RESEARCH ARTICLE OPEN ACCESS

ATTENTION DRIVEN CNN-TRANSFORMER FRAMEWORK FOR INTRUSION DETECTION IN INTERNET OF VEHICLES

Mugeshkumar S[1], Thulasimani K[2]
[1] Department of Computer Science and Engineering, Government College of Engineering, Tirunelveli, TamilNadu, India
E-mail address: mugesh12052002@gmail.com
[2] Department of Computer Science and Engineering, Government College of Engineering, Tirunelveli, TamilNadu, India
E-mail address: thulasimani@gcetly.ac.in

--************************--

Abstract:

The Internet of Vehicles (IoV) has emerged as a vital enabler of Intelligent Transportation Systems (ITS), offering seamless communication between vehicles, roadside units, and cloud servers. By enabling real-time data exchange, IoV improves traffic monitoring, collision avoidance, fleet management, and autonomous driving. However, the openness of wireless vehicular communication makes IoV networks highly vulnerable to cyber threats such as denial-of-service (DoS), probing, spoofing, and malware propagation. These threats compromise service availability and data integrity, ultimately endangering human safety. Thus, intrusion detection becomes a crucial layer of defense. Traditional intrusion detection methods based on machine learning, such as Support Vector Machines (SVM), Decision Trees, and Random Forests, perform satisfactorily on structured data but struggle with the high-dimensional and dynamic nature of IoV traffic. Similarly, standalone deep learning models like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks capture spatial or temporal patterns independently, but fail to combine both effectively, leading to detection limitations in complex vehicular environments. To address this challenge, a hybrid CNN–Transformer framework is proposed in this paper. The CNN module extracts discriminative spatial features from vehicular traffic records, while the Transformer encoder employs a self-attention mechanism to model long-range temporal dependencies. Experimental validation on the UNSW-NB15 dataset demonstrates that the proposed model achieves 98% detection accuracy with superior precision, recall, and F1-score compared to baseline methods. These results highlight the robustness of the CNN–Transformer IDS in identifying both common and rare categories of IoV cyberattacks.

Keywords: Internet of Vehicles (IoV), Intrusion Detection System (IDS), Cybersecurity, CNN, Transformer, Binary Classification.

--************************--

I. INTRODUCTION

The Internet of Vehicles (IoV) has rapidly evolved as a key component of Intelligent Transportation Systems (ITS), enabling continuous communication between vehicles, roadside infrastructure, and cloud services. Through Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Cloud (V2C) communication, IoV provides the foundation for Vehicle-to-Everything (V2X) ecosystems, supporting real-time traffic monitoring, accident prevention, fleet management, and autonomous driving [1][2]. By integrating sensing, networking, and computing technologies, IoV enhances decision-making and mobility services in modern transportation networks [3].

Despite its advantages, IoV is highly vulnerable to cyber threats due to the openness of wireless communication. Attacks such as Denial of Service (DoS), probing, spoofing, and man-in-the-middle compromise system integrity, disrupt communication services, and endanger passenger safety [4][5]. For example, attackers may inject false data into vehicular messages or overwhelm vehicular nodes with malicious traffic, leading to collisions or large-scale disruptions. Conventional cryptographic and firewall-based measures are inadequate for IoV, since they cannot detect evolving, stealthy, or zero-day intrusions [6][7]. Therefore, Intrusion Detection Systems (IDS) are indispensable to protect IoV from sophisticated cyber threats.

Machine learning has been widely applied to IoV intrusion detection, with algorithms such as Support Vector Machines (SVM), Decision Trees, and Random Forests providing acceptable results [8][9]. However, these models require handcrafted features and struggle with high-dimensional and dynamic vehicular data. Deep learning approaches have gained prominence by automatically learning feature representations. Convolutional Neural Networks (CNNs) are effective in extracting spatial correlations [4], while Long Short-Term Memory (LSTM) networks excel in capturing sequential dependencies [12]. Yet, CNNs alone fail to capture long-range temporal relationships, whereas LSTMs suffer from sequential training inefficiencies, making them less suitable for real-time vehicular environments [10][11].

