Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5069104, 13 pages
https://doi.org/10.1155/2022/5069104

Research Article

Intelligent Intrusion Detection System for VANET Using Machine Learning and Deep Learning Approaches

B. Karthiga,[1] Danalakshmi Durairaj,[2] Nishad Nawaz,[3] Thiruppathy Kesavan Venkatasamy,[4] Gopi Ramasamy,[5] and A. Hariharasudan[6]

[1]*Faculty of Electronics and Communication Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur, India*
[2]*Faculty of Electrical and Electronics Engineering, GMR Institute of Technology, Rajam, Andhra Pradesh, India*
[3]*Department of Business Management, College of Business Administration, Kingdom University, Bahrain*
[4]*Faculty of Computer Science and Engineering, Visvodaya Engineering College, Kavali, Andhra Pradesh, India*
[5]*Faculty of Computer Science and Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamil Nadu, India*
[6]*Faculty of English, Kalasalingam Academy of Research and Education, Krishnankoil, 626128 Tamil Nadu, India*

Correspondence should be addressed to Thiruppathy Kesavan Venkatasamy; vtkesavan@gmail.com

Received 19 January 2022; Revised 20 September 2022; Accepted 21 September 2022; Published 13 October 2022

Academic Editor: Hasan Ali Khattak

Detecting the attacks in Vehicular Ad hoc Network (VANET) system is very important to provide more secure and reliable communication between all vehicles in the system. In this article, an effective Intelligent Intrusion Detection System (IDS) is proposed using machine learning and deep learning approaches such as Adaptive Neuro Fuzzy Inference System (ANFIS) and Convolutional Neural Networks (CNN), respectively. The existing methods focus on detecting only the known attacks in VANET environment. This limitation is overcome by proposing the Intelligent IDS system using soft computing techniques. The proposed method consists of Known IDS (KIDS) and Unknown IDS (UIDS) modules, which detect both known attacks and unknown attacks. The KIDS module uses ANFIS classification module to detect the known malicious attacks, whereas the UIDS module uses a deep learning algorithm to detect the unknown attacks in VANET. Modified LeeNET (MLNET) architecture is proposed in this article to identify the type of unknown attacks. In this work, DoS attacks, Botnet attacks, PortScan attacks, and Brute Force attacks are detected using this hybrid learning algorithm. The proposed system obtains 96.9% of Pr, 98.3% of Se, 98.7% of Sp, and 98.6% of Acc and consumed 1.75 s for detecting the DoS attack on i-VANET dataset. The proposed system obtains 98.1% of Pr, 98.9% of Se, 98.1% of Sp, and 98.1% of Acc and consumed 0.95 s for detecting the Botnet attack. The proposed system obtains 98.7% of Pr, 99.1% of Se, 98.9% of Sp, and 99.2% of Acc and consumed 1.38 s for detecting the PortScan attack. The proposed system obtains 99.1of Pr, 97.8% of Se, 98.7% of Sp, and 98.5% of Acc and consumed 1.29 s for detecting the Brute Force attack. The developed methodology is tested on the real-time CIC-IDS 2017 dataset, and the experimental results are compared with other state-of-the-art methods.

1. Introduction

Communication technology plays an essential role in recent vehicle network management. In conventional methods, the wired communication protocols were developed to control the various internal parts of the vehicle under single devised system architecture. This wired method increases the system and maintenance cost of the vehicle. In order to improve cost efficiency, modern vehicular networks use wireless protocols to transfer or receive the data wirelessly within or outside the vehicles. VANET is the recent efficient wireless technology which is presently used in many intelligent transportation networks [1–3], carpooling [4], and even using fifth-generation small-cell networks [5, 6]. Each vehicle belonging to VANET system consists of multiple wireless sensors, converting equipment, and mapping units. Also, the VANET system consists of two interfacing modules, ad On-Board Unit (OBU) and Road Side Units (RSU). The OBU module is integrated within the vehicle and connects to all the wireless sensors within the vehicle. The RSU

module is fitted in roadside buildings with individual transmitter and receiver units to communicate each vehicle's OBU module. When the vehicle enters the VANET system, it senses the vehicle information through the multiple sensors fitted in it and sends all this data to the RSU module. The accidents will be prevented if there is confident coordination between the vehicle OBU module and RSU module. The performance between the OBU module and RSU module will be affected by the presence of intruders. Hence, there is a need to provide a security mechanism between OBU and RSU modules.

By implementing these VANET techniques, accidents are significantly reduced by exchanging the vehicle information with its nearby or surrounding vehicles. This VANET can be categorized into Vehicle-to-Vehicle (VV) and Vehicle-to-Infrastructure module (VI). The VV module of the VANET system transfers the information between vehicle and vehicle. In the case of VI module, if the VANET system, the information is transferred from one vehicle to the centralized system or controller. The real-time environment scenario of the VANET is dynamic, and its topology system is changing with respect to the distance and location of vehicles. The factors such as environmental noises affect the quality of the information passage between the vehicles [7–9]. This type of vehicle environment is called a rugged VANET environment, which is easily affected by external attacks such as eavesdropping and hacking the data. Figure 1 illustrates the VANET environment where all the vehicles are connected wirelessly to the centralized controller. The vehicles in VANET and centralized controller are attacked by the attacker. Figure 1 shows the VANET systems, which connect multiple vehicles to the centralized controller, which is called as RSU module. The attackers mostly affected the interference between each vehicle and the interference between the vehicle and the centralized controller.

The attackers generate different types of attacks to collide with the functional activities of the network environment in VANET system. This will also affect the lives of people who are driving vehicles in these environmental conditions. Therefore, detecting the attacks in VANET system is very important to provide more secure and reliable communication between all vehicles in the system. The attacks in VANET are classified into either external attacks or internal attacks. Internal attacks can be detected or identified using cryptography methods, which use a digital signature to perform encryption and decryption. These methods are not able to detect the external attacks [10–15]. Therefore, the IDS is required in VANET to provide security from external attacks. The external attacks are categorized into Denial of Service (DoS) attacks, Botnet attacks, PortScan attacks, and Brute Force attacks. DoS attack can be generated by any attacker who statically launches the attack in a particular location, or any moving vehicle can launch the attack. The attacker intends to disrupt the network services that are used by the vehicles. Botnet attack is generated due to the devices which are affected by malware. The ports in the device can be affected or attacked by the PortScan attack. The login credentials and passwords of the network devices can be affected by the Brute Force attack. In this article, the attacks in VANET system are detected using deep learning methodologies. The main objective of this article is to design an intelligent IDS system for VANET which detects both known and unknown attacks. Also, the novel hybrid deep learning architecture is proposed in this article to classify various attacks in VANET.

The notations and descriptions are given in Table 1:

This article is structured as follows: Section 2 states the conventional methodologies for detecting the attacks in IDS in VANET, Section 3 proposes an intelligent IDS system using hybrid classification approach, Section 4 discusses the experimental results of this extensive proposed methods, and Section 5 concludes this article.

