

# Mohamed Faheej N

*Department of Computer Applications*

** mohamedfaheej.n2023@vitstudent.ac.in

# Mudassir Khan G

*Department of Computer Applications*

** mudassirkhan.g2023@vitstudent.ac.in

# Jashwanth Kumar S

*Department of Computer*

*Applications*

** jashwanthkumar.s2023@vitstudent.ac.in

***Abstract*—** **In today's fast-changing technological environment, advancements like smart cars, autonomous vehicles, and connected cars have become widespread. However, these developments have also made modern vehicles vulnerable to cyber threats due to their integration with external networks. Therefore, implementing intrusion detection systems (IDS) is vital to improve security in vehicle networks. This research presents a new approach for deploying IDS in the Internet of Vehicles, utilizing machine learning, ensemble learning, and transfer learning methods. By analyzing datasets such as Car-Hacking and CICIDS2017, the study showcases the effectiveness of IDS in identifying cyberattacks using recurrent neural networks (RNN) and hyper-parameter optimization techniques. These findings emphasize the importance of IDS in strengthening security in contemporary automotive systems.**

***Keywords*—Intrusion Detection System, RNN, Transfer learning, Ensemble learning, Internet of Vehicles.**

1. Introduction

Modern vehicles have evolved into network-controlled systems, predominantly relying on the Controller Area Network (CAN) bus for intra-vehicle communication, owing to advancements in Web of Things technology. However, the increased accessibility and interconnectedness of automotive networks have expanded the potential attack surface of contemporary vehicles, rendering them susceptible to various threats such as spoofing, fuzzing, and denial-of-service attacks. The vulnerability to cyberattacks is exacerbated by the lack of essential security measures in CAN packet handling. The aim of this research is to develop a system leveraging cutting-edge deep learning techniques such as Convolutional Neural Networks (CNN) and transfer learning. The proposed Intrusion Detection System (IDS) endeavors to achieve optimal learning models by training base learners with automotive cyber network traffic data and employing Particle Swarm Optimization for hyper-parameter optimization. Evaluation of the performance and efficacy of the proposed IDS system using publicly available vehicle network datasets is presented.

II. Proposed Framework

The goal of this project is to protect both internal and external vehicle networks by creating an Intrusion Detection System (IDS) that can detect different types of threats.

This IDS is suggested for use in both autonomous vehicles and external networks. It can be used to detect unusual CAN communications and raise alarms within the system. Additionally, it has the potential to be incorporated into gateways within external networks to detect and prevent malicious packets aimed at compromising vehicle security. This research suggests using a specialized Convolutional Neural Network (CNN) to identify various attack types in the Internet of Vehicles, alongside an IDS that utilizes transfer learning.

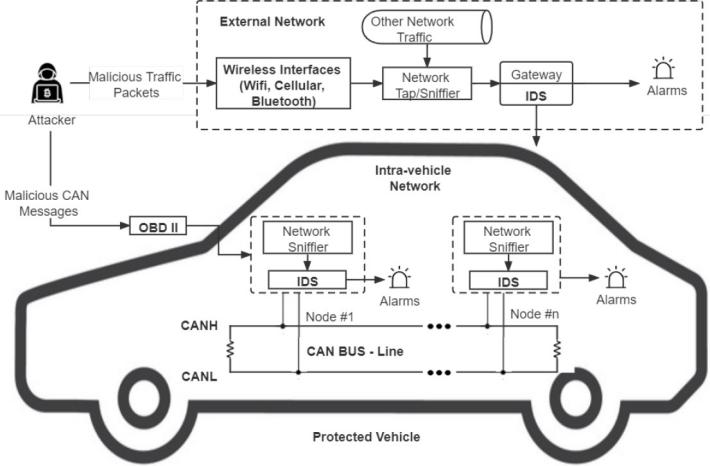


Fig. 1. Architecture of IDS-Protected Vehicle

Five leading CNN models (VGG16, VGG19, Xception, Inception, and InceptionResnet) are employed, trained on time-based segmented network data that has been transformed using quantile transform. These CNN models undergo enhancement through hyper-parameter optimization using Particle Swarm Optimization (PSO), and the ultimate detection models are screated through fusion and confidence averaging.

