RESEARCH ARTICLE

Vehicular Network Security Through Optimized Deep Learning Model with Feature Selection Techniques

Fida Muhammad Khan[1], **Taj Rahman**[1,*], **Asim Zeb**[2], **Zeeshan Ali Haider**[1], **Inam Ullah Khan**[1], **Hazrat Bilal**[3], **Muhammad Abbas Khan**[4] and **Inam Ullah**[5,*]

[1] Department of Computer Science, Qurtuba University of Science & Information Technology, 25000 Peshawar, Pakistan
[2] Department of Computer Science, Abbottabad University of Science and Technology, Abbottabad, Pakistan
[3] College of Mechatronics and Control Engineering; and College of Computer Science and Software Engineering, Shenzhen University, Shenzhen 518060, China
[4] Faculty of Electrical Engineering, West Pomeranian University of Technology, Szczecin, Poland
[5] Department of Computer Engineering, Gachon University, Seongnam 13120, Republic of Korea

Abstract

In recent years, vehicular ad hoc networks (VANETs) have faced growing security concerns, particularly from Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. These attacks flood the network with malicious traffic, disrupting services and compromising resource availability. While various techniques have been proposed to address these threats, this study presents an optimized framework leveraging advanced deep-learning models for improved detection accuracy. The proposed Intrusion Detection System (IDS) employs Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Deep Belief Networks (DBN) alongside robust feature selection techniques, Random Projection (RP) and Principal Component Analysis (PCA). This framework extracts and analyzes significant features using a publicly available application-layer DoS attack dataset, achieving higher detection accuracy than traditional methods. Experimental results indicate that combining CNN, LSTM networks, and DBN with feature selection techniques like Random Projection (RP) and PCA results in improved classification performance, achieving an accuracy of 0.994, surpassing the state-of-the-art machine learning models. This novel approach enhances the reliability and safety of vehicle communications by providing efficient, real-time threat detection. The findings contribute significantly to VANET security, laying a robust foundation for future advancements in connected vehicle protection.

Keywords: vehicular networks security, denial of service (DoS) detection, deep learning intrusion detection, feature optimization techniques, connected vehicle protection.

Academic Editor:
Habib Khan

Submitted: 03 December 2024
Accepted: 26 December 2024
Published: 31 December 2024

Vol. 1, **No.** 2, 2024.
10.62762/TSCC.2024.626147

***Corresponding authors:**
✉ Taj Rahman
tajuom@gmail.com
✉ Inam Ullah
inam@gachon.ac.kr

1 Introduction

Vehicular Ad Hoc Networks (VANETs) are considered the next generation of ITS since they make it possible

Citation
Khan, F. M., Rahman, T., Zeb, A., Haider, Z. A., Khan, I. U., Bilal, H., Khan, M. A. & Ullah, I. (2024). Vehicular Network Security Through Optimized Deep Learning Model with Feature Selection Techniques. *ICCK Transactions on Sensing, Communication, and Control*, 1(2), 136–153.

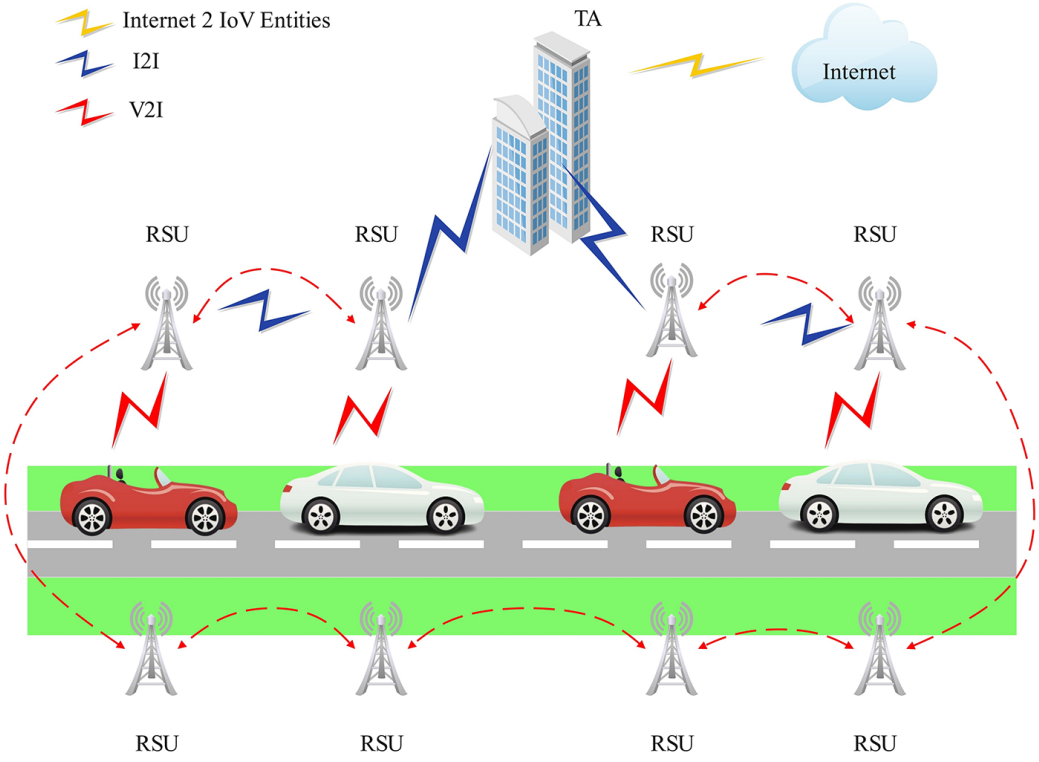

Figure 1. Smart City Infrastructure for Internet of Vehicles (IoV).

for the vehicles to communicate with each other, that is, vehicle to vehicle (V2V) and with different structures, for instance, vehicle to Infrastructure (V2I). This technology increases road safety, traffic manageability, and real-time information transfer [1]. A recent projection indicated that global internet users would be 5.3 billion by 2023, while networked devices per capita rose from 2.4 in 2018 to 3.6 in 2023, implying that modern life is increasingly characterized by devices such as connected vehicles [2, 3]. Using sophisticated wireless communication technologies, VANETs provide auxiliary services, including traffic information, weather conditions, and real-time entertainment, besides using Roadside Units (RSUs) for communication [4]. The communication architecture of a VANET is illustrated in the following Figure 1. The goal is to demonstrate how the cars communicate through V2V and V2I. The figure shows that RSUs are set to act as intermediaries in data exchange between vehicles and the network infrastructure. In addition, these RSUs communicate over the Internet with the Transport Authority (TA), also known as the other IoV entity. This architecture facilitates real-time data exchange, traffic surveillance, and reliable communication crucial for enhancing road security and traffic flow.

However, with the recent widespread use of VANETs, they have become prone to advanced cyber threats such as DoS and DDoS attacks. These attacks overwhelm the network with considerably invasive traffic that plugs its facilities and causes service interruption [5]. DOS attacks, including the HULK and Slowloris types, affect network services by consuming server resources or exploiting connection management mechanisms, respectively. These vulnerabilities undermine the network's ability to provide the rightful users' services [6, 7].

Various approaches have been implemented to address these threats. Traditional Syntactic Intrusion Detection Systems (IDS) compare events to a database of attack signatures, and the newly realized Anomaly IDS identifies events that deviate from the expected norm [8, 9]. The use of fuzzy logic [10], clustering [11], and hybrid systems [12] have been used in efforts to improve the detection ability of systems further. However, these approaches are computationally expensive, capable of scaling down, and less precise against advanced attacks [13, 14].

The basic illustrations of DoS and DDoS attacks on VANET are depicted in the following figure, as shown in Figure 2. In this diagram, an attacker

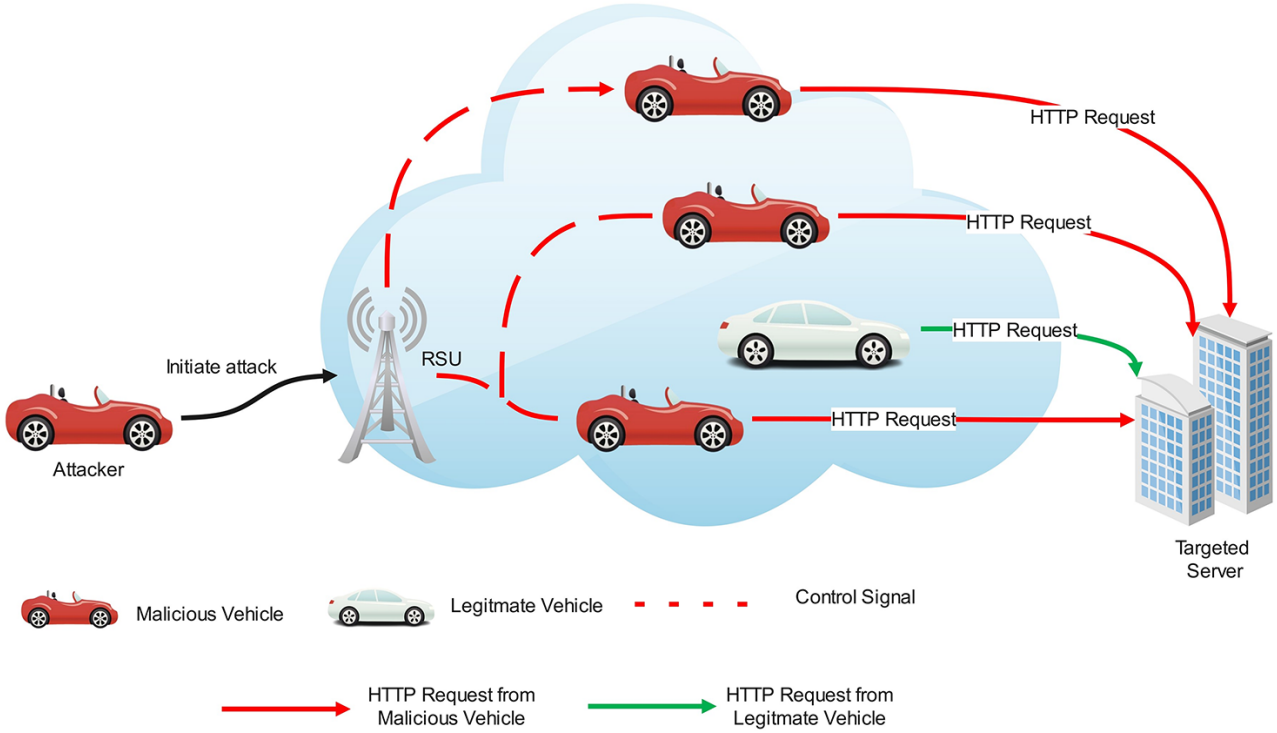

Figure 2. DoS and DDoS attack in VANET.

