Intrusion Detection System for Internet of Vehicles using Optimized CNN

# 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 world rapidly evolving technological landscape, various advancements such as electric vehicles, autonomous vehicles, and connected vehicles have emerged. It highlights the vulnerability of modern vehicles, interconnected with the external world, to cyber threats, necessitating the deployment of Intrusion Detection Systems (IDSs) to enhance security in vehicular networks. The paper proposes a novel approach utilizing Transfer Learning, machine learning, and ensemble learning techniques to implement IDS in the Internet of Vehicles (IoV). It employs Recurrent Neural Network (RNN) and hyper-parameter optimization techniques and demonstrates the effectiveness of the proposed IDS in detecting cyber-attacks using datasets such as Car-Hacking and CICIDS2017. The research aims to emphasize the efficacy of the IDS in bolstering cybersecurity in modern vehicle systems**

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

1. Introduction

Modern vehicles, driven by advancements in Internet of Things (IoT) and Internet of Vehicles (IoV) technologies, have become network-controlled, with intra-vehicle communications predominantly facilitated by the Controller Area Network (CAN) bus. However, the increased identity and accessibility of automotive networks have expanded the cyber-attack surface of contemporary automobiles, making them vulnerable to various attacks such as DoS, fuzzy, and spoofing attacks. The absence of fundamental security safeguards in processing CAN packets heightens the risk of cyber threats. Leveraging advancements in machine learning (ML) and deep learning (DL), this research proposes an intelligent IDS model based on enhanced Convolutional Neural Networks (CNNs), transfer learning, and ensemble learning techniques. By training base learners using state-of-the-art CNN models on car network traffic data and employing Particle Swarm Optimization (PSO) for hyper-parameter optimization, the proposed IDS aims to provide optimal learning models. Evaluation using open-source vehicle network datasets demonstrates the efficacy and efficiency of the proposed IDS system.

The study's main contributions include:

1. Introducing a novel framework using CNN, transfer learning, ensemble learning, and HPO for efficient cyber-attack detection in both internal and external networks.
2. Proposing a data transformation technique to convert car network traffic data into visuals, aiding in the identification of various cyber-attack patterns.
3. 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.