III. Data Description and Transformation

This study develops a system for autonomous vehicles using two datasets: the Car-Hacking dataset provides intra-vehicle data, including CAN (ID) and 8-bit values, covering techniques like gear spoofing, RPM spoofing, fuzzing, and DoS attacks. The CICIDS2017 dataset contributes external network data showcasing attack patterns such as brute force, DoS attacks, botnets, port scan attacks, and web attacks.

Pre-processing involves transforming raw network data into image formats and applying normalization techniques for consistency. Quantile normalization is chosen for its resilience against outliers compared to min-max normalization, which often results in excessively low values.

This technique recalibrates feature values based on a normal distribution, effectively managing outliers. The transformed data samples depend on timestamps and feature sizes. The Car-Hacking dataset's nine essential characteristics, each block of nine characteristics, and the cumulative feature values of 27 consecutive samples are transformed into 9 by 9 by 3 shape images.

Each transformed image is square and in color, resulting in a three-channel image (blue, red, and green). Similarly, the CICIDS2017 dataset, with 20 significant traits, transforms each picture into 20 by 20 by 3 color images. This dataset chunk consists of 60 consecutive data samples.

IV. CNN and knowledge transfer

CNN models are highly effective at tasks like image recognition and categorization because they can directly analyze images without needing separate feature extraction steps. These models are composed of convolutional, pooling, and fully-connected layers, which simplify data, generate output, and automatically extract feature patterns, respectively. Transfer learning involves transferring the learned weights of a deep neural network (DNN) model from one dataset to another, leveraging identified feature patterns.

It has shown success in various image classification tasks by utilizing specific characteristics from the top layers of CNN models and general patterns from their lower layers. Fine-tuning involves adjusting a few top layers while keeping most pre-trained model layers frozen to adapt to new data.

This study employs primary models such as VGG16, VGG19, Xception, Inception, and InceptionResnet, which have shown impressive performance in image classification tasks, especially after pre-training on the ImageNet dataset.

This dataset contains over a million images classified into 1,000 categories. In the ImageNet Challenge, VGG16 and VGG19 models exhibited strong performance, with VGG16 featuring five blocks of convolutional layers and three fully connected layers, while VGG19 included three additional convolutional layers..

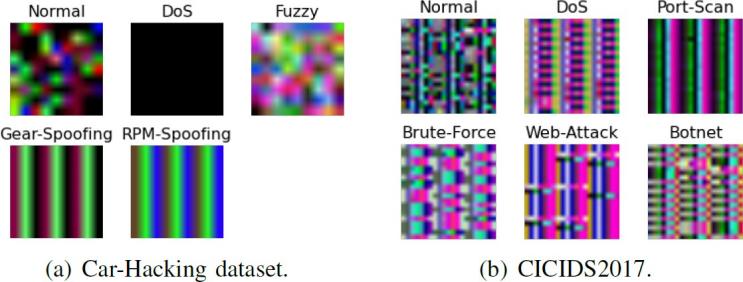


Fig. 3. Sample photos from two datasets, one for each class: a) The dataset on car hacking; b) CICIDS2017.

V. Proposed Ensemble Learning Model

Ensemble learning is employed to enhance efficiency by amalgamating multiple learning models into a single ensemble model. Its popularity in data analytics stems from the fact that ensembles often surpass individual learners in performance. Confidence averaging, a technique used in ensemble learning, combines the classification probability values of learners to identify the most confident group. This approach utilizes softmax layers in deep learning models to compute posterior probabilities for each class, with the final classification outcome being determined by selecting the class with the highest average confidence.



