Defense Mechanisms for Vehicular Networks: Deep Learning Approaches for Detecting DDoS Attacks

Lekshmi V[1], R. Suji Pramila[2], Tibbie Pon Symon V A[3]
Research Scholar, Department of Computer Science and Engineering,
Noorul Islam Centre for Higher Education, Kumaracoil, Tamil Nadu, India[1]
Assistant Professor, Department of Computer Science and Engineering,
Mar Baselios Institute of Technology and Science, Nellimattom, India[2]
Assistant Professor, Department of Electrical and Electronics Engineering,
Noorul Islam Centre for Higher Education, Kumaracoil, Tamil Nadu, India[3]

***Abstract*—Vehicular Ad-hoc Networks (VANETs) are engineered to meet the distinctive demands of vehicular communication, facilitating interactions between vehicles and roadside infrastructure to enhance road safety, traffic efficiency, and diverse applications such as traffic management and infotainment services. However, the looming threat of Distributed Denial of Service (DDoS) attacks in VANETs poses a significant challenge, potentially disrupting critical services and compromising user safety. To address this challenge, this study proposes a novel deep learning (DL)-based model that integrates Long Short-Term Memory (LSTM) architecture with self-attention mechanisms to effectively detect DDoS attacks in VANETs. By incorporating autoencoders for feature extraction, the model leverages the sequential nature of VANET data, prioritizing relevant information within input sequences to accurately identify malicious activities. With an impressive accuracy of 98.39%, precision of 97.79%, recall of 98.00%, and F1-score of 98.20%, the proposed approach demonstrates remarkable efficacy in safeguarding VANETs against cyber threats, thereby contributing to enhanced road safety and network reliability.**

Keywords*—Vehicular Ad-hoc Networks; Denial of Service attacks; deep learning; auto encoder; Long Short-Term Memory; self-attention mechanism; cyber threats; network reliability

I. Introduction

Securing communication among vehicles has become a significant focus in computer science recently. Employing a spontaneously formed network installed on a vehicle is a method to achieve this. A mobile ad hoc network, VANET, facilitates communication between nearby cars. Vehicles in VANETs are furnished with wireless communication tools, such as Dedicated Short-Range Communication (DSRC) or Cellular-Vehicle-to-Everything (C-V2X) technology, allowing direct communication between vehicles (V2V) and between vehicles and infrastructure (V2I). These communication capabilities facilitate the transmission of essential safety information, including vehicle location, velocity, and heading, as well as non-safety-related information, such as traffic conditions and service advertisements [1]. The dynamic nature of vehicular environments poses several challenges to the design and operation of VANETs. Vehicles move at high speeds, leading to rapidly changing network topologies and communication conditions.

Moreover, VANETs are subject to intermittent connectivity, network partitions, and unpredictable communication delays due to factors such as vehicle mobility, radio interference, and obstacles in the environment. Despite these challenges, VANETs offer immense potential to improve traffic safety and effectiveness via the deployment of intelligent transportation systems (ITS). By enabling vehicles to cooperate and share information in real time, VANETs can mitigate accidents, reduce traffic congestion, and provide drivers with timely and context-aware services.

In recent years, research efforts in VANETs have focused on addressing key issues such as communication reliability, security, privacy, and scalability. Advanced communication protocols, routing algorithms, and congestion control mechanisms have been proposed to optimize the performance of VANETs in dynamic and resource-constrained environments [2]. Additionally, protective metrics such as verification, data encryption, and threat detection are crucial to defend VANETs from harmful intrusions and illegal access. As the automotive industry continues to embrace connected and autonomous vehicles (CAVs), the role of VANETs is expected to become increasingly prominent. CAVs rely on VANETs for cooperative perception, decision-making, and coordination, enabling them to safely and effectively manoeuvre through intricate traffic situations. Additionally, advancing technologies like 5G and edge computing offer promising possibilities to further enhance the capabilities of VANETs by providing high-speed connectivity and low-latency communication services. Various attack types in VANETs are classified by origin and behavior. External attacks, originating outside the network, aim to disrupt VANET operations through unauthorized access or denial-of-service tactics. Internal attacks originate from compromised nodes within the network, challenging detection and mitigation efforts. Active attacks manipulate or disrupt communication, while passive attacks eavesdrop to gather data. Area attacks target specific regions, affecting multiple vehicles or units, and communication attacks disrupt communication channels. Rational attackers engage in malicious activities without personal gain, complicating security measures [3]. These attack types emphasize the need for comprehensive strategies to protect VANET integrity and user privacy.

A. DDoS Attack in VANET

In a Denial of Service (DoS) attack, the attacker interferes with the services provided by a service provider, preventing legitimate users from accessing the network despite the availability of resources [4]. The attacker achieves this by blocking the communication medium in specific areas, limiting the attack to the service provider's scope. This can be done in two ways: the attacker either floods the resources with an overwhelming number of requests, keeping them occupied with fake requests, or extends the attack by sending numerous requests to block communication, thus preventing the RSU from processing any OBU requests. Conversely, DDoS attacks are a distributed form of DoS attacks where multiple attackers from various locations simultaneously target one or more service providers, causing significant inconvenience.

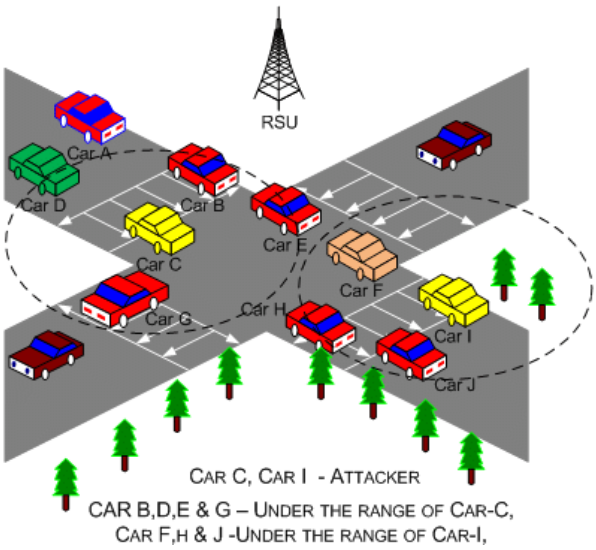

Fig. 1. DDoS attack.