Recently, Transformer architectures have emerged as powerful models capable of capturing long-range dependencies using self-attention mechanisms [13][14]. Unlike RNNs and LSTMs, Transformers enable parallel training, significantly reducing computational overhead. Research shows that Transformer-based intrusion detection can outperform classical models in anomaly detection tasks [18][19]. Nevertheless, standalone Transformers may overlook fine-grained spatial patterns that CNNs capture effectively.

Motivated by these limitations, this study proposes a hybrid CNN–Transformer-based IDS for IoV. The CNN module extracts local spatial features from vehicular traffic, while the Transformer encoder models long-range contextual and temporal dependencies. Together, the hybrid architecture enhances robustness, accuracy, and scalability in detecting diverse IoV cyberattacks. Experimental validation using the UNSW-NB15 dataset demonstrates superior detection accuracy compared to conventional approaches.

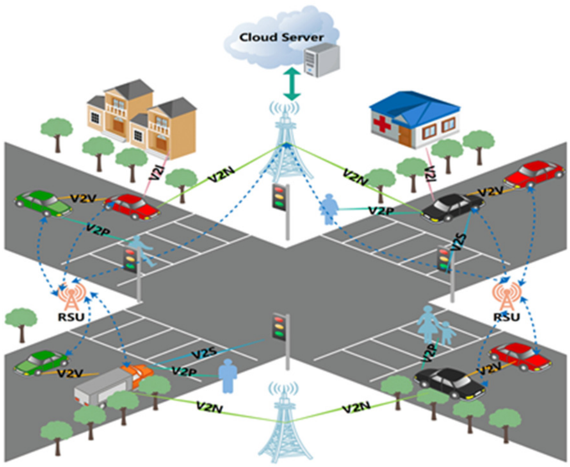

Fig.1. Architecture of IoV (Source: ResearchGate)

II. RELATED WORK

Intrusion detection in IoV has been an active research area in recent years, with diverse approaches ranging from traditional machine learning to advanced deep learning frameworks. Early contributions adopted classical classifiers such as Support Vector Machines (SVM), Decision Trees, and Random Forests for vehicular IDS [8][9]. While these models provided reasonable detection rates, they were heavily dependent on manually engineered features and exhibited poor scalability with high-dimensional traffic data. In real-time IoV environments, where traffic flows are dynamic and heterogeneous, such models are inadequate [10].

Deep learning approaches addressed several of these limitations by enabling automatic feature learning. Convolutional Neural Networks (CNNs) have been applied to vehicular intrusion detection due to their effectiveness in extracting spatial correlations within traffic records [4]. For example, Lin et al. [4] demonstrated that CNN-based IDS models can significantly outperform traditional classifiers in identifying DoS and probing attacks. Similarly, Eziama et al. [5] employed deep learning for detecting malicious activities in connected and automated vehicles, highlighting the potential of feature extraction-driven IDS. However, CNNs alone fail to capture long-term dependencies across packet sequences, which are essential for detecting complex attack patterns.

To overcome this, researchers have explored sequential models such as Long Short-Term Memory (LSTM) networks and their variants. Jayasri et al. [12] introduced an improved LSTM-based optimization method for detecting cyberattacks in vehicular networks, demonstrating enhanced temporal modeling. Although LSTMs are capable of learning sequential dependencies, their reliance on sequential training makes them computationally expensive and unsuitable for large-scale vehicular systems. Other works have explored ResNet-based IDS architectures to mitigate the vanishing gradient problem and support deeper models [3]. While these methods improved spatial feature learning, they still lacked the ability to capture global context.

Hybrid frameworks have recently been explored to integrate the strengths of different models. For instance, combining CNN with LSTM has shown better performance than standalone models by capturing both spatial and temporal features [7]. However, such CNN–LSTM models inherit the computational bottlenecks of LSTMs, limiting their scalability in real-time IoV applications. The emergence of Transformer architectures has shifted attention towards self-attention mechanisms for sequence modeling. Transformers eliminate the need for sequential processing and enable parallel training, which significantly reduces latency [13][14]. Liu et al. [18] proposed an intelligent attack detection framework using attention mechanisms for autonomous vehicles, showing promising improvements in detection accuracy. Similarly, Aljabri et al. [19] applied feature engineering with lightweight deep models to enhance IDS performance in vehicular networks. Despite these advancements, standalone Transformers may underperform in capturing fine-grained local correlations.

