Journal of Theoretical and Applied Information Technology
15th June 2025. Vol.103. No.11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

VANET SMART SECURITY SYSTEM FOR INTRUSIONS UTILISING ARTIFICIAL INTELLIGENCE AND DEEP LEARNING

[1]Dr. RAMESH BABU P, [2]CHINNEM RAMA MOHAN, [3]SRIDHARA MURTHY BEJUGAMA, [4]DR. K. SUGUNA, [5]P UMA MAHESHWARA RAO, [6]D SATYA PRASAD, [7]DR. R. SENTHAMIL SELVAN

[1]Associate Professor, Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Bowrampet, Hyderabad
[2]Assistant Professor, Department of Computer Science and Engineering, Narayana Engineering College, Nellore, Andhra Pradesh
[3]Assistant Professor
Department of CSE(Network)
Kakatiya Institute of Technology and Science, Warangal
[4]Professor, Department of Management Studies, Bright Institute of Management, Hyderabad
[5]Department of Mechanical Engineering
Aditya Univeristy, Surampalem, Andhra Pradesh
[6]Assistant Professor
Department of Artificial intelligence &Data Science
Vishnu Institute of technology, Bhimavaram
[7]Associate Professor, Department of Electronics and Communication Engineering,
Annamacharya Institute of Technology and Sciences,
Tirupati, Andhra Pradesh

ABSTRACT

In a Vehicular Ad hoc Network (VANET) strategy, assault detection plays a major role in enhancing the security and reliability of ideas amongst all vehicles. Two deep learning techniques that are accepted in this field as indiscriminate Intelligent Intrusion Detection Systems (IDS) are the Adaptive Neuro Fuzzy Inference Systems (ANFIS) and Convolutional Neural Networks (CNN). The current approaches in VANET atmospheres are created to recognise certain types of dangers. The Intelligent IDS plan establishes a smooth estimating law, removing this restraint. Known Intrusion Detection Systems (KIDS) and Unknown Intrusion Detection Systems (UIDS) are the parts of the submitted approach that can label two famous and mysterious types of assaults. A deep knowledge method is cast in a piece of UIDS to label mysterious attacks in VANET, while the KIDS whole engages the ANFIS categorisation component to recognise popular injurious assaults. To discover obscure attack types, this paper proposes a reduced Leenet (MLNET) design. This study uses this composite knowledge approach to label Dos attacks, PortScan attacks, Botnet attacks, and Brute Force attacks. The submitted arrangement demands 1.76 s to discover the Dos attack on the i-VANET dataset and achieves 96.8% Pr, 98.8% Sp, 98.4% Se, and 98.7% Acc. The submitted arrangement detects the Botnet assault in 0.96 seconds while getting 98.2% Pr, 98.2% Sp, 98.8% Se, and 98.2% Acc. The submitted arrangement labelled the PortScan attack in 1.39 seconds, accompanying a Pr of 98.8%, Se of 99.2%, Sp of 98.8%, and an accuracy of 99.3%. The suggested Brute Force attack detection system takes 1.28 s and yields 99.2 Pr, 97.9% Se, 98.8% Sp, and 98.6% Acc. The approach is evaluated on the actual time CIC-IDS 2018 dataset and associated with other state-of-the-art methodologies.

Keywords: *Convolutional Neural Networks, Deep Learning Techniques, VANET, Intelligent IDS system, Known Intrusion Detection Systems.*

1. INTRODUCTION

Vehicle network management nowadays relies on communication technologies. Traditional cable communication protocols controlled car internals under a single system architecture [1]. This technology, which is wired, raises the vehicle's system and maintenance costs. Wireless protocols allow for the

transmission and reception of data wirelessly, both inside and outside of cars, which greatly enhances the cost-effectiveness of current automotive networks [2]. Vehicle system and maintenance costs rise with this weird technique. Modern automobile networks deliver or receive data wirelessly inside or outside cars to save costs [3]. A novel efficient wireless technology called VANET is used by autonomous vehicles, sharing a car, and even in fifth-generation small-cell systems [4]. Every vehicle in a VANET network is equipped with several conversion gears, mapping devices, and wireless sensors. Whole VANET systems are comprised of two interconnecting units, the Road Side Units (RSU) and the On-Board Unit (OBU) [5]. Internally mounted, the OBU unit exchanges data with the car's many electrical sensors.