In these attacks, a larger number of malicious OBU nodes block legitimate users from accessing services through multiple RSUs by spamming the network, leading to increased transmission delays. This type of attack poses a significant threat to VANETs, as illustrated in Fig. 1, where cars C and I disrupt services provided by an RSU by preventing cars B, D, E, G, F, H, and J from accessing it. The primary objectives of the paper are as below:

- To propose a novel DL-based method for the effective detection of DDoS attacks in VANET.
- To incorporate auto encoders for better feature extraction.
- Evaluate the efficiency of the proposed model with the current approaches.

The remaining of the paper is structured as: Section II provides an overview of existing methodologies for detecting attacks in VANETs, laying the foundation for the proposed research. Section III outlined the method details of the proposed approach. The outcomes of the study, including the efficiency of the suggested approach in detecting alternative approaches, are discussed in Section IV. Final, Section V offers remarks summarizing the findings and implications of our work.

II. LITERATURE REVIEW

Zu et al. [5] introduced a detection method that utilized beacon packets in vehicles to trace malicious vehicle sources. Their approach involved Roadside Units (RSUs) instructing vehicles to execute key transmission and reception, enabling them to assert their physical presence. RSUs then analyzed beacon packets to construct a neighbor graph, determining vehicle credibility. Experimental findings validated the efficacy of the proposed method, achieving identification and monitoring of Sybil vehicles with accuracy and recall rates of 98.53% and 95.93%, respectively. Significantly, the approach surpassed current solutions, especially in sustaining consistent detection rates in conditions of high vehicular density.

The FC-LSR system, proposed by Almazroi et al. [6], introduced a fog computing-based lightweight solution to combat Sybil attacks in 5G-equipped vehicular networks. Utilizing Modified Merkle Patricia Trie (MMPT) and Merkle Hash Tree (MHT), the system securely stored vehicles' 'current status' values while ensuring data anonymity. Significantly, the approach surpassed current solutions, especially in sustaining consistent detection rates in conditions of high vehicular density. However, limitations involve vulnerability to neighbor-based manipulation and single-point failure risks.

Ahmed et al. [7] proposed an Intrusion Detection System (IDS) utilizing ML to mitigate DDoS attacks in VANETs. The approach addressed rising security concerns, particularly due to DoS and DDoS attacks flooding the network with malicious packets. By combining Random Projection (RP) and Randomized Matrix Factorization (RMF) methods, the IDS sought to improve detection abilities by extracting significant features from network traffic data. Experimental evaluation revealed outstanding accuracy compared to existing methods, with a combined accuracy of 0.98. However, research focused specifically on the identification of DoS and DDoS attacks and did not address energy consumption or computational complexity.

Dayyani & Abbaspour [8] proposed the SybilPSIoT method, which proposed a combined method integrating prevention and detection in a decentralized manner in Social Internet of Things (SIoT) based on smart contracts. A model utilized signed SIoT network entities and labels functioning as points in a network, and incorporating trust paths to assess the target node. Game theory was employed for access control to prevent Sybil from creating new objects. The method was found to be efficient in rapid detection and prevention of Sybil, considering the limitations of smart contracts. Evaluation data showed its superior performance compared to the SybilSCAR approach.

A DL model based on GRU was proposed by ALMahadin et al. [9] for detecting anomalies in VANET network traffic hence it is crucial for identifying unknown threats like DoS floods and providing security insights for multimedia services. The proposed model, SEMI-GRU, utilized a semi-supervised approach to enhance accuracy. Results showed that SEMI-GRU outperformed existing methods with low false positive rates. However, challenges remained, including real-time detection and limited labeled data accessibility.

Vermani et al. [10] suggested a framework utilizing ensemble learning to identify malicious nodes. in SDN-based VANETs, with a particular emphasis on internal position falsification attacks. Various ML algorithms, including SVM, k-NN, Logistic Regression (LR), Naïve Bayes (NB), and Random Forest (RF), were evaluated using the VeReMi dataset. Among the ML algorithms tested, Random Forest demonstrated the most effective performance in identifying attacks. Additionally, the study compared two collective classification techniques, voting and stacking, used for the purpose of decision-making. Both approaches improved classification accuracy and reduced prediction time, with stacking requiring less time than voting while achieving comparable accuracy levels to Random Forest. However, the study's focus on internal position falsification attacks within SDN-based VANETs limited its generalizability to other attack types and VANET configurations.

Magsi et al. [11] aimed to propose a comprehensive solution addressing the security, privacy, and routing challenges in Vehicular Named Data Networking (VNDN). Introduced three key components: an ML-based reputation evaluation model, a decentralized blockchain system for privacy preservation, and the enhancement of VNDN routing through a transition from pull to push-based content dissemination using a Publish-Subscribe (Pub-Sub) approach. The approach utilised ML techniques for attacker detection, blockchain for privacy preservation, and Pub-Sub for efficient content distribution. For evaluation, utilized the BurST-Australian dataset for Misbehavior Detection (BurST-ADMA) and applied five ML classifiers, including LR, Decision Tree, KNN, RF, and NB. The outcomes demonstrated that the RF achieved the highest accuracy rate in identifying attackers, followed by Decision Tree. Despite promising outcomes, the study faced limitations, such as reliance on simulation-based datasets and potential scalability challenges associated with blockchain integration.

Alsarhan et al. [12] proposed the utilization of SVM along with three intelligent optimization algorithms - Genetic Algorithm, Particle Swarm Optimization, and Ant Colony Optimization for attack detection in VANET. The primary objective was to optimize the accuracy of intrusion detection in VANETs by fine-tuning the parameters of the SVM classifier using optimization algorithms. The model addressed the security vulnerabilities in VANETs and improve the reliability of communication among smart vehicles. To assess how well the suggested approach works, trials were carried out utilizing the NSL-KDD dataset, and the performance of each optimization algorithm in optimizing SVM parameters was assessed based on classification accuracy. The study sought to contribute to the development of more robust intrusion detection systems for VANETs, thereby enhancing the security of vehicular communication systems. Despite the promising results obtained, the study acknowledged limitations such as reliance on simulated data and the exclusive focus on SVM-based detection methods.