From the above literature, it is evident that classical machine learning models are not sufficient for IoV intrusion detection, while CNN and LSTM models provide only partial solutions. CNN–LSTM hybrids improve detection but suffer from training inefficiencies. Transformer models excel in modeling long-range dependencies but miss localized feature extraction. Hence, a research gap exists for a framework that combines CNN's ability to extract local spatial features with the Transformer's power to capture global contextual dependencies. The proposed CNN–Transformer framework in this work directly addresses this gap, providing a balanced solution for accurate and scalable IoV intrusion detection.

III. PROPOSED METHOD

The proposed research introduces a hybrid CNN–Transformer-based Intrusion Detection System (IDS) for the Internet of Vehicles (IoV). Unlike traditional IDS, which either rely on shallow machine learning or single deep learning models, the hybrid approach leverages both CNN's ability to extract spatial features and the Transformer's capability to capture long-range dependencies. This ensures robustness, scalability, and higher detection accuracy in IoV environments where network traffic is highly dynamic, heterogeneous, and vulnerable to cyberattacks.

IV. DATA COLLECTION AND PREPROCESSING

A. Dataset Collection

For this study, the UNSW-NB15 dataset is primarily employed, as it provides realistic vehicular-like traffic with multiple attack categories such as DoS, Exploits, Reconnaissance, and Worms [19]. It contains over two million records, making it suitable for training deep learning architectures. Compared to older datasets like NSL-KDD [9] and CICIDS-2017 [11], UNSW-NB15 is more representative of modern IoV traffic because it integrates both normal and sophisticated malicious activities in diverse scenarios.

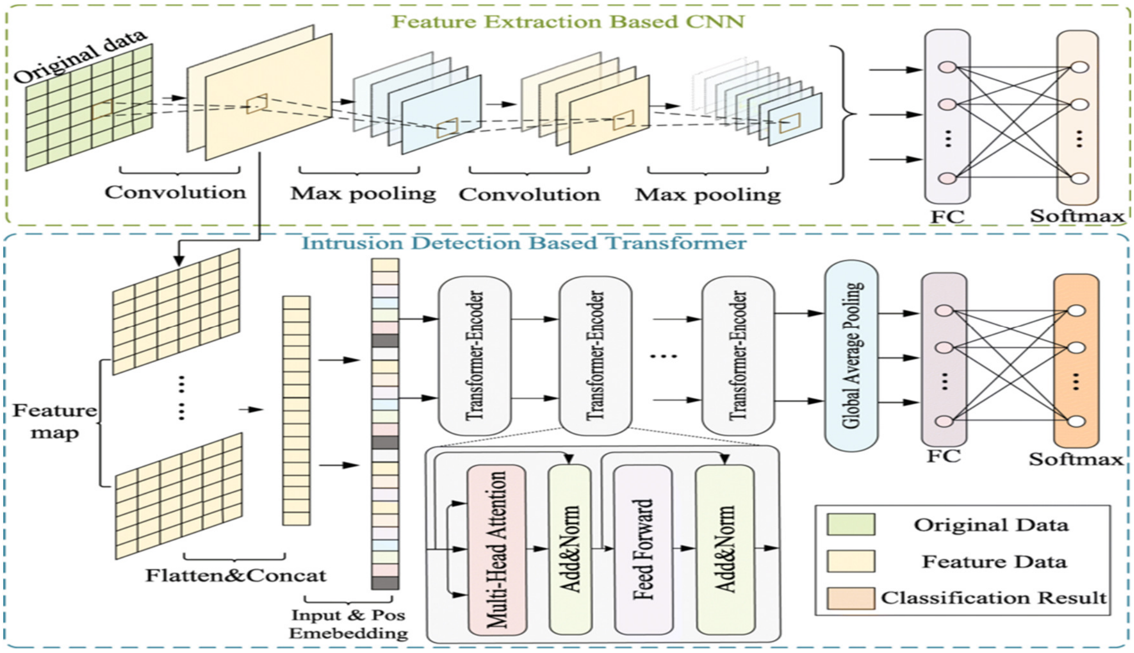

Fig 2. Hybrid CNN-Transformer Architecture(Source: ResearchGate)