2. Related Works

Hind Bangui et al. [16] used a hybrid data-driven methodology for detecting the various attacks in the VANET IDS system. This methodology used the integration approach for combining the various data models to identify the malicious nodes in the VANET system using the data-driven model. This methodology was tested on various environmental VANET systems to validate the proposed hybrid data-driven model. Alsarhan et al. [17] used a rule-based security filter for filtering the anomaly nodes in the VANET system. These filtered nodes were used to extract the linear properties using Dempster–Shafer's theory. The authors tested this rule-based anomaly-driven approach on a large real-time dataset to optimize the detection rate of the VANET system. The positive impact of the developed anomaly detection method was tested and compared with various machine learning-based IDS systems in the VANET environment. Rasika et al. [18] used a deep learning algorithm for detecting intruders in VANET by improving the basic architecture of the IDS module. This work mainly concentrated on detecting the attacks between the modules in roadside units and vehicles. The authors used Deep Belief Networks (DBF) deep learning algorithm for detecting the attacks, and this method was tested on CIC-IDS2017 dataset to validate the experimental results. Abdulaziz Alshammari et al. [19] designed an advanced IDS module in VANET using different classification methods. The extensive experimental results were analyzed through different validation methods. Zeng et al. [20] used the machine learning algorithm Neural Networks (NN) to improve the performance efficiency of the VANET environment. The developed model was analyzed to a number of internal layers and its weighting bias.

Erfan A Shams et al. [21] developed a machine learning classifier-based intrusion detection system for detecting the various forceful attacks in networks. The kernel-based Support Vector Machine (SVM) was used to classify the known IDS from the unknown IDS in the VANET system. This method failed to detect the attacks when there were high numbers of vehicle nodes in the VANET system. Muder Almi'ani et al. [22] devised a non-linear intrusion detection method for detecting malicious attacks in the VANET system. The authors computed the number of clusters for determining the self-organizing maps in VANET. These self-

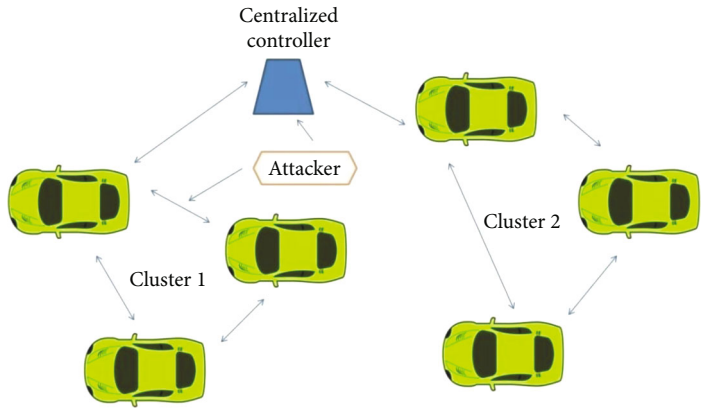

Figure 1: VANET system.

Table 1: Notations and descriptions.

Acronyms	Abbreviations
ADR	Attack Detection Rate
Acc	Accuracy
ANN	Artificial Neural Networks
ANFIS	Adaptive Neuro Fuzzy Inference System
CNN	Convolutional Neural Networks
DBF	Deep Belief Networks
DoS	Denial of Service
DDoS	Distributed Denial of Service
FCNN	Fully Connected Neural Networks
IDS	Intrusion Detection System
KIDS	Known IDS
KNN	K-Nearest Neighbor
MLNET	Modified LeeNET
NN	Neural Networks
PNN	Probabilistic Neural Network
Pr	Precision
ReLu	Rectified Linear Unit
ROC	Receiver Operating Characteristics
S	Seconds
Se	Sensitivity
Sp	Specificity
SVM	Support Vector Machine
UIDS	Unknown IDS
VANET	Vehicular Ad hoc Network
VWCA	Vehicular Weighing Clustering Algorithm
VV	Vehicle-to-Vehicle

organizing maps were used to classify the attacks in network system. This intelligent intrusion detection system was tested with various VANET environmental systems to validate the obtained self-organizing and clustered maps. Laisen Nie et al. [23] used CNN methodology to improve the learning and testing rate of the anomaly identification system in VANET. The authors computed various spatio-temporal properties from the vehicle or nodes in VANET, and these features were learned and classified using this CNN method. Kang et al. [24] implemented deep learning architecture for the detection of anomaly nodes in the VANET system. The authors tested the real-time traffic network through different numbers of deep learning algorithms to verify the effectiveness of the network architecture.

Danalakshmi et al. [25] proposed an IDS technique in which the Deep Belief Network is used by enhancing with a rule-based technique to improve the accuracy of the detection rate and reduce the false alarm rate as well. The authors concentrated only on False Data Injection and DoS attacks. To identify the port scan attacks, efficient detection rules are generated in the IDS, which detects the real-time native port scan attacks using Snort [10]. But the snort has some limitations that, due to noise, can limit the effectiveness of IDS. Guangzhen Zhao et al. [26] utilized two classification models, DBF and Probabilistic Neural Network (PNN), for detecting intrusion in the VANET system. The authors analyzed the performance of the system by implementing the IDS system with these two classification models. Hao [27] used an encryption-based key management system for detecting the various attacks in IDS system of the VANET environment. The developed key management system provided different encrypted keys for handling a large amount of data between the roadside unit and the vehicles. Daeinabi et al. [28] proposed a vehicular weighing clustering algorithm (VWCA) for improving the security level of the nodes in VANET. The authors constructed a weight-based clustering framework for detecting the nodes being attacked by the host node.

Mengting Yao et al. [29] proposed mutual authentication method for improving the security enhancement in VANET using a forward secrecy approach. The shared key in this method was verified through the batch normalization process. The authors detected impersonation and forgery attacks using this mutual authentication technique. Shen et al. [30] developed a data aggregation approach for VANET to improve security performance. The authors used a batch verification approach between each transmission process of sender and receiver in order to provide a trust behavior network. Gope et al. [31] improved security authentication of VANET by developing a privacy-preserving approach between vehicle and grid. The authors

applied and tested the developed security authentication scheme in different rouged environments. Zhang et al. [15] improved the intrusion detection system of VANET using distributed preserving approach. The authors significantly analyzed the impact of these distributed preserving techniques on different VANET environments. Gayathri et al. [32] used certificateless approach to prove the authentication scheme in the VANET environment. This method used certificateless keys between the roadside units and central units in VANET. The effectiveness of this keyless approach was analyzed using hit rate and miss rate analysis parameters.

Nayyar et al. [33] developed a hybrid data model for the detection of intrusion in the VANET environment. This method was based on the hybrid model and integrated with the non-linear prediction flow to determine the intrusion activities in VANET. Naqvi et al. [34] detected the malicious activities or any misbehavior activities of the vehicle in VANET using IDS flow. The authors mainly focused on providing more reliability and security for the vehicle nodes in VANET. The experimental results of this proposed method were compared with other similar algorithms in the same VANET environment. Jabar Mahmood et al. [35] analyzed and synthesized various problems faced in the security flow of the VANET system. The determined countermeasures in VANET identified the major security threats and resolved the issues in VANET, which also optimized the efficiency of the entire network. Irshad et al. [36] proposed a security key authentication system for the VANET system to provide reliable and secure access to vehicle users. The authors discussed various authentication protocols to improve the security of the VANET system. Faisal et al. [37] detected the location coordinates of the Sybil attacks in the VANET system. The authors analyzed the effectiveness of the developed attack prevention system in static and dynamic environments to provide reliability for all the nodes in the VANET system. Mahmood et al. [38] proposed an anonymous identity-based key agreement protocol for maintaining the attack prevention system for the applications of smart grid environments. The authors also discussed the various key agreement protocols for comparing the proposed method in this work.

