Communication Papers of the 18th Conference on Computer Science and Intelligence Systems pp. 229–236
DOI: 10.15439/2023F7757
ISSN 2300-5963 ACSIS, Vol. 37

To propose an attack detection model for enhancing the security of 5G-enabled Vehicle-to-Everything (V2X) communication for smart vehicle

Prince Rajak,
Dept. of Information Technology
National Instiute of Technology Raipur
Raipur, India
rajakprince123@gmail.com

Pavan Kumar Mishra
Dept. of Information Technology
National Instiute of Technology Raipur
Raipur, India
pavan_km.it@nitrr.ac.in

***Abstract*—The evolution of 5G technology has revolutionized the communication landscape, enabling faster speeds, low latency, and increased capacity. The integration of 5G technology and the emergence of the 5G-enabled V2X communication network are driving the transformation of the automotive industry. Connected cars and the software-defined vehicle concept enable new business models and enhanced safety measures. However, ensuring the security of the 5G-enabled V2X communication network is crucial to mitigate potential attacks and protect the integrity of the ecosystem. To identify this potential attack, we have proposed a novel deep learning-based attack detection model (ADM) for detecting attack in 5G-enabled V2X communication network. In this we have used correlation coefficient as the feature selection method and used the deep learning-based stacked LSTM model for attack detection. The performance metrices are detection rate, accuracy, precision and F1-score.**

***Index Terms*—5G, V2X Communication Network, Stacked LSTM, ADM.**

I. Introduction

THE AUTOMOTIVE industry is undergoing a profound transformation, driven by the integration of 5G technology and connected cars. 5G has become a pivotal component in revolutionizing how automotive OEMs (original equipment manufacturers) design, build, and operate their vehicles, as well as how customers interact with them [1]. This evolution is not limited to hardware advancements but extends to the software-defined vehicle concept, where a significant portion of a vehicle's functionalities are implemented through software that can be updated or even upgraded over time. This paradigm shift allows automotive OEMs to embrace new business models, such as subscription-based or on-demand "as-a-service" offerings, and opens up opportunities for monetization.

A key enabler of this transformative journey is the 5G-enabled Vehicle-to-everything (V2X) communication network. V2X leverages the power of 5G to create a highly connected ecosystem where vehicles can communicate not only with other vehicles but also with various entities, including infrastructure, pedestrians, and smart city systems. This connectivity enables the real-time exchange of critical information, leading to enhanced road safety, improved traffic management, and a more efficient use of resources. There are several types of 5G-enabled V2X communication networks [2] that relate to different aspects of V2X connectivity and some of them are as follow:

- Vehicle-to-Vehicle (V2V): It enables direct communication between vehicles. This allows vehicles to share information such as speed, position, acceleration, and braking, fostering cooperative behaviour, enhancing safety on the road, and also providing the necessary updates on collisions, etc.
- Vehicle-to-Infrastructure (V2I): V2I communication networks involve the exchange of information between vehicles and infrastructure components such as traffic lights, road signs, and toll booths and receive real-time traffic updates, traffic signal timing information, and road condition alerts, optimizing traffic flow and improving overall efficiency.
- Vehicle-to-Pedestrian (V2P): V2P communication networks focus on the interaction between vehicles and pedestrians. These networks allow vehicles to detect the presence of pedestrians and provide warnings to both the driver and the pedestrian, reducing the risk of accidents and enhancing pedestrian safety.
- Vehicle-to-Network (V2N): V2N communication networks involve the interaction between vehicles and the cellular network infrastructure. Vehicles can access cloud-based services, download software updates, and leverage network resources to enhance their functionalities and performance.
- Vehicle-to-Device (V2D): V2D communication networks encompass the connectivity between vehicles and external devices, such as smartphones, wearables, or smart home systems.

However, as with any connected system, the 5G-enabled V2X communication network faces potential security threats and attacks. V2X communication networks are susceptible to various types of attacks due to their interconnected and wireless nature. Adversaries may exploit vulnerabilities in the network infrastructure, software, or hardware components to launch attacks with malicious intent. Some common attack on V2X communication networks include: Man-in-the-Middle (MitM) attack, DoS, Distributed Denial of Service (DDoS), Spoofing attack, etc [3]. These attacks can have severe consequences, including compromised vehicle control, privacy breaches, and even physical harm to road users. Therefore, it is imperative to address the security challenges and implement effective prevention techniques to ensure the integrity and reliability of the 5G-enabled V2X communication network [4]. To handle these issues in this

Thematic track: Internet of Things – Enablers, Challenges and Applications

paper we have presented the novel ADM based on deep learning techniques which uses correlation coefficient-based feature selection method as its core and stacked Long Short-Term Memory (LSTM) based attack detection model. The model is tested with newly release dataset.

