rahman, A., & Mohammad, R. M. (2023). Intrusion detection system using feature extraction with machine learning algorithms in IoT. *Journal of Sensor and Actuator Networks*, 12(2), 29. https://doi.org/10.3390/jsan12020029

Roshan, K., & Zafar, A. (2024). Ensemble adaptive online machine learning in data stream: A case study in cyber intrusion detection system. *International Journal of Information Technology*, *16*(8), 5099-5112. https://doi.org/10.1007/s41870-024-01727-y

Saiyed, M. F., & Al-Anbagi, I. (2024). A genetic algorithm- and t-test-based system for DDoS attack detection in IoT networks. *IEEE Access*, 12, 25623-25641. https://doi.org/10.1109/access.2024.3367357

Yadav, S., Hashmi, H., Vekariya, D., Khan, Z. A., & Fidelis, J. V. (2024). Mitigation of attacks *via* improved network security in IoT network environment using RNN. *Measurement: Sensors*, 32, 101046. https://doi.org/10.1016/j.measen.2024.101046

Yaras, S., & Dener, M. (2024). IoT-based intrusion detection system using new hybrid deep learning algorithm. *Electronics*, *13*(6), 1053. https://doi.org/10.3390/electronics13061053