Kumar et al. [39] used blockchain model with deep learning for a privacy-preserving secure framework in the VANET system. The authors discussed various blockchain models to validate the proposed security network. Randhir Kumar et al. [40] developed a privacy preservation model for the VANET system to provide privacy and security in C-ITS infrastructure. The proposed framework provides two levels of security and privacy using blockchain and deep learning modules. Kumar et al. [41] proposed a security strategy that uses artificial intelligence models to understand cyber-attacks and can proficiently protect IoT-enabled Maritime Transportation System (MTS) data. Randhir Kumar et al. [42] proposed blockchain and deep learning (DL)-enabled secure data processing framework for an edge-envisioned green CAV environment.

Sourabh Sharma et al. [43] used Singular Value Decomposition (SVD) method for color image watermarking based on bee colony algorithm. Dibakar Sinha et al. [44] used CNN for the detection of coronary artery disease. Idio Guarino et al. [45] applied a different set of machine learning approaches for identifying intrusion detections with respect to various forms. The limitations of the various machine learning approaches were discussed in this work. Bovenzi et al. [46] developed a model used for intrusion detection framework using Internet of Things (IoT) with the help of machine learning models. The authors discussed certain exhibited limitations of the current intrusion model and provided a prominent solution for intrusion detection. Mirsky et al. [47] designed an autoencoder which was constructed based on the ensemble structural algorithm for detecting intruders on the online platform.

Table 2 shows the existing methods with their limitations. These limitations are overcome by the proposed method.

The main limitations of the conventional methods are stated as follows,

(i) The present IDS systems only focused on detecting the known attacks in VANET

(ii) Most IDS system using deep learning algorithms has a cascade structure, increasing the detection time

The conventional IDS systems used a mathematical complex model for detecting intrusion in VANET. This article proposes a soft computing approach for detecting intrusion, which combines machine and deep learning algorithms to improve the IDS detection rate. Also, most IDS system using deep learning algorithms has a cascade structure, which increases the detection time.

The main contributions of this paper are stated below.

(i) An effective IDS is proposed using machine learning and deep learning approaches

(ii) The proposed IDS framework is designed with KIDS and UIDS modules, which detect both known and unknown attacks

(iii) The known malicious attacks are detected using the proposed KIDS framework, which uses ANFIS, and the unknown malicious attacks are detected using the proposed UIDS, which uses a deep learning algorithm

(iv) Modified LeeNET (MLNET) architecture is proposed in this article to identify the type of unknown attacks. In this work, DoS attacks, Botnet attacks, PortScan attacks, and Brute Force attacks are detected using this hybrid learning algorithm

3. Proposed Methodologies for IDS in VANET

This article proposes an effective IDS methodology using machine and deep learning approaches. The proposed method consists of Known IDS (KIDS) and Unknown IDS (UIDS) modules, which detect both known and unknown attacks. The KIDS module uses a machine learning

Table 2: Existing methods with their limitations.

Conventional methods	Distinctive characteristics	Limitations
Hind Bangui et al. [16]	Hybrid data-driven model	Detected known attacks only
Alsarhan et al. [17]	Features optimizations	Consumed high detection time for attacks
Rasika et al. [18]	Non-linear testing	Complex detection algorithm
AbdulazizAlshammari et al. [19]	Robust algorithm	Detected known attacks only
Zeng et al. [20]	Required minimum hardware resources	Complex detection algorithm
Erfan A Shams et al. [21]	Hybrid model	Low sensitivity rate

algorithm to detect known malicious attacks. The UIDS module uses a deep learning algorithm to detect unknown attacks in VANET. The entire algorithm or workflow of the proposed IDS of VANET is depicted in Figure 2.

3.1. Signature Model. The proposed IDS system of VANET is designed with a training model and testing model. The training model uses the signature module and the ANFIS classifier to produce the trained patterns. These trained patterns from the training module are used to classify the attacks in VANET into known or unknown attacks. The size of the network data from VANET is huge, which degrades the conventional IDS system. Hence, data pre-processing is used in the training module to detect and eliminate duplicate and redundant data in network traffic. The removed data from the pre-processing module is fed into the signature module, which is used to separate the header information from the data. The header data from the known malicious attacks (x) and unknown attacks (y) are trained using ANFIS classifier, which produces the trained patterns in the training model of the proposed IDS system. The ANFIS architecture of the proposed IDS system is depicted in Figure 3.

The ANFIS module is designed with five layers: the first layer is the input layer, the fifth layer is the output layer, and the remaining three layers are called hidden layers. The input layer receives the header data from known malicious attacks, and they are normalized using the normalization factors A1 and A2. Similarly, the input layer receives the header data from unknown attacks, and they are normalized using the normalization factors B1 and B2. Layer 2 performs the fuzzification process, and layer 3 performs the defuzzification process of the normalized header values of both known and unknown attacks. Layer 5 uses a summation function to add the responses from the layer 3 nodes.

In this article, ANFIS is constructed with five numbers of internal layers and each layer is designed with a set of intrinsic equations. Layer 1 is called as adaptive node layer. All nodes in this layer are represented by the following equations.

Layer 1 is called as adaptive node layer. All nodes in this layer are represented by the following equations.

$$\begin{aligned} L_{1,ix} &= \mu_A(x)\,;\, i = 1, 2, \\ L_{1,iy} &= \mu_B(y)\,;\, i = 3, 4. \end{aligned} \tag{1}$$

The mean values ($\mu(x)$ and $\mu(y)$) are computed using the following equations.

$$\begin{aligned} \mu_A(x) &= \frac{1}{1 + \left|(x-c)/a\right|^{2b}}, \\ \mu_B(y) &= \frac{1}{1 + \left|(y-c)/a\right|^{2b}}, \end{aligned} \tag{2}$$

where $\{a, b, c\}$ are the intrinsic parameter set.

Layer 2 is called a fixed node layer, and the response of this layer 2 is given as

$$L_{2,i} = w_i = \mu_A(x) * \mu_B(y). \tag{3}$$

The firing strength of each node in layer 3 is computed using the following equation.

$$L_{3,i} = S_i = \frac{w_i}{w_1 + w_2}\,;\, i = 1, 2. \tag{4}$$

The response of Layer 4 node is determined using the firing strength of the response of layer 3.

$$L_{4,i} = S_i * f_i. \tag{5}$$

The final response of Layer 5 is given as

$$L_{5,i} = \sum S_i * f_i. \tag{6}$$

3.2. KIDS Model. This module receives the real-time network traffic from various nodes or vehicles in VANET environment system, and all these obtained real-time traffic data are applied to pre-processing data module. This module identifies each vehicle's data from the real-time traffic by its individual ID and separates the header information from each data. This header information is fed into the testing phase of the ANFIS classifier with respect to the trained patterns, which are obtained from the training module of the IDS system.