Fig. 4. softmax formula

VI. Perform Hyperparameter tuning

To enhance the performance of CNN models on the chosen datasets, hyperparameters must be fine-tuned and optimized. These hyperparameters include aspects like batch size, number of epochs, early stopping, and proportion of frozen layers, which are crucial during model training. Additionally, hyperparameters related to model creation, such as learning rate and dropout rate, also play a significant role. Hyperparameter optimization (HPO) is an automated process that utilizes optimization techniques to adjust these parameters. Particle swarm optimization (PSO) is a popular metaheuristic optimization method used for HPO. In PSO, particles collaborate to discover the optimal hyperparameter values by initializing their positions and velocities and updating them based on the global best position and their personal best position.

VII. Performance and Evaluation

1. *Experimental setup*

The studies utilized two Python packages, Scikit-learn and Keras. The Raspberry Pi 3 and Dell Precision 3630 were employed as replacements for the internet of cars hub computer and the automation driving level local mechanism, respectively, for training and evaluating the DL models. To prevent biased and overfitted outcomes, the proposed architecture underwent testing with the benchmark CICIDS2017 and Car-Hacking datasets. Performance assessment was conducted through fivefold cross-validation.

1. *Experiments and Results*

To achieve optimal results, Particle Swarm Optimization (PSO) was utilized to optimize the key hyperparameters of each basic CNN model. Hyperparameter Optimization (HPO) was specifically tailored to the CICIDS2017 dataset, as the initial configurations of the CNN models had already achieved nearly perfect precision on the Car-Hacking dataset. Subsequent to HPO, the enhanced CNN models were employed as base learners to construct ensemble models.

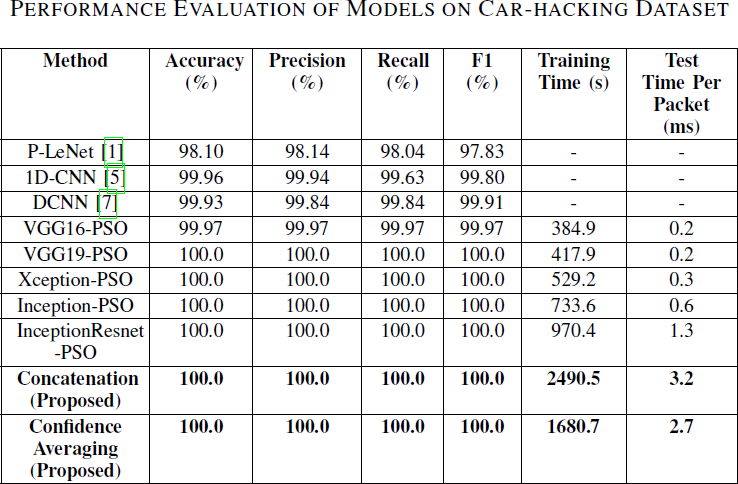
The results of utilizing the improved CNN models, as well as the proposed Car hacking and combined models on the CICIDS2017 dataset, are presented in Tables II and III. Except for VGG16, every enhanced basic CNN model achieved 100% accuracy and F1-scores, facilitated by discernible patterns in the modified images. Additionally, two other ensemble approaches concatenation and confidence averaging processes were employed.

Fig. 5. Model evaluation using the Car Hacking Dataset

.

After undergoing data transformation and optimization with PSO, the enhanced base CNN models for the CICIDS2017 dataset achieved impressive F1-scores ranging from 99.674% to 99.850%. Moreover, the confidence averaging ensemble model exhibited slightly superior performance compared to the concatenation model, achieving an F1-score of 99.925%.

These ensemble models surpassed the performance of more contemporary methods found in existing literature. Notably, the confidence averaging method required significantly less training time compared to the concatenation technique.

The higher performance of the suggested models, when compared to other state-of-the-art intrusion detection systems, highlights the effectiveness of CNN, transfer learning (TL), and hyperparameter optimization (HPO) techniques. Additionally, the average prediction timings of the suggested ensemble models indicated their suitability for real-time implementation in Internet of Vehicles (IoV) systems.