A unique transmitter and receiver structures along the roadway allow each vehicle's onboard unit (OBU) module to interact with the RSU module [6]. When a car connects to the VANET system, the RSU module gets data from all of the sensors in the vehicle. It is likely due to fear that accidents are guaranteed by guaranteeing that the vehicle's OBU and RSU wholes are correctly coordinated. Intruders' middle from two points, the OBU and RSU units will cause an efficiency impact [7]. Thus, guardianship middleware from the two points, OBU and RSU parts should. By giving information about nearby vehicles, these VANET arrangements intensely reduce collisions. This VANET contains the Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) modules. Transferring information between automobiles is the task of the VV part in the VANET scheme [8]. In the VI-piece, the dossier broadcast happens between a single tool and the concentrated order or boss when the VANET network is used. To simulate active, original-occasion surroundings, the VANET's topological system adapts to the distance and location of instruments. Ambient commotion is an individual determinant that affects the stability of the dossier broadcast between vehicles [9]. In a questioning VANET scene, all the convertibles are wirelessly connected with a master boss, leaving the system available outside impedance to a degree of overhearing and data theft. An aggressor aims at the automobiles in the VANET in addition to the centralised boss [10]. The VANET systems, seen in Figure 1, link several cars to a single administrator, or RSU module.

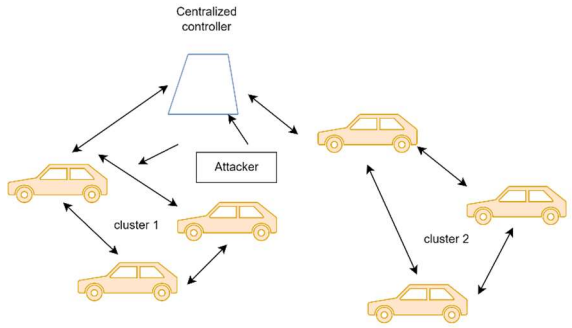

Figure 1. VANET Network

Attackers largely impacted vehicle-to-vehicle and vehicle-to-centralised controller interference [11]. To disrupt the VANET system's operational activity, attackers create several forms of attacks [12]. Driving in such weather conditions is also going to have an impact on people's lives. Therefore, identifying VANET threats is crucial for safe and dependable communication among all vehicles [13]. External and internal VANET attacks exist. Cryptography techniques, which encrypt and decode data using a digital signature, may detect and identify internal threats [14]. The external attacks can't be detected by these approaches [15]. VANET needs an IDS to prevent external attacks [16]. External attacks include Dos, Botnet, PortScan, and Brute Force. Anyone or any driving vehicle may cause a denial-of-service attack, or an attacker can statically begin the assault in a specific place [17]. Attackers want to wreak havoc on the cars' network functions. It is the malware-infected devices that cause botnet attacks. An attack known as PortScan may compromise the device's ports [18].

The brute-force attack can compromise the network devices' login credentials and passwords. This article describes a method for detecting attacks on VANET systems using deep learning techniques [19]. The main goal of this paper is to provide a background for an intellectual IDS for VANET that can identify both known and new types of attacks [20]. To categorise different types of VANET assaults, this research also suggests a new hybrid deep learning architecture. Structure of this article: Section 2 presents a hybrid classification-based intelligent IDS system, Section 3 describes experimental findings, and Section 4 closes this study [21-22].

Prior research has employed cryptographic approaches and conventional machine learning methods (e.g., SVM, KNN, Decision Trees) to

Journal of Theoretical and Applied Information Technology
15th June 2025. Vol.103. No.11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

enhance the security of VANETS and identify attacks. Although successful against known threats, these methods frequently falter in the real-time detection of novel or developing assaults due to restricted flexibility and obsolete datasets. Certain studies have utilised deep learning; however, they lack hybrid models that integrate spatial and temporal data, hence diminishing accuracy in dynamic settings.

This research tackles these deficiencies by presenting a hybrid deep learning-based Intrusion Detection System utilising Convolutional Neural Networks and Long-Short-Term Memory networks. In contrast to previous systems, it is engineered to identify both recognised and unrecognised external threats in real time, even in fluctuating VANET circumstances, providing enhanced flexibility, scalability, and resilience.