Patil & Mallapur [13] enhanced the security of message dissemination within VANET by integrating ML, blockchain, and the interplanetary file system (IPFS). The methodology involved blockchain technology to create immutable records of events in a distributed environment, complemented by IPFS for storing event content with addressability. Metadata information from IPFS was managed using smart contracts and uploaded to a distributed ledger. Subsequently, K-means clustering was employed to classify vehicles as malicious or benign, followed by the use of a SVM classifier to find malicious event messages. The evaluation of the proposed system demonstrated its effectiveness in identifying and filtering out malicious messages, thereby ensuring the transmission of only secure messages within the network. Furthermore, the approach exhibited minimal consumption time compared to existing methods, indicating its efficiency in event detection and validation. However, limitations included the reliance on theoretical analysis and simulations for evaluation.

Canh & HoangVan [14] proposed a ML-driven strategy to identify blackhole attacks within VANET, aiming to fortify network security. Initially, a thorough dataset comprising both normal and malicious traffic flows was compiled to facilitate analysis. Distinctive features were identified to differentiate blackhole attacks from typical network behavior. Subsequently, a range of ML algorithms, including Gradient Boosting (GR), RF, SVMs, KNN, NB, and LR, were evaluated for their efficacy in differentiating between normal and harmful nodes. Experimental outcomes showcased the superior performance of GR and RF algorithms in pinpointing blackhole nodes, followed by SVMs and KNN. Although NB and LR demonstrated relatively lower effectiveness, they offered valuable insights into the detection process.

In response to the urgent need for robust detection mechanisms to safeguard VANET against DDoS attacks, a hybrid algorithm based on SVM kernels, AnovaDot, and RBFDot, was proposed by Adhikary et al. [15]. The aim was to enhance the DDoS attacks detection in VANETs and mitigate potential threats to commuter safety and network integrity. The proposed hybrid algorithm leveraged features such as packet drop, jitter, and collisions to simulate network communication scenarios under both normal conditions and DDoS attacks. The hybrid model exhibited higher accuracy and effectiveness in differentiating between normal and DDoS attacks, as evidenced by improved performance metrics across the evaluation criteria. One limitation was the complexity of implementing and fine-tuning the hybrid model, which required significant computational resources and expertise. Additionally, the effectiveness of the algorithm varied depending on the specific characteristics of the VANET environment and the nature of the DDoS attacks encountered.

Anyanwu et al. [16] introduced an IDS targeting DDoS attacks. With the Radial Basis Function (RBF) kernel of the SVM classifier and a Grid Search Cross-Validation (GSCV) method, the IDM aimed to enhance detection accuracy. Deployed on OBUs, it analysed vehicular data to classify messages as benign of a DDoS attack. Experimental results demonstrated superior performance compared to alternative ML algorithms, with optimal RBF-SVM parameters of "C"=100 and "gamma" (γ)=0.1. Achieving an accuracy 99.33% and a detection rate 99.22%, the IDM outperformed existing benchmarks, highlighting its efficacy in detecting DDoS intrusions.

A fog computing-based Sybil attack detection framework (FSDV) was proposed by Paranjothi & Atiquzzaman.[17]

FSDV utilized onboard units (OBUs) installed in vehicles to establish a dynamic fog for detecting rogue nodes, aiming to mitigate scenarios with high vehicle density. Evaluations conducted through simulations using OMNET++ and SUMO simulators revealed significant improvements with FSDV, achieving a reduction of 43% in processing delays, 13% in overhead, and 35% in FPR compared to existing schemes. Notably, FSDV demonstrated scalability and efficiency, outperforming previous techniques by up to 32%. Furthermore, it eliminated the reliance on roadside infrastructures or historical vehicle data for rogue node detection, providing a notable advantage. Despite its effectiveness, FSDV is subject to simulation-based constraints.

Velayudhan et al. [18] developed the Emperor Penguin Optimization (EPO) based Routing protocol (EPORP) to tackle the challenge of identifying Sybil attacks and enhancing system efficiency in VANETs. The main goal was to detect Sybil attacks and bolster security within VANETs, achieved through the utilization of the Rumour riding technique for Sybil attack detection and the Split XOR (SXOR) operation for safeguarding messages and data. In SXOR, the optimal key was generated using the EPO algorithm. Results indicated that the EPORP protocol outperformed others with a higher delivery ratio (0.96), demonstrating superior message delivery capabilities. However, the study faced limitations including reliance on simulation-based assessments.

The Sybil Detection using Classification (SDTC) approach was introduced by Kakulla & Malladi [19] to mitigate Sybil attacks within VANETs. SDTC leveraged Extreme Learning Machine (ELM) to enhance detection accuracy while reducing false positives. Through extensive simulations conducted in realistic VANET environments, the performance of SDTC was assessed across various metrics, including accuracy, and processing time. The outcomes indicated that SDTC achieved superior detection accuracy compared to existing methodologies, accompanied by a notable decrease in false positives. Nonetheless, limitations were identified, such as reliance on simulated environments, potential performance variability under diverse conditions, and concerns regarding scalability.

Despite advancements in security solutions for VANET, a notable gap persists in the realm of DDoS attack detection tailored explicitly to VANET environments. Existing studies have predominantly focused on traditional DDoS detection methods, often adapted from general network security approaches, which may not adequately address the unique characteristics and challenges of VANETs. The limited emphasis on DDoS attacks within VANET contexts underscores the necessity for dedicated research efforts aimed at developing specialized detection mechanisms capable of efficiently and effectively identifying and mitigating DDoS threats in VANETs. DDoS attacks pose significant risks to VANETs by disrupting critical services, compromising traffic management systems, and jeopardizing the safety of drivers and passengers. Thus, there is an urgent need for innovative approaches that leverage VANETs' dynamic nature, such as the mobility of vehicles and the dynamic network topology, to develop robust and adaptive DDoS detection mechanisms.

III. Materials and Methods

Attack detection in VANETs is essential to ensure the dependability and safety of vehicular communication networks because it allows mitigation actions to be implemented in a timely manner, preventing disruptions to vital services and possible risks to pedestrians and passengers. So, in this paper a novel DL model is proposed incorporating the self-attention in LSTM architecture for efficient detection of DDoS attack in VANET. The workflow of the suggested method is depicted in block in Fig. 2.