The same architecture depicted in Figure 3 is also used in testing phase of the ANFIS classifier, where the trained patterns are fed into "x", and the testing pattern is fed into "y" of the architecture. The ANFIS in testing module produces a binary response (f). The response has the following criteria.

$$\text{attack}_{\text{type}} = \begin{cases} \text{Knownattack}\,;\, \text{if} f \geq 0 \\ \text{Unknownattack}\,;\, \text{ifelse} \end{cases}. \tag{7}$$

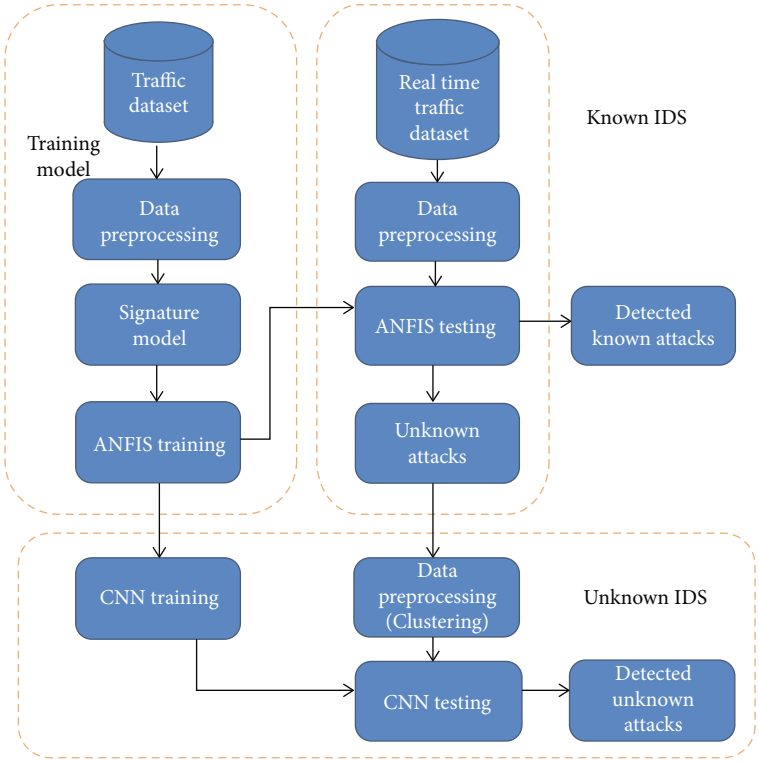

Figure 2: Hybrid deep learning model for IDS in VANET.

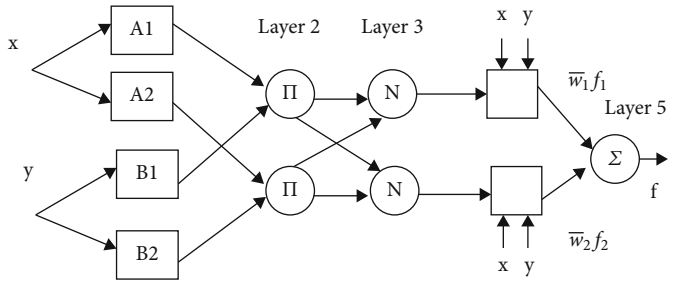

Figure 3: ANFIS for IDS system in VANET.

The training and classification algorithm of ANFIS in the proposed IDS system of VANET is given in the following steps:

3.3. UIDS Model. The vehicle node which is affected by known attacks from the KIDS module is mitigated by other vehicle nodes in VANET system. The unknown attacks cannot be identified by the machine learning classifier due to its training algorithm. Hence, there is a need for a deep learning classifier for the detection of unknown attack types in VANET system. Though many conventional deep learning architectures have been available from the past decade, LeeNET is a simple and efficient deep learning architecture designed using fewer internal layers than the other conventional deep learning architectures. In this article, Modified LeeNET (MLNET) architecture is proposed to identify the type of unknown attacks. The conventional LeeNET and proposed MLNET architectures are depicted in Figures 4(a) and 4(b), respectively.

The conventional LeeNET is designed with two numbers of Conv_layer and two numbers of Pool_layer, and three numbers of Fully Connected Neural Networks (FCNN), as illustrated in Figure 4(a). The trained patterns are passed through Conv_layer1, and its output response size is reduced using Pool_layer1.

The Rectified Linear Unit (ReLu) module is placed between each convolutional layer and pooling layer in order to remove the negative responses from output of each convolutional layer. The function of ReLu module is described in the following equation.

$$f(x) = \begin{cases} 0\,; \text{if } x < 0 \\ x\,; \text{if } x \geq 0 \end{cases}, \tag{8}$$

where x is the response of the convolutional layer, and $f(x)$ is the output of ReLu module.

Input: Real-time traffic from VANET;
Output: Known and unknown attack;
1. Receives the real-time traffic from VANET environmental system;
2. Apply pre-processing to separate the header of individual data from each attacked vehicle
$dia = \{d1a, d2a, d3a, \cdots \cdots \cdots dna\}$, where na is the total number of vehicles in VANET system.
3. Apply pre-processing to separate the header of individual data from each non-attacked vehicle $di = \{d1, d2, d3, \cdots \cdots \cdots dn\}$, where n is the total number of vehicles in VANET system.
4. For each traffic do
5. Compute $\text{ANFIS}_{\text{trained}} = \{dia, di\}$
6. End for
7. Sort the trained patterns. $\text{ANFIS}_{\text{sort}} = \{\text{ANFIS}_{\text{trained}}\}$
8. Apply pre-processing to separate the header of individual data from each test vehicle
$dt = \{dt1, dt2, dt3, \cdots \cdots \cdots dtn\}$, where tn is the total number of test vehicles in VANET system.
9. For each test traffic do
10. Compute $\text{ANFIS}_{\text{tested}} = \{\text{ANFIS}_{\text{sort}}, dt\}$
11. End for
12. Apply the criteria to identify the known attacks and unknown attacks using

$$\text{attack\_type} = \begin{cases} \text{Known attack ; if } f \geq 0 \\ \text{Unknown attack ; if else} \end{cases}$$

Algorithm 1: Attack detection and classification using ANFIS.

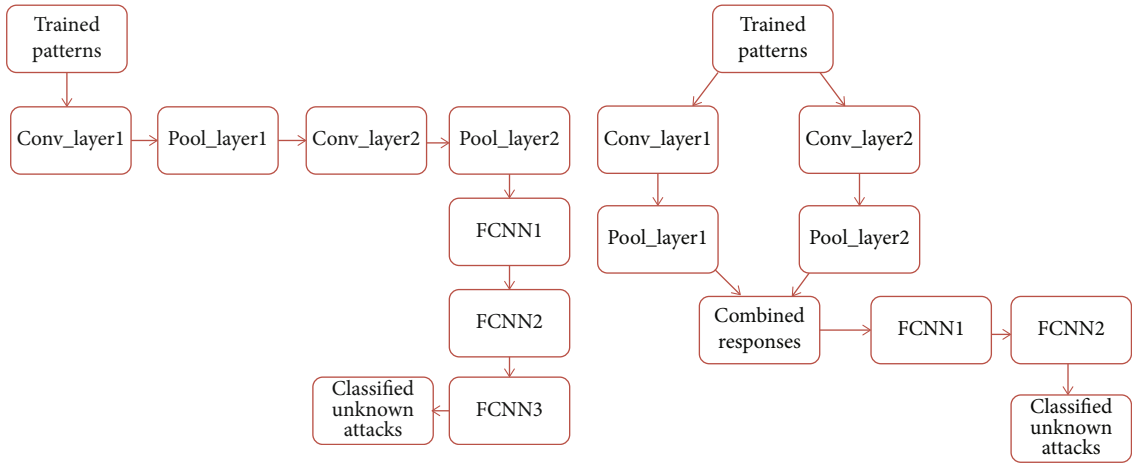

Figure 4: (a) Conventional LeeNET. (b) Proposed MLNET architecture.