The remaining portions of this paper are organised as follows: In Section II, we provide a brief overview of related work. In Section III, we discuss occurrences of attack on 5G enabled V2X communication network. In Section IV, we illustrated the architecture of the proposed attack detection model is described. In Section V, the effectiveness of the proposed detection model is evaluated using AIoT-SoL dataset. In section VI of the paper served as its conclusion.

II. Literature Survey

Many researchers have been interested in V2X communication network and 5G network security in the past, and many researchers are working on different parts of 5G technology right now. Many studies on 5G network attack detection have been conducted. There are various feature selection and reduction methodologies discussed in the literature for attack detection. The author [5] proposed an IDS for connected vehicles for smart cities environment. In this Deep Belief Network is used as the dimension reduction method and uses Decision Tree as the classifier for attack detection model. The dataset used are NSL-KDD and NS-3 Network simulator for model evaluation.

The author [6] proposed the anomalous event detection for intelligent transportation systems. They proposed an LSTM-based Autoencoder. Here they have extracted the feature in two phase such as Feature extraction phase (FEP) and Statistical FEP and then train using the LSTM autoencoder. The dataset used are car hacking dataset and UNSW-NB15. The author [7] proposed an IDS for IoV. The hybrid deep learning method consist of LSTM and GRU (Gated Recurrent Unit) layers are developed. They combined the DDoS dataset which is the combination of CIC_DoS 2016, CIC_IDS 2017, and CSE-CIC_IDS 2018 and make the binary label dataset consist of normal and attack labels. The car attack dataset is also used which shows higher performance.

The author [8] proposed an intrusion detection approach to early detect the cyber–physical attacks targeting Fast Charging Station (FCS) considering Vehicle-to-Grid (V2G) operation. In this discreate power samples data is used and use the Gini index for calculation of power mid-point and then use the DT for the detection of DoS attack. They create their own test environment with 3 DoS attack profile and generate data for 4 Scenario and the major feature is power which help in identification of attack on FCS. Author [9] work on in-vehicle network to proposed the IDS based on DCNN (Deep Convolution Neural Network) to protect CAN bus of the vehicle. The DCNN is built by removing the unwanted layer from the ResNet architecture and reducing the model complexity. The dataset is self-generated which consist of five types of DoS attack label.

The authors of [10] proposed tree-based ensemble intrusion detection using the stacking ensemble methodology. They used the selectkbest feature selection method and selected the top 20 significant features from NSLKDD and UNSW-NB15. The dataset consists of binary classes. The author [11] suggested a software-defined network with an IDS that is smart for the 5G network. Firstly, we performed feature importance to select the significance feature using random forest. Then we used k-means clustering to divide the traffic into five clusters, i.e., normal and attacking clusters, and used Adaboost as a classifier. For the evaluation, they used the KDD Cup 1999 dataset. There are many cases discussed by different researchers [12] that the KDDCup1999 is biased towards eliminating redundancies, which helps all of them achieve higher accuracy.

III. Occurance of attack over the 5G-enabled V2X communication network scenrio

The 5G-enabled V2X communication network is a promising technology that has the potential to revolutionize automobile industry and many other services. The transition to 5G technology brings both opportunities and challenges. With increased bandwidth, lower latency, and improved connectivity, 5G enables faster and more efficient communication between vehicles and the surrounding infrastructure. To protect the integrity, privacy, and security of the v2X communication ecosystems, new security issues are also raised that must be resolved.

5G-enabled V2X communication networks are vulnerable to a variety of attacks. These attacks can be carried out by malicious individuals or organizations, and they can have a significant impact on the safety and security of vehicles and infrastructure. Some of the most common attacks that can be carried out on 5G-enabled V2X communication networks include [13]:

- *Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attack:* These attacks aim to disrupt the availability and performance of the V2X network by overwhelming it with a flood of illegitimate requests or malicious traffic. By overloading the network resources or specific V2X components, attackers can prevent legitimate communication and potentially cause safety risks on the road.

- *Man-in-the-Middle (MitM) Attack: In* this type of attack, an unauthorized entity intercepts and alters the communication between two legitimate parties. In the context of a 5G-enabled V2X network, an attacker could position themselves between a vehicle and another vehicle, infrastructure, or device, and manipulate the information being exchanged. This could lead to unauthorized access, data tampering, or the injection of malicious commands.

- *Spoofing Attacks:* In a spoofing attack, an attacker impersonates a legitimate entity or device to deceive other participants in the V2X network. This could involve forging the identity of a vehicle, an infrastructure unit, or even a traffic management system, leading to unauthorized access or the manipulation of information. For example, an attacker could send false traffic information or alter

the location of a vehicle, causing confusion or accidents.