A. Dataset

The study utilized VeReMi dataset sourced from Kaggle [20]. The VeReMi dataset is a simulated dataset developed for assessing attack detection mechanisms in VANETs and offers a diverse range of traffic behaviors and attacker scenarios. The dataset includes multiple scenarios featuring different vehicle and attacker densities (high, medium and low), as well as repeated parameter sets to ensure randomness. Each scenario contains detailed message logs from both attacking and benign vehicles, capturing various attributes like reception timestamps, claimed transmission times, sender IDs, GPS positions, RSSI values, and noise vectors. Additionally, a ground truth file accompanies the dataset, documenting the true Basic Safety Messages (BSM) attribute values for both attackers and benign vehicles. With a total of 225 simulation runs categorized by density, the dataset provides insight into the performance of attack detection methods across different VANET settings. Table I illustrates the parameters of the attacks in VeReMi dataset. Table II provides a comprehensive description of the VeReMi dataset, detailing the attributes and categories of attacks included in the dataset.

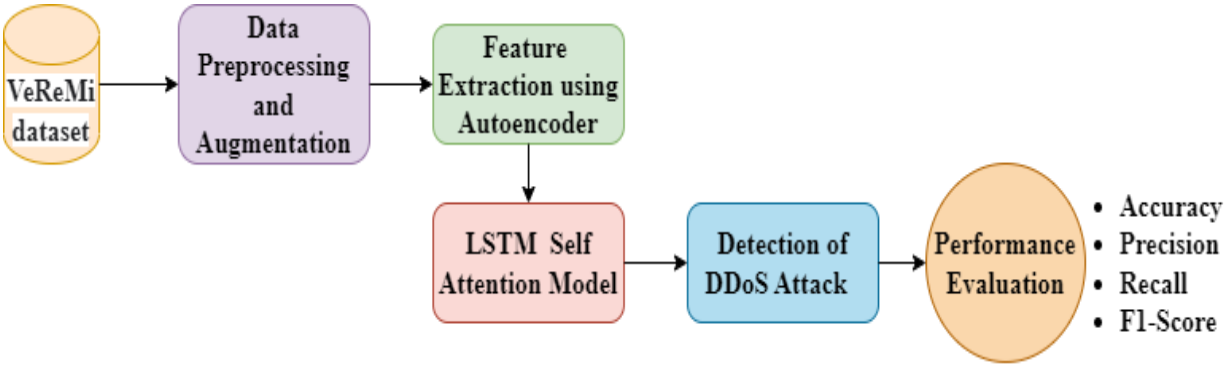

Fig. 2. Illustration of the proposed model.

TABLE I. DESCRIPTION OF VEREMI ATTACK TYPE

ID (ATTACK)	PARAMETERS
1 (Constant)	x= 5560, y=5820
2 (Constant offset)	$\Delta x = 250$, $\Delta y = -150$
4 (Random)	uniformly random in playground
8 (Random offset)	Δx, Δy uniformly random from [−300, 300]
16 (Eventual stop)	stop probability + = 0.025 each position update (10Hz)

TABLE II. VEREMI DATASET DESCRIPTION

Attributes	Description
Reception Timestamp	Timestamp of message reception
Claimed Transmission Time	Time claimed by the sender
Sender ID	Unique identifier for the sender
GPS Position	Geographic coordinates (latitude, longitude)
RSSI Value	Received Signal Strength Indicator
Noise Vector	Noise values associated with the message
Attack Type	Type of attack (Constant, Constant offset, Random, Random offset, Eventual stop)
Ground Truth	True values of Basic Safety Messages (BSM) attributes for both attackers and benign vehicles

B. Data Preprocessing and Augmentation

Preprocessing is the cornerstone for robust and effective DDoS attack detection in VANETs, as it ensures that the data is cleansed, transformed, and structured to empower subsequent analysis and modeling. Its significance cannot be overstated, serving as the pivotal stage where raw data from the Veremi dataset is refined into a form conducive to accurate detection. By systematically cleaning the data, handling missing values, removing duplicates, and normalizing numerical features, preprocessing establishes a solid foundation for subsequent analysis. Also, noise reduction techniques enhanced the data quality. Data augmentation complements preprocessing efforts, enhancing the diversity and size of the dataset for robust model training. Through synthetic data generation techniques, such as data mirroring or noise injection, the dataset's diversity is increased, allowing models to generalize better to unseen scenarios. Random perturbation introduces variations to existing data samples, simulating different environmental conditions and enhancing model robustness. Augmentation via simulation further enriches the dataset by modeling diverse traffic conditions, network configurations, and attack scenarios.

C. Feature Selection and Extraction using Convolution Autoencoder

In the study, convolutional autoencoders are used for the feature extraction method. Autoencoders present a compelling approach for feature extraction including spatial patterns in DDoS attack detection within VANETs, utilising the Veremi dataset. Comprising an encoder and decoder as shown in Fig. 3, Autoencoders aim to condense input information into a reduced-dimensional latent space while endeavouring to accurately reproduce the initial input. This condensed representation, often referred to as the latent space or bottleneck layer, encapsulates essential features crucial for distinguishing between normal and anomalous traffic behavior, including potential DDoS attacks. By training on the Veremi dataset, autoencoders efficiently reduce the dimensionality of the high-dimensional input data while preserving critical information, aiding in mitigating the curse of dimensionality inherent in VANET data analysis. Moreover, their capability to capture complex patterns and relationships throughout the data makes them particularly adept at identifying subtle deviations indicative of DDoS attacks. As autoencoders operate in an unsupervised manner, they alleviate the need for labeled attack data, thereby enabling the learning of representations directly from raw input data without manual feature engineering or annotation. This underscores their significance as a potent tool for facilitating robust DDoS attack detection mechanisms to the unique challenges posed by VANET environments and the characteristics of the Veremi dataset.