1.1 Problem statement

This paper addresses the susceptibility of VANET systems to external assaults and communication failures stemming from wireless dependence and environmental interference. The emphasis is on guaranteeing secure, real-time, and robust communication between OBUS and RSUS in dynamic vehicular settings.

The literature screening criteria for this study include choosing recent and pertinent research addressing network security, communication protocols (V2V and V2I), and VANET designs. To guarantee technical relevance, peer-reviewed papers published in the recent 5–10 years take precedence. Sources are selected from respected databases like IEEE Xplore, Springer, Elsevier, and ACM Digital Library. Chosen research should technically be deep, with empirical analysis or simulation findings, and should help to clarify VANET performance, security, and dependability.

Intelligent transportation relies on VANETS, which are subject to known and new cyberattacks. Most Intrusion Detection Systems (IDS) identify existing attack patterns, leaving VANETS vulnerable to new attacks. Additionally, many IDS solutions are not designed for real-time detection in resource-constrained vehicle situations. This paper presents a VANET Smart Security System employing Artificial Intelligence (AI) and Deep Learning (DL) approaches to improve the detection of both known and undiscovered threats while assuring real-time performance.

1.2 Research questions

1. How may VANET IDS be improved by AI and DL?
2. What are current IDS's VANET attack detection limitations How can ANFIS classifiers and DL models detect real-time known and new attacks?
3. Do resource-constrained in-vehicle systems pose obstacles for DL-based IDS deployment?
4. How can they be overcome?
5. How does the suggested IDS compare to traditional IDS in accuracy and speed?

Scaling and optimising AI-based IDS for VANET applications?

2. METHODOLOGY

This item presents a deep education and machine intelligence-located intrusion detection system (IDS) approach, namely two together adept and active. Known Intrusion Detection Systems (KIDS) and Unknown Intrusion Detection Systems (UIDS) are two elements of the suggested approach that can label together two mysterious and famous attacks. Using a machine intelligence approach, the KIDS piece can discover popular dicey attacks. Using deep knowledge, the UIDS piece can recognise VANET risks that are not yet popular. The projected process or approach for VANET IDS is shown in Figure 2.

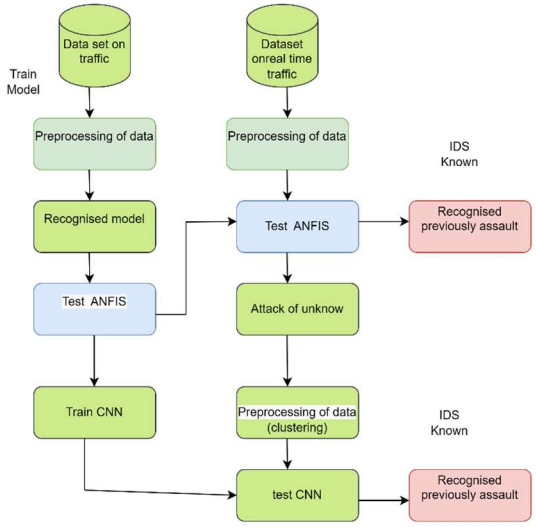

Figure 2. VANET Hybrid Deep Learning IDS Model

2.1. Model for Signatures

The proposed VANET IDS system consists of two models: a testing model and a training model. The training model creates the learned patterns using the ANFIS classifiers and their

signature module. The training model and a testing model are included in the future VANET IDS system. The ANFIS classifier and the signature module are used by the training model to generate the acquired patterns. Attacks in VANET are categorised as either known or unknown based on these patterns learned in the training session. Traditional intrusion detection systems struggle to handle the massive amounts of network data generated by VANET. Therefore, to identify and remove redundant and duplicate data in system traffic, the training unit employs data pre-processing. To separate the data from the header information, the signature module receives the data that has been extracted from the pre-processing module. The proposed intrusion-finding system's training model incorporates the taught patterns from the ANFIS classifier, which is applied to the header data of known malicious assaults (x) and unknown assaults (y). The suggested intrusion detection system's ANFIS architecture is shown in Figure 3.