Table 3: Specification of the proposed MLNET architecture.

Internal layers name	Specification values
Conv_layer1	512 filters, $2 * 2$ stride
Pool_layer1	$3 * 3$ max pool algorithm
Conv_layer2	512 filters, $2 * 2$ stride
Pool_layer2	$3 * 3$ max pool algorithm
FCNN1	1028 neurons
FCNN2	2 neurons

The size-reduced matrix from Pool_layer1 is passed through Conv_layer2, and its output response size is reduced using Pool_layer2. The size-reduced matrix from Pool_layer2 is passed through three consecutive FCNN layers. In this conventional architecture, all the internal modules are functioned in serial mode, and hence the attack detection time is high. This limitation is overcome by proposing MLNET architecture which is constructed using parallel internal modules, as illustrated in Figure 4(b). Also, this modified MLNET uses two FCNN layers instead of three FCNN layers in conventional LeeNET architecture. The specification of the proposed MLNET architecture is depicted in Table 3.

The Softmax module or normalized exponential function is used after FCNN2 layer to perform the exponential-based normalization process to eliminate the over-fitting problems in the output. The function of Softmax module is

Inputs: Unknown attacks from KIDS module;
Output: Types of unknown attack;
Start;
1.The unknown attacks are separated into various clusters using K-Nearest Neighbor (KNN) clustering approach using the following equation.
$[c1, c2, \cdots..cn] = \mathrm{KNN}(C)$, where C is the unknown attack sequences from KIDS module.
2.For each ANFIS_trained do
3.Compute $\mathrm{MLNET}_{\mathrm{trained}} = \mathrm{MLNET}\{\mathrm{ANFIS\_trained}\}$
4.End for
5.Sort the trained patterns. $\mathrm{MLNET}_{\mathrm{sort}} = \{\mathrm{MLNET}_{\mathrm{trained}}\}$
6.For each C do
7.Compute $\mathrm{MLNET\_tested} = \{\mathrm{MLNET}_{\mathrm{sort}}, C\}$
8.End for
Apply the following criteria to identify the type of the unknown attacks based on the response of FCNN2 (y1) using
9. End

$$\mathrm{Unknown}_{\mathrm{attack}_{\mathrm{type}}} = \begin{cases} \text{Botnet attack ; if } y1 > 0 \\ \text{PortScan attack ; if } y1 = 0 \\ \text{Brute Force attack ; if } y1 < 0 \end{cases}$$

Algorithm 2: Attack detection and classification using MLNET.

Table 4: ADR analysis of proposed IDS VANET system on CIC-IDS 2017 dataset.

Attack types	Number of records	Correctly detected records	Attack Detection Rate (ADR) in %
DoS attack	15,000	14,789	98.5
Botnet attack	75,000	74,192	98.9
PortScan attack	89,000	88,762	99.7
Brute Force attack	17,000	15, 972	93.9
	196,000	193,715	97.7

depicted in the following equation.

$$\mathrm{Softmax}(xi) = \frac{\exp\,(xi)}{\sum \exp(xi)}, \tag{9}$$

where xi is the response element from FCNN2 layer.

The training and classification algorithm of MLNET in the proposed IDS system of VANET is given in the following steps;

4. Results and Discussion

In this article, CIC-IDS 2017 [48] and i-VANET [49] datasets are used to validate the proposed VANET system using machine and deep learning algorithms. The CIC-IDS 2017 dataset consists of real-world traffic with attacks and non-attack data from various vehicle nodes from the VANET system. The attacks in this real-time dataset consist of Brute Force attacks, heart-bleed attacks, botnet attacks, DoS attacks, DDoS attacks, web attacks, and infiltration attacks. In this article, 1,32,000 records in the category of the data without any attack from this dataset are obtained. Also, 75,000 botnet attack records and 89,000 PortScan attack records and 17,000 Brute Force attack records are obtained from the dataset to verify the effectiveness of the proposed IDS VANET system. The i-VANET dataset is constructed by following IEEE 802.11p protocol for measuring the performance of the proposed IDS system. In this article, 1,12,000 records in the category of the data without any attack from this dataset are obtained. Also, 65,000 botnet attack records and 75,000 PortScan attack records and 15,000 Brute Force attack records are obtained from the dataset to verify the effectiveness of the proposed IDS VANET system.

The proposed IDS VANET system model is evaluated using MATLAB R2020 version, and the following metrics are used in this article for validation.

$$\begin{aligned} \mathrm{Precision(Pr)} &= \frac{t1}{t1+t3}, \\ \mathrm{Sensitivity(Se)orRecall} &= \frac{t1}{t1+t4}, \\ \mathrm{Specificity(Sp)} &= \frac{t2}{t2+t3}, \\ \mathrm{Accuracy(Acc)} &= \frac{t1+t2}{t1+t2+t3+t4}, \end{aligned} \tag{10}$$

where $t1$ and $t2$ are the detected attack records and attack-free records, respectively. $t3$ and $t4$ are the falsely detected attack records and attack-free records, respectively.

In this article, 1,96,000 records from open dataset are tested using the proposed intelligent IDS module and the proposed system stated in this article correctly detected 1,93,715 records. Table 4 is the ADR analysis of the proposed IDS VANET system using machine and deep learning methods. The average ADR of the proposed IDS-VANET system is 97.7%, and the same is illustrated in Figure 5.

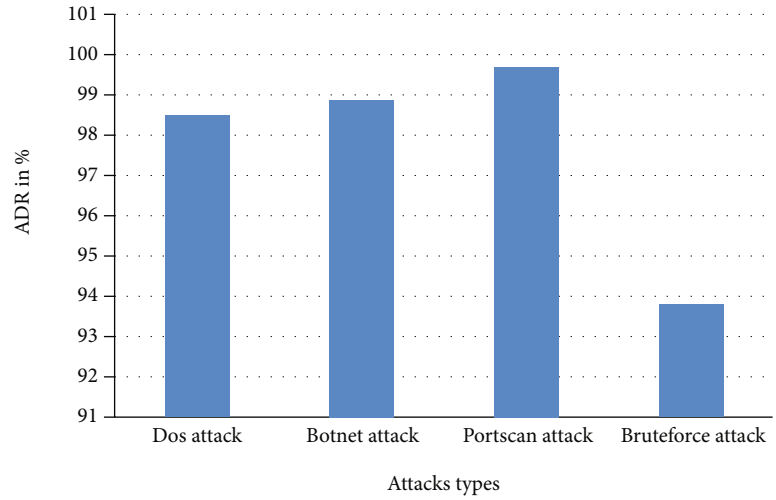

Figure 5: ADR analysis.

Table 5: ADR analysis of proposed IDS VANET system on i-VANET dataset.