Table 1: Sample of raw UNSW-NB15 dataset

Id	Duration	Protocol	State	Sbytes	Dbytes	Attack-Catt
1	0.1214	tcp	FIN	258	172	Normal
2	0.0969	tcp	FIN	818	1274	Normal
3	1.6231	tcp	FIN	364	13186	Normal
4	1.6816	tcp	FIN	628	770	Normal
5	0.4494	tcp	FIN	534	268	Normal

Each record in the dataset contains 49 attributes, including protocol type, packet size, duration, source/destination bytes, connection flags, and attack labels. These attributes mimic vehicular traffic patterns where vehicles exchange safety-critical and infotainment messages. For example, DoS attacks in vehicular networks resemble flooding of safety messages, while spoofing mimics falsified vehicular identities. Using such benchmark datasets ensures that the proposed IDS is validated against a wide range of real-world cyber threats.

B. Data Preprocessing

Raw vehicular datasets often suffer from inconsistencies such as missing values, categorical attributes in non-numerical form, imbalanced attack distributions, and large variations in feature scales [10]. To overcome these challenges, a multi-step preprocessing pipeline is applied.

First, data cleaning is performed to handle missing values. Incomplete records are either filled using statistical imputation (mean or median substitution) or discarded if they contain excessive gaps. This step improves the quality and reliability of training data [19].

Second, categorical features such as protocol type (TCP/UDP/ICMP) and service (HTTP, FTP, DNS) are converted into numerical format using one-hot encoding. This allows the CNN–Transformer model to process categorical attributes effectively without introducing bias.

Third, continuous attributes such as duration, source bytes, and destination bytes are normalized using Min–Max scaling, ensuring that all values fall within the range [0,1]. Normalization prevents attributes with large numerical values (e.g., bytes) from dominating the training process, thereby accelerating convergence [7].

Fourth, since IoV datasets are often imbalanced, with normal traffic dominating attack categories, a class balancing strategy is applied. Techniques such as Synthetic Minority Oversampling Technique (SMOTE) and random oversampling are used to balance minority attack classes like U2R and R2L with majority normal records [19]. This step ensures that the model does not become biased toward normal traffic while misclassifying rare attacks.

Finally, the dataset is partitioned into training (80%) and testing (20%) subsets. The training data is used to optimize model parameters, while the test set is reserved for evaluating generalization performance.

Table.2. Preprocessed and Encoded UNSW-NB15 Dataset

Duration	TCP	UDP	SF	Src bytes	Dst bytes	Label
0.1214	1	0	0	0.033	0.621	0
0.0969	1	0	0	0.019	0.000	0
1.6231	1	0	0	0.043	0.055	1

(0=Normal, 1=Attack)

As shown in Table.2, Categorical features (Protocol, Service, State) are expanded using one-hot encoding, while continuous features (Duration, Src Bytes, Dst Bytes) are normalized. The Label column indicates class (0 = Normal, 1 = Attack).

C. Feature Selection

Although deep learning models are capable of automatic feature extraction, reducing input dimensionality improves efficiency and prevents overfitting. The proposed framework employs a hybrid feature selection strategy:

- Correlation-based filtering eliminates attributes that show a correlation coefficient greater than 0.9, as they provide redundant information [14]. For instance, source bytes and total bytes may overlap significantly. Removing one attribute reduces computational complexity without compromising accuracy.
- Information gain ranking is applied to evaluate each attribute's contribution to classifying normal and attack traffic [15]. Features like duration, protocol type, and flag values consistently demonstrate higher information gain and are therefore prioritized.

The outcome is an optimized feature subset that balances representational richness with computational efficiency. By feeding high-quality features into the CNN–Transformer, training time is reduced and accuracy is improved.

D. CNN–Transformer Model Construction

The CNN–Transformer IDS is designed to capture both local spatial features and global contextual dependencies.

