Intrusion Detection System for Internet of Vehicles Using Optimized CNN

Under the guidance of

Prof. Jayalakshmi.P
Associate professor Sr. Grade 2, SCORE
Vellore Institute of Technology, Vellore
pjayalakshmi@vit.ac.in

by

Mohamed Faheej N
Department of Computer Application
Vellore Institute of Technology
Vellore, India.
mohamedfaheej.n2023@vitstudent.ac.in

Mudassir Khan G
Department of Computer Application
Vellore Institute of Technology
Vellore, India.
mudassirkhan.g2023@vitstudent.ac.in

Jashwanth Kumar S
Department of Computer Application
Vellore Institute of Technology
Vellore, India.
jashwanthkumar.s2023@vitstudent.ac.in

***Abstract*— In today's Technology Smart cars, driverless cars, and linked cars are just a few of the innovations that have surfaced in today's world of fast changing technology. It draws attention to how vulnerable modern vehicles are to cyberattacks due to their interconnectedness with the outside world, making the installation of intrusion detection systems necessary to improve security in vehicular networks. The research suggests a unique method for implementing IDS in the Internet of Vehicles that makes use of machine learning, ensemble learning, and transfer learning approaches. Using datasets like Car-Hacking and CICIDS2017, it uses RNN and hyper-parameter optimization techniques to show how successful the suggested IDS is in detecting cyber-attacks. In order improve security in modern car systems, the research aims to highlight how effective IDS is.**

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

I. Introduction

Modern cars have become network-controlled systems, mostly depending on the Controller Area Network bus for intra-vehicle communications, thanks to developments in Internet of Things (IoT) and Internet of Vehicles (IoV) technology. But the greater accessibility and connectedness of automotive networks has also enlarged the attack surface of modern cars, making them vulnerable to spoofing, fuzzy, and denial-of-service attacks, among other risks. The susceptibility to cyberattacks is increased by the absence of crucial security procedures in the handling of CAN packets. The goal of this research is to develop an intelligent model for an intrusion detection system (IDS) that takes use of recent developments in deep learning (DL) and machine learning (ML), particularly in the areas of ensemble learning, improved CNNs and transfer learning. The suggested IDS attempts to provide optimum learning models by training base learners with state-of-the-art CNN models on automobile network traffic data and utilizing Particle Swarm Optimization for hyper-parameter tuning. Analysis of the suggested IDS system's performance and effectiveness using freely accessible vehicle network datasets is provided.

The study's main contributions include:

- Introducing a novel framework using CNN, transfer learning, ensemble learning, and HPO for efficient cyber-attack detection in both internal and external networks.
- Proposing a data transformation technique to convert car network traffic data into visuals, aiding in the identification of various cyber-attack patterns.
- Comparing the performance of the proposed method with state-of-the-art approaches using benchmark cyber-security datasets reflecting data from both internal and external networks.

II. Proposed Framework

The goal of this endeavor is to safeguard both internal and external vehicular networks by developing an Intrusion Detection System (IDS) capable of recognizing various threats. This IDS is engineered to shield vehicles from both internal attacks via the On-Board Diagnostics II (OBD II) interface and external intrusions through wireless interfaces. It is proposed for deployment in both intra-vehicle networks (IVNs) and external networks. In IVNs, the IDS can be installed on the CAN-bus to detect abnormal CAN messages and issue alerts. Moreover, it can be integrated into gateways within external networks to identify and block malicious packets targeting vehicle breaches. This study proposes a specialized CNN for identifying different attack types in the Internet of Vehicles, along with an IDS based on transfer learning.