Attack types	Number of records	Correctly detected records	Attack Detection Rate (ADR) in %
DoS attack	20,000	18,985	94.9
Botnet attack	65,000	63,638	97.9
PortScan attack	75,000	73,963	98.6
Brute Force attack	15,000	14,749	98.3
	175,000	171,335	97.4

Table 6: Experimental analysis of proposed IDS VANET system on CIC-IDS 2017 dataset.

Attack types	Pr in %	Se in %	Sp in %	Acc in %	Detection time (s)
DoS attack	97.9	98.9	99.3	98.7	1.87
Botnet attack	98.1	97.7	98.7	98.4	2.19
PortScan attack	97.8	98.3	98.6	98.8	0.98
Brute Force attack	98.3	98.2	99.1	98.5	1.04
Average	98.02	98.27	98.92	98.6	1.52

The ADR of the malicious attack detection is about 98.5%, Botnet attack is about 98.9%, PortScan attack is about 99.7%, and Brute Force attack is about 93.9%. From the extensive simulation results obtained in this article, the proposed intelligent IDS module obtains a high value of ADR for detecting the PortScan attack in the VANET environment.

Table 5 shows the ADR analysis of the proposed IDS VANET system on i-VANET dataset. In this article, 1,75,000 records from the open dataset are tested using the proposed intelligent IDS module and the proposed system stated in this article correctly detected 1,71,335 records. The average ADR of the proposed IDS-VANET system is 97.4%. The ADR of the malicious attack detection is about 98.5%, Botnet attack is about 97.9%, PortScan attack is about 98.6%, and Brute Force attack is about 98.3%. From the extensive simulation results obtained in this article, the proposed intelligent IDS module obtains a high value of ADR for detecting the PortScan attack in the VANET environment.

Table 6 is the experimental analysis of the proposed IDS VANET system with respect to the performance metrics on CIC-IDS 2017 dataset. The proposed system obtains 97.9% of Pr, 98.9% of Se, 98.3% of Sp, and 98.7% of Acc and consumes 1.87 s for detecting the DoS attack. The proposed system obtains 98.1% of Pr, 97.7% of Se, 98.7% of Sp, and 98.4% of Acc and consumes 2.19 s for detecting the Botnet attack. The proposed system obtains 97.8% of Pr, 98.3% of Se, 98.6% of Sp, and 98.8% of Acc and consumes 0.98 s for detecting the PortScan attack. The proposed system obtains 98.3of Pr, 98.2% of Se, 99.1% of Sp, and 98.5% of Acc and consumed 1.04 s for detecting the Brute force attack. From the extensive simulation results obtained in this article, the proposed intelligent IDS module consumed more detection time for Botnet attacks and consumed less detection time for PortScan attacks. The accuracy efficiency of the PortScan attack is higher than the accuracy level of the other attacks in the VANET system due to its non-linear functional activities. The proposed IDS-VANET system obtains 98.27% of Se, 98.92% of Sp, 98.6% of Acc, and 1.52 s of detection time, which is illustrated in Figure 6. The average accuracy of the proposed IDS model is about 98.6. The ROC of the proposed IDS model is about 98.6, which is similar to the experimental results obtained in this article; hence, the results are validated.

Table 7 is the experimental analysis of the proposed IDS VANET system for the performance metrics on i-VANET dataset. The proposed system obtains 96.9% of Pr, 98.3% of Se, 98.7% of Sp, and 98.6% of Acc and consumes 1.75 s

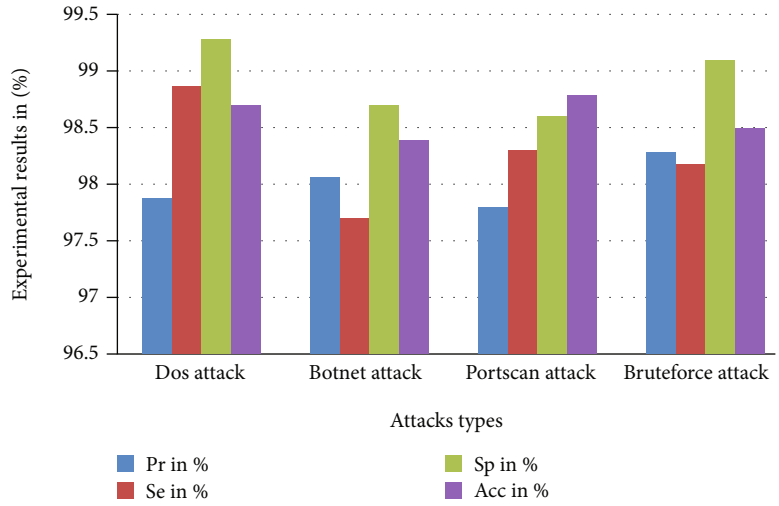

Figure 6: Analysis of proposed IDS VANET system in terms of performance metrics.

Table 7: Experimental analysis of proposed IDS VANET system on i-VANET dataset.

Attack types	Pr in %	Se in %	Sp in %	Acc in %	Detection time (s)
DoS attack	96.9	98.3	98.7	98.6	1.75
Botnet attack	98.1	98.9	98.1	98.1	0.95
PortScan attack	98.7	99.1	98.9	99.2	1.38
Brute Force attack	99.1	97.8	98.7	98.5	1.29
Average	98.2	98.5	98.6	98.6	1.34

for detecting the DoS attack. The proposed system obtains 98.1% of Pr, 98.9% of Se, 98.1% of Sp, and 98.1% of Acc and consumes 0.95 s for detecting the Botnet attack. The proposed system obtains 98.7% of Pr, 99.1% of Se, 98.9% of Sp, and 99.2% of Acc and consumes 1.38 s for detecting the PortScan attack. The proposed system obtains 99.1of Pr, 97.8% of Se, 98.7% of Sp, and 98.5% of Acc and consumes 1.29 s for detecting the Brute Force attack.

Receiver Operating Characteristics (ROC) are used to analyze the exactness of the proposed IDS model stated in this article. It is computed between the values sensitivity and 1-specificity. The average accuracy of the proposed IDS model is about 98.6%. The ROC of the proposed IDS model is about 98.6%, which is similar to the experimental results obtained in this article; hence, the results are validated.

Table 8 is the comparative analysis of proposed IDS VANET systems with other similar methods in terms of ADR. Figure 6 is the graphical analysis of comparison between the proposed and conventional IDS methods in the VANET system.

The proposed KIDS-UIDS method is compared with Hind Bangui et al. [16], Naqvi et al. [33], Jabar Mahmood et al. [34], Faisal et al. [35], Mahmood et al. [37], Nayyar et al. [32], Erfan et al. [21], Muder Almi'ani et al. [22] and

Table 8: Comparative analysis of proposed IDS VANET systems on CIC-IDS 2017 dataset.