launches an attack by sending tainted HTTP requests through the compromised vehicles to the target server. These auto-generated malicious vehicles flood the network with HTTP request rates denoted by the red arrows. In contrast, vehicles upload normal HTTP requests, as denoted by the green arrows. The targeted server cannot distinguish between crafted and normal requests; this causes a resource overload issue and affects the services. This figure shows the effects of such attacks on vehicular communication networks and emphasizes the detection of such attacks.

The current and future use of Machine Learning (ML) and Deep Learning (DL) methods have proven effective in managing such issues. Recent literature shows that using random forests and support vector machines can help analyze the network's traffic data and flag irregularities [15, 16]. Based on this, DL models provide superior functionality compared to traditional machine learning techniques because the former can learn high-level features directly from big data without requiring developers to hand code those features [17], which proves beneficial in intrusion detection.

This research presents an improved scenario integrating deep learning models such as CNNs, LSTMs, and DBNs to identify DoS and DDoS attacks in VANETs. To further improve detection accuracy and efficiency, the framework integrates two robust feature selection techniques: Random Projection (RP) and Principal Component Analysis (PCA). As in the case of the RP, the method proved successful in bringing dimensionality down while at the same time minimizing data loss; PCA, on the other hand, is efficient in its identification of features that can be suppressed to improve the performance of the model [18, 19].

The effectiveness of the proposed framework is tested using a real dataset, including application-layer DoS attacks. The experimental results presented in this paper show that integrating CNN, LSTM, and DBN with RP and PCA brings about a remarkable enhancement in accuracy and time compared to other machine-learning models. This research works in VANET security. It presents a scalable, robust solution and is capable of providing real-time solutions against DoS and DDoS attacks for trusty and secure communication between vehicles.

This study presents important contributions to advancing VANET security since it compares and extends solutions for detecting and handling DoS

and DDoS attacks through a refined deep-learning approach. Mitigating DoS and DDoS attacks in VANETs is crucial due to their potential to disrupt critical services in real-world scenarios. For instance, a coordinated DoS attack on vehicle-to-infrastructure (V2I) systems could paralyze traffic management systems, leading to severe congestion or accidents. Similarly, targeting V2V communication during emergencies could delay critical safety alerts, endangering lives. In smart cities, such attacks on autonomous vehicle fleets could compromise public transportation reliability, causing significant economic and societal impacts. The proposed framework's ability to detect such attacks in real-time enhances the resilience and security of VANETs, ensuring safer and more efficient vehicular communication in these scenarios.

Various IDS have been proposed for VANETs in recent years, but they face significant limitations. Traditional signature-based methods struggle to detect new and evolving attacks, relying on predefined attack patterns. Meanwhile, anomaly-based systems often suffer from high computational costs and a higher rate of false positives, making them inefficient for real-time applications. Furthermore, state-of-the-art machine learning and deep learning models are often plagued by scalability issues when dealing with high-dimensional data in VANETs, as they require substantial computational resources and are not well-suited for the dynamic nature of vehicular environments. This study addresses these gaps by proposing a novel hybrid intrusion detection framework that integrates advanced deep learning models, including Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and Deep Belief Networks (DBN), with robust feature selection techniques such as Random Projection (RP) and Principal Component Analysis (PCA). By combining these methods, we significantly improve detection accuracy, reduce computational overhead, and enable real-time, scalable detection, thus overcoming the limitations of previous methods and ensuring enhanced security for VANETs. The key contributions of this study are outlined below:

- This study introduces an optimized deep learning-based IDS combining CNN, LSTM, and Deep Belief Networks (DBN) with robust feature selection techniques, Random Projection (RP), and PCA. This framework enhances the detection accuracy and efficiency of DoS and DDoS attacks in VANETs.
- <UNK> Integrating deep learning models and advanced feature selection methods significantly improves classification performance, achieving higher accuracy than state-of-the-art machine learning approaches. The framework demonstrates superior real-time threat detection with reduced computational complexity, making it suitable for practical VANET applications.
- The study extensively validates the proposed framework using a publicly available application-layer DoS attack dataset. It presents a detailed comparison with existing methods, highlighting the approach's effectiveness in ensuring the reliability and safety of vehicular communication systems.

The study consists of five major sections. Section 2: Related Work assesses existing literature on intrusion detection in VANETs, and discusses the limitations of existing approaches. Section 3: The research methodology section Discusses the CNN, the LSTM, and the DBN model used in the proposed framework; it also provides information on the Feature selection methods, such as Recursive partitioning and the principal component analysis. Section 4: Results and discussion describe how the experiment was conducted, the comparison of the proposed framework to previous work using metrics such as accuracy and precision, and the interpretations of the results section explore other difficulties, including dataset dependency and computational cost, and venue for future studies. Section 5: Concisely, this research's key findings are discussed, and it is concluded that the VANET security benefits from the proposed model, which incorporates advanced deep learning and feature selection mechanisms.

2 Related Work

This section presents a review of the existing literature concerning the IDS in VANETs, and the weaknesses that inspired the creation of the proposed framework. In [20], the authors considered the capability of IDS for malicious activity detection in VANETs, focusing on the algorithms. Thus, while their study offered an abundant review, no corresponding applications or uses could be directly implemented into a setting. Like this [21] developed a mutual authentication scheme for VANETs that employ forward secrecy for impersonation and forgery detection. Although presenting strong psychological protection courses, the technique had not been compared with other approaches and had

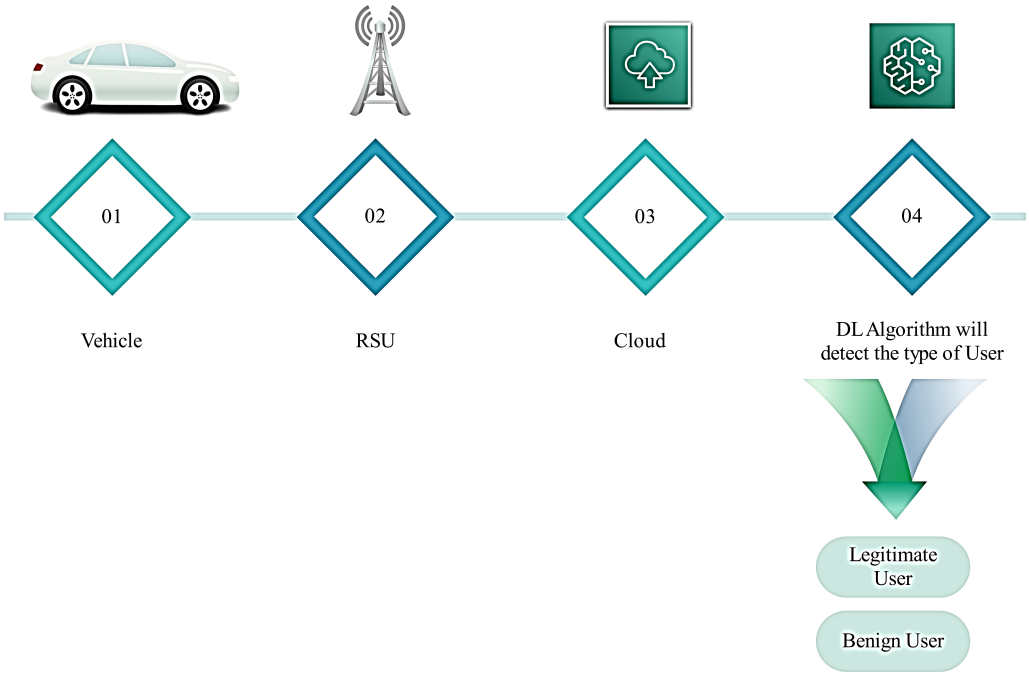

Figure 3. Secure data transmission and threat detection Using Deep Learning Models.

not undergone extensive empirical assessment in functional studies.