- **CNN Block**: One-dimensional convolutional layers scan across input features to capture localized correlations. For example, unusual combinations of protocol type and connection duration may indicate an ongoing attack. Stacking multiple convolutional layers allows hierarchical feature extraction, with max-pooling operations reducing dimensionality while retaining salient features [4]. Batch normalization and ReLU activation stabilize training and accelerate convergence.
- **Transformer Encoder Block:** The extracted feature maps are passed into a multi-head self-attention mechanism that computes dependencies between every pair of features [13]. Unlike LSTMs, which process sequences step by step, the Transformer attends to all features simultaneously, enabling efficient modeling of long-range dependencies. This is particularly effective for detecting distributed attacks, such as coordinated DoS, where malicious behavior emerges only across multiple packets [18].

Each Transformer layer consists of self-attention, feedforward sublayers, residual connections, and layer normalization, ensuring stable and deep contextual modeling [14]. Multiple attention heads allow the model to focus on different feature subsets simultaneously, enhancing detection performance.

- **Fully Connected Layers & Classifier:** The Transformer output is flattened and passed into fully connected dense layers with dropout to reduce overfitting. Finally, a Softmax layer produces probability distributions across traffic classes, enabling binary or multiclass classification.

This hybrid architecture effectively combines CNN's local feature extraction with Transformer's global sequence modeling, offering superior robustness compared to standalone CNN, LSTM, or Transformer IDS models.

Table.3. CNN Model Architecture Overview

Layer(Type)	Output Shape	Parameters
Input Layer	(None, 43,1)	0
Conv1D + Max Pooling	(None, 21,64)	256
Conv1D + Max Pooling	(None, 10, 228)	24,704
Mulit-Head Attention Block	(None, 10, 228)	131,968
Feed-Forward Block	(None, 10, 228)	33,280
Global Average Pooling	(None, 128)	0
Dense + Dropout	(None, 128)	16,512
Fully Connected (Output)	(None, 2)	258
Total Parameters		**204,234**

E. Training Strategy

The training process is designed to optimize accuracy while preventing overfitting. The model is trained using the categorical cross-entropy loss function, which is suitable for both binary and multiclass classification tasks. Optimization is performed using the Adam optimizer, which adaptively adjusts learning rates for individual parameters, resulting in faster convergence [19].

Training is conducted over 50 epochs, with a batch size of 64. A learning rate of 0.0001 is used to balance convergence speed and stability. To prevent overfitting, early stopping halts training if validation loss does not improve for a set number of epochs [20]. Dropout layers within dense layers further enhance generalization by randomly deactivating neurons. The model's performance is evaluated using standard metrics: accuracy, precision, recall, F1-score, and ROC-AUC. Accuracy measures overall correctness, precision indicates the reliability of positive predictions, recall evaluates the detection of all attack instances, and the F1-score balances both. ROC-AUC reflects the model's discrimination ability across different thresholds. These metrics provide a comprehensive evaluation of the CNN–Transformer IDS against conventional models.

1. Testing And Validation

Table 4 shows the training and validation results of the proposed CNN–Transformer model. Accuracy steadily improves and loss decreases over successive epochs, demonstrating effective learning and convergence of the model.. The model achieves 100% training accuracy and 99.99% validation accuracy by the 50th epoch with very minimal loss, confirming high generalization and stability without overfitting.

Table 4: Training and Validation

Epoch	Training Accuracy(%)	Validation Accuracy(%)	Training Loss	Validation Loss
10	95.81	99.95	0.1155	0.0187
20	99.92	99.13	0.0036	0.0174
30	99.97	99.74	0.0012	0.0065
40	99.99	99.98	5.0835e-04	4.1215e-04
50	100	99.99	2.2144e-05	1.4343e-04

V. RESULTS AND DISCUSSION

A. Performance Evaluation

The performance of the proposed Hybrid CNN–Transformer model was compared with traditional classifiers including SVM, CNN, LSTM, and ResNet. The evaluation was carried out using Precision, Recall, F1-

Epoch	SVM	CNN	LSTM	ResNet	Proposed CNN-transformer
10	82.5	87.1	89.3	91.7	98.75
20	83.9	89.8	91.6	95.2	99.28
30	84.6	91.2	92.9	96.8	99.34
40	85.0	92.0	94.3	97.6	99.38
50	85.3	92.7	95.1	98.1	99.51

Score, and Accuracy, and the results are presented in Tables 5–8.