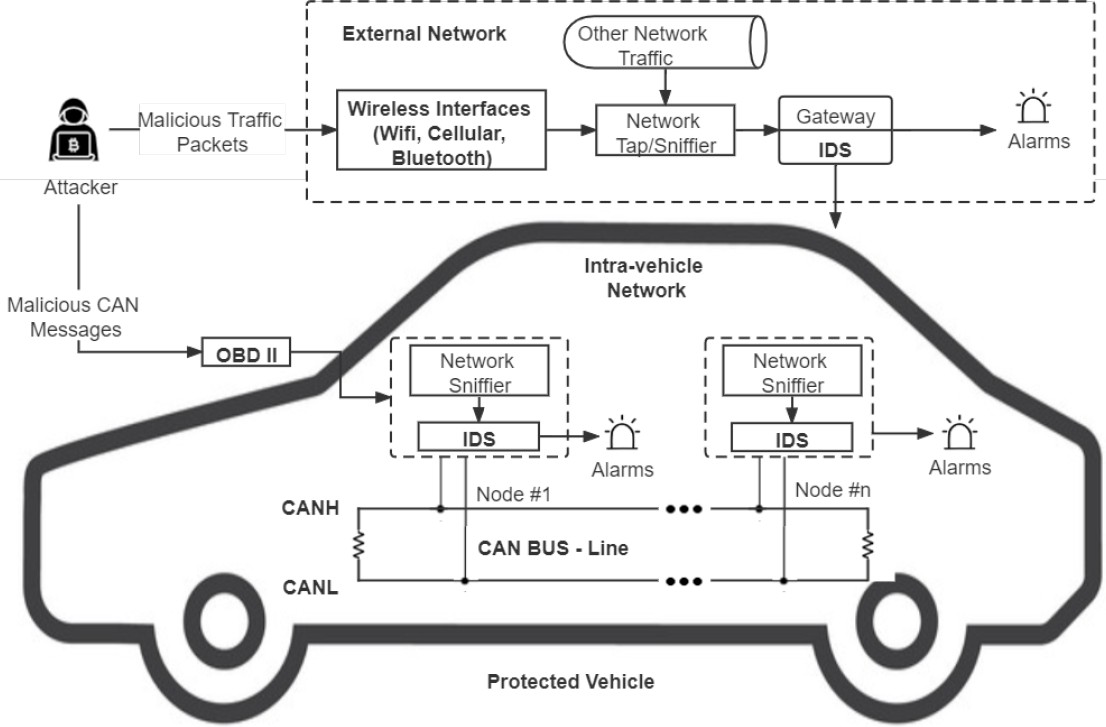


Fig. 1. Architecture of IDS-Protected Vehicle

1. Proposed Framework

This effort aims to defend both internal and external vehicular networks by creating an IDS capable of identifying various threats. The IDS is designed to protect vehicles from both internal attacks via the On-Board Diagnostics II (OBD II) interface and external assaults through wireless interfaces. It is proposed to be implemented in both intra-vehicle networks (IVNs) and external networks. The IDS can be installed on the

CAN-bus in IVNs to detect unusual CAN messages and generate alarms. Additionally, it can be integrated into gateways in external networks to detect and filter malicious packets aimed at breaching vehicles. This research proposes a unique optimized CNN and transfer learning-based IDS to identify different types of attacks in IoV systems. The proposed IDS framework utilizes quantile transform to convert time-based chunked network data into images, which are then used to train five cutting-edge CNN models (VGG16, VGG19, Xception, Inception, and InceptionResnet). Hyper-parameter optimization using Particle Swarm Optimization (PSO) is employed to optimize the CNN models, and ensemble techniques such as confidence averaging and concatenation are used to construct final detection models.

III. Data Description and Transformation

In this study, two datasets are utilized to develop the proposed IDS for both intra-vehicle networks (IVNs) and external vehicular networks. The Car-Hacking dataset provides intra-vehicle data, including CAN identification (ID) and 8-bit data field of CAN packets, covering attacks like DoS, fuzzy, gear spoofing, and RPM spoofing. The CICIDS2017 dataset offers external network data, showcasing attack patterns such as DoS assaults, port-scan attacks, brute-force attacks, web attacks, and botnets. Data preprocessing involves converting original network data into image forms, with normalization techniques applied for 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 normalisation. de- pending on the timestamps and size of the features of datasets for network traffic. As it has done for the Car-Hacking dataset 9 key characteristics (CAN ID and DATA[0]–DATA[7]), each of which block of 9 characteristics and 27 consecutive samples (279 = 243) [8] feature values combined) are converted into a shape picture. 9x9x3 [14].

Each modified picture is a square colour as a result. [9] a three-channel picture (red, green, and blue). Similarly, the CICIDS2017 dataset that produced 20 significant characteristics Each image from is converted to 20203 colour images. This dataset’s chunk has 203 = 60 consecutive data. samples. Since the timestamps are used to produce the photos the initial time-series correlations of the data samples, network data can be retained.

 IV. CNN and Transfer Learning

CNN models excel at image classification and recognition tasks by directly processing images, avoiding the need for additional feature extraction. They comprise convolutional, pooling, and fully-connected layers, which automatically extract feature patterns, reduce data complexity, and generate output.

Transfer Learning (TL) involves transferring a DNN model's weights from one dataset to another, leveraging learned feature patterns. TL has been successful in various picture classification tasks, utilizing specific characteristics from the top layers of CNN models and generic patterns from the bottom layers. Fine-tuning involves freezing most pre-trained model layers while unfreezing a few top layers to adapt to new data.In this work, VGG16, VGG19, Xception, Inception, and InceptionResnet are chosen as base models. These models have shown outstanding performance in image classification tasks, especially after pre-training on the ImageNet dataset, which consists of over a million photos in 1,000 classes. VGG16 and VGG19 models achieved decreased error rates in the ImageNet Challenge, with VGG19 having three additional convolutional layers compared to VGG16's five blocks of convolutional layers and three fully connected layers.