Comprehensive research in [22] classified IDS into signature-based, anomaly-based, and hybrid techniques. While in the case of signature-based IDS, false positives can be low and are very good at detecting known attack types, the anomaly-based IDS is more suitable for unknown attack types since it identifies deviation from normal operation patterns. However, no attention was paid to the machine learning approaches and their optimizations that can be applied to deep learning methods. The study in [23] showed that there are a lot of limitations with existing IDS, especially with signature-based IDS, which depends on a large attack signature database, and updating the same can be a difficult task of the day. Although the concept of Anomaly-based IDS is rather flexible, this approach costs a lot of computational capacity. This conflict of utilization within efficiency-consciousness is still an open problem. Another related research [24] used the MLP and RF for detecting DDoS attacks at the application layer. Even though RF reached an accuracy of 99.9%, the study had limitations in data set dependence and no particular feature selection, so it remains not easily scalable or optimized.

Figure 3 shows a VANET-based model for secure transmission of data and threat identification. The flow starts with the data collected in the cars being sent through booth Roadside Units (RSUs) This data is then processed and analyzed in the cloud where a deep learning algorithm assigns users a green or red label. The framework is the combination of VANET components with newly developed deep learning techniques to make vehicular communication more secure and robust.

The study in [25] focused on the use of statistical methods paired with machine mining techniques such as KNN, Bayesian Naive Bayes, and Logistic Regression for DDoS detection in Software-Defined Networking (SDN). The results identified the promising features of KNN while also revealing resource requirements and a range of issues regarding implementation that prevent the spread of the method. Likewise, [26] employed multi-feature approaches and multiple classifiers for the detection of malicious traffic, and gained noticeable performance. However, its applicability to various types of datasets and its use in a real environment needed further investigation.

In [27], supervised learning with recursive feature addition was used to improve the intricacy of intrusion detection. Although this approach provided enhanced classification accuracy it did not address class imbalance and did not consider various attack cases which restricted its application. Deep learning methods were proposed for anomaly-based IDS in

VANETs in the work reported in [28]. However, one disadvantage of using such models such as the Deep Belief Networks (DBN) that it adds to the operational complexity.

Authors in [29] proposed a bit nevertheless highly secure authentication protocol for VANETs with an emphasis on protection against unauthorized nodes. While it provided a comparison of the detection techniques, it did not assess the efficiency of its methods in a real environment. Similarly, [30] also developed an intrusion detection framework based on various machine learning algorithms employing ensemble techniques that proposed considerable accuracy gains. However, the computational cost of model stacking imposed a constraint on it to the extent that it could not be implemented on larger datasets. The summary of the related work in the field of IDS for VANET is discussed in Table 1, along with the details of datasets, ML/DL methods used, objectives, and drawbacks in each of the studies. It shows the limitations of existing approaches, including scalability, computational complexity, dependence on the used dataset, and low optimization of feature selection. These limitations highlight the need for a better architecture that would embed enhanced Deep learning models and feature selection methods that could enhance the recognition of DoS and DDoS attacks in a real-time VANET environment.

In the study of [31], the authors proposed a CNN-based approach for traffic anomaly detection, thereby presenting the network's capability to learn spatial information patterns. As analyzed in [32], LSTM models provided good performance for predicting time dependencies of sequential data, for example, the network logs. Although both methods were promising they were not complemented by feature selection methods which could increase accuracy and decrease complexity. Finally, [33] has presented a deep learning model that is a combination of CNN and DBN to detect intrusion. While this approach yielded good accuracy, it punctuated the model with complications and training times inconducive to real-time periods.

As evidenced by the existing studies, IDS has achieved vast improvements in the security of VANETs; however, issues of dataset dependency, high computational complexity, and system scalability remain challenges. These gaps turn the spotlight on the importance of fine-tuned IDS framework using deep learning models such as CNN, LSTM, and DBN on feature selection techniques, namely RP and PCA, for better detection accuracy and prompt information detection in VANET networks. Feature selection techniques like random projection structure and dimensionality reduction techniques are important in intrusion detection. Thus, efficiency was increased within the framework of the proposed study when RP was used in connection with deep learning classifiers. This was achieved when a feature extraction algorithm such as PCA was adopted in IDS, where noise was minimized and classification improved.

Existing intrusion detection techniques for VANETs have significant limitations. Traditional signature-based IDS can only detect known attacks, making them unsuitable for dynamic environments, while anomaly-based systems face challenges with high computational costs, false positives, and poor scalability. Recent machine learning (ML) and deep learning (DL) models often fail to efficiently handle high-dimensional data or incorporate proper feature selection, limiting their real-time applicability. This study addresses these issues by proposing a hybrid deep learning framework that combines CNN, LSTM, and DBN with Random Projection (RP) and PCA for efficient feature selection. Our approach improves detection accuracy, reduces computational overhead, and ensures real-time scalability, offering a more effective solution for detecting DoS and DDoS attacks compared to traditional IDS and existing DL methods.

3 Methodology

In this section, the framework designed in the context of the present research study, to identify DoS and DDoS attacks in VANETs, has been described in detail. The framework works as follows: vehicles send information to Roadside Units (RSUs) which are data relayers. The RSUs transmit the gathered data to a cloud server and the data is then enlightened by a combined deep-learning program to distinguish between good and dangerous users. These results are transmitted back to the vehicles to facilitate real-time threat detection together with accurate attack categorization within the VANET context. Specific features of the research include an overview of the approaches to the formation of the dataset, an analysis of the preprocessing of LIDAR data, and a comprehensive description of the classifiers based on deep learning used in the work. Also, the measures employed in evaluating the model's efficiency are presented. To enhance externally provided cues to facilitate further research, the study adheres to

Table 1. Summary of Related Work and their Limitation

Ref	Dataset	ML/DL Technique	Aim/Target	Limitation
[20]	KDD Cup 99 and NSL-KDD	SVM method	Preventing mutation of well-classified events in *VANETs*.	Inadequate vehicle communication and massive data integration for SVM training.
[21]	Application-layer DDoS dataset	MLP and RF	Identifying DDoS attacks with high accuracy.	Lacked practical implementation and comparative validation in real-world scenarios.
[22]	IoTID20 and UNSW-NB15	GBM, RF, ETC	Ensemble-learning-based malicious traffic detection.	The computational cost of stacked models limits scalability and real-time applicability.
[23]	DDOS open-source dataset	KNN, SVM, RF	Protecting IoT devices in banking from DoS attacks.	Accuracy improvements were needed and lacked optimized feature selection techniques.
[24]	NSL-KDD dataset	Regression, Naive Bayes, SVM, KNN	Effective detection of DDoS attacks in SDN environments.	Additional hardware/software requirements increase complexity and implementation cost.
[25]	CICIDS2017	RF, SVM, MLP, CNN	ML-based model for detecting DDoS attacks at the application layer.	Feature extraction and preprocessing techniques were not explicitly detailed.
[26]	NS3 simulation and NSL-KDD dataset	Decision Tree (DT), SVM, KNN	Hybrid data-driven model for malicious traffic detection.	Can only detect known attacks; lacks adaptability to novel intrusion patterns.
[27]	CICIDS2017	RF and recursive feature addition	Enhancing detection accuracy through feature selection.	Ignored class imbalances and focused only on binary classification scenarios.
[28]	Custom VANET security dataset	DBN, CNN	Anomaly-based intrusion detection system for *VANETs*.	High computational complexity and lack of real-world deployment.
[29]	ISCX 2012	Multi-feature techniques with ML	Efficient detection of DoS and DDoS attacks across local networks.	Applicability to diverse datasets and real-world scalability was not fully explored.
[30]	Custom VANET authentication dataset	ML ensemble techniques	Security-critical authentication system for *VANETs*.	Lacked in-depth real-world evaluation of proposed methods.
[31]	UNSW-NB15	RP with ML classifiers	Reducing dimensionality for efficient intrusion detection.	Only RP was considered; combined feature selection techniques were not explored.
[33]	CICIDS2017	CNN	Learning spatial patterns for anomaly detection in *VANETs*.	Lack of integration with feature selection techniques for improved efficiency.
[34]	CICIDS2017	LSTM	Capturing temporal dependencies in sequential network traffic.	Focused only on time-series data; lacked adaptability to mixed traffic patterns.
[35]	ISCX 2012	Hybrid CNN-DBN model	Improved accuracy for intrusion detection in *VANETs*.	High complexity and training time limited its applicability for real-time intrusion detection.