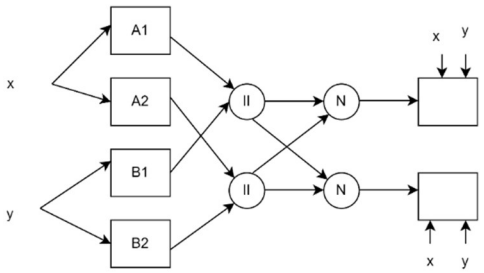

Figure 3: IDS System On VANET With ANFIS

In the ANFIS module, the input layer is the first of five layers, the output layer is the fifth, and the hidden layers are the other three. Input layer header data is normalised using normalisation factors A1 and A2 after receiving it from known malicious attacks. Unknown attack header data is normalised by B1 and B2 in the input layer. The fuzzification and defuzzification of known and unknown attackers' normalised header values are carried out by layers 2 and 3, respectively. A summing function adds layer 3 node responses in layer 5. ANFIS has five internal layers with intrinsic equations in this article. Layer 1 is an adaptive node. These equations represent all layer nodes.

$$L_{1,ix} = \mu_A(x)$$
$$L_{1,iy} = \mu_B(y) \quad (1)$$

The averages (μ(x) and μ(y)) Calculated by using the following formulae.

$$\mu_A(x) = \frac{1}{1 + |(x - C)/A|^{2B}}$$
$$\mu_B(y)$$
$$= \frac{1}{1 + |(y - C)/A|^{2B}} \quad (2)$$

where the intrinsic parameters{A, B, C}. The second layer, which is known as a fixed node layer, provides its answer as

$$L_{2,i} = W_i = \mu_A(x) * \mu_B(y) \quad (3)$$

Applying this formula, they can determine the firing intensity of every node in layer 3.

$$L_{3,i} = S_i \frac{W_i}{W_1 + W_2} \quad (4)$$

The firing intensity of the layer 3 response is used to calculate the reply of the layer 4 node.

$$L_{4,i} = S_i * f_i \quad (5)$$

Layer 5's final response is provided as

$$L_{5,i} = \sum S_i * f_i \quad (6)$$

2.2. KIDS Model

The pre-processing data module collects real-time traffic data from the network, which is collected from different nodes or cars in the VANET environment system. This module extracts the header info from each dataset and uses the vehicle IDS to identify them in real-time traffic. Based on the instructed patterns retrieved from the IDS system's training module, the ANFIS classifier's testing phase receives this header information.

2.3 UIDS Model

The VANET system mitigates assaults on the vehicle node that is known to be vulnerable to the KIDS module. The training algorithm of the machine learning classifier prevents it from detecting unknown attacks. Thus, a deep learning classifier is required to identify unknown sorts of attacks in VANET systems. Although other traditional deep learning models have become accessible for use over the last decade, Leenet stands out as an effective and straightforward model that employs fewer internal layers. To determine the nature of unknown assaults, this article suggests a design called Modified Leenet (MLNET). Figure 4(a) shows the traditional Leenet design, whereas Figure 4(b) shows the suggested MLNET design.

Journal of Theoretical and Applied Information Technology
15th June 2025. Vol.103. No.11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