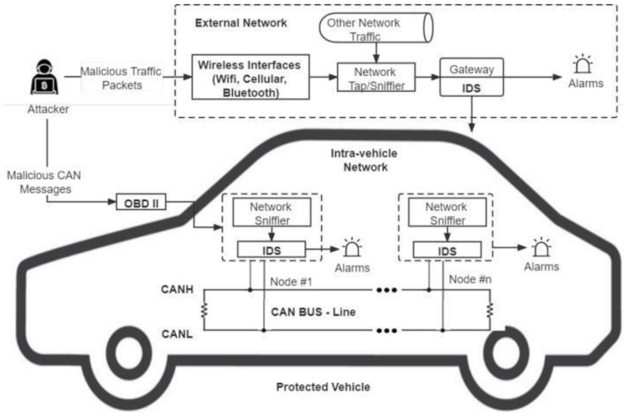


Fig. 1. Architecture of IDS-Protected Vehicle

It utilizes five top CNN models (VGG16, VGG19, Xception, Inception, and InceptionResnet) trained on time-based chunked network data transformed using quantile transform. The CNN models are improved by hyper-parameter optimization with Particle Swarm Optimization (PSO), and the final detection models are developed via fusion and confidence averaging.

III. Data Description and Transformation

The suggested IDS for both external vehicular networks and intra-vehicle networks (IVNs) is developed in this study using two datasets. Intra-vehicle data, such as CAN identification (ID) and the 8-bit data field of CAN packets, covering techniques such gear spoofing, RPM spoofing, fuzzy, and DoS, is provided by the Car-Hacking dataset. External network data is provided by the CICIDS2017 dataset, which displays attack patterns such as Brute force, DoS attack, Botnets, Port scan attacks and Web attacks. Pre-processing data include transforming raw network data into picture formats and applying normalization procedures to ensure consistency.

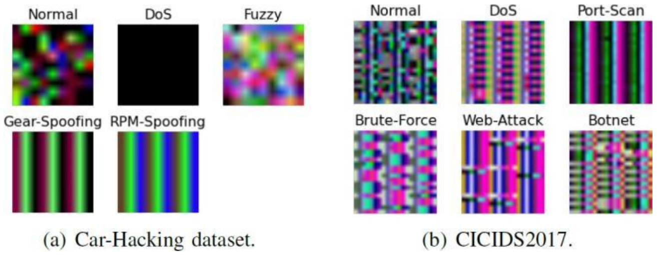
Quantile normalization is employed in the proposed architecture due to its resilience against outliers, unlike min-max normalization, which often yields excessively low values in the majority of data samples. This technique recalibrates all feature values based on a normal distribution, resulting in most variable values being within a few standard deviations of the median, effectively managing outliers. The data samples are transformed following data normalization. de- pending on the timestamps and size of the features of datasets for network traffic. The Car-Hacking dataset's nine essential characteristics (CAN ID and DATA[0]– DATA[7]), each block of nine characteristics, and the cumulative feature values of 27 consecutive samples (279 = 243) are transformed into a shape image. 9 by 9 by 3. Every transformed image is now square in color, creating a three-channel image (Blue, Red and Green). Likewise, the data set from CICIDS2017 yielded 20 noteworthy traits. Every picture is transformed into 20203 color images. There are 203 = 60 consecutive data samples in this dataset chunk. Network data may be kept as timestamps are utilized to create the first time-series correlations of the data samples.

IV. CNN and Transfer Learning

CNN models excel at image recognition and categorization tasks due to their ability to directly analyze images without requiring additional feature extraction. These models consist of convolutional, pooling, and fully-connected layers, which simplify data, produce output, and automatically extract feature patterns, respectively.

Transfer learning involves transferring the weights of a DNN model from one dataset to another, leveraging identified feature patterns. TL has proven successful across various image classification tasks by utilizing specific characteristics from the top layers of CNN models and general patterns from their lower layers. Fine-tuning entails unfreezing a few top layers and freezing most of the pre-trained model layers to adapt to new data.

The primary models used in this study include VGG16, VGG19, Xception, Inception, and InceptionResnet. These models have demonstrated impressive performance in image classification tasks, particularly after pre-training on the ImageNet dataset, which contains over a million images categorized into 1,000 classes. In the ImageNet Challenge, the VGG16 and VGG19 models outperformed each other, with VGG16 featuring five blocks of convolutional layers and three fully connected layers, while VGG19 included three additional convolutional layers.