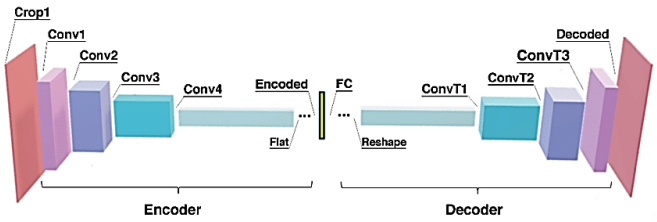

Fig. 3. Basic architecture of convolution autoencoder.

In a convolutional autoencoder, the encoder operation involves convolutional layers followed by down sampling operations such as max-pooling. Mathematically, the output feature map Z at each layer can be represented as Eq. (1).

$$Z = f_{conv}(X) \quad (1)$$

where f_{conv} denotes the convolutional operation applied to the input data X. The decoder operation comprises up sampling operations followed by convolutional layers. The reconstructed output $\hat{X}$ is given by Eq. (2),

$$\hat{X} = f_{deconv}(Z) \quad (2)$$

where f_{deconv} represents the deconvolutional operation applied to the latent representation. Autoencoders operate by minimizing the reconstruction error between the input data and the output reconstructed by the decoder. The loss function measures the discrepancy between the original input data X and its reconstruction $\hat{X}$. The mean square error (MSE) is a

commonly used loss function for autoencoders as given by Eq. (3),

$$L_{MSE} = \frac{1}{N}\sum_{i=1}^{N}\left\|X_i - \hat{X}_i\right\|^2 \quad (3)$$

where, N is the number of samples in the dataset. The convolution operation involves sliding a kernel over the input data to perform feature extraction [23]. Mathematically, the output feature map Z at each layer can be calculated by Eq. (4),

$$Z_{i,j} = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1}(X_{i+m,j+n} \times K_{m,n}) + b \quad (4)$$

Max-pooling is frequently used following convolutional layers to decrease the size of feature maps and diminish spatial dimensions. This process involves choosing the highest value from a group of neighboring values. In mathematical terms, the result of the max-pooling operation can be represented by Eq. (5),

$$Z_{i,j} = max_{m,n \in pooling\ region} X_{i+m,j+n} \quad (5)$$

The algorithm for the Convolution Autoencoder is given below.

Algorithm 1 Convolution Autoencoder

Input: Veremi dataset, num_epochs: Number of training epochs, mini_batch_size: Size of mini-batches for stochastic gradient descent, learning_rate: Learning rate for optimization algorithm
Output:Trained convolutional autoencoder model
Initialize parameters:
- Initialize weights and biases for convolutional and deconvolutional layers randomly
Define Loss Function:
- Define Mean Squared Error (MSE) loss function
Training Loop:
for epoch in range(num_epochs):
for each mini-batch in training set:
a. Forward Pass:
- Compute encoder output (latent representation) using Equation (1)
- Compute decoder output (reconstruction) using Equation (2)
b. Compute Loss:
- Compute MSE loss between input and reconstruction using Equation (3)
c. Backpropagation:
- Update encoder and decoder parameters using gradient descent
d. Validate model performance:
- Compute MSE loss on validation set
Feature Extraction:
- Use trained encoder to extract features from VANET dataset:
- Pass input data through encoder to obtain latent representations (encoded features)
Output: Extracted features serve as input for downstream analysis tasks

D. LSTM Self Attention Model

A self-attention mechanism-equipped LSTM model is proposed in this paper for effectively detecting DDoS attacks in VANETs utilizing the sequential nature of the data and focusing on relevant parts of the input sequence. The basic architecture of LSTM model is given in Fig. 4. The LSTM, type of recurrent neural network (RNN), especially proficient at managing sequential data, like time-series information, found in VANETs. It maintains state, allowing it to acquire long-range dependencies in the data while mitigating the vanishing gradient problem. The LSTM model consists of LSTM cells, each of which has input, forget, and output gates to regulate the flow of information. The state equations for the LSTM network are given as follows,

$$\text{Input Gate, } I_t = \sigma(W_i.[h_{t-1}, x_t] + b_i) \quad (6)$$

$$\text{Forget Gate, } F_t = \sigma\left(W_f.[h_{t-1}, x_t] + b_f\right) \quad (7)$$

$$\text{Candidate Memory, } \tilde{C_t} = tanh\left(W_c.\left[h_{t-1}, x_t\right] + b_c\right) \quad (8)$$

$$\text{Memory Cell, } C_t = f_t * C_{t-1} + i_t * \tilde{C_t} \quad (9)$$

$$\text{Output Gate, } O_t = \sigma(W_0.[h_{t-1}, x_t] + b_o) \quad (10)$$

$$\text{Hidden State, } h_t = O_t * tanh(c_t) \quad (11)$$

where, x_t is the input variable at each time step t. The input vectors are represented by several weight matrices W_i, W_f, and W_c. The sigmoid activation function is shown by σ, Furthermore, the bias values for the input, cell state, forget gate, and output gate are indicated by b_i b_f, b_c, and b_o, respectively.

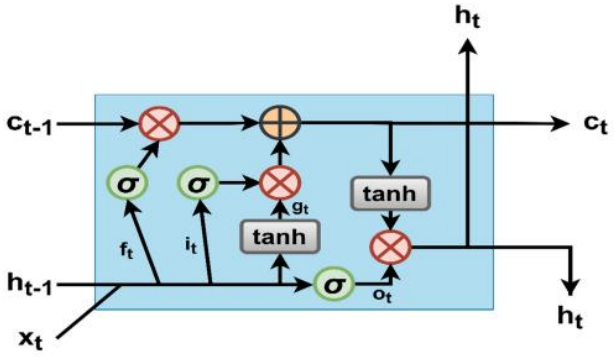

Fig. 4. LSTM architecture.

Self-attention allows the model to focus on different parts of the input sequence, prioritizing important information and disregarding unimportant sections. It computes attention weights for each time step based on the input sequence. The model architecture of LSTM with Self-attention mechanism is provided by Fig. 5.