- *Eavesdropping Attacks:* As V2X communication transmits sensitive information, such as location data or personal details, eavesdropping attacks pose a significant threat. Attackers may attempt to intercept and capture this information to gain insights into driver behaviour, track vehicle movements, or conduct targeted attacks based on the obtained data.
- *Malware and Code Injection:* Attackers could develop and deploy malware specifically designed to exploit vulnerabilities in the software or firmware of V2X components. Once compromised, the attacker can take control of these devices, potentially enabling unauthorised access, data theft, or further network exploitation.
- *Sybil Attacks:* It occurs when an attacker generates multiple fake identities or vehicles in the V2X network, effectively multiplying their influence and capabilities. This can lead to malicious activities such as flooding the network with false information, manipulating traffic patterns, or disrupting the overall operation of the system.
- *Physical Attacks:* In addition to cyber threats, physical attacks on the infrastructure supporting the 5G-enabled V2X network could also disrupt its functionality. For example, an attacker could physically damage communication equipment, power sources, or sensor arrays, leading to communication failures, misdirection, or safety hazards.

IV. Proposed Methodology

In this section, Fig. 2 shows a detailed description of the proposed framework. It is also showing a detailed description of an attack detection model (ADM) for V2X communication network environment with 5G-enabled network. This ADM used the correlation-based feature selection for removal of highly correlated features which will help in improving the performance and reducing the computational cost. The phases and the functional component of this framework include data pre-processing of

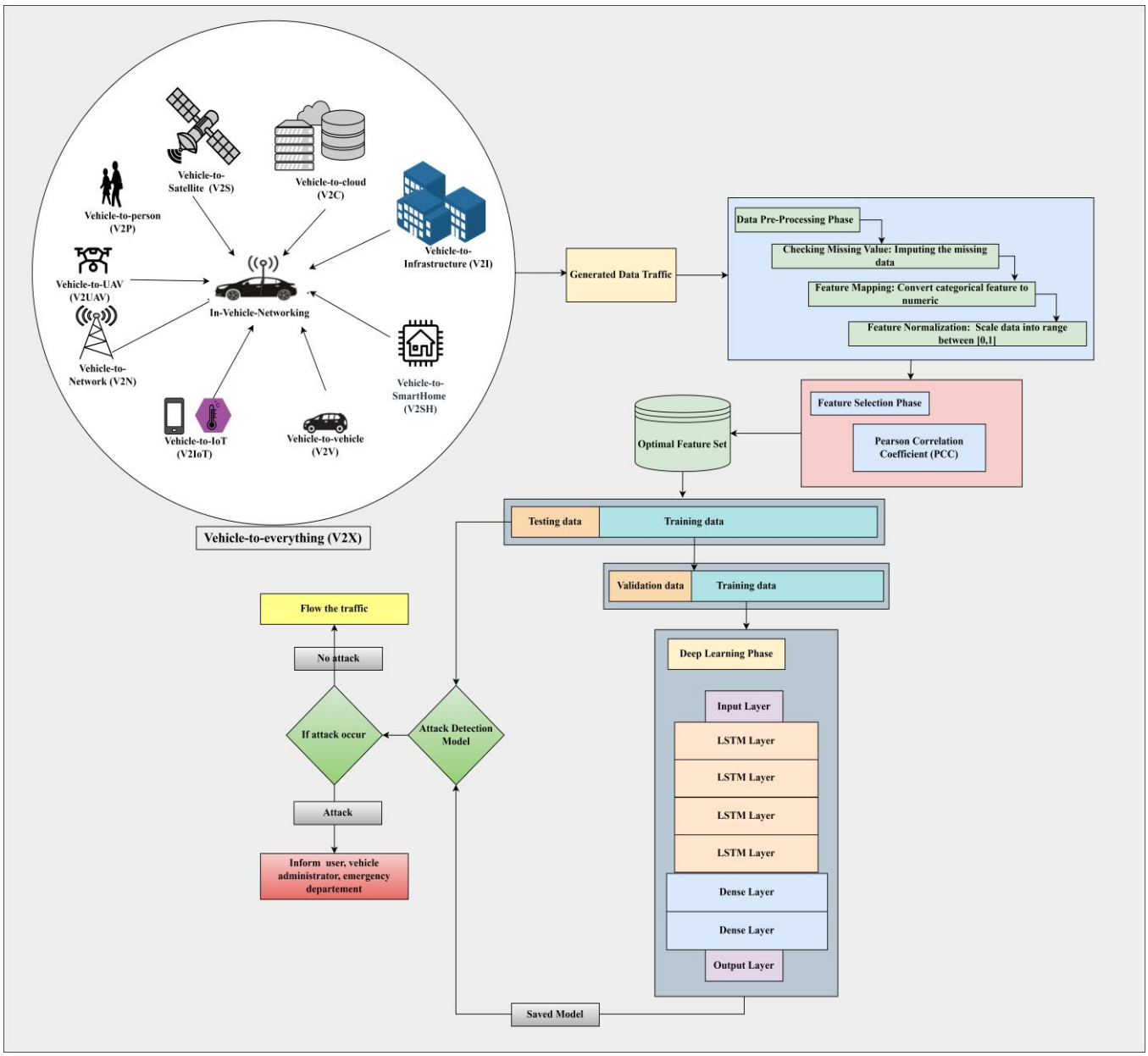

Fig. 1. Working architecture of proposed framework for an ADM for 5G-enabled V2X communication network using the Stacked LSTM

incoming V2X communication network traffic and used correlation coefficient-based feature selection method. Then the selected features are used optimal feature set to train the deep learning based Stacked LSTM-based attack classification model to identify the attack in a 5G-enabled V2X communication network. Each phase of the proposed model contributes significantly to the improvement of the overall performance. Following is a concise description of each phase of the proposed work:

A. Data Preprocessing Phase

This section describes in detail the data preparation steps for the proposed ADM. Due to the fact that V2X communication network traffic is generated by various smart sensors and smart vehicles in the 5G-enabled V2X communication environment, it includes both categorical and numeric values. It is necessary to pre-process this traffic in order to design an effective and robust ADM. Following is a brief summary of the discussion:

1) Checking Missing Values: The incoming network traffic data is missing a few values. These missing values should be handled correctly, as they will affect the model's overall performance. There are numerous methods for dealing with missing values. In the proposed detection system, missing values are substituted with the mean of the specific characteristics present in the dataset. Imputing these values will improve the quality of the data and increase the classifier's predictive ability.

2) Feature Mapping: The 5G-enabled V2X communication network traffic may frequently include various categorical variables. Some components of the ML and DL model are incompatible with categorical variables. As a solution, one must convert these categorical values to numeric values, we have used one-hot encoder techniques. This method will make the dataset sparser and increase the number of features to match the number of distinct categorical values present in each categorical feature.

3) Feature Normalization: It is observed in the network traffic data that attributes have drastically different scales, which will result in slow data-driven learning. By comparing the characteristics of each data point, a number of machine learning algorithms attempt to discover patterns hidden in the data. Different scales can result in increased processing and resource consumption. MinMaxScaler normalization techniques are employed in the proposed attack-detection model in order to discover hidden patterns, reduce training time, and enhance convergence. The MinMaxScaler techniques transform all dataset values by scaling each feature to a given range, in this case, 0 to 1. The following formula, as shown in equation 1, is utilized.

$$f_n = \frac{f_i - f_{\min}}{f_{\max} - f_{\min}} \tag{1}$$

Where f_i is the feature to scaled down, f_{min} is the minimum value and f_{max} is the maximun value for a particular feature present in the dataset and f_n is the new value.

B. Feature Selection Phase

Feature selection is the process of identifying and selecting the best subset of features from a dataset. For a machine learning and deep learning model to function well and have a quicker predictive power, these features are essential. Since the V2X communication network traffic contains a variety and a very large number of features, processing this data would require a significant amount of power and time if all features were used. The issue is resolved by using feature selection techniques to decrease the power and time without significantly affecting the classifier's predictive ability. Processing time and testing are also reliable, and feature selection aids in reducing the size of the training dataset. Numerous studies were compared and showed that data with repetitive and irrelevant features had an adverse effect on the accuracy of the learning model.

Correlation Coefficient: In next step correlation coefficient-based feature selection techniques is used. Most of the incoming V2X communication network traffic contains different features which are irrelevant and have same pattern of values. The independent features which are uncorrelated with the target attribute are the best candidate to be removed. In addition, if two independent features are highly correlated with each other than using both of them will not increase the performance but will make detection model more complex and will increase the computation time. Therefore, the proposed model removes all the features from the raw dataset and provides a simpler model for easy and efficient detection of attacks. In this model, PCC (Pearson Correlation Coefficient) is used. It works on the principle that tries to calculate the linear dependencies of two features. If the features are independent, then PCC value will be 0 and if features are dependent then the PCC value will be ± 1. So, it tries to calculate the covariance of the two features divided by the product of their standard deviation, the representation is given in equation 2.

$$p(f,t) = \frac{\mathrm{cov}(f,t)}{\sigma_f * \sigma_t} \tag{2}$$

where p is PCC, $f \in \{F_1, F_2, F_3, F_{4, \dots}, F_n\}$, t target variable, cov is the covariance between the features f and t and σ_f , σ_f is the standard deviation of features and target variable.

The covariance between the features and the target is computed using equation 3, standard deviation σ_f , σ_t can be calculated using equation 4. and the mean μ_f , μ_t of feature and target is calculated in equation 5.

$$\mathrm{cov}(f,t) = \frac{1}{N}\sum_{i=1}^{N}(f_i - \mu_f)(t_i - \mu_t) \tag{3}$$

$$\sigma_k = \sqrt{\mathrm{var}(\sigma_k^2)} = \frac{1}{N}\sum_{i=1}^{N}(f_i - \mu_k)^2 \tag{4}$$

$$\mu_k = \frac{\sum_{i=1}^{N} val_i}{N} = \frac{(val_1 + val_2 + val_3 + \cdots + val_N)}{N} \tag{5}$$

Where $k \in (f,t)$ for feature and target, N is the total number of values present in each feature, var(σ_k^2) is the variance and val_i is the values for the corresponding features in the dataset.