(a) Car-Hacking dataset.

(b) CICIDS2017.

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

V. Proposed Ensemble Learning Model

To increase efficiency, ensemble learning creates an ensemble model by combining many learning models. The reason for its widespread usage in data analytics is that ensembles frequently outperform individual learners. One technique, confidence averaging, combines learners' categorization probability values to identify the most confident group. This method uses softmax layers in DL models to generate posterior probabilities for each class; the final classification result is determined by selecting the class with the highest average confidence.

$$\text{Softmax}(\mathbf{z})_i = \frac{e^{\mathbf{z}_i}}{\sum_{j=1}^{C} e^{\mathbf{z}_j}}$$

Fig. 4. softmax formula

VI. Hyper-Parameter Optimization (HPO)

Hyperparameters need to be tuned and improved in order to improve CNN models' performance on the selected datasets. Some of these hyperparameters are relevant to training the model such batch size, number of epochs, early stopping, and frozen layer proportion they are also related to creating the model, like frozen layer proportion, learning rate, and dropout rate. Hyperparameter optimization (HPO) is an automated procedure that uses optimization methods to adjust these parameters. PSO, or particle swarm optimization, is a well-liked metaheuristic optimization technique for HPO in which particles cooperate to find the best hyperparameter values. PSO initializes the location and velocity of each particle, and updates its velocities according to both the global best position and its personal best position.

VII. Performance and Evaluation

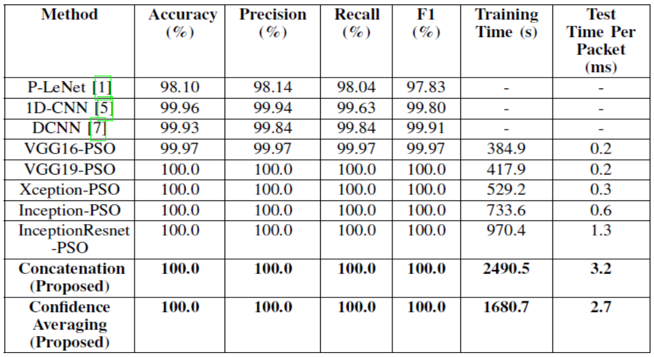
A. *Experimental setup*

Scikit-learn and Keras are two Python packages that were used in the studies. The Dell Precision 3630 and Raspberry Pi 3, which stand in for an IoV central server computer and a vehicle-level local machine, respectively, were used to train and assess the DL models. In order to avoid biased and over-fitted results, the suggested architecture was tested using the benchmark CICIDS2017 and Car-Hacking datasets. Performance was evaluated using fivefold cross-validation.

B. *Experiments and Results*

To get the best results, PSO was used to optimize each basic CNN model's key hyperparameters. Given that CNN models with default parameters had previously achieved almost 100% accuracy on the Car-Hacking dataset, HPO was specially applied to the CICIDS2017 dataset. The improved CNN models were used as basis learners to build ensemble models after HPO.