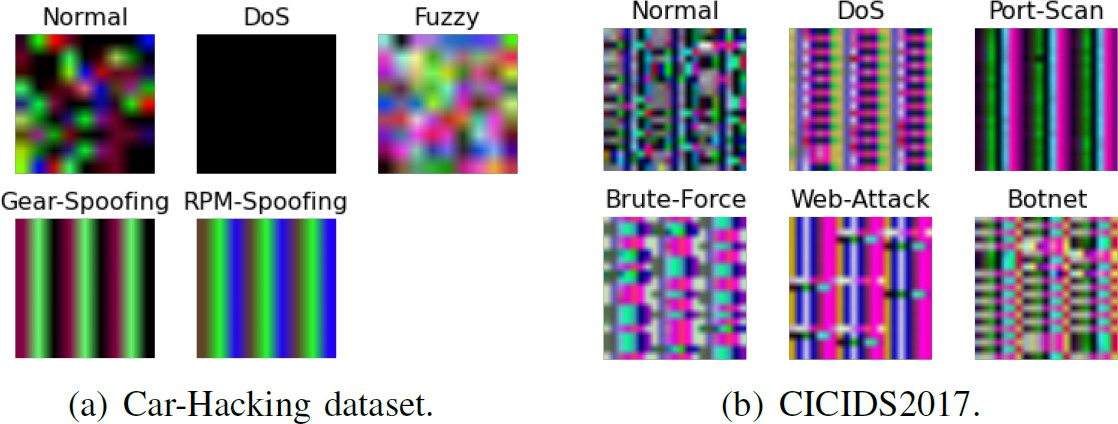


Fig. 3. Sample images of each class in two datasets: a) Car-Hacking dataset;

b) CICIDS2017.

V. Proposed Ensemble Learning Model

Ensemble learning combines multiple learning models to create an ensemble model, boosting efficiency. It's widely used in data analytics because ensembles often outperform individual learners. One technique, confidence averaging, combines learners' categorization probability values to identify the most confident group. In this approach, softmax layers in DL models produce posterior probabilities for each class, and the class with the highest average confidence is chosen as the final categorization outcome.

VI. Performance and Evaluation

To enhance the performance of CNN models on the chosen datasets, hyperparameters must be adjusted and optimized. These hyperparameters include those related to model creation, such as frozen layer proportion, learning rate, and dropout rate, as well as those for model training, such as early stopping, number of epochs, and batch size. Hyperparameter Optimization (HPO) is an automated process that fine-tunes these parameters using optimization techniques. Particle Swarm Optimization (PSO) is a popular metaheuristic optimization method used for HPO, where particles in a swarm exchange information to determine optimal hyperparameter values. Each particle in PSO is initialized with a position and velocity, and their velocities are updated based on their own best position and the global best position.

Fig. 4. softmax formula

VII. Performance and Evaluation

1. *Experimental setup*

The experiments were conducted using Python libraries, specifically Scikit-learn and Keras. The DL models were evaluated on a Raspberry Pi 3 and trained on a Dell Precision 3630, representing an IoV central server machine and a vehicle-level local machine, respectively. The proposed architecture was tested using the benchmark CICIDS2017 and Car-Hacking datasets, with performance assessed using fivefold cross-validation to prevent biased and over-fitted findings.

1. *Experiments and Results*

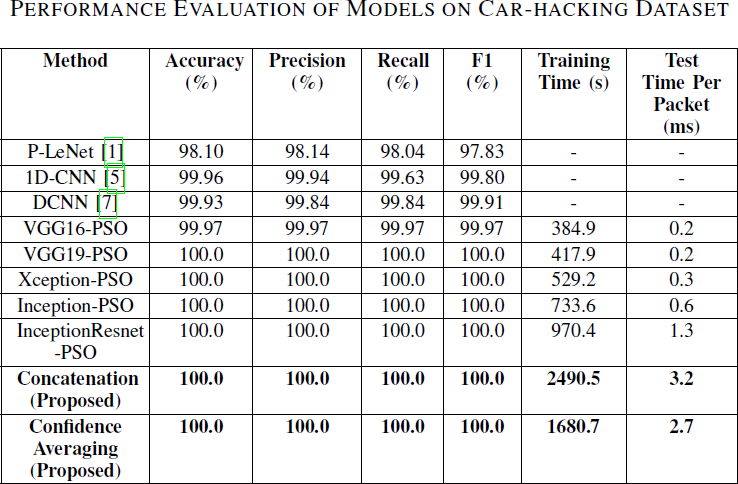
The primary hyperparameters of each basic CNN model were optimized using PSO to achieve the best performance. HPO was specifically applied to the CICIDS2017 dataset, given that CNN models with default settings already achieved close to 100% accuracy on the Car-Hacking dataset. Following HPO, ensemble models were constructed using the optimized CNN models as base learners. Tables II and III present the results of testing the enhanced CNN models and the suggested ensemble models on the Car-Hacking and CICIDS2017 datasets. Except for VGG16, all improved basic CNN models achieved 100% accuracy and F1-scores, facilitated by distinct patterns in the modified pictures. Concatenation and confidence averaging procedures, two ensemble methodologies, were also utilized. Following data transformation and PSO, the optimized base CNN models for the CICIDS2017 dataset attained high F1-scores ranging from 99.674% to 99.850%. Additionally, the confidence averaging ensemble model slightly outperformed the concatenation model, achieving an F1-score of 99.925%. These ensemble models exhibited better performance than recent approaches in the literature. Notably, the confidence averaging method required significantly less training time overall than the concatenation strategy. The efficacy of CNN, TL, and HPO approaches was evident in the superior performance of the proposed models compared to other cutting-edge IDSs. Additionally, the average prediction times of the proposed ensemble models demonstrated their suitability for real-time implementation in IoV systems.