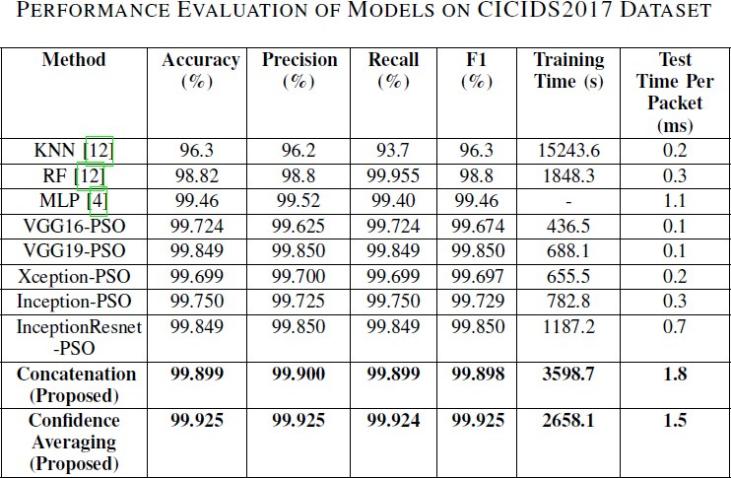


Fig. 6. Analyzing Models Using the CICIDS2017 Dataset

VIII. Conclusion

This project presents an Intrusion Detection System (IDS) architecture for securing Internet of Vehicles (IoV) against cyberthreats. It employs transfer learning and ensemble learning techniques, using CNN models to detect various attacks. A chunk-based data transformation method is proposed for processing automotive network traffic data. Experimental results on Car-Hacking and CICIDS2017 datasets show superior performance, with F1-scores of 100% and 99.925% respectively. Validation testing at the vehicle level confirms the system's effectiveness in real-world scenarios. Future work includes developing a virtual dynamic model to address concept drift in car network data and enable remote learning.

References

1. Yang, L., and Shami, A., "A Exchange Learning and Optimized CNN Based Interruption Location Framework for Web of Vehicles," arXiv preprint arXiv: pp. 2201.11812 (2022).
2. S. T. Mehedi, A. Anwar, Z. Rahman, and K. Ahmed, “Deep Trade Learning Based Impedances Disclosure System for Electric Vehicular Networks,” Sensors, vol. 21, no. 14, 2021.
3. L. Yang, A. Moubayed, and A. Shami, “MTH-IDS: A Multi-Tiered Crossover Interruption Discovery Framework for Web of Vehicles,” IEEE Web Things J., 2021.
4. Fanjiang, Y.Y.; Lee, C.C.; Du, Y.T.; Horng, S.J. Palm Vein Acknowledgment Based on Convolutional Neural Organize. Informatica 2021, 32, 687–708.
5. L. Yang and A. Shami, “A Lightweight Concept Float Discovery and Adjustment System for IoT Information Streams,” IEEE Web Things Mag., vol. 4, no. 2, pp. 96–101, 2021.
6. Thakkar, A., and Lohiya, R., "A survey on machine learning and profound learning points of view of IDS for IoT: later overhauls, security issues, and challenges," Files of Computational Strategies in Building, 28(4), 3211-3243 (2021).
7. Mehedi, S. T., Anwar, A., Rahman, Z., and Ahmed, K., "Profound exchange learning based interruption location framework for electric vehicular systems," Sensors, 21(14): pp. 4736 (2021).
8. Kim, D.Y.; Jung, M.; Kim, S. An web of vehicles (IoV) get to door plan considering the proficiency of the in-vehicle ethernet spine. Sensors 2021, 21, 98.
9. Yang, L.; Moubayed, A.; Shami, A. MTH-IDS: A Multi-Tiered Crossover Interruption Discovery Framework for Web of Vehicles. IEEE Web Things J. 2021, 9, 616–632.
10. Zhang, S.; Xie, X.; Xu, Y. A Viable Strategy to Assault Profound Learning Based Have Interruption Discovery Frameworks. Int. J. Netw. Secur. 2021, 23, 663–676.