Performance Evaluation of Models on Car-hacking Dataset



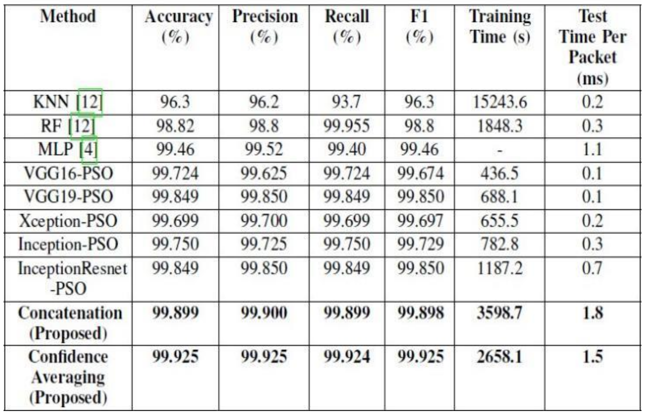
Method	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)	Training Time (s)	Test Time Per Packet (ms)
P-LeNet [1]	98.10	98.14	98.04	97.83	-	-
1D-CNN [5]	99.96	99.94	99.63	99.80	-	-
DCNN [7]	99.93	99.84	99.84	99.91	-	-
VGG16-PSO	99.97	99.97	99.97	99.97	384.9	0.2
VGG19-PSO	100.0	100.0	100.0	100.0	417.9	0.2
Xception-PSO	100.0	100.0	100.0	100.0	529.2	0.3
Inception-PSO	100.0	100.0	100.0	100.0	733.6	0.6
InceptionResnet -PSO	100.0	100.0	100.0	100.0	970.4	1.3
Concatenation (Proposed)	**100.0**	**100.0**	**100.0**	**100.0**	**2490.5**	**3.2**
Confidence Averaging (Proposed)	**100.0**	**100.0**	**100.0**	**100.0**	**1680.7**	**2.7**

Fig. 5. Model evaluation using the Car Hacking Dataset.

The outcomes of testing the proposed ensemble models and the improved CNN models on the CICIDS2017 and Car-Hacking datasets are shown in Tables II and III. With the exception of VGG16, every enhanced basic CNN model attained 100% accuracy and F1-scores, made possible by discernible patterns in the altered images. Two more ensemble approaches that were used were concatenation and confidence averaging processes.

The improved base CNN models for the CICIDS2017 dataset achieved high F1-scores ranging from 99.674% to 99.850% after undergoing data transformation and PSO. Furthermore, with an F1-score of 99.925%, the confidence averaging ensemble model performed somewhat better than the concatenation model. The performance of these ensemble models outperformed more contemporary methods seen in the literature. Interestingly, compared to the concatenation technique, the confidence averaging method needed substantially less training time overall. When compared to other cutting-edge intrusion detection systems, the suggested models' higher performance demonstrated the effectiveness of the CNN, TL, and HPO techniques. Furthermore, the suggested ensemble models' average prediction timings showed that they were appropriate for use in real-time IoV system implementation.

Performance Evaluation of Models on CICIDS2017 Dataset



Method	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)	Training Time (s)	Test Time Per Packet (ms)
KNN [12]	96.3	96.2	93.7	96.3	15243.6	0.2
RF [12]	98.82	98.8	99.955	98.8	1848.3	0.3
MLP [4]	99.46	99.52	99.40	99.46	-	1.1
VGG16-PSO	99.724	99.625	99.724	99.674	436.5	0.1
VGG19-PSO	99.849	99.850	99.849	99.850	688.1	0.1
Xception-PSO	99.699	99.700	99.699	99.697	655.5	0.2
Inception-PSO	99.750	99.725	99.750	99.729	782.8	0.3
InceptionResnet -PSO	99.849	99.850	99.849	99.850	1187.2	0.7
Concatenation (Proposed)	**99.899**	**99.900**	**99.899**	**99.898**	**3598.7**	**1.8**
Confidence Averaging (Proposed)	**99.925**	**99.925**	**99.924**	**99.925**	**2658.1**	**1.5**

Fig. 6. Evaluation Of Models On CICIDS2017 Dataset

VIII. Conclusion

In order to defend IoV systems from cyberthreats, this research presents an IDS architecture based on transfer learning and ensemble learning. To identify different types of attacks, it makes use of most effective CNN models and suggests a chunk-based data transformation method for handling traffic data from automobile networks. Utilizing the Car-Hacking and CICIDS2017 datasets, the experimental findings demonstrate better performance than previous methods, with F1-scores of 100% and 99.925%. The efficiency of the IDS in real-time networks is validated by testing conducted on equipment at the vehicle level. The goal of future research is to create an online adaptive model that can facilitate online learning and handle concept drift in automobile network data.

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 Recognition Based on Convolutional Neural Network. *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.

1.

2.

3.

Signature (Students)

Signature (Guide)