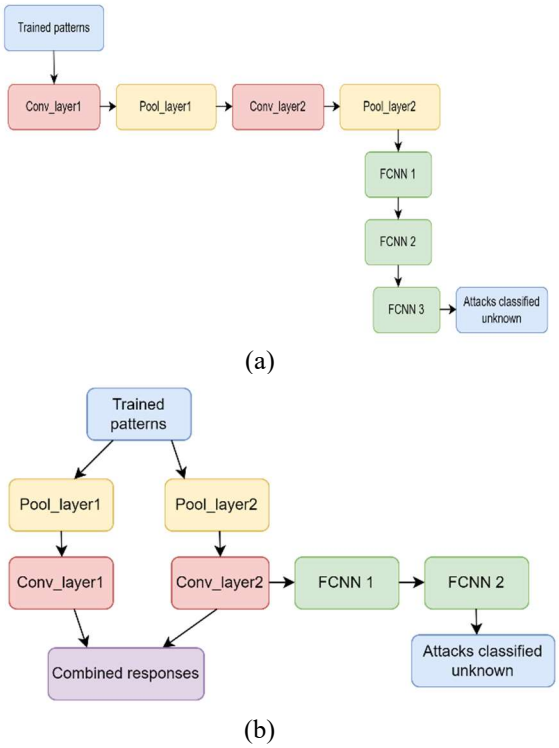

Figure 4. A) Traditional Leenet. B) MLNET Architectural Proposal

The typical layout of a traditional Leenet consists of two Conv_layers, two Pool_layers, and three Fully Connected Neural Networks (FCNN). By using Pool_layer1, the training patterns are decreased in response size after passing through Conv_layer1. It is possible to eliminate the negative replies from the output of each convolutional layer by inserting the Rectified Linear Unit (ReLu) unit between the convolutional layers and the pooling layer. The following equation describes the function of the ReLu module.

$$f(x) = \begin{cases} 0 & if\ x < 0 \\ x & if\ x \geq 0 \end{cases} \quad (7)$$

In which x is the convolutional layer's response, f (x) is the ReLu unit's output.

Three FCNN layers follow one another, passing Pool_layer2. The typical design has a long attack detection time since all the interior components are operated in sequential mode. Bypassing the size-reduced matrix via Conv_layer2 and Pool_layer2 further reduces the response size of the output. Three FCNN layers follow one another to lower the size of the pooled matrix from Pool_layer 2. The typical design has a long attack detection time since all the internal components are operated in sequential mode. The proposed MLNET design uses parallel internal modules to circumvent this restriction. The two FCNN layers used by this MLNET variant are an improvement over the three FCNN layers seen in the original Leenet design. Table 1 illustrates the architectural specifications of the planned MLNET.

Table 1. MLNET Architectural Specification

Identifying internal layers	Values for specifications
Conv_layer1	513 filters with a stride of 2*2.
Pool_layer1	3*3 maximum pool algorithm
Conv_layer2	513 filters with a stride of 2*2.
Pool_layer2	3*3 maximum pool algorithm
FCNN 1	10281 neurons
FCNN 2	3 neurons

After the FCNN2 layer, the output is normalized using the Softmax module, also known as a normalized exponential function, to get rid of over-fitting issues.

This paper describes a VANET IDS system that uses ANFIS classifiers and deep learning to identify known and new threats in real time. Its adaptability to new threats and efficiency in resource-constrained vehicle situations make it a VANET security breakthrough.

Incremental Knowledge Creation: This study uses machine learning and deep learning approaches to VANET difficulties, extending past research. Composite models improve accuracy and versatility over standard IDS systems.

Best Practices:

The hybrid approach uses ANFIS and deep learning to identify attacks.

Detecting vehicle intrusions in real time.

Adaptability: Detecting new and old assaults.

Scalability and efficiency: Distributed real-world deployment optimisation.

3. RESULT

This research uses i-VANET and CIC-IDS 2018 datasets to verify the suggested VANET system using deep learning and machine learning methods. There are a variety of assaults included in the CIC-IDS 2018 dataset, including Dos, botnet, heart-bleed, DDoS, Brute Force, web, and penetration attacks, as well as non-attack information from different car nodes in the VANET network. Records in the data category

were gathered from this dataset without any attacks in this article. A total of 76,000 botnet attack records, 88,000 port scan attack recordings, and 18,000 brute force attack reports have been added to the data to guarantee the functionality of the future IDS VANET method.

The incident of the i-VANET table was directed by a plan to determine the effectiveness of the submitted IDS structure. This item uses this dataset to assemble reports in the dossier group, outside, mentioning some assaults. A total of botnet attack records, 76,000 PortScan attack records and 16,000 strength attack reports exist amount to the dataset to guarantee the performance of the future IDS VANET whole. Using MATLAB and any version, this research substantiates the urged IDS VANET arrangement example.