Fig. 5. Evaluation of models on car hacking dataset.

VIII. Conclusion

References

1. Yang, L., and Shami, A., "A Transfer Learning and Optimized CNN Based Intrusion Detection System for Internet of Vehicles," arXiv preprint arXiv: pp. 2201.11812 (2022).
2. S. T. Mehedi, A. Anwar, Z. Rahman, and K. Ahmed, “Deep Transfer Learning Based Intrusion Detection System for Electric Vehicular Networks,” Sensors, vol. 21, no. 14, 2021.
3. L. Yang, A. Moubayed, and A. Shami, “MTH-IDS: A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles,” IEEE Internet Things J., 2021.
4. L. Yang et al., ”Multi-Perspective Content Delivery Networks Security Framework Using Optimized Unsupervised Anomaly Detection,” IEEE Trans. Netw. Serv. Manag., 2021.
5. L. Yang and A. Shami, “A Lightweight Concept Drift Detection and Adaptation Framework for IoT Data Streams,” IEEE Internet Things Mag., vol. 4, no. 2, pp. 96–101, 2021.
6. Thakkar, A., and Lohiya, R., "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges," Archives of Computational Methods in Engineering, 28(4), 3211-3243 (2021).
7. Mehedi, S. T., Anwar, A., Rahman, Z., and Ahmed, K., "Deep transfer learning based intrusion detection system for electric vehicular networks," Sensors, 21(14): pp. 4736 (2021).
8. Kim, D.Y.; Jung, M.; Kim, S. An internet of vehicles (IoV) access gateway design considering the efficiency of the in-vehicle ethernet backbone. *Sensors* 2021, *21*, 98.
9. Yang, L.; Moubayed, A.; Shami, A. MTH-IDS: A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles. *IEEE Internet Things J.* 2021, *9*, 616–632.
10. Latif, S.; e Huma, Z.; Jamal, S.S.; Ahmed, F.; Ahmad, J.; Zahid, A.; Dashtipour, K.; Muhmmad, U.A.; Ahmad, M.; Abbasi, Q.H. Intrusion Detection Framework for the Internet of Things using a Dense Random Neural Network. *IEEE Trans. Ind. Inform.* 2021, 1–10.

Fig. 2. CNN based IDS-Framework

of which block of 9 characteristics and 27 consecutive samples (279 = 243) [8] feature values combined) are converted into a shape picture. 9x9x3 [14]. Each modified picture is a square color as a result. [9] a three-channel picture (red, green, and blue). Similarly, the CICIDS2017 dataset that produced 20 significant characteristics Each image from is converted to 20203 color images. This dataset’s chunk has 203 = 60 consecutive data. samples. Since the timestamps are used to produce the photos the initial time-series correlations of the data samples, network data can be retained. [**?**]

1. CNN and Transfer Learning

DL models like CNN are frequently employed in picture classification and recognition issues. Without the need for ad- ditional feature extraction and data reconstruction procedures,

the images can be immediately entered into CNN models. Convolutional, pooling, and fully-connected layers make up the majority of layers in a CNN. The feature patterns of images can be automatically retrieved by convolution operations in convolutional layers. Local correlations can be used in pooling layers to minimize data complexity without sacrificing crucial information and prevent over-fitting. All features are connected through fully connected layers, which also produce the output.