The attention weights α_t are evaluated as a function of the hidden states h_t of the LSTM cells as given in Eq. (12).

$$\alpha_t = softmax(W_\alpha h_t) \quad (12)$$

The context vector c is evaluated as the weighted sum of the hidden states a in Eq. (13).

$$c = \sum_{t=1}^{T} \propto_t h_t \quad (13)$$

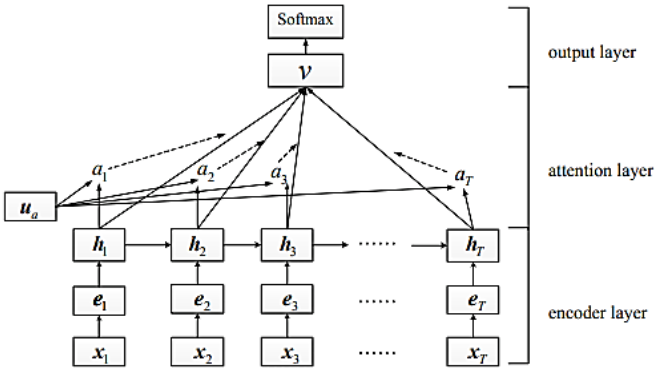

Fig. 5. LSTM Self attention model.

The context vector c obtained from the self-attention mechanism is then used as input to a classification layer, a fully connected layer followed by a softmax activation function, to predict the probability of DDoS attacks.

The context vector c obtained from the self-attention mechanism is then used as input to a classification layer, a fully connected layer followed by a softmax activation function, to predict the probability of DDoS attacks. By integrating the LSTM with self-attention, the model effectively captures long-term dependencies and relevant features in the sequential data, which are critical for identifying DDoS attacks. This combined approach utilizes the strengths of both LSTM and self-attention, making it a potent tool for robust DDoS attack detection in the challenging VANET environment. The self-attention mechanism, in particular, makes the model prioritize crucial parts of the input sequence, thus improving detection performance without requiring extensive labeled data, which is a significant advantage in unsupervised learning contexts.

E. Hardware and Software Setup

The model was developed and trained using Google Collaboratory with GPU acceleration. The software environment for the detection of DDoS attacks in VANET is implemented in Python using TensorFlow which is known for its scalability and deployment capabilities. The extensive computing resources of Google Colab combined with Keras's user-friendly interface made the process of developing models easier and guaranteed the successful training and application of intricate neural network designs. The system with Intel Core i5-8300H CPU, 16GB RAM, and a GTX1050 GPU is used to perform this research. Hyperparameters are essential configuration parameters that define the behavior and operation of a DL framework during training. Table III represents the hyperparameters used.

TABLE III. HYPERPARAMETER SPECIFICATION

Hyperparameters	Values
Optimizer	Adam
No. of epochs	50
Loss Function	Binary Cross Entropy
Activation Function	Softmax
Batch size	32

IV. RESULT AND DISCUSSION

A. Performance Evaluation

The performance was evaluated using the evaluation metrics as shown in Table IV. These metrics provide quantifiable assessments of the model's performance and aid in determining how effectively it can detect DDoS attack in VANET. To assess the impact of feature selection, experiments are conducted before and after feature selection. The classification report of the DDoS attack detection using LSTM self-attention model is given in Table V. From Table V, it is clear that the model demonstrates high performance across various evaluation metrics, indicating its effectiveness in correctly identifying both positive and negative instances with an 98.39% accuracy, 97.79% precision, 98.00% recall, and 98.20% F1-score, these metrics highlight the model's ability to achieve a balance between minimizing FP and FN, making it reliable for real-world applications where precision and recall are equally important. The visual depiction of the assessment outcome of the suggested model is given in Fig. 6.

TABLE IV. EVALUATION PARAMETERS

Performance Metrics	Equations
Accuracy	$(TP + TN) / (TP + TN + FP + FN)$
Precision	$TP / (TP + FP)$
Recall	$TP / (TP + FN)$
F1 Score	$2 * (Precision * recall) / (Precision + recall)$
where, TP-true positives, FP-false positives, TN-true negatives and FN-false negatives	

TABLE V. CLASSIFICATION REPORT OF PROPOSED METHOD BEFORE AND AFTER FEATURE SELECTION

Evaluation Metrics	Before Feature Selection	After Feature Selection
Accuracy	97.20%	98.39%
Precision	96.80%	97.79%
Recall	97.00%	98.00%
F1- Score	96.90%	98.20%

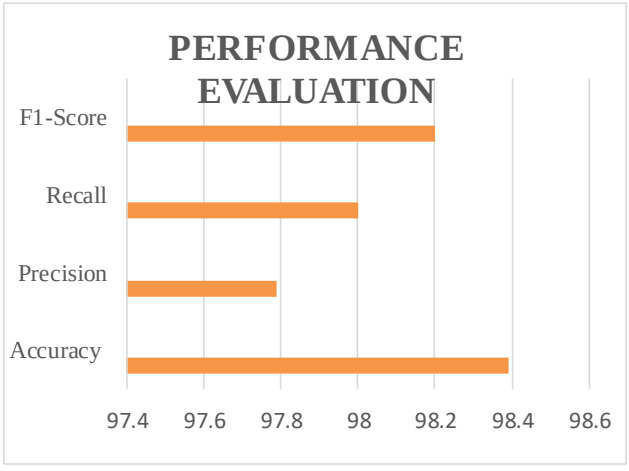

Fig. 6. Graphical representation of performance evaluation.

The Receiver Operating Characteristic (ROC) curve is crucial for evaluating the performance of the proposed model. It plots the TP Rate (TPR) against the FP Rate (FPR) as in Fig. 7, showcasing the trade-off between sensitivity and specificity. The Area Under the ROC Curve (AUC) acts as a singular numerical representation capturing the model's capacity to differentiate between different classes. The proposed model provides an AUC of 0.985 indicating perfect classification whether the VANET is detected with DDoS attack or not. This graphical representation and the accompanying AUC offer meaningful observations about the model's efficacy, making the ROC curve an essential component in the assessment of classification algorithms.