Above all the equation are used as a function to rank and to obtain the optimal feature set.

C. Attack Detection using Deep Learning Techniques

The proposed V2X communication network AMD uses the deep learning based Stacked LSTM techniques. It is the

type of recurrent neural network (RNN) that has multiple LSTM layers which allows the model to learn increasingly complex pattern and representation. The advantages of using a Stacked LSTM model are that improved the performance and can able to handle complex data and pattern. Second it learns multiple level of abstraction from input data which lead to better feature representation and improved detection power and has more efficient than training than CNN and other deep learning method. The Stacked LSTM are less prone to overfitting than other deep learning architectures because of their ability to learn multiple levels of abstraction from the input data.

In the proposed deep learning architecture, we have used the combination of LSTM and Dropout layers. Four LSTM layers are configured to return sequences, meaning they pass their outputs to then next LSTM layers. The input shape of the first LSTM layer is specified based on the shape of the training data. Each LSTM layer consists of 64 units, which represent the number of hidden units or memory cells in the layer. After each LSTM layer, a dropout layer is added. Dropout is a regularization technique that randomly sets a fraction of the input units to zero during training, preventing overfitting by reducing interdependencies between neurons. Following the LSTM layers, two dense layers are added. Dense layers are fully connected layers where each neuron is connected to every neuron in the previous layer. The first dense layer has 32 units and uses the ReLU activation function, which introduces non-linearity into the model. A dropout layer is added after the first dense layer to further prevent overfitting. The second dense layer has 16 units with the ReLU activation function. Finally, a dense layer with five units and the softmax activation function are added. The softmax function converts the model's outputs into probabilities, indicating the likelihood of each class. The model is trained using the categorical cross-entropy loss function, which is suitable for multi-class classification problems. The model is compiled with the Adam optimizer, which is an efficient optimizer for gradient-based optimization algorithms. During training, the model's performance is evaluated using accuracy as a metric.

V. Experiment Result

This section presents a brief discussion about the AIoT-SoL dataset used with the proposed work. The proposed experiment is conducted using the Python programming language, and the system configuration is described in Table I.

TABLE I. System configration description

System	Configuration
Processor	Intel(R) Xeon(R) CPU E3-1240v6 @ 3.70GHZ
RAM	16 GB
GPU	NVIDIA Quadro P1000 4 GB
Operating System	Window 10
Programming Language	Python 3.9.12

A. Dataset Description

AIoT-SoL Dataset: For constructing the proposed attack detection model, we have used the AIoT-SoL dataset. The authors [14] created this new dataset because they noticed that the existing data does not more closely relate to web- and IoT-specific attacks. However, they have released the AIoT-SoL dataset, which contains a greater variety of attack types than others but does not include botnet attacks because they are available in the existing dataset. Some of the attack types may overlap with the existing ones, but they crafted a more realistic and comprehensive attack scenario for data generation. The dataset is generated from the testbed, which consists of various IoT devices, vulnerable applications as victim machines, MQTT components, and different software to connect the testbed. They generated both benign and attack traffic. The attack traffic consists of 16 types of attacks, which are discussed in Table II. These 16 attacks are classified into 4 categories: web, denial of service, network, and web IoT Message Protocol attacks. They have used CIC FlowMeter [14] for extracting features from the pcap file and generating them into the csv file

TABLE II. The AIoT-SoL daset attack type categorization

Binary Categories	Categorical Categories	Sub-Categorical Categories	Instance
Benign	Benign	Benign	2403450
Anomaly	Denial of Service Attack	SSL Regression Attack	10454
		SYN Flood Attack	1000000
		SSDP Flood Attack	970418
	Network Attack	ARP MITM Attack	2307
		Network Logan Bruteforce	44915
		Network Scanning	105417
	Web attack	Cross- site Request Forgery	5117
		Cross-site Scripting	2676
		XML External Entity	47459
		Open Redirect	1237
		Directory Traversal	4998

		Server-side Request Forgery	1756
		Command Injection	12894
		SQL Injection	16046
		Web Directory Bruteforce	23031
	Web IoT Message Protocol Attack	MQTT Bruteforce	482558

The AIoT-SoL dataset is publicly available at GitHub [16]. The size of the dataset is 1.82 GB in a csv file, and it consists of 85 attributes and 5134728 instances, with 2403450 benign instances and 2731278 attack instances. The label attributes consist of 5 different types of categories, such as Benign, DoS Attack, Network Attack, Web Attack and Web IoT Message Protocol Attack.