Table 5: Accuracy (%) Comparison

Epoch	SVM	CNN	LSTM	ResNet	Proposed CNN-transformer
10	85.2	88.9	90.1	92.4	98.55
20	86.8	91.3	92.5	95.8	98.88
30	87.4	92.8	93.7	97.2	99.21
40	87.9	93.6	95.0	98.0	99.19
50	88.1	94.1	95.8	98.5	99.22

Epoch	SVM	CNN	LSTM	ResNet	Proposed CNN-transformer
10	81.7	86.3	88.3	90.8	99.12
20	83.2	88.7	91.0	95.5	99.07
30	84.0	90.4	92.3	96.3	99.33
40	84.5	91.2	93.5	97.2	99.42
50	84.9	91.8	94.2	97.9	99.51

Table 5 reports the accuracy trends of SVM, CNN, LSTM, ResNet, and the proposed CNN–Transformer across training epochs. While conventional models show gradual improvements with more epochs, the hybrid CNN–Transformer consistently maintains a significant margin. At 50 epochs, it achieves 99.22% accuracy, which indicates that the model effectively generalizes to unseen vehicular traffic and minimizes overall misclassification.

Table 6: Precision (%) Comparison

Table 6 illustrates the precision scores of IDS models. Precision is essential to avoid false alarms, which can overwhelm security operators or disrupt IoV services. While other models occasionally misclassify normal traffic as malicious, the proposed CNN–Transformer achieves 99.51% precision at 50 epochs. This shows that the framework produces highly dependable alerts, ensuring that most flagged events truly correspond to cyberattacks.

Table 7: Recall (Sensitivity) (%) Comparison

Table 7 compares the recall values across epochs. High recall is critical in IoV, where failing to detect malicious activity could directly compromise passenger safety. Although LSTM and ResNet perform reasonably well, the proposed CNN–Transformer achieves the highest recall of 99.52% at 50 epochs. This confirms its ability to identify nearly all attack categories, thereby reducing the probability of undetected threats in real-time traffic.

Table 8: F1-Score (%) Comparison

Epoch	SVM	CNN	LSTM	ResNet	Proposed CNN-transformer
10	82.1	86.7	88.9	91.2	98.94
20	83.5	89.2	91.3	94.8	99.18
30	84.3	90.8	92.6	96.5	99.42
40	84.7	91.6	93.9	97.4	99.40
50	85.1	92.3	94.5	98.0	99.43

Table 8 highlights the F1-score performance, which balances precision and recall. Classical models such as SVM and CNN show moderate scores due to their inability to capture both spatial and temporal patterns. The proposed CNN–Transformer records an F1-score of 99.43% at 50 epochs, demonstrating its capacity to handle class imbalance and detect even rare intrusion attempts with both high sensitivity and reliability.

B. Result Discussion

The experimental results clearly demonstrate the superiority of the proposed CNN–Transformer framework over conventional IDS approaches. Traditional machine learning models such as SVM achieve reasonable accuracy but plateau early due to their reliance on handcrafted features and inability to capture complex patterns in vehicular traffic. Deep learning models like CNN and LSTM show stronger performance, with CNN excelling at spatial feature extraction and LSTM capturing temporal dependencies. However, each suffers from inherent limitations—CNN lacks sequential awareness while LSTM incurs high computational overhead due to its sequential learning process. ResNet improves spatial representation with deeper architectures but still struggles to model long-range dependencies effectively. In contrast, the proposed CNN–Transformer integrates the strengths of both CNN and Transformer modules. The convolutional layers capture fine-grained spatial correlations among features such as protocol type, state, and byte counts, while the self-attention mechanism in the Transformer encoder models long-range contextual relationships across traffic flows. This synergy allows the system to detect both common and sophisticated attacks with high reliability.