[10] Transfer Learning (TL) is the process of moving a Deep Neural Network (DNN) model’s weights from one dataset to another for DL models. [11]

Numerous picture types have successfully used the TL approach. processing activities This is due to the learnt feature patterns. Only the features learnt by the top layers of CNN models are specific characteristics for a given dataset, whereas the features learned by the bottom layers of CNN models are often generic patterns that are relevant to many different jobs . As a result, the CNN models’ base layers may be used directly to various applications. Fine-tuning may be applied to the TL process of DL models to increase its efficacy. Most of the pre- trained model’s layers are frozen (i.e., their weights are kept) during fine-tuning, while a few of the top layers are unfrozen to retrain the model on fresh data. [8]

We have chosen VGG16, VGG19, Xception, Inception, and InceptionResnet as the basis models for the proposed system. Considering the effectiveness of CNN models in the ma- jority of picture categorization issues, These CNN models have shown excellent performance on a variety of picture classification tasks after being pre-trained on the ImageNet dataset. A benchmark image processing dataset with more than a million photos in 1,000 classes is called ImageNet. On the ImageNet Challenge, the 16-layer (VGG16) and 19-layer (VGG19) VGG16 models suggested in had a decreased error rate of 7.3 percentage. While the VGG19 design adds three more convolutional layers, the VGG16 architecture consists of five blocks of convolutional layers and three fully linked

layers.

1. Proposed Ensemble Learning Model

Ensemble learning is a method that combines several using fundamental learning models to build an ensemble model increased efficiency. The use of ensemble learning is common in data analytics issues because a combination of several

Learners typically outperform solitary learners. An technique to ensemble learning called confidence averaging combines the basic learners’ categorization probability values. To identify the group with the greatest confidence level. In Softmax layers in DL models can produce a posterior probability, list that includes each class’s categorization confidence. [11] For each class, the confidence averaging approach determines the average classification probability of base learners. the class label with the highest average confidence is returned. As the ultimate categorization outcome.



Fig. 4. softmax formula

1. Hyper-Parameter Optimization (HPO)

To further improve the foundation models’ fit to the chosen datasets and enhance the performance of the models, and the hyper-parameters CNN models must be adjusted and improved. CNN models, like other DL models, have a sub- stantial how many hyper-parameters need to be tuned. This set of hyperparameters can be categorized as hyper-parameters for model creation. and hyper-parameters for model training. Model-design The hyper-parameters that need to be set are hyper-parameters. when developing a model. The suggested TL structure includes The number or range of the model- design hyper-parameters can be frozen layer proportion, learning rate, and dropout rate. Hyper-parameters for model training, on the other hand are employed to balance model performance and training pace, an early stop, the number of epochs, and the batch size patience.

The structure, potency, and efficiency of CNN models are directly influenced by the aforementioned hyper-parameters. HPO is an automated procedure that uses optimization ap- proaches to fine-tune the hyper-parameters of ML or DL models [10]. PSO is a popular metaheuristic optimization methodology for HPO issues that determines optimal hyper- parameter values through information exchange and teamwork among the particles in a swarm [10]. Each member of the group is initialized with a location xi and velocity vi at the beginning of PSO. Each particle’s velocity is updated depending on its own most recent best position, pi, and the most recent global ideal position, p.

1. Performance and Evaluation
2. *Experimental setup*

Python libraries called Scikit-learn and Keras were used to carry out the studies. The suggested DL models were evaluated on a Raspberry Pi 3 with a BCM2837B0 64-bit CPU and 1 GB of memory and trained on a Dell Precision 3630 with an i7-8700 processor and 16 GB of memory, which

represented an IoV central server machine and a vehicle- level local machine, respectively. As stated in Section III- B, the proposed architecture is tested using the benchmark CICIDS2017 and Car-Hacking datasets for vehicle network security. The suggested model is assessed using fivefold cross- validation, which can prevent biassed and over-fitted findings. [18]

On the other hand, as network traffic data is typically very unbalanced and only contains a tiny proportion of attack samples, performance is assessed using four separate metrics: accuracy, precision, recall, and F1- scores. Additionally, model training time on the server-level machine and model testing time on the vehicle-level machine are tracked and compared to assess the efficacy of the proposed strategy.