In the proposed work, we have only considered categorical category data because for sub-categorical dataset is imbalance in nature. So, we try to evaluate our proposed attack detection model on a five categorical data respectively. We have not chosen binary categories as more work has been done on binary attack detection.

B. Description of Evaluation Metrics

The most commonly used evaluation metrics for attack detection are accuracy, precision, detection rate, and F1-Score For computing these metrics, various parameters are required and used, which are given as follows:

- True Positive (T_P): It calculates the number of attack instances in the MassiveIoT network traffic that are correctly classified as attacks by the detection model.
- True Negative (T_N): It calculates the number of benign instances in the MassiveIoT network traffic that are correctly classified as benign by the detection model.
- False Positive (F_P): It calculates the number of benign instances in the MassiveIoT network traffic that are incorrectly classified as attacks by the detection model.
- False Negative (F_N): It calculates the number of attack instances in the MassiveIoT network traffic that are incorrectly classified as benign by the detection model.

From the above discussed parameter, we can evaluate the detection model through various metrics. These metrics are discussed below:

Accuracy: It calculates the ratio of correctly classified instances by the detection model to the total number of instances present in the test set. It takes both into account when calculating the accuracy of the model.

$$\text{Accuracy} = \frac{T_P + T_N}{T_P + T_N + F_P + F_N} \quad (7)$$

Precision: It calculates the number of attack activities detected by the detection model divided by the total number of instances detected as attacks by the detection model.

$$\text{Precision} = \frac{T_P}{T_P + F_P} \quad (8)$$

Detection Rate: It calculates the number of attack activities detected by the detection model divided by the total number of activities present in the test set and is also known as recall.

$$\text{Detection Rate} = \frac{T_P}{T_P + F_N} \quad (9)$$

F1-Score: It calculates the weighted average of precision and recall. It is primarily used when the class distribution is imbalanced and is more useful than accuracy as it takes decision-making into account.

$$\text{F1 Score} = 2 * \frac{(\text{Precision} * \text{Recall})}{(\text{Presion} + \text{Recall})} \quad (10)$$

C. Result Analysis

For performance evaluation of the Stacked LSTM classifier, we split the AIoT-SoL into two parts in the ratio of 70:30 which is known as 70 for training and 30 for testing. Again, we use the 70 percent training data and spit it into the ratio of 80: 20 for generating the validation set for deep learning model training. The size of training data contains 2846748 rows, validation data contain711688 rows and testing data contain 1525044 rows. In Table III we have shown the performance evaluation of proposed work with validation and testing set. In Table IV we have shown the class-wise detection rate, precision, and F1-Score of validation and testing set. In Table V we have shown the comparison of proposed work with other existing work. Figures 2 and 3 represent the training and validation loss and accuracy for Stacked LSTM model. In Figs. 4 and 5 we have shown the confusion matrix of testing set and validation set. Our proposed model work well and have a good detection rate to detect the attack.

TABLE III. PERFORMANCE OF PROPSED WORK WITH AIOT-SOL VALIDATION SET AND TESTING SET DATA

Evaluation Set	Accuracy	Precision	Detection Rate	F1-Score
Validation	99.8	99.1	99.1	99.1
Testing	99.8	99.2	99.2	99.1