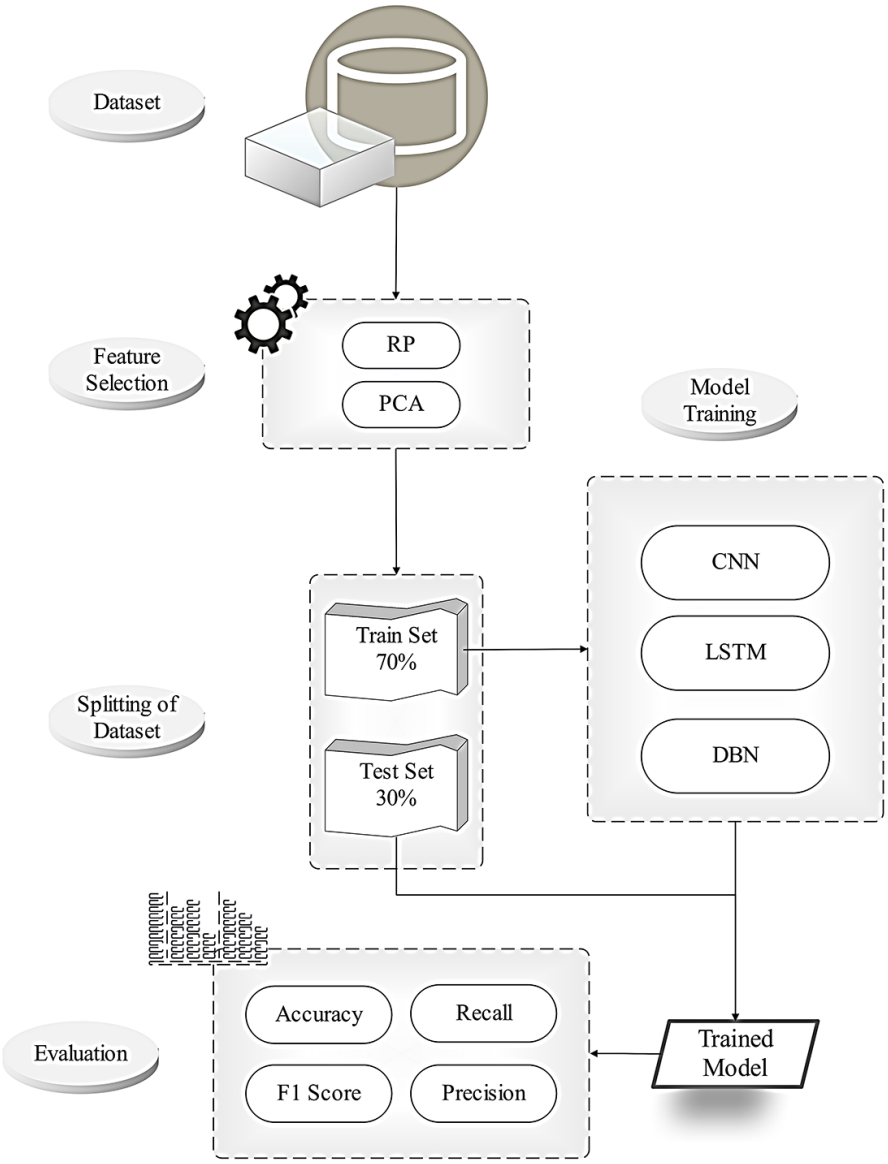

Figure 4. Proposed Deep Learning Framework.

predetermined procedures based on four principles: clarity, accuracy, completeness, and reproducibility.

The framework incorporates deep learning techniques like CNN, LSTM, and DBN and feature selection methods like Random Projection (RP) and PCA. For this work, a publicly available application-layer DoS attack dataset is obtained and undergoes further feature extraction that boosts the detection rate. The experiments were performed on an Intel Core i5 8th generation laptop that came with 16 GB RAM and 1TB SSD and preloaded with Windows 11. Specifically, the successful deep learning paradigms in Python were deployed using the TensorFlow and Scikit-learn libraries within a Jupyter Notebook framework. The proposed framework is designed to classify and predict DoS and DDoS attacks better to provide a better solution for intrusion detection at VANETs. Finally, after training the deep learning model, the framework produces decision-making inputs for real-time system control for secure and reliable communication within the vehicular network. For clarity, all the steps are incorporated in the presented methodology and illustrated in the flowchart in Figure 4.

3.1 Dataset

We selected the Application-Layer DoS Attack Dataset, containing the analysis of the application layer DoS and DDoS attacks originating from Kaggle. This dataset includes 78 attributes and 809,361 records,

categorized into three classes: benign traffic, which is actual network traffic, DoS Slowloris attack, and DDoS Hulk attack. This research aims to categorize and investigate the features of the aforementioned attack types to design effective countermeasures to protect VANETs against these menacing threats.

3.2 Data Preparation and Feature Selection for Deep Learning-Based Intrusion Detection

Data management in deep learning is mainly the process by which the key features that would enable the efficient working of a particular model are selected from the data set. One of the more important steps is selecting optimal features, which contributes to enhanced general effectiveness and reliability of the deep learning models and attacks [34, 36]. The application-layer DoS attack dataset has been chosen in this study, and the data preprocessing steps featured extraction using RP and PCA. The dataset was then partitioned into a training data set comprising 70 percent and a testing data set of 30 percent. The selection of the features was performed to improve the learning process, making the deep learning models achieve the greatest level of accuracy. After that, deep learning classifiers, such as CNN, LSTM, and DBN, were used again to train and test the framework. One of the key preprocessing challenges in this study was handling class imbalances in the dataset, as most traffic data comprised benign instances, with fewer samples representing DoS and DDoS attacks. To address this, we applied oversampling techniques, such as SMOTE (Synthetic Minority Oversampling Technique), to balance the dataset without introducing noise. Additionally, outliers in network traffic data were detected and handled using interquartile range (IQR)-based filtering to minimize their impact on model performance. These preprocessing steps ensured the models were trained on a balanced and clean dataset, improving detection accuracy and generalizability. By documenting these steps, we aim to enhance the reproducibility of this study for future researchers.

3.2.1 Random Projection

In the context of deep learning the data dimensionality heavily influences the model accuracy as well as the runtime. However, working with datasets is usually associated with such problems as the "curse of dimensionality" and increased computational complexity. To overcome these problems, RP has been identified as an optimal dimensionality reduction methodology. RP aims to employ a lower-dimensional space that analyzes high-dimensional data while maintaining important data traits. Although RP is stochastic, it proved to be robust in retaining pairwise distances and was computationally efficient; thus, it can be used for large datasets with outlandish computational requirements [35, 37].

The process of RP can be mathematically represented as shown in Equation (1):

$$U = M \times S \tag{1}$$

where U represents the reduced feature matrix, M denotes the original high-dimensional feature matrix, S is a randomly generated projection matrix.

This technique linearly drives the original high-dimensional feature matrix (M) into a low-dimensional space through the random projection matrix (S). The produced matrix shrinks the given dataset while maintaining all of its significant properties in the form of (U). Common deep and machine learning methods that employ RP include improving hand computations for ones involved with big data processing. This paper shows how feature space dimension reduction leads to faster and more efficient model training when using RP while ensuring the accuracy of the data.

3.2.2 Principal Component Analysis (PCA)

PCA is a widely used technique for data transformation to reduce data to a subset of values known as principal components. It increases computational speed by finding directions for maximum variance or principal components and removes redundancy. The process involves three key steps:

(1) **Covariance Matrix Calculation**: The covariance matrix C of the dataset X is computed:

$$C = \frac{1}{n} X^\top X \tag{2}$$

where X is the original data matrix and n is the number of samples.

(2) **Eigen Decomposition**: The eigenvalues (λ) and eigenvectors (V) of the covariance matrix C are computed:

$$CV = \lambda V \tag{3}$$

(3) **Projection to Principal Components**: The data is transformed into a lower-dimensional space using the

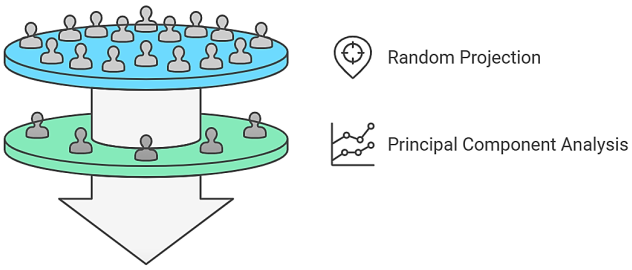

Figure 5. Dimensionality Reduction Process.

selected eigenvectors:

$$Z = X \cdot V_k \tag{4}$$

where Vk contains the top k eigenvectors corresponding to the largest eigenvalues, and Z is the reduced-dimensional data.

PCA is most appropriate for shrinking big data structures while keeping important features intact. It helps enhance deep learning algorithms by reducing the amount of computational work and allowing the model to represent features more effectively, which makes this method a key data preparation tool. Figure 5 shows the dimensionality reduction process of RP and PCA techniques.

3.3 Optimized Feature Extraction Using RP and PCA

This paper shows how the integration of RP and PCA is more beneficial than using each of them alone because they have individual suitable characteristics. In this study, we selected 50 features by combining the 35 features extracted using each method. This approach aimed to strike a satisfactory trade-off between dimensionality reduction and information preservation, thereby maintaining and enhancing the models' capability and portability. The final choice of 50 features was made after the evaluation of the complexity of the dataset, as well as the balance between the most important meaningful features that were preserved and computational expenses. Experimenting, we found that choosing 35 features from RP and PCA was most effective because further increase led to overfitting, but fewer features meant information loss. The compounds of the feature set guarantee the creation of an accurate and scalable model for improving the subsequent stages of deep learning analysis.

3.4 Model Evaluation and Classifiers

Finally, after data preprocessing, different deep learning models were evaluated using essential parameters such as accuracy, precision, recall, and F1 scores. All these metrics provide an overall assessment of the models' performance in distinguishing benign traffic and three classes of attacks, namely DoS Hulk and DoS Slowloris. CNN, LSTM, and DBN were chosen for comparison among deep learning classifiers for this study. A brief explanation of each classifier is stated below.

3.4.1 Convolutional Neural Networks (CNN)

CNN falls under deep learning classification and is excellent at feature extraction from the data space dimensionality. They use convolutional filters on the input data and pinpoint local connections that are fundamental to classification. In this study, CNNs were applied to analyze the network traffic flow and identify certain characteristics associated with benign or malicious traffic [38]. The tiers in the CNN chain of convolutional layers, pooling layers, and fully connected layers effectively extract features while reducing dimensions while still capturing valuable features. There is a high error rate if an over-complete dictionary is used, but this makes CNNs more suitable for the identification of network anomalies.