1. *Experiments and Results*

The primary hyper-parameters of each basic CNN model in the suggested framework were all tuned using PSO to provide the best models possible. The HPO technique was only used for the CICIDS2017 dataset because CNN models with default hyperparameter settings can already attain accuracy levels of close to 100 percentage on the Car-Hacking dataset.

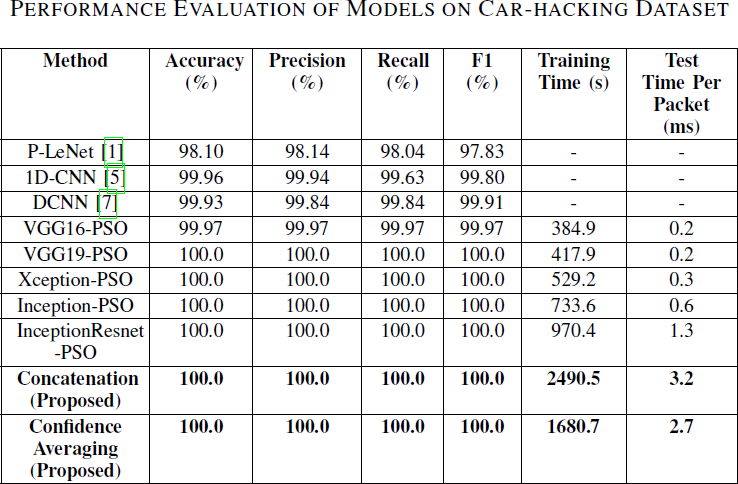


Fig. 5. Evaluation of models on car hacking dataset.

The starting search space and the ideal hyperparameter settings. Following HPO, the suggested ensemble models were built using the optimized CNN models as foundation learners. Tables II and III, respectively, present the findings of testing the enhanced CNN models and the suggested ensemble models on the Car-Hacking and CICIDS2017 datasets. Table II demonstrates that, with the exception of VGG16, all improved basic CNN models attain 100 percentage accuracy and F1- scores. This is mostly due to the fact that the modified pictures displayed in Fig. 3 make it easy to discern between the normal and attack patterns in the Car-Hacking dataset. Concatenation and confidence averaging procedures, two ensemble method- ologies, can also Follows, data transformation and PSO, the optimized base CNN models for the CICIDS2017 dataset attain high F1-scores of 99.674 percent to 99.850 percent, as shown in fig 6. Additionally, the suggested confidence

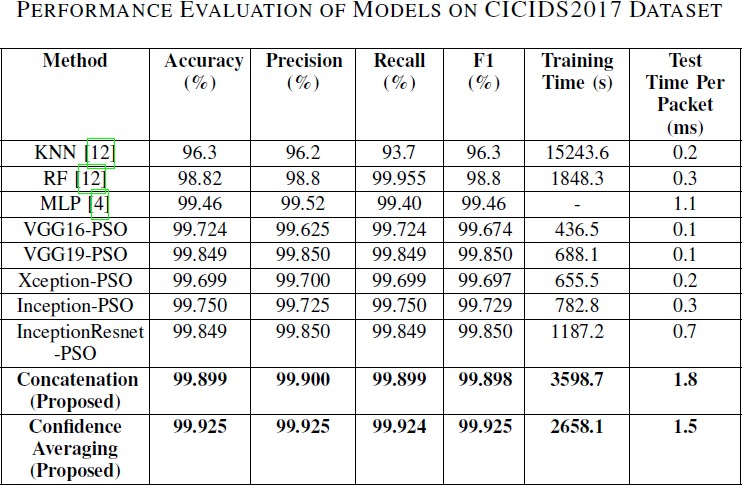


Fig. 6. EVALUATION OF MODELS ON CICIDS2017 DATASET

averaging ensemble model has the greatest F1-score of 99.925 percent, just edging out the concatenation model’s F1-score of 99.899 percent. Additionally, the two ensemble models perform better than other recent approaches in the literature. Additionally, the confidence averaging method requires sig- nificantly less training time overall [**?**] than the concatenation strategy. The advantages of utilizing CNN, TL, and HPO approaches are supported by the suggested models’ superior performance when measured against other cutting-edge IDSs.

Additionally, the average length of the proposed ensemble models’ test and prediction cycles Each packet on the Rasp- berry Pi computer is running at a modest volume, according to fig 5 and 6, ranging from 1.5 ms to 3.2 ms. As the demand for real-time in vehicle anomaly detection systems about 10 ms for each packet’s inspection, the low The presented models’ prediction times demonstrate their viability. on real-time IoV

systems of implementing the suggested IDS.