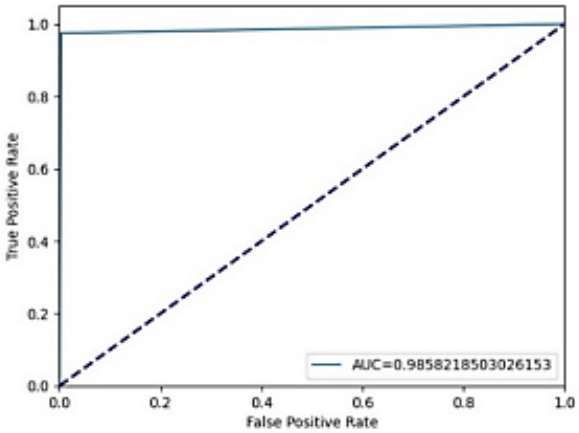

Fig. 7. ROC curve.

To provide a detailed breakdown of the model's performance, the confusion matrix is presented in Fig. 8. This matrix offers insights into the model's ability to correctly classify instances of DDoS attacks and benign activities.

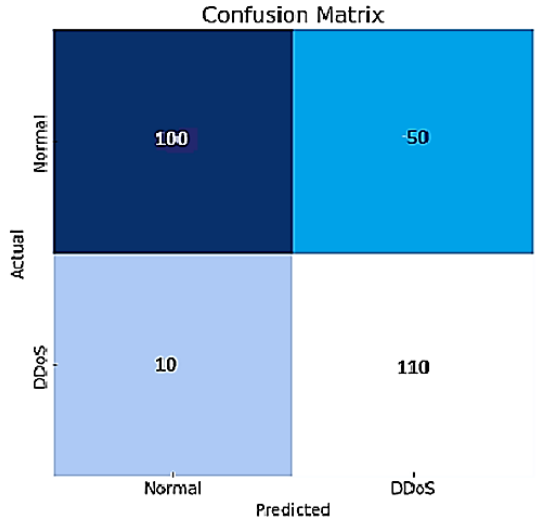

Fig. 8. Confusion matrix.

To further evaluate the training process of our proposed model, we present the accuracy and loss curves over the training epochs. Fig. 9 depicts the accuracy and loss curves respectively, showcasing the convergence behavior and stability of the model during training.

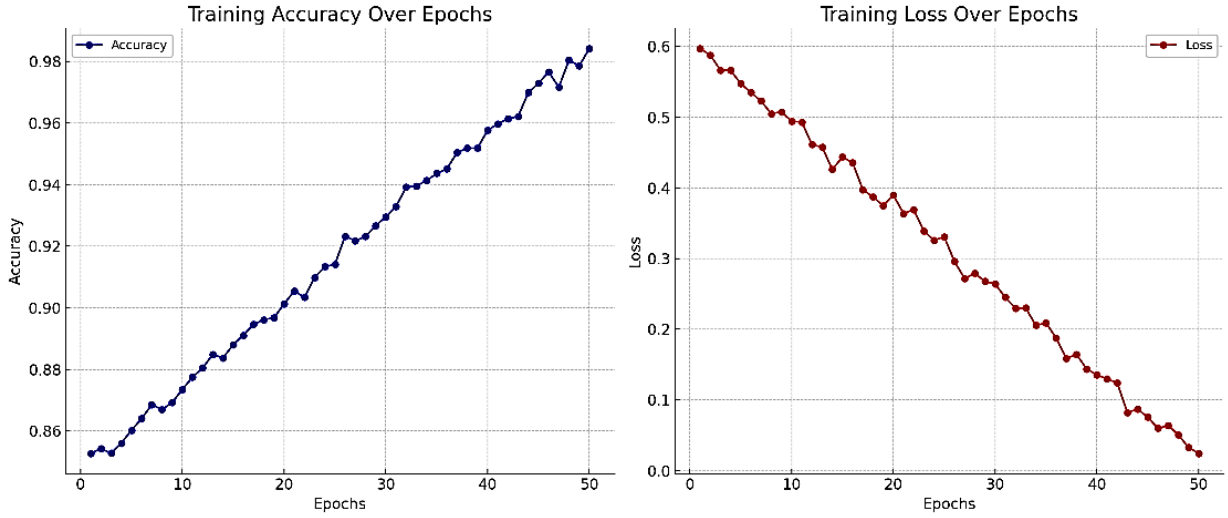

Fig. 9. Accuracy and Loss plot of the proposed model.

B. Performance Comparison

The proposed method is compared with existing models for various attack detection which utilises both DL and ML. Table IV shows the effectiveness of the suggested method in comparison with the current techniques regarding accuracy.

In addition to performance metrics, the training times of various models were recorded to assess computational efficiency. Table VII presents the training times for the proposed model and other baseline models.

In addition to its superior performance metrics (98.39% accuracy, 97.79% precision, 98.00% recall, and 98.20% F1-score), the proposed model demonstrates efficient training with a time of just 3.5 hours [24]. This outperforms the training times of other baseline models, highlighting the proposed model's advantage in both computational efficiency and detection capability. The proposed model's balanced approach to minimizing both training time and achieving high detection accuracy makes it an optimal choice for real-time DDoS attack detection in VANETs.

TABLE VI. PERFORMANCE COMPARISON

Methodology	Accuracy
GRU [9]	90.89
SVM + ANOVA [15]	97.20
SVM+GSCV [16]	96.40
DT+NN [21]	95.00
Deep Belief Network [22]	96.00
PROPOSED MODEL	**98.39**

TABLE VII. TRAINING TIME COMPARISON

Model	Training time (hours)
GRU	4.8
SVM+ANOVA	5.0
SVM+GSCV	5.2
DT+NN	4.0
Deep Belief Network	5.6
Proposed model	3.5

V. CONCLUSION

DDoS detection in VANETs arises from the critical importance of maintaining the reliability and security of vehicular communication networks. As vehicles increasingly rely on VANETs for real-time communication and cooperation to enhance road safety, and traffic efficiency, and enable various applications, the potential impact of DDoS attacks becomes increasingly significant. The proposed method for DDoS attack detection in VANETs, which combines LSTM with a self-attention mechanism, exhibits outstanding performance across multiple evaluation metrics. With an 98.39% accuracy, 97.79% precision, 98.00% recall, and 98.20% F1-score, the model demonstrates remarkable efficacy in accurately identifying instances of DDoS attacks while maintaining a balance between minimizing FP and FN. The ROC curve analysis further validates the model's effectiveness, yielding an AUC of 0.985, signifying its excellent ability to discern between classes. Comparison with existing methods underscores the superiority of the proposed approach, solidifying its position as a robust and efficient resolution for amplifying the safety and dependability of automotive communication networks. Future research could focus on incorporating real-time adaptive learning mechanisms to improve the model's responsiveness to emerging DDoS attack patterns. Additionally, integrating this model with other cybersecurity frameworks could create a comprehensive, multi-layered defence system for VANETs, enhancing overall network resilience and safety.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to all those who contributed to the completion of this research paper. I extend my heartfelt thanks to my supervisor, my family, my colleagues and fellow researchers for their encouragement and understanding during the demanding phases of this work.