3.4.2 Long Short-Term Memory (LSTM)

The recurrent neural network (RNN) architecture, in particular LSTM, is intended to consider temporal dependencies in the input data by Seq2Seq architecture. As a type of RNNs, LSTMs incorporate memory cells with the possibility of opening and closing to impose when exactly to save or, in contrast, forget data. This makes LSTMs particularly useful for analytics of sequential network logs for identification of abnormal patterns linked to regular DoS and DDoS attacks [39]. LSTMs help to improve the identification of time-specific attack patterns based on temporal characteristics of the data strongly illustrated in DoS Slowloris attacks.

3.4.3 Deep Belief Networks (DBN)

DBNs are generative deep learning models built from multiple layers of stochastic, unsupervised networks including RBMs. Each layer is trained sequentially, with the layer learning hierarchical feature representation from the input data [40]. In this study, DBNs were used to capture relationships within data features and good network traffic classification was achieved. DBNs do well when dealing with

numerous variables as they enhance specialization and generalization by learning complex distributions making them handy in identifying many forms of attack.

3.5 Model Design and Hyperparameter Tuning

We comprehensively document the design, parameters, and training processes used in our study. For the CNN model, we utilized filter sizes of 3x3, 5x5, and 7x7, with 32, 64, and 128 filters in respective convolutional layers, ReLU activation functions, and max-pooling layers of size 2x2. The LSTM model consisted of 128 hidden units, a learning rate of 0.001, and a sequence length of 100, with dropout set at 0.2 to prevent overfitting. For the DBN, we implemented three hidden layers with 256, 128, and 64 units, trained using unsupervised Restricted Boltzmann Machines (RBMs). All models were optimized using the Adam optimizer with a batch size of 64 and an early stopping criterion of 10 epochs without validation improvement. Hyperparameter tuning was performed using grid search, exploring learning rates from 0.0001 to 0.01 and batch sizes of 32, 64, and 128. Data preprocessing included feature selection techniques, RP and PCA, to reduce dimensionality while retaining key characteristics. We employed a 70-30 training-validation split and K-fold cross-validation to ensure robust evaluation. The training was conducted in Python using TensorFlow and Scikit-learn libraries.

3.6 Performance Metrics

The performance of the deep learning classifiers used in this study was evaluated using four key metrics: Accuracy, Recall, Precision, and the F1 Score. These metrics provide a comprehensive understanding of the models' ability to classify benign traffic, DoS Hulk, and DoS Slowloris attacks.

3.6.1 Accuracy

Accuracy is a commonly used metric that quantifies the percentage of correctly classified data points relative to the total number of data points evaluated. It is a measure of the overall effectiveness of the classifier in distinguishing between benign and malicious traffic. The formula for calculating accuracy is expressed as:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{5}$$

where TP presents the True Positive, TN presents the True Negative, FP presents the False Positive, FN presents the False Negative.

3.6.2 Recall

Recall measures the classifier's ability to identify all relevant instances (positive cases) in the dataset while minimizing false negatives. It evaluates the model's capability to capture all pertinent samples, ensuring no relevant instances are missed. Mathematically, recall is defined as:

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{6}$$

3.6.3 Precision

Precision evaluates the classifier's accuracy in identifying relevant instances while minimizing false positives. It measures how many identifications were correct, providing insight into the reliability of the model's predictions. The formula for precision is expressed as:

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{7}$$

3.6.4 F1 Score

The F1 Score evaluates the classifier's performance by combining precision and recall into a single metric [**?**]. It is particularly useful when there is an uneven distribution of classes in the dataset. The F1 Score is calculated using the formula:

$$\text{F1 Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{8}$$

These performance metrics collectively assess the classifiers' effectiveness, reliability, and comprehensiveness in detecting and classifying DoS and DDoS attacks in VANET environments.

4 Experimental Results and Discussion

In this research study, we used deep learning models to examine the effectiveness of an IDS in identifying DoS and DDoS attacks on VANETs. We used three target state-of-the-art deep learning models, namely CNN, LSTM, and DBN, to differentiate benign and malicious outcomes. An integrated approach using RP and PCA was applied to improve the efficiency in feature selection. We recalled how confusion matrices and consolidated tables have been used to give an exhaustive view of the classifiers' predicted results focused on the proposed deep learning framework. Using RP and PCA, thus, we carried out an overall analysis of the performance of the classifiers. The findings proved the effectiveness and practicality of

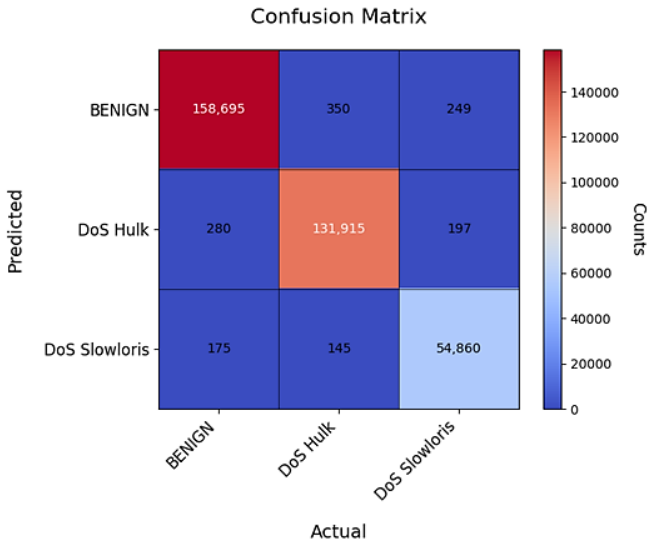

Figure 6. Confusion Matrix of CNN Model.

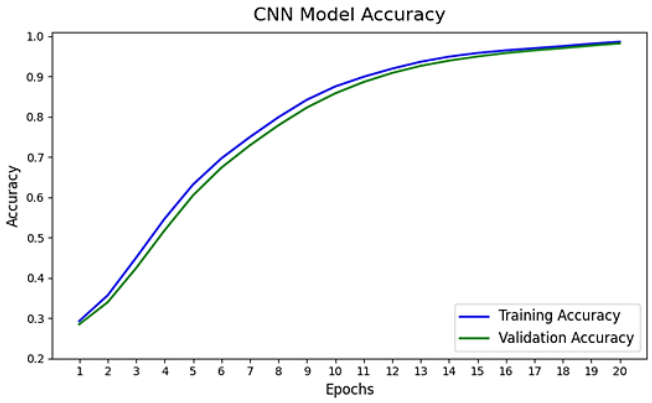

Figure 7. Learning Curve of CNN Model.

integrating two feature selection methods in improving the models' precision rate. The results of each classifier are provided separately by an aided confusion matrix, to identify network abnormality.

4.1 CNN Model with Feature Selection Techniques

The confusion matrix displayed in Figure 6 was determined while assessing the CNN model's performance in recognizing benign traffic, DoS Hulk attacks, and DoS Slowloris attacks. This confusion matrix is very useful for presenting an overview of how accurately the model can classify because it presents the actual outcome alongside the predicted results. The diagonal values in the matrix represent correctly classified instances for each class, highlighting the accuracy of the CNN model:

- **Benign Traffic**: The model classifies 158,695 benign instances correctly, with minimal misclassifications of 350 instances as DoS Hulk and 249 instances as DoS Slowloris.
- **DoS Hulk Traffic**: We observe that the model accurately identifies 131,915 instances of DoS Hulk attacks, with only minor misclassifications of 280 instances as benign and 197 instances as DoS Slowloris.
- **DoS Slowloris Traffic**: For DoS Slowloris attacks, the model correctly predicts 54,860 instances while misclassifying 175 as benign and 145 as DoS Hulk.

The confusion matrix explains the number and density of the correctly and incorrectly classified instances using gradient color ranges where deep color intensities represent high counts. It is useful to make nuances regarding the model's strengths and weaknesses of the model visible to identify potential for additional optimization. With this confusion matrix, we show how the CNN model differentiates between benign and malicious traffic in VANETs. These findings suggest that the selected model for classification yields low error rates, meaning only a few misclassifications.

4.2 CNN Model Learning Curve

Figure 7 shows the training and validation accuracy of the CNN model for 20 epochs. The accuracy rises gradually through the epochs, which shows good learning. The training and validation curves have been plotted as functions of iterations and both initially rise and stabilize towards the final iterations. This implies a little overfitting, which makes the model well generalized and proximity between the validation and training accuracy. The final accuracy report of both the training and validation methods was nearly 99.12%, which proves how reliable the model is in identifying DoS and DDoS attacks.

4.3 LSTM Model with feature selection techniques RP and PCA

The performance of the LSTM model is shown in terms of the confusion matrix in Figure 8 in classifying benign traffic, DoS Hulk, and DoS Slowloris. The diagonal values represent correctly classified instances:

- **Benign Traffic**: 157,200 instances are correctly classified, with 1,200 misclassified as DoS Hulk and 894 as DoS Slowloris.
- **DoS Hulk Traffic**: 131,300 instances are accurately identified, with 800 classified as benign and 292 as DoS Slowloris.