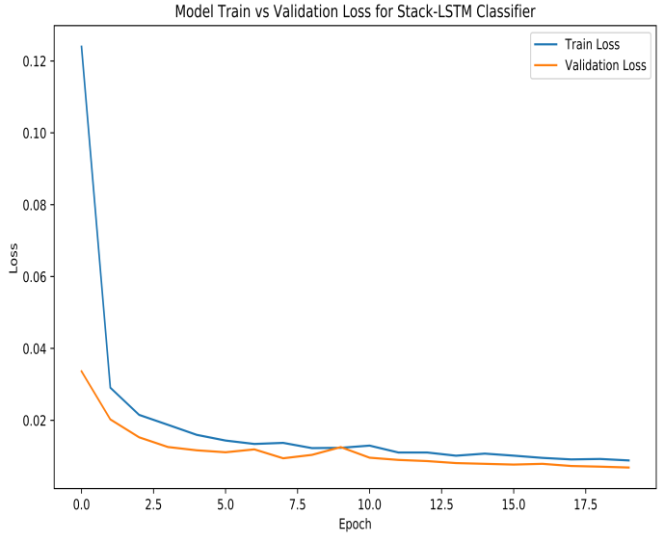

Fig. 2. Training and validation loss of the Stacked LSTM model

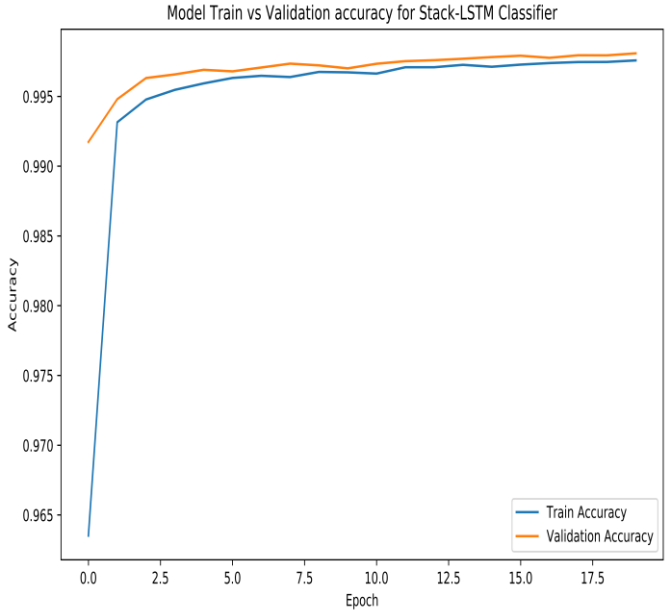

Fig. 3. Training and validation accuracy of the Stacked LSTM model

TABLE IV. PERFORMANCE OF PROPSED WORK WITH TESTING SET CLASS-WISE PRECISON, DETECTION RATE AND F1-SCORE

Evaluation set	Attack	Precision	Detection rate	F1-Score
Testing set	0	99.83	1.00	99.91
	1	99.51	96.80	98.14
	2	99.94	99.90	99.92
	3	97.19	99.25	98.20
	4	99.90	99.64	99.76
Validation set	0	99.83	1.00	99.91
	1	99.51	96.70	98.08
	2	99.94	99.89	99.91
	3	96.79	99.32	98.03
	4	99.80	99.61	99.70

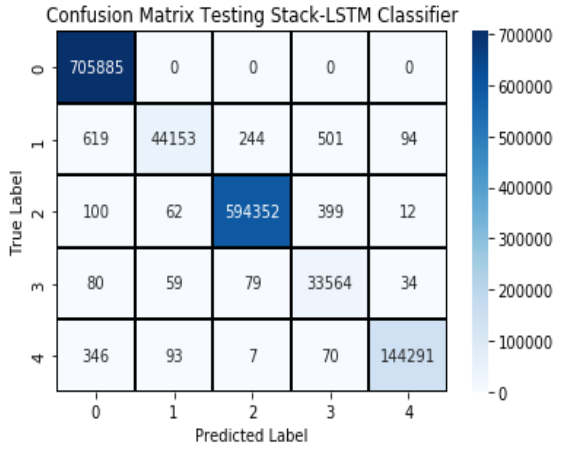

Fig. 4. Confusion matrix of testing set

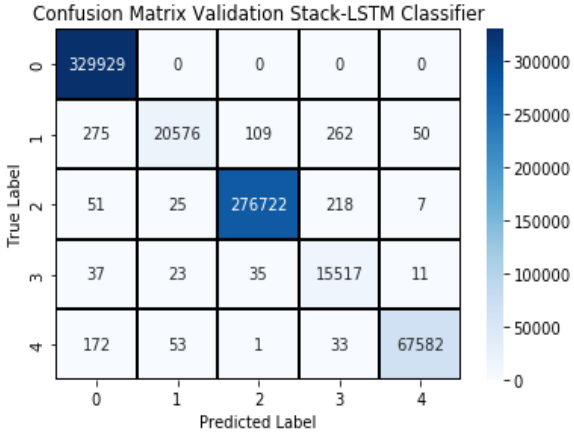

Fig. 5. Confusion matrix of validation set

TABLE V. PERFORMANCE COMPARISION OF PROPSED WORK WITH OTHER EXISTING WORK

Author	Model	Dataset	Feature selection	Target label	Detection Rate
proposed	Stacked LSTM	AIoT-SoL	Yes	5	99.2
[5]	DBN and DT, RF,	NSL-KDD	Yes	5	96
[6]	Autoencoder LSTM	UNSW-NB15	N.A.	9	97
[17]	Stacking Ensemble	CIC-IDS2017	Yes	7	99.05

VI. CONCLUSION

This paper proposes a novel ADM for 5G-enabled V2X communication network using DL techniques for smart vehicles. A feature selection method is used to find the optimal feature, which is the core of the proposed ADM. The proposed framework works at different stages. In the first stage, various pre-processing methods are used to convert the categorical values to numerical form and to scale the network traffic within a specific range. In the second stage, feature selection is applied, which consists of correlation coefficient-based feature selection methods to get the optimal feature set. Now we get the optimal feature set, which is used as the reduced feature set from the original data. In the last stage, Stacked LSTM-Based DL techniques are deployed as a detection tool that enables quick and effective decision-making in massively connected V2X communication networks in order to analyze large

amounts of data and ensure a secure and reliable V2X environment. The performance of the proposed novel ADS framework is compared and evaluated with some of the recent state-of-the-art frameworks using the recently published AIoT-SoL dataset. The proposed framework outperforms the current state-of-the-art detection framework in terms of detection rate, accuracy, precision, and F1 scores, according to extensive result analysis. We intend to expand the suggested framework in the future by utilizing large real-time 5G-V2X Communication network data.