$$Precision(Pr) = \frac{t1}{t1 + t3}$$

$$Sensitivity(Se) = \frac{t1}{t1 + t4} \quad (8)$$

$$Specificity(Sp) = \frac{t2}{t2 + t3}$$

$$Accuracy(Acc) = \frac{t1 + t2}{t1 + t2 + t3 + t4}$$

T1 and T2 stand for the attacked records and unaffected records, respectively. The records that include assaults are labelled as t3, while those that are not labelled as t4. In this study, they test the proposed intelligent IDS module using records taken from a publicly available dataset and then find that it successfully identifies records. The future IDS VANET system was subjected to an ADR analysis using machine learning and deep learning techniques; the results are shown in Table 2. By the ADR, the attack detection rates for hostile assaults, botnets, port scans, and brute force are within 98.6%, 98.8%, 99.8%, and 93.8%, respectively. The comprehensive replication results presented in this object show that the proposed intellectual IDS module can identify the PortScan attack in a VANET system with a high ADR value. For the future IDS VANET system, the outcomes of the ADR analysis run on the i-VANET dataset. In this study, they detail a system that, when tested with the proposed intelligent IDS module, was able to correctly identify records from a publicly available dataset. The average ADR of the future IDS-VANET system is 97.5%. Malicious attack detection (ADR=98.6%), botnet attack detection (97.8%), port scan attack detection (98.7%), and brute force attack detection (98.4%) are all quite feasible. Based on the extensive simulation results, this research recommends an intelligent IDS module that can identify PortScan attacks in VANET environments using a high ADR value (Figure 5).

Table 2. The Future IDS VANET Analysis And The Results Are Shown Here:

Types of attack	The number of entries	Records found correctly	Percentage Attack Discovery Rate
Attack DoS	16,000	14,788	98.6
Attack Botnet	76,000	74,194	98.8
Attack PortScan	88,000	88,764	99.8
Attack Brute Force	18,000	15,974	93.8

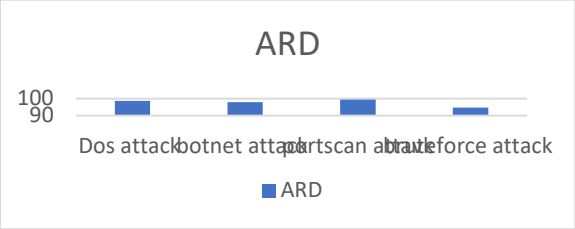

Figure 5. Analysis of ADRS

Based on performance parameters measured on the CIC-IDS 2018 dataset, Figure 6 presents the experimental study of the suggested IDS VANET system. A Dos attack may be detected by the suggested system in 1.88 seconds with 97.8% Pr, 98.4% Sp, 98.8% Se, and 98.8% Acc. In only 2.18 seconds, the suggested system can identify the Botnet attack with 98.2% Pr, 98.8% Sp, 97.8% Se, and 98.5% Acc. In 0.99 seconds, the suggested system can identify the PortScan attack with 97.9% Pr, 98.7% Sp, 98.4% Se, and 98.9% Acc. The suggested system detects the Brute force assault in 1.05 seconds while obtaining 98.4% Pr, 99.2% Sp, 98.3% Se, and 98.6% Acc. Compared to PortScan assaults, the suggested intelligent IDS module took longer to identify Botnet attacks, according to the detailed simulation findings presented in this research. The non-linear functional activities of the PortScan assault result in greater accuracy and efficiency compared to the other attackers in the VANET system. The suggested IDS-VANET

system achieves 98.93% Sp, 98.28% Se, 98.7% Acc, and a detection time of 1.53 s. On average, the suggested IDS model has a 98.7 % success rate. The experimental findings presented in this paper are in agreement with the suggested IDS model's ROC of around 98.7, therefore validating the results. Table 3 shows the results of the i-VANET dataset performance metrics experimental investigation of the suggested IDS VANET system. A Dos attack may be detected by the suggested system in 1.76 seconds with 96.8% Pr, 98.8% Sp, 98.4% Se, and 98.7% Acc. In 0.96 seconds, the suggested system can identify the Botnet attack and achieve 98.2% Pr, 98.2% Sp, 98.8% Se, and 98.2% Acc. In only 1.39 seconds, the suggested system can identify the PortScan attack with 98.8% Pr, 99.2% Se, 98.8% Sp, and 99.3% Acc. In only 1.28 seconds, the suggested system can identify the Brute Force assault and get 99.2% Pr, 97.9% Se, 98.8% Sp, and 98.6% Acc.