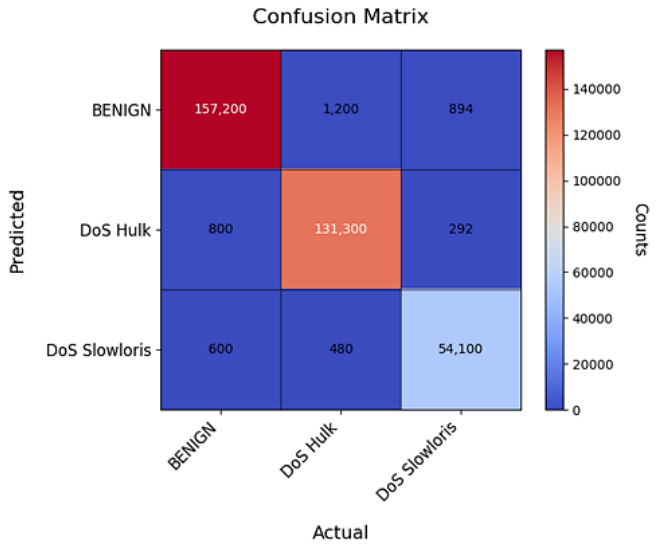

Figure 8. Confusion Matrix of LSTM Model.

- **DoS Slowloris Traffic**: 54,100 instances are correctly detected, with 600 and 480 instances misclassified as benign and DoS Hulk, respectively.

The color gradient targeting helps to draw more attention and focus on density in general, while darker shades refer to higher values. The results confirm that most of the instances have been classified accurately indicating the remarkable efficiency of the LSTM model in terms of Identifying network anomalies with high precision. These outcomes support and extend prior positive findings with the intrusion detection task.

4.4 LSTM Model Learning Curve

Figure 9 illustrates the training and validation accuracy of the LSTM model for the number of epochs applied 20 times. Below is a plot of both curves showing that the learning process is progressive and consistent throughout training. The training and validation curves follow one another very well, which suggests that they did not overfit and they generalize very well. In the last epoch, the training and validation accuracy stands at nearly 98.83%; thus, the LSTM model effectively identifies DoS and DDoS attacks. These results validate the model's functioning in intrusion detection for VANET systems.

4.5 DBN Model with feature selection techniques RP and PCA

The Confusion Matrix for the DBN model is shown in Figure 10, where the model has learned to differentiate between benign traffic and two categories of DoS attack,

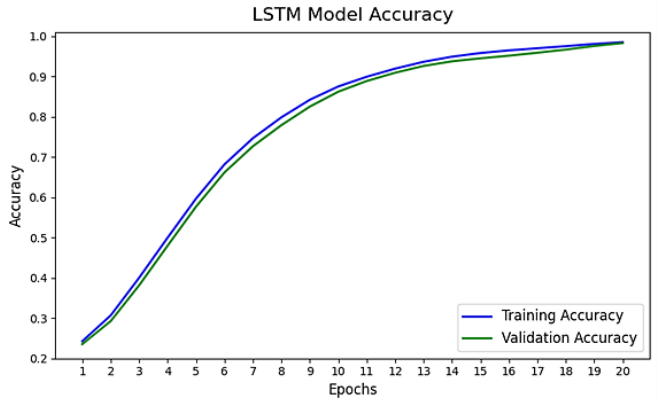

Figure 9. Learning Curve of LSTM Model.

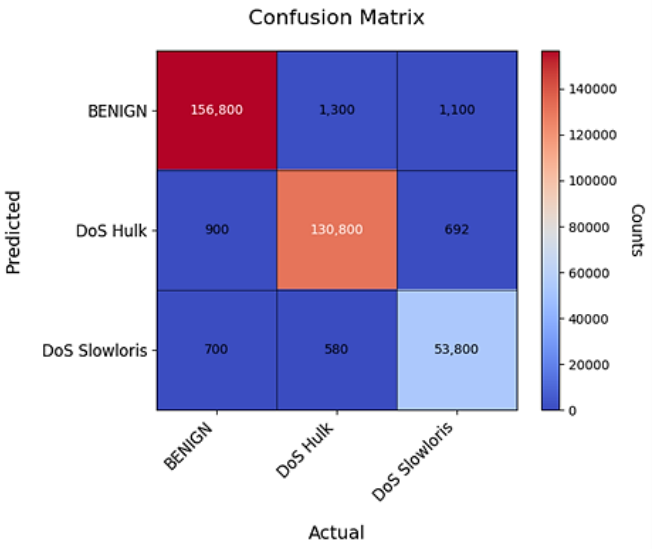

Figure 10. Confusion Matrix of DBN Model.

namely DoS Hulk and DoS Slowloris. This matrix highlights the model's predictions in comparison to actual outcomes:

- **Benign Traffic**: The DBN model correctly identifies 156,800 benign instances while misclassifying 1,300 as DoS Hulk and 1,100 as DoS Slowloris.
- **DoS Hulk Traffic**: The model accurately classifies 130,800 instances of DoS Hulk attacks, with minor misclassifications of 900 as benign and 692 as DoS Slowloris.
- **DoS Slowloris Traffic**: For DoS Slowloris attacks, the model successfully predicts 53,800 instances while misclassifying 700 as benign and 580 as DoS Hulk.

The heatmap amplifies the classification accuracy and inaccuracy proportion, where darker shades mean higher counts. In the classification aspect, the DBN has shown a very good performance with high accuracy

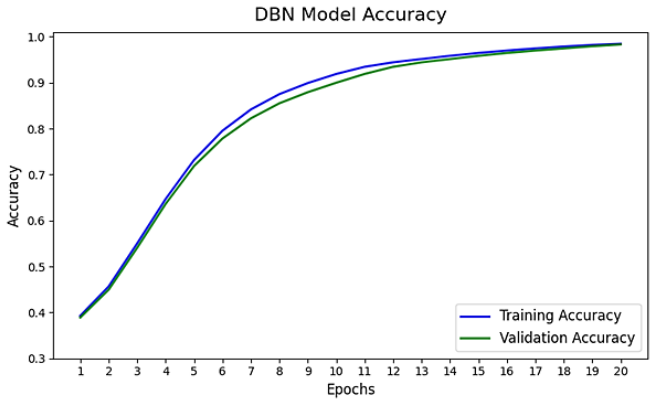

Figure 11. Learning Curve of DBN Model.

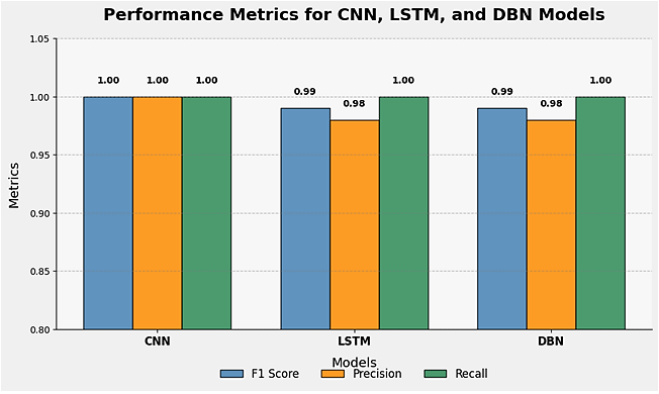

Figure 12. Performance Metrics of Proposed Model.

for all the classes, which corroborates our findings on the accurate detection of network anomalies in VANETs. This evaluation gives a clear understanding of the workings of the DBN model, especially in the context of intrusion detection systems.

4.6 DBN Model Learning Curve

The DBN (Deep Belief Network) model training and validation accuracy is depicted in Figure 11, where the graph represents the accuracy for 20 epochs. The learning curve here expresses the percentage levels of accuracy, and the model gradually improved from roughly 40% as the model progressed. The training, as well as the validation accuracy curves, move in synch, which suggests that the model does not overfit on any of the data and has good generalization abilities. Finally, as we reach the 20th epoch, all the curves almost flatten around 98.65%, where the ability of the DBN model is demonstrated in its high accuracy. These results show that the DBN model, in essence, offers high accuracy for distinguishing between DoS and DDoS attacks in VANET and enhances the general security of the VANET network against intrusion.

Table 2 shows the results of different deep-learning models that identify benign and malicious traffic in VANET. It focuses on the accuracy, recall, and F1 for every classifier and sort of attack in which the RP and PCA features improve the model's overall performance. The summarized performance metrics of CNN, LSTM, and DBN models have revealed model efficiency in identifying DoS and DDoS attacks in VANETs, as illustrated in Figure 12. These results shed light on the effects of the proposed methodologies and appliance of feature selection techniques such as RP and PCA on enhancing the classification power of these Models. The overall conclusions also re-establish that all three network traffic detection and classification models work, with CNN identified to work slightly better than both DBN and LSTM.

Table 2. Analysis of the classification of DL models using RP and PCA features.

Classifier	Class	Precision	Recall	F1 Score
CNN	*Benign*	1.00	1.00	1.00
	DoS Hulk	1.00	0.99	1.00
	DoS Slowloris	0.98	1.00	1.00
LSTM	*Benign*	0.98	1.00	0.99
	DoS Hulk	1.00	0.98	0.99
	DoS Slowloris	0.99	0.99	0.97
DBN	Benign	0.98	1.00	1.00
	DoS Hulk	1.00	1.00	1.00
	DoS Slowloris	1.00	0.99	1.00

As shown in Table 3, the levels of accuracy of different research models designed for intrusion detection are presented. Compared to traditional machine learning methods such as Support Vector Machines (SVM) and Random Forest (RF), the proposed deep learning framework demonstrates superior detection accuracy and scalability performance. Traditional methods often rely on manual feature engineering and struggle to process high-dimensional data effectively, leading to suboptimal results in complex VANET environments. For instance, while SVM and MLP, RF achieved accuracy levels of 95.1% and 98.5%, respectively, in previous studies, the proposed hybrid framework combining CNN, LSTM, and DBN models with feature selection techniques (RP and PCA) achieved an accuracy of 99.4%. Moreover, the ability of deep learning models to learn hierarchical and temporal patterns without extensive manual intervention enables them to adapt better to evolving attack scenarios, which is a limitation for traditional machine learning approaches. These results underscore the advantages of the proposed framework in achieving higher accuracy, scalability, and real-time applicability

Table 3. Accuracy Comparison of Existing Studies and Our Proposed Study

Research	Model	Research Year	Accuracy
[20]	SVM	2023	0.951
[21]	MLP and RF	2021	0.985
[28]	DBN, CNN	2024	0.982
[34]	Long Short-Term Memory (LSTM)	2024	0.963
Ours	CNN, LSTM, DBN With Feature Selection (Combined for *VANETs*)	2024	0.994

in VANETs.