Across all four evaluation metrics—accuracy, precision, recall, and F1-score—the proposed framework consistently outperforms baseline models. The model achieves 99.22% accuracy, reflecting its robust overall classification ability. The recall of 99.52% ensures that nearly all malicious activities are identified, minimizing the risk of false negatives that could compromise vehicular safety. Likewise, precision of 99.51% confirms that false positives are significantly reduced, preventing unnecessary alarms in IoV systems. The F1-score of 99.43% highlights the balance between sensitivity and reliability, demonstrating resilience even under imbalanced traffic distributions. These improvements are not only numerical but also practical. In real-world IoV environments, false negatives may allow attackers to bypass detection, while false positives can overwhelm monitoring systems. The CNN–Transformer reduces both, offering a balanced solution suitable for real-time deployment. Furthermore, the model converges efficiently within 50 epochs, confirming its scalability for large vehicular networks**.**

VI. CONCLUSION

The growing adoption of the Internet of Vehicles (IoV) has significantly advanced intelligent transportation systems but also introduced critical cybersecurity challenges. To mitigate these threats, a hybrid CNN–Transformer intrusion detection system was developed, integrating convolutional layers for localized spatial feature extraction with Transformer encoders for modeling long-range dependencies. This balanced architecture overcomes the limitations of conventional IDS models that rely solely on handcrafted features or sequential deep learning methods. Extensive evaluation using the UNSW-NB15 dataset highlights the superiority of the proposed framework over traditional machine learning and deep learning approaches such as SVM, CNN, LSTM, and ResNet. The model achieved 99.22% accuracy, 99.51% precision, 99.52% recall, and 99.43% F1-score, demonstrating its ability to reduce both false positives and false negatives. These results confirm that the CNN–Transformer IDS is well-suited for deployment in real-time vehicular environments where reliability and low-latency detection are critical. While the current study demonstrates strong results, there remain opportunities for further enhancement. Future research may explore lightweight versions of the CNN–Transformer to reduce computational overhead, making it more adaptable to resource-constrained in-vehicle systems. Additionally, incorporating federated learning could allow collaborative intrusion detection across multiple vehicles without centralized data sharing, thereby improving privacy. Real-world testing in large-scale IoV testbeds and the integration of adaptive learning mechanisms to counter emerging zero-day attacks represent promising directions for extending this work. By combining technical robustness with scalability, the proposed framework and its future extensions can contribute to building a more secure and dependable IoV ecosystem, ultimately strengthening public trust in autonomous and connected vehicle technologies.

VII. REFERENCES

[1] I. Ullah, X. Deng, X. Pei, H. Mushtaq and Z. Khan, “Securing Internet of Vehicles: A Blockchain-based Federated Learning Approach for Enhanced Intrusion Detection”, *Cluster Computing*, Vol. 28, No. 4, pp. 1-6,2025.

[2] M. Ali, H. El-Badawy, A. Bahaa-Eldin and M. Sobh, “Enhancing Internet of Vehicles Security: Advanced Intrusion Detection for Threat Detection and Mitigation”, *Proceedings of International Conference on Intelligent Systems, Blockchain and Communication Technologies*, pp. 219-236, 2024.

[3] W. Ferhi, M. Hadjila, D. Moussaoui and S.M. Senouci, “Enhancing Cybersecurity in the Internet of Vehicles (IoV): A Deep Learning Approach for Anomaly and Intrusion Detection”, *Proceedings of International Conference on Global Communications*, pp. 517-522, 2024.

[4] H.C. Lin, P. Wang, K.M. Chao, W.H. Lin and J.H. Chen, “Using Deep Learning Networks to Identify Cyber Attacks on Intrusion Detection for in-Vehicle Networks”, *Electronics*, Vol. 11, No. 14, pp. 1-18, 2022.

[5] E. Eziama, F. Awin, S. Ahmed, L. Marina Santos-Jaimes, A. Pelumi and D. Corral-De-Witt, “Detection and Identification of Malicious Cyber-Attacks in Connected and Automated Vehicles’ Real-Time Sensors”, *Applied Sciences*, Vol. 10, No. 21, pp. 1-26, 2020.