ABBREVIATIONS

ADM	Attack Detection Model
5G	Fifth Generation
V2X	Vehicle-to-everything
LSTM	Long Short-Term Memory
IDS	Intrusion Detection System
IoV	Internet of Vehicles
CNN	Convolutional Neural Network
DT	Decision Tree
V2S	Vehicle-to-Satellite
V2C	Vehicle-to-Cloud
V2I	Vehicle-to-Infrastructure
V2SH	Vehicle-to-Smart Home
V2V	Vehicle-to-Vehicle
V2IoT	Vehicle-to-IoT
V2N	Vehicle-to-Network
V2P	Vehicle-to-Person
V2UAV	Vehicle-to-UAV
UAV	Unmanned Aerial Vehicle
IoT	Internet of Thing
CAN	Controller Area Network

ACKNOWLEDGMENT

This work (Project No: 13(23/2020-CC & BT)) has been sponsored for R&D in Convergence Communications & Broadband Technologies (CC & BT) and Strategic Electronics., Ministry of Electronics & Information Technology (MeitY), Government of India.

REFERENCES

[1] 5G Connected Cars Changing Automotive Experiences - Ericsson, www.ericsson.com/en/blog/2021/10/powering-connected-cars-with-5g. Accessed 22 May 2023.

[2] Chen, Huimin, et al. "Towards Secure Intra-Vehicle Communications in 5G Advanced and Beyond: Vulnerabilities, Attacks and Countermeasures." *Vehicular Communications* (2022): 100548.

[3] Dibaei, Mahdi, et al. "Attacks and defences on intelligent connected vehicles: A survey." *Digital Communications and Networks* 6.4 (2020): 399-421.

[4] Noor-A-Rahim, Md, et al. "6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities." *Proceedings of the IEEE* 110.6 (2022): 712-734.

[5] Aloqaily, Moayad, et al. "An intrusion detection system for connected vehicles in smart cities." *Ad Hoc Networks* 90 (2019): 101842.

[6] Ashraf, Javed, et al. "Novel deep learning-enabled LSTM autoencoder architecture for discovering anomalous events from intelligent transportation systems." *IEEE Transactions on Intelligent Transportation Systems* 22.7 (2020): 4507-4518.

[7] Ullah, Safi, et al. "HDL-IDS: A hybrid deep learning architecture for intrusion detection in the internet of vehicles." *Sensors* 22.4 (2022): 1340.

[8] Warraich, Z. S., and W. G. Morsi. "Early detection of cyber–physical attacks on fast charging stations using machine learning considering vehicle-to-grid operation in microgrids." *Sustainable Energy, Grids and Networks* 34 (2023): 101027.

[9] Song, Hyun Min, Jiyoung Woo, and Huy Kang Kim. "In-vehicle network intrusion detection using deep convolutional neural network." *Vehicular Communications* 21 (2020): 100198.

[10] Rashid, Mamunur, et al. "A tree-based stacking ensemble technique with feature selection for network intrusion detection." *Applied Intelligence* 52.9 (2022): 9768-9781.

[11] Li, Jiaqi, Zhifeng Zhao, and Rongpeng Li. "Machine learning-based IDS for software-defined 5G network." *Iet Networks* 7.2 (2018): 53-60.

[12] Sapre, Suchet, Pouyan Ahmadi, and Khondkar Islam. "A robust comparison of the KDDCup99 and NSL-KDD IoT network intrusion detection datasets through various machine learning algorithms." *arXiv preprint arXiv:1912.13204* (2019).

[13] Hakak, Saqib, et al. "Autonomous Vehicles in 5G and beyond: A Survey." *Vehicular Communications* (2022): 100551.

[14] Min, Nay Myat, et al. "OWASP IoT Top 10 based Attack Dataset for Machine Learning." *2022 24th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2022.

[15] "Search UNB." University of New Brunswick Est.1785, www.unb.ca/cic/research/applications.html. Accessed 22 May 2023.

[16] NayMyatMin. "Naymyatmin/Aiot-Sol." GitHub, github.com/NayMyatMin/AIoT-Sol. Accessed 22 May 2023.

[17] Rani, Preeti, and Rohit Sharma. "Intelligent transportation system for internet of vehicles based vehicular networks for smart cities." *Computers and Electrical Engineering* 105 (2023): 108543.

[18] Banafshehvaragh, Samira Tahajomi, and Amir Masoud Rahmani. "Intrusion, anomaly, and attack detection in smart vehicles." *Microprocessors and Microsystems* 96 (2023): 104726.