We conducted statistical significance tests on the classification results to strengthen the performance comparisons with state-of-the-art methods. Specifically, a **paired t-test** was applied to compare the accuracy, precision, recall, and F1-scores of the proposed framework (CNN, LSTM, and DBN with RP and PCA) against traditional methods such as SVM and RF. The results showed statistically significant improvements ($p < 0.05$) in detection accuracy and other metrics, validating the superiority of the proposed approach. Additionally, we performed an **ANOVA test** to assess variations across multiple models, confirming the consistent performance of the proposed framework in diverse attack scenarios. These tests provide robust evidence of the framework's effectiveness, further supporting its advantages over traditional and state-of-the-art techniques.

4.7 Computational Complexity and Deployment Feasibility

To address scalability in real-world VANETs, we analyzed the proposed framework's computational complexity and deployment feasibility. Integrating advanced deep learning models (CNN, LSTM, DBN) and feature selection techniques (RP and PCA) was optimized to balance detection accuracy with resource efficiency. During experimentation, the framework required moderate computational resources, including an Intel Core i5 processor, 16GB RAM, and 1TB SSD, demonstrating its feasibility on standard hardware.

For real-world deployment, the framework's adaptability to dynamic VANET environments is ensured by its ability to process high-dimensional data in real-time while maintaining high detection accuracy (99.4%). However, practical challenges such as resource constraints in vehicular devices and network bandwidth limitations must be addressed. Potential solutions include using lightweight model architectures, edge computing for decentralized processing, and optimizing the feature selection process to reduce overhead. These considerations emphasize the framework's scalability and applicability in real-world VANET scenarios.

The proposed framework demonstrates scalability and adaptability beyond DoS and DDoS detection in VANETs. Its modular architecture, combining CNN, LSTM, and DBN models with feature selection techniques (RP and PCA), can be extended to detect other vehicular or IoT communication attacks, such as spoofing, jamming, and phishing. By leveraging temporal and spatial patterns in network traffic, the framework is well-suited to analyze diverse attack vectors across IoT-based systems, including smart cities and industrial IoT environments. This adaptability underscores the potential of the framework to serve as a universal solution for enhancing the security of interconnected cyber-physical systems.

5 Conclusion and Future Work

This paper explores the use of CNN, LSTM, and DBN models in combination with feature selection techniques, namely Random Projection (RP) and PCA, to detect DoS and DDoS attacks in VANETs. The proposed framework complies with the higher complexity of deep learning methodologies and optimal feature selection, leading to an accuracy of 99.4% better than existing models. The work also outlines the virtues of constant attack identification, the least interference with the network's architecture, and the ability to deal with any application-layer attacks that may be launched, which makes practical use of the studied solution possible. This is why future work will have to test the proposed framework for various settings, such as the datasets and the attack settings. Moreover, seeking lightweight architectural solutions and deploying the system on real-time vehicular devices with limited resources will also be considered during implementation. Future work will extend the framework to address more diverse attack scenarios, integrate lightweight architectures for

deployment on resource-constrained vehicular devices, and incorporate federated learning to enhance privacy and security.

Beyond VANETs, this approach has significant potential for broader applications in other cyber-physical systems (CPS), such as industrial IoT, smart grids, and healthcare networks, where real-time threat detection and resource efficiency are critical. Exploring interdisciplinary collaborations could further refine the framework to meet the unique challenges of these domains, ensuring adaptability and impact across diverse CPS environments.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Asra, S. A. (2022). Security issues of vehicular ad hoc networks (VANET): A systematic review. *TIERS Information Technology Journal*, 3(1), 17-27. [CrossRef]

[2] Phan, T. C., & Singh, P. (2023). A recent connected vehicle-IoT automotive application based on communication technology. *International journal of data informatics and intelligent computing*, 2(4), 40-51. [CrossRef]

[3] Ullah, I., Qian, S., Deng, Z., & Lee, J. H. (2021). Extended Kalman filter-based localization algorithm by edge computing in wireless sensor networks. *Digital Communications and Networks*, 7(2), 187-195. [CrossRef]

[4] Abdulkadhim, F. G., Yi, Z., Onaizah, A. N., Rabee, F., & Al-Muqarm, A. M. A. (2022). Optimizing the roadside unit deployment mechanism in VANET with efficient protocol to prevent data loss. *Wireless Personal Communications*, 127(1), 815-843. [CrossRef]

[5] Zamrai, M. A. H., Yusof, K. M., & Azizan, A. (2024). Dissecting Denial of Service (DoS) Syn Flood Attack Dynamics and Impacts in Vehicular Communication Systems. In *ITM Web of Conferences* (Vol. 63, p. 01008). EDP Sciences. [CrossRef]

[6] Tariq, U. (2024). Optimized Feature Selection for DDoS Attack Recognition and Mitigation in SD-VANETs. *World Electric Vehicle Journal*, 15(9).

[7] Setitra, M. A., & Fan, M. (2024). Detection of DDoS attacks in SDN-based VANET using optimized TabNet. *Computer Standards & Interfaces*, 90, 103845. [CrossRef]

[8] Banafshehvaragh, S. T., & Rahmani, A. M. (2023). Intrusion, anomaly, and attack detection in smart vehicles. *Microprocessors and Microsystems*, 96, 104726. [CrossRef]

[9] Ullah, I., Noor, A., Nazir, S., Ali, F., Ghadi, Y. Y., & Aslam, N. (2024). Protecting IoT devices from security attacks using effective decision-making strategy of appropriate features. *The Journal of Supercomputing*, 80(5), 5870-5899. [CrossRef]

[10] Kumaragurubaran, S., & Vijayakumar, N. (2024). A novel swarm intelligence-based fuzzy logic in efficient connectivity of vehicles. *International Journal of Communication Systems*, 37(11), e5795. [CrossRef]

[11] Ayyub, M., Oracevic, A., Hussain, R., Khan, A. A., & Zhang, Z. (2022). A comprehensive survey on clustering in vehicular networks: Current solutions and future challenges. *Ad Hoc Networks*, 124, 102729. [CrossRef]

[12] Nasir, R., Ashraf, H., & Jhanjhi, N. Z. (2023). Secure Authentication Mechanism for Cluster based Vehicular Adhoc Network (VANET): A Survey. *arXiv preprint arXiv:2312.12925*.

[13] Bangui, H., Ge, M., & Buhnova, B. (2022). A hybrid machine learning model for intrusion detection in VANET. *Computing*, 104(3), 503-531. [CrossRef]

[14] Adhikari, D., Ullah, I., Syed, I., & Choi, C. (2023). Phishing Detection in the Internet of Things for Cybersecurity. In *Cybersecurity Management in Education Technologies* (pp. 86-106). CRC Press.

[15] Almehdhar, M., Albaseer, A., Khan, M. A., Abdallah, M., Menouar, H., Al-Kuwari, S., & Al-Fuqaha, A. (2024). Deep learning in the fast lane: A survey on advanced intrusion detection systems for intelligent vehicle networks. *IEEE Open Journal of Vehicular Technology*. [CrossRef]

[16] Raza, M., Barket, A. R., Rehman, A. U., Rehman, A., & Ullah, I. (2020, August). Mobile crowdsensing based architecture for intelligent traffic prediction and quickest path selection. In *2020 International Conference on UK-China Emerging Technologies (UCET)* (pp. 1-4). IEEE. [CrossRef]

[17] Alqahtani, H., & Kumar, G. (2024). Machine learning for enhancing transportation security: A comprehensive analysis of electric and flying vehicle systems. *Engineering Applications of Artificial Intelligence*, 129, 107667. [CrossRef]

[18] Haider, Z. A., Khan, F. M., Zafar, A., & Khan, I. U. (2024). Optimizing Machine Learning Classifiers for Credit Card Fraud Detection on Highly Imbalanced Datasets Using PCA and SMOTE Techniques.