Methods	Attack Detection Rate (ADR) in %			
	DoS attack	Botnet attack	PortScan attack	Brute Force attack
Proposed KIDS-UIDS method	98.5	98.9	99.7	93.9
Hind Bangui et al. [16]	97.9	97.8	97.2	93.2
Naqvi et al. [34]	98.1	97.9	97.3	92.8
Jabar Mahmood et al. [35]	97.1	97.5	96.8	91.4
Faisal et al. [32]	96.9	98.1	97.9	90.3
Mahmood et al. [38]	96.7	95.9	96.1	92.7
Nayyar et al. [33]	97.1	96.8	97.3	96.9
Erfan et al. [21]	96.5	96.9	97.2	90.7
MuderAlmi'ani et al. [22]	96.9	97.1	98.6	89.7
LaisenNie et al. [23]	96.3	97.3	97.7	90.9

LaisenNie et al. [23] methods for the detection of various attacks in VANET environment. The conventional methods used different numbers of records for IDS to validate the results. In order to make the proposed method uniformly, all the conventional methods or algorithms are tested on the records used in the proposed method. Therefore, the results from the conventional methods and the proposed method can be compared to validate the effectiveness of the proposed intelligent IDS system. Table 9 shows the comparative analysis of proposed IDS VANET systems on i-VANET dataset.

Computational complexity is the estimation of the computing resources such as time and memory for implementing the proposed algorithms for IDS system in VANET environment. Table 10 is the computational complexity analysis of the proposed IDS algorithm.

Table 9: Comparative analysis of proposed IDS VANET systems on i-VANET dataset.

Methods	Attack Detection Rate (ADR) in %			
	DoS attack	Botnet attack	PortScan attack	Brute Force attack
Proposed KIDS-UIDS method	98.5	98.9	99.7	93.9
Hind Bangui et al. [16]	93.2	95.1	96.4	90.3
Naqvi et al. [34]	94.6	94.9	96.2	92.1
Jabar Mahmood et al. [35]	94.1	94.2	97.2	90.3
Faisal et al. [32]	93.9	94.8	96.9	91.7
Mahmood et al. [38]	93.2	94.2	97.4	90.3
Nayyar et al. [33]	95.2	94.1	98.2	91.5
Erfan et al. [21]	94.2	95.7	97.3	91.2
MuderAlmi'ani et al. [22]	95.6	94.8	98.1	90.3
LaisenNie et al. [23]	94.8	94.1	97.9	91.8

Table 10: Computational complexity analysis of the proposed IDS algorithm.

Datasets	Time (ms)	Memory (MB)
CIC-IDS 2017	1.52	14567
i-VANET	1.34	16295

5. Conclusions

In this article, an intelligent IDS is proposed by integrating machine and deep learning algorithms to improve the efficiency of the VANET. The novelty of this article is that the intelligent IDS system is proposed in VANET, which detects both known and unknown attacks using a signature model. Also, the novel hybrid deep learning architecture is proposed in this article to classify various attacks in VANET. The known attacks in VANET are detected using ANFIS classifier, and the unknown attacks are detected using a deep learning algorithm. In this article, the conventional LeNET algorithm is modified in the proposed IDS to improve the detection time of the various attacks. The ADR of the malicious attack detection is about 98.5%, Botnet attack is about 98.9%, PortScan attack is about 99.7%, and Brute Force attack is about 93.9%. The proposed IDS-VANET system obtains 98.27% of Se, 98.92% of Sp, 98.6% of Acc, and 1.52 s of detection time on CIC-IDS 2017 dataset. The proposed system obtains 96.9% of Pr, 98.3% of Se, 98.7% of Sp, and 98.6% of Acc and consumes 1.75 s for detecting the DoS attack on i-VANET dataset. The proposed system obtains 98.1% of Pr, 98.9% of Se, 98.1% of Sp, and 98.1% of Acc and consumes 0.95 s for detecting the Botnet attack. The proposed system obtains 98.7% of Pr, 99.1% of Se, 98.9% of Sp, and 99.2% of Acc and consumes 1.38 s for detecting the PortScan attack. The proposed system obtains 99.1of Pr, 97.8% of Se, 98.7% of Sp, and 98.5% of Acc and consumes 1.29 s for detecting the Brute Force attack. The future extension of this article is to implement intelligent key management and deep learning methods to improve the security of the IDS in VANET. It could be implemented in an embedded hardware system to validate the effectiveness if the developed IDS method stated in this paper as the future scope. In the future, the performance can be optimized using the extension of the proposed methods stated in this article.

Data Availability

The CIC-IDS dataset (2017) used to support the findings of this study is included on the following web page: https://www.unb.ca/cic/datasets/ids-2017.html.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

References

[1] F. Chiti, R. Fantacci, Y. Gu, and Z. Han, "Content sharing in Internet of Vehicles: two matching-based user-association approaches," *Vehicular Communications*, vol. 8, pp. 35–44, 2017.

[2] F. A. Ghaleb, M. A. Maarof, A. Zainal, B. A. Saleh Al-Rimy, A. Alsaeedi, and W. Boulila, "Ensemble-based hybrid context-aware misbehavior detection model for vehicular ad hoc network," *Remote Sensing*, vol. 11, no. 23, p. 2852, 2019.

[3] B. A. S. Al-Rimy, M. A. Maarof, M. Alazab et al., "A pseudo feedback-based annotated TF-IDF technique for dynamic crypto-ransomware pre-encryption boundary delineation and features extraction," *IEEE Access*, vol. 8, pp. 140586–140598, 2020.

[4] F. Zafar, H. A. Khattak, M. Aloqaily, and R. Hussain, "Carpooling in connected and autonomous vehicles: current solutions and future directions," *ACM Computing Surveys*, vol. 54, no. 10s, pp. 1–36, 2022.

[5] R. Gopi and A. Rajesh, "Securing video cloud storage by ERBAC mechanisms in 5g enabled vehicular networks," *Cluster Computing*, vol. 20, no. 4, pp. 3489–3497, 2017.

[6] S. K. Tayyaba, H. A. Khattak, A. Almogren et al., "5G vehicular network resource management for improving radio access through machine learning," *IEEE Access*, vol. 8, pp. 6792–6800, 2020.

[7] J. Liang, J. Chen, Y. Zhu, and R. Yu, "A novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on differences of traffic flow and position," *Applied Soft Computing*, vol. 75, pp. 712–727, 2019.

[8] F. A. Ghaleb, M. Aizaini Maarof, A. Zainal, B. A. S. Al-Rimy, F. Saeed, and T. Al-Hadhrami, "Hybrid and multifaceted context-aware misbehavior detection model for vehicular ad hoc network," *IEEE Access*, vol. 7, pp. 159119–159140, 2019.

[9] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: an efficient pseudonymous authentication-based conditional privacy protocol for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 3, pp. 736–746, 2011.

[10] S. K. Patel and A. Sonker, "Rule-based network intrusion detection system for port scanning with efficient port scan detection rules using snort," *International Journal of Future*

Generation Communication and Networking, vol. 9, no. 6, pp. 339–350, 2016.

[11] P. Parameshwarappa, Z. Chen, and A. Gangopadhyay, "Analyzing attack strategies against rule-based Intrusion Detection Systems," in *Proceedings of the Workshop Program of the 19th International Conference on Distributed Computing and Networking*, Varanasi, India, January 2018, Association for Computing Machinery, New York, NY, United States.

[12] F. Salo, M. Injadat, A. B. Nassif, A. Shami, and A. Essex, "Data mining techniques in intrusion detection systems: a systematic literature review," *IEEE Access*, vol. 6, pp. 56046–56058, 2018.