REFERENCES

[1] Lee, M., & Atkison, T. (2021). VANET applications: Past, present, and future. Vehicular Communications, 28, 100310.

[2] Tonguz, O., Wisitpongphan, N., Bai, F., Mudalige, P., & Sadekar, V. (2007, May). Broadcasting in VANET. In 2007 mobile networking for vehicular environments (pp. 7-12). IEEE.

[3] Zaidi, T., & Faisal, S. (2018, December). An overview: Various attacks in VANET. In 2018 4th International Conference on Computing Communication and Automation (ICCCA) (pp. 1-6). IEEE.

[4] Upadhyaya, A. N., & Shah, J. S. (2018). Attacks on vanet security. Int J Comp Eng Tech, 9(1), 8-19.

[5] Zhu, Y., Zeng, J., Weng, F., Han, D., Yang, Y., Li, X., & Zhang, Y. (2024). Sybil attacks detection and traceability mechanism based on beacon packets in connected automobile vehicles. Sensors, 24(7), 2153.

[6] Almazroi, A. A., Alkinani, M. H., Al-Shareeda, M. A., Alqarni, M. A., Almazroey, A. A., & Gaber, T. (2024). FC-LSR: Fog Computing-Based Lightweight Sybil Resistant Scheme in 5G-Enabled Vehicular Networks. IEEE Access.

[7] Ahmed, N., Hassan, F., Aurangzeb, K., Magsi, A. H., & Alhussein, M. (2024). Advanced machine learning approach for DoS attack resilience in internet of vehicles security. Heliyon, 10(8).

[8] Dayyani, A., & Abbaspour, M. (2024). SybilPSIoT: Preventing Sybil attacks in signed social internet of things based on web of trust and smart contract. IET Communications, 18(3), 258-269.

[9] ALMahadin, G., Aoudni, Y., Shabaz, M., Agrawal, A. V., Yasmin, G., Alomari, E. S., ... & Maaliw, R. R. (2023). VANET Network Traffic Anomaly Detection Using GRU-Based Deep Learning Model. IEEE Transactions on Consumer Electronics.

[10] Vermani, K., Noliya, A., Kumar, S., & Dutta, K. (2023). Ensemble Learning Based Malicious Node Detection in SDN-Based VANETs. Journal of Information Systems Engineering & Business Intelligence, 9(2).

[11] Magsi, A. H., Ghulam, A., Memon, S., Javeed, K., Alhussein, M., & Rida, I. (2023). A machine learning-based attack detection and prevention system in vehicular named data networking. Comput. Mater. Contin, 77(2), 1445-1465.

[12] Alsarhan, A., Alauthman, M., Alshdaifat, E. A., Al-Ghuwairi, A. R., & Al-Dubai, A. (2023). Machine Learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks. Journal of Ambient Intelligence and Humanized Computing, 14(5), 6113-6122.

[13] Patil, A. N., & Mallapur, S. V. (2023). Original Research Article Novel machine learning based authentication technique in VANET system for secure data transmission. Journal of Autonomous Intelligence, 6(2).

[14] Canh, T. N., & HoangVan, X. (2023, December). Machine Learning-Based Malicious Vehicle Detection for Security Threats and Attacks in Vehicle Ad-Hoc Network (VANET) Communications. In 2023 RIVF International Conference on Computing and Communication Technologies (RIVF) (pp. 206-211). IEEE.

[15] Adhikary, K., Bhushan, S., Kumar, S., & Dutta, K. (2020). Hybrid algorithm to detect DDoS attacks in VANETs. Wireless Personal Communications, 114(4), 3613-3634.

[16] Anyanwu, G. O., Nwakanma, C. I., Lee, J. M., & Kim, D. S. (2022). Optimization of RBF-SVM kernel using grid search algorithm for DDoS attack detection in SDN-based VANET. IEEE Internet of Things Journal.

[17] Paranjothi, A., & Atiquzzaman, M. (2021). Enhancing security in vanets with efficient sybil attack detection using fog computing. arXiv preprint arXiv:2108.10319.

[18] Velayudhan, N. C., Anitha, A., & Madanan, M. (2022). Sybil attack with RSU detection and location privacy in urban VANETs: An efficient EPORP technique. Wireless Personal Communications, 1-29.

[19] Kakulla, S., & Malladi, S. (2022). Sybil attack detection in vanet using machine learning approach. Journal homepage: http://iieta. org/journals/isi, 27(4), 605-611.

[21] Haider, M. (2023). VEREMI Dataset. Kaggle.

[22] A. Kaushik, B. Shashi, K. Sunil, and D. Kamlesh, "Decision Tree and Neural Network Based Hybrid Algorithm for Detecting and Preventing DDoS Attacks in VANETS," International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 9, 2020.

[23] M.S. Rocha, G.D.G. Bernardo, L. Mundim, B.B. Zarpelao, ˜ R.S. Miani, Supervised machine learning and detection of unknown attacks: an empirical evaluation, in: L. Barolli (Ed.), Advanced Information Networking and Applications, Lecture Notes in Networks and Systems, vol. 654, Springer, Cham, 2023, https://doi.org/ 10.1007/978-3-031-28451-9_33. AINA 2023.

[24] Maggipinto, M., Masiero, C., Beghi, A., & Susto, G. A. (2018). A convolutional autoencoder approach for feature extraction in virtual metrology. Procedia Manufacturing, 17, 126-133.

[25] Xiao, Z., Xu, X., Xing, H., Luo, S., Dai, P., & Zhan, D. (2021). RTFN: A robust temporal feature network for time series classification. Information sciences, 571, 65-86.