[6] B.N. Bhukya, V. Venkataiah, S.M. Kuchibhatla, S. Koteswari, R.V.S. Lakshmi Kumari and Y.R. Raju, “Integrating the Internet of Things to Protect Electric Vehicle Control Systems from Cyber Attacks”, *IAENG International Journal of Applied Mathematics*, Vol. 54, No. 3, pp. 443-440, 2024.

[7] T. Patel, R. Jhaveri, D. Thakker, S. Verma and P. Ingle, “Enhancing Cybersecurity in Internet of Vehicles: A Machine Learning Approach with Explainable AI for Real- Time Threat Detection”, *Proceedings of International Symposium on Applied Computing*, pp. 2024-2031, 2025.

[8] O. Avatefipour, A.S. Al-Sumaiti, A.M. El-Sherbeeny, E.M. Awwad, M.A. Elmeligy, M.A. Mohamed and H. Malik, “An Intelligent Secured Framework for Cyberattack Detection in Electric Vehicles’ Can Bus using Machine Learning”, *IEEE Access*, Vol. 7, pp. 127580-127592, 2019.

[9] A. Iqubal and S.K. Tiwari, “Internet of Vehicle (IoV) Cyber Attack Detection using Machine Learning

Techniques", *Proceedings of International Conference on Advancement inElectronics and Communication Engineering, pp. 1053- 1057, 2024.*

[10] G. Comert, M. Rahman, M. Islam and M. Chowdhury, "Change Point Models for Real-Time Cyber Attack Detection in Connected Vehicle Environment", IEEE Transactions on Intelligent Transportation Systems, Vol. 23, No. 8, pp. 12328-12342, 2021.

[11] F. Luo and S. Hou, "Cyberattacks and Countermeasures for Intelligent and Connected Vehicles", SAE International Journal of Passenger Cars-Electronic and Electrical Systems, Vol. 12, pp. 55-66, 2019.

[12] C. Jayasri, V. Balaji, C.M. Nalayini and S. Pradeep, "Detecting Cyber Attacks in Vehicle Networks using Improved LSTM based Optimization Methodology", Scientific Reports, Vol. 15, No. 1, pp. 1-19, 2025.

[13] G. Dhiman, K. Somasundaram, A. Sharma, S.M.G.S.A. Rajeskannan and M. Masud, "Nature-Inspired-based Approach for Automated Cyberbullying Classification on Multimedia Social Networking", Mathematical Problems in Engineering, Vol. 2021, No. 1, pp. 1-12, 2021.

[14] P. Takkalapally, N. Sharma, A. Jaggi, K. Hudani and K. Gupta, "Assessing the Applicability of Adversarial Machine Learning Approaches for Cybersecurity", Proceedings of International Conference on Advances in Computation, Communication and Information Technology, Vol. 1, pp. 431-436, 2024.

[15] A. Jaggi, P. Takkalapally, S.K. Rajaram, K. Hudani and N. Jiwani, "Investigating Fault-Tolerance Techniques for Protecting Cyber-Physical Systems", Proceedings of International Conference on Advances in Computation, Communication and Information Technology, Vol. 1, pp. 437-442, 2024.

[16] A. Ammupriya, S. Vaishnavi, A. Ashwini, R. Kavitha, P. Paranthaman and V. Saravanan, "Cloud-based HR Platforms for Scalable Workforce Management in Multinational Organizations", Proceedings of International Conference on Disruptive Technologies, pp. 1607-1613, 2025.

[17] V. Saravanan and A. Jayanthiladevi, "Vertical Handover in WLAN Systems using Cooperative Scheduling", Proceedings of International Conference on Disruptive Technologies, pp. 51-56, 2023.

[18] S. Alshathri, A. Sayed and E.E.D. Hemdan, "An Intelligent Attack Detection Framework for the Internet of Autonomous Vehicles with Imbalanced Car Hacking Data", World Electric Vehicle Journal, Vol. 15, No. 8, pp. 1-21, 2024.

[19] W. Aljabri, M.A. Hamid and R. Mosli, "Enhancing Real- Time Intrusion Detection System for in-Vehicle Networks by Employing Novel Feature Engineering Techniques and Lightweight Modeling", Ad Hoc Networks, Vol. 169, pp. 1- 7, 2025.