[13] G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," *Expert Systems with Applications*, vol. 41, no. 4, pp. 1690–1700, 2014.

[14] M. Zhou, L. Han, H. Lu, and C. Fu, "Distributed collaborative intrusion detection system for vehicular Ad Hoc networks based on invariant," *Computer Networks*, vol. 172, p. 107174, 2020.

[15] T. Zhang and Q. Zhu, "Distributed privacy-preserving collaborative intrusion detection systems for VANETs," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 148–161, 2018.

[16] H. Bangui, M. Ge, and B. Buhnova, "A hybrid data-driven model for intrusion detection in VANET," *Procedia Computer Science*, vol. 184, pp. 516–523, 2021.

[17] A. Alsarhan, A. R. Al-Ghuwairi, I. T. Almalkawi, M. Alauthman, and A. Al-Dubai, "Machine learning-driven optimization for intrusion detection in smart vehicular networks," *Wireless Personal Communications*, vol. 117, no. 4, pp. 3129–3152, 2021.

[18] R. S. Vitalkar, S. S. Thorat, and D. V. Rojatkar, "Intrusion detection for vehicular ad hoc network based on deep belief network," in *Computer Networks and Inventive Communication Technologies*, S. Smys, R. Bestak, R. Palanisamy, and I. Kotuliak, Eds., vol. 75 of Lecture Notes on Data Engineering and Communications Technologies, Springer, Singapore, 2022.

[19] A. Alshammari, M. A. Zohdy, D. Debnath, and G. Corser, "Classification approach for intrusion detection in vehicle systems," *Wireless Engineering and Technology*, vol. 9, no. 4, pp. 79–94, 2018.

[20] Y. Zeng, M. Qiu, Z. Ming, and M. Liu, "Senior2Local: a machine learning based intrusion detection method for VANETs," in *Smart Computing and Communication. SmartCom 2018*, M. Qiu, Ed., vol. 11344 of Lecture Notes in Computer Science(), Springer, Cham, 2018.

[21] E. A. Shams, A. Rizaner, and A. H. Ulusoy, "Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks," *Computers & Security*, vol. 78, pp. 245–254, 2018.

[22] M. Almi'Ani, A. A. Ghazleh, A. Al-Rahayfeh, and A. Razaque, "Intelligent intrusion detection system using clustered self organized map," in *2018 Fifth International Conference on Software Defined Systems (SDS)*, Barcelona, Spain, April 2018.

[23] L. Nie, Y. Li, and X. Kong, "Spatio-temporal network traffic estimation and anomaly detection based on convolutional neural network in vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 40168–40176, 2018.

[24] M. J. Kang and J. W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PLoS One*, vol. 11, no. 6, 2016.

[25] D. Durairaj, T. K. Venkatasamy, A. Mehbodniya, S. Umar, and T. Alam, "Intrusion detection and mitigation of attacks in microgrid using enhanced deep belief network," *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects*, pp. 1–23, 2022.

[26] G. Zhao, C. Zhang, and L. Zheng, "Intrusion detection using deep belief network and probabilistic neural network," in *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, Guangzhou, China, July 2017.

[27] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 616–629, 2011.

[28] A. Daeinabi, A. G. Pour Rahbar, and A. Khademzadeh, "VWCA: an efficient clustering algorithm in vehicular ad hoc networks," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 207–222, 2011.

[29] M. Yao, X. Wang, Q. Gan, Y. Lin, and C. Huang, "An improved and privacy-preserving mutual authentication scheme with forward secrecy in VANETs," *Security and Communication Networks*, vol. 2021, Article ID 6698099, 12 pages, 2021.

[30] J. Shen, D. Liu, X. Chen, J. Li, N. Kumar, and P. Vijayakumar, "Secure real-time traffic data aggregation with batch verification for vehicular cloud in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 807–817, 2020.

[31] P. Gope and B. Sikdar, "An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6607–6618, 2019.

[32] N. B. Gayathri, G. Thumbur, P. V. Reddy, and M. Z. Ur Rahman, "Efficient pairing-free Certificateless authentication scheme with batch verification for vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 31808–31819, 2018.

[33] A. Nayyar, "Flying adhoc network (FANETs): simulation based performance comparison of routing protocols: AODV, DSDV, DSR, OLSR, AOMDV and HWMP," in *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, Durban, South Africa, August 2018.

[34] I. Naqvi, A. Chaudhary, and A. Rana, "Intrusion detection in VANETs," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, India, September 2021.

[35] J. Mahmood, Z. Duan, Y. Yang, Q. Wang, J. Nebhen, and M. N. M. Bhutta, "Security in vehicular ad hoc networks: challenges and countermeasures," *Security and Communication Networks*, vol. 2021, Article ID 9997771, 20 pages, 2021.

[36] A. Irshad, M. Usman, S. Ashraf Chaudhry, H. Naqvi, and M. Shafiq, "A provably secure and efficient authenticated key agreement scheme for energy internet-based vehicle-to-grid technology framework," *IEEE Transactions on Industry Applications*, vol. 56, p. 1, 2020.

[37] S. M. Faisal and T. Zaidi, "Timestamp based detection of Sybil attack in VANET," *International Journal of Network Security*, vol. 22, no. 3, pp. 399–410, 2020.

[38] K. Mahmood, J. Arshad, S. A. Chaudhry, and S. Kumari, "An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure," *International Journal of Communication Systems*, vol. 32, no. 16, 2019.

[39] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, N. Kumar, and M. M. Hassan, "A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 16492–16503, 2021.

[40] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, and N. Kumar, "P2SF-IoV: a privacy-preservation-based secured framework for internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–12, 2021.

[41] P. Kumar, G. P. Gupta, R. Tripathi, S. Garg, and M. M. Hassan, "DLTIF: deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2021.

[42] P. Kumar, R. Kumar, G. P. Gupta, and R. Tripathi, "BDEdge: blockchain and deep-learning for secure edge-envisioned green CAVs," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 3, pp. 1330–1339, 2022.

[43] S. Sharma, H. Sharma, and J. B. Sharma, "An adaptive color image watermarking using RDWT-SVD and artificial bee colony based quality metric strength factor optimization," *Applied Soft Computing*, vol. 84, p. 105696, 2019.

[44] D. Sinha, A. Sharma, and S. Sharma, "Automated detection of coronary artery disease comparing arterial fat accumulation using CNN," *Journal of Electronic Imaging*, vol. 31, no. 5, 2022.

[45] I. Guarino, G. Bovenzi, D. Di Monda, G. Aceto, D. Ciuonzo, and A. Pescape, "On the use of machine learning approaches for the early classification in network intrusion detection," in *2022 IEEE International Symposium on Measurements & Networking (M&N)*, pp. 1–6, Padua, Italy, July 2022.

[46] G. Bovenzi, G. Aceto, D. Ciuonzo, V. Persico, and A. Pescape, "A hierarchical hybrid intrusion detection approach in IoT scenarios," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, Taipei, Taiwan, December 2020.

[47] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, *Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection*, 2018.

[48] University of New Brunswick, "No title," August 2021, https://www.unb.ca/cic/datasets/ids-2017.html.

[49] N. S. Rajput, "Measurement of IEEE 802.11p performance for basic safety messages in vehicular communications," in *2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Indore, India, December 2018.