1. Conclusion

The cyberthreats to IoV systems are considerably growing as modern automobiles become more linked. This paper suggested a transfer learning and ensemble learning-based IDS framework that employs optimal CNN models to recognize various forms of assaults in IoV systems in order to safeguard connected cars from being infiltrated by cyber- attacks. A chunk-based data transformation technique is also suggested for converting car network traffic data into picture data for CNN models. The Car-Hacking and CICIDS2017 datasets, which contain intra-vehicle and external network data, respectively, are used to test the proposed IDS. The experimental findings demonstrate that, when compared to existing state-of-the-art approaches on the two benchmark datasets, the proposed IDS framework can more successfully identify different types of attacks with higher F1-scores of 100 percent and 99.925 percent. Additionally, the model testing outcomes on a machine at the vehicle level demonstrate the

viability of the suggested IDS in real-time vehicle networks. Future research will build on this framework to create an

online adaptive model that can solve concept drift in time- series car network data and accomplish online learning.

References

1. Yang, L., and Shami, A., "A Transfer Learning and Optimized CNN Based Intrusion Detection System for Internet of Vehicles," arXiv preprint arXiv: pp. 2201.11812 (2022).
2. S. T. Mehedi, A. Anwar, Z. Rahman, and K. Ahmed, “Deep Transfer Learning Based Intrusion Detection System for Electric Vehicular Networks,” Sensors, vol. 21, no. 14, 2021.
3. L. Yang, A. Moubayed, and A. Shami, “MTH-IDS: A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles,” IEEE Internet Things J., 2021.
4. L. Yang et al., ”Multi-Perspective Content Delivery Networks Security Framework Using Optimized Unsupervised Anomaly Detection,” IEEE Trans. Netw. Serv. Manag., 2021.
5. L. Yang and A. Shami, “A Lightweight Concept Drift Detection and Adaptation Framework for IoT Data Streams,” IEEE Internet Things Mag., vol. 4, no. 2, pp. 96–101, 2021.
6. Thakkar, A., and Lohiya, R., "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges," Archives of Computational Methods in Engineering, 28(4), 3211-3243 (2021).
7. Mehedi, S. T., Anwar, A., Rahman, Z., and Ahmed, K., "Deep transfer learning based intrusion detection system for electric vehicular networks," Sensors, 21(14): pp. 4736 (2021).
8. Kim, D.Y.; Jung, M.; Kim, S. An internet of vehicles (IoV) access gateway design considering the efficiency of the in-vehicle ethernet backbone. *Sensors* 2021, *21*, 98.
9. Yang, L.; Moubayed, A.; Shami, A. MTH-IDS: A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles. *IEEE Internet Things J.* 2021, *9*, 616–632.
10. Latif, S.; e Huma, Z.; Jamal, S.S.; Ahmed, F.; Ahmad, J.; Zahid, A.; Dashtipour, K.; Muhmmad, U.A.; Ahmad, M.; Abbasi, Q.H. Intrusion Detection Framework for the Internet of Things using a Dense Random Neural Network. *IEEE Trans. Ind. Inform.* 2021, 1–10.
11. Zhang, S.; Xie, X.; Xu, Y. A Practical Method to Attack Deep Learning Based Host Intrusion Detection Systems. *Int. J. Netw. Secur.* 2021, *23*, 663–676.
12. Thapa, K.N.K.; Duraipandian, N. Malicious Traffic classification Using Long Short-Term Memory (LSTM) Model. *Wirel. Pers. Commun.* 2021, *119*, 2707–2724.
13. Latif, S.; Driss, M.; Boulila, W.; Jamal, S.S.; Idrees, Z.; Ahmad, J. Deep Learning for the Industrial Internet of Things (IIoT): A Comprehensive Survey of Techniques, Implementation Frameworks, Potential Applications, and Future Directions. *Sensors* 2021, *21*, 7518.
14. Bai, J.; Ding, B.; Xiao, Z.; Jiao, L.; Chen, H.; Regan, A.C. Hyperspectral Image Classification Based on Deep Attention Graph Convolutional Network. *IEEE Trans. Geosci. Remote Sens.* 2021, *60*, 5504316.
15. 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.