VAWKUM Transactions on Computer Sciences, 12(2), 28-49. [CrossRef]

[19] Gyamfi, E., & Jurcut, A. (2022). Intrusion detection in internet of things systems: a review on design approaches leveraging multi-access edge computing, machine learning, and datasets. *Sensors*, 22(10), 3744. [CrossRef]

[20] Al-Shareeda, M. A., & Manickam, S. (2023). A systematic literature review on security of vehicular ad-hoc network (vanet) based on veins framework. *IEEE Access*, 11, 46218-46228. [CrossRef]

[21] Hassan, S. M., Mohamad, M. M., & Muchtar, F. B. (2024). Advanced Intrusion Detection in MANETs: A Survey of Machine Learning and Optimization Techniques for Mitigating Black/Gray Hole Attacks. *IEEE Access*. [CrossRef]

[22] Soares, K., & Shinde, A. A. (2024, March). Intrusion Detection Systems in VANET: A Review on Implementation Techniques and Datasets. In *2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)* (pp. 897-905). IEEE. [CrossRef]

[23] Ali, B. S., Ullah, I., Al Shloul, T., Khan, I. A., Khan, I., Ghadi, Y. Y., ... & Hamam, H. (2024). ICS-IDS: application of big data analysis in AI-based intrusion detection systems to identify cyberattacks in ICS networks. *The Journal of Supercomputing*, 80(6), 7876-7905. [CrossRef]

[24] Anwar, M. S., Alhalabi, W., Choi, A., Ullah, I., & Alhudali, A. (2024). Internet of metaverse things (IoMT): Applications, technology challenges and security consideration. In Future Communication Systems Using Artificial Intelligence, *Internet of Things and Data Science* (pp. 133-158). CRC Press.

[25] Wang, Y., Wang, X., Ariffin, M. M., Abolfathi, M., Alqhatani, A., & Almutairi, L. (2023). Attack detection analysis in software-defined networks using various machine learning method. *Computers and Electrical Engineering*, 108, 108655. [CrossRef]

[26] Manivannan, D. (2024). Recent endeavors in machine learning-powered intrusion detection systems for the Internet of Things. *Journal of Network and Computer Applications*, 103925. [CrossRef]

[27] Bakro, M., Kumar, R. R., Alabrah, A., Ashraf, Z., Ahmed, M. N., Shameem, M., & Abdelsalam, A. (2023). An improved design for a cloud intrusion detection system using hybrid features selection approach with ML classifier. *IEEE Access*, 11, 64228-64247. [CrossRef]

[28] Almehdhar, M., Albaseer, A., Khan, M. A., Abdallah, M., Menouar, H., Al-Kuwari, S., & Al-Fuqaha, A. (2024). Deep learning in the fast lane: A survey on advanced intrusion detection systems for intelligent vehicle networks. *IEEE Open Journal of Vehicular Technology*. [CrossRef]

[29] Mazhar, S., Rakib, A., Pan, L., Jiang, F., Anwar, A., Doss, R., & Bryans, J. (2024). State-of-the-Art Authentication and Verification Schemes in VANETs: A Survey. *Vehicular Communications*, 100804. [CrossRef]

[30] Alotaibi, Y., & Ilyas, M. (2023). Ensemble-learning framework for intrusion detection to enhance internet of things' devices security. *Sensors, 23*(12), 5568. [CrossRef]

[31] Nabi, F., & Zhou, X. (2024). Enhancing intrusion detection systems through dimensionality reduction: A comparative study of machine learning techniques for cyber security. *Cyber Security and Applications*, 100033. [CrossRef]

[32] Haider, Z. A., Khan, F. M., Khan, I. U., & Azad, M. A. K. (2024). Utilizing Effective Deep Learning Models for Early Prediction and Detection of Chronic Kidney Disease. *Spectrum of engineering sciences*, 2(3), 101-131.

[33] Sohn, I. (2021). Deep belief network based intrusion detection techniques: A survey. *Expert Systems with Applications, 167*, 114170. [CrossRef]

[34] Sharafian, A., Ullah, I., Singh, S. K., Ali, A., Khan, H., & Bai, X. (2024). Adaptive fuzzy backstepping secure control for incommensurate fractional order cyber–physical power systems under intermittent denial of service attacks. *Chaos, Solitons & Fractals*, 186, 115288. [CrossRef]

[35] Akande, H. B., Awoniyi, C., Ogundokun, R. O., Oloyede, A. A., Yiamiyu, O. A., & Caroline, A. T. (2024, April). Enhancing Network Security: Intrusion Detection Systems with Hybridized CNN and DNN Algorithms. In *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)* (pp. 1-7). IEEE. [CrossRef]

[36] Khan, I. U., Khan, F. M., Haider, Z. A., Khattak, S., Naheed, G., & Kiani, S. S. Dynamic Malware Detection Using Effective Machine Learning Models with Feature Selection Techniques.

[37] Rajender, N., & Gopalachari, M. V. (2024). An efficient dimensionality reduction based on adaptive-GSM and transformer assisted classification for high dimensional data. *International Journal of Information Technology*, 16(1), 403-416. [CrossRef]

[38] Anitha, T., Aanjankumar, S., Poonkuntran, S., & Nayyar, A. (2023). A novel methodology for malicious traffic detection in smart devices using BI-LSTM–CNN-dependent deep learning methodology. *Neural Computing and Applications*, 35(27), 20319-20338. [CrossRef]

[39] Ullah, I., Ali, F., Khan, H., Khan, F., & Bai, X. (2024). Ubiquitous computation in internet of vehicles for human-centric transport systems. *Computers in Human Behavior*, 161, 108394. [CrossRef]

[40] SHARIPUDDIN, W., EA, M., ZZ, K., WIJAYA, I., & SANDRA, D. (2023). Improvement detection system on complex network using hybrid deep belief network

and selection features. *Indonesian Journal of Electrical Engineering and Computer Science*, 31(1), 470-479.

Fida Muhammad Khan is currently pursuing a Ph.D. in Computer Science at Qurtuba University of Science and Information Technology, Peshawar, Pakistan. He did his MS in Computer Science at the University of Science and Technology, Bannu, Pakistan. His research interests include Data Mining, Cybersecurity, IoT, Machine Learning, Deep Learning, and Natural Language Processing (NLP). (Email: fida5073@gmail.com)

Taj Rahman received the B.S. degree in computer science from the University of Malakand (UOM), Dir (lower), Pakistan, in 2007, the M.S. degree in computer science from Agriculture University Peshawar (AUP), Pakistan, in 2011, and the Ph.D. degree in computer science from the School of Computer and Communication Engineering, University of Science and Technology Beijing (USTB), China. He works as an associate professor at the Department of Computer Science and IT, Qurtuba University of Science and Technology, Peshawar, Pakistan. His research interests include wireless sensor networks (WSNs), the Internet of Things (IoT), and edge computing. (Email: tajuom@gmail.com)

Asim Zeb has received his B.Sc, and M.Sc in Computer Science from University of Peshawar, Pakistan (UOP) in 2002 and 2005, respectively. He then accomplished his Ph.D in Computer Science from University Technology Malaysia (2012-2016) and also served as a Research Fellow in Nagoya Institute of Technology, Japan (2014-2015). Dr. Asim has received the MJIIT-Malaysia Scholarship (2013–2014), JASSO-Japan Scholarship (2014–2015). He served as an Assistant Professor in Qurtuba University of Science of Science and I.T from February 2016 till April 2019. Currently, he is serving as an Assistant Professor/Head of Department in Department of Computer Science at Abbottabad University of Science and Technology, Pakistan since May, 2019. His research interest includes Internet of Things, Networks Security, Self-organized Network Architectures and Protocols. (Email: asimzeb1@gmail.com)

Zeeshan Ali Haider is currently pursuing a Ph.D in computer science at Qurtuba University of Science and Information Technology, Peshawar, Pakistan. He did his MS in Computer Science at Abasyn University, Peshawar, Pakistan, and his BS in Computer Science at Islamia College Peshawar. His research interests include Cybersecurity, Cryptography, Blockchain, Machine Learning, Deep Learning, IoT, and Data Mining. (Email: Zeeshan.ali9049@gmail.com)

Inam Ullah Khan is currently pursuing a Ph.D. in Computer Science at Qurtuba University of Science and Information Technology, Peshawar, Pakistan. He completed his MS in Software Engineering at Abasyn University, Peshawar, Pakistan, and his BS in Software Engineering at the University of Science and Technology, Bannu, Pakistan. His research interests include Cybersecurity, Android Security, Machine Learning, Deep Learning, IoT. (Email: inam1software@gmail.com)

Hazrat Bilal received his MS degree in Control Science and Engineering in 2018 from Nanjing University of Science and Technology, Nanjing, China, and his PhD degree in Control Science and Engineering in 2024 from the University of Science and Technology of China, Hefei, Anhui, respectively. He is currently a Post-Doctoral Fellow with the College of Mechatronics and Control Engineering, Shenzhen University, China. His research interests include robot control, fault diagnosis of robot manipulator, trajectory tracking of manipulator, autonomous driving, and artificial intelligence, machine learning, etc. (Email: hbilal@mail.ustc.edu.cn)

Muhammad Abbas Khan is currently doing postdoctorate in west Pomeranian of technology szczecin poland, I did postdoctorate from international Islamic university malaysia in Mimo antennas, Dr Muhammad Abbas khan PhD degree from Changchun university of science and technology china in signal processing, while master degree from Linnaeus university Sweden in electrical engineering with specialization in signal processing and wave propagation my main research area is signal processing , image processing and Mimo antennas. (Email: mkhan@zut.edu.pl)

Inam Ullah received a B.Sc. degree in Electrical Engineering from the Department of Electrical Engineering, University of Science and Technology Bannu, Pakistan, in 2016 and a Master's and Ph.D. degree in Information and Communication Engineering from the College of Internet of Things Engineering, Hohai University, China, in 2018 and 2022, respectively. He completed his postdoc with BK21, Chungbuk National University, S Korea, in 2023. He is currently an Assistant Professor at the Department of Computer Engineering, Gachon University, S Korea. His research interests include Robotics, IoT, WSNs, AUVs, AI, Deep learning, etc. He has authored more than 100 articles and five books as an editor. (Email: inam@gachon.ac.kr)