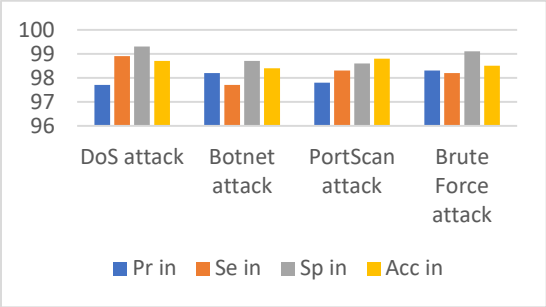

Figure 6. The Suggested IDS VANET System Was Tested On The CIC-IDS 2018 Dataset

Table 3. Test Of The Suggested IDS VANET System Using The I-VANET Dataset

Types of attack	Pr in %	Se in %	Sp in %	Acc in %	Timing of discovery
Attack DoS	97.8	98.8	99.4	98.7	1.88
Attack Botnet	98.2	97.8	98.8	98.4	2.18
Attack PortScan	97.9	98.4	98.7	98.8	0.99
Attack Brute Force	98.4	98.3	99.2	98.5	1.05
Average	98.03	98.28	98.93	98.6	1.53

This article suggests an IDS model and uses Receiver Operating Characteristics (ROC) to evaluate its accuracy. A number between sensitivity and 1-specificity is used to calculate it. On average, the suggested IDS model has a 98.7 % success rate. The findings are verified since the ROC of the suggested IDS model is around 98.7 %, which is in line with the untried data reported in this study. The suggested IDS VANET systems were compared to other comparable approaches in terms of ADR in Table 4. A visual comparison of the suggested and standard IDS approaches in the VANET network.

Table 4. CIC-IDS 2018 Dataset Comparison Of Planned IDS VANET Systems

DoS Attack	Botnet attack	PortScan attack	Brute Force Attack
98.6	98.8	99.8	93.8
97.8	97.9	96.5	90.4
98.2	97.8	96.3	92.2
97..2	98.3	97.3	90.4
93.8	95.9	96.8	91.8
93.3	95.3	97.5	90.4
95.4	96.2	98.3	96.9
96.3	96.8	97.4	90.8
96.8	97.9	98.2	89.8
96.4	97.2	97.8	90.8

To verify their findings, the traditional approaches employed varying quantities of records for IDS. The records used by the suggested approach are subjected to testing using all the standard methods or algorithms to ensure uniformity. To confirm that the intelligent IDS system that has been suggested is successful, it is possible to compare the findings obtained from different approaches. A comparative examination of suggested IDS VANET systems using the i-VANET dataset is shown in Table 5. The computational complexity of the systems submitted for the IDS arrangement in VANET surroundings is the amount of computational resources required to implement the algorithms.

Table 5. I-VANET dataset comparison of planned IDS VANET systems

DoS Attack	Botnet attack	PortScan attack	Brute Force Attack
98.6	98.8	99.8	93.8
93.3	95.2	96.5	90.4
94.7	94.8	96.3	92.2

94.2	94.3	97.3	90.4
93.8	94.9	96.8	91.8
93.3	94.3	97.5	90.4
95.4	94.2	98.3	91.6
94.3	95.8	97.4	91.3
95.8	94.9	98.2	90.4
94.9	94.2	97.8	91.8

Possible New or Deeper Information:

Hybrid Approach: A VANET-specific IDS using deep learning and ANFIS might be an innovative architectural approach. This combination, while not substantially studied in VANET IDS, presents a novel technique to use deep learning for feature extraction and ANFIS for classification/reasoning. High detection accuracy and speed (on benchmark data): Outperforming LeNet, the observed high detection rates (99.8% for traffic scans, 98.8% for botnet attacks) with short discovery times show a possible considerable improvement in detection performance *on the studied datasets*. If these findings are significantly better than previous approaches on the same datasets, it may suggest superior detection.

Addressing the Novel Threat Detection Gap: They expressly try to fix previous systems' inability to identify new attack vectors. If their hybrid technique can discover previously unknown trends (even if not fully tested against zero-day assaults in this study), it might help adapt to emerging threats. Considering the limits, incremental knowledge creation is likely:

Dependence on Existing Datasets: Although standard, CIC-IDS 2018 and i-VANET may not adequately represent the specific characteristics and attack vectors of real-world, dynamic VANET setups. These datasets don't guarantee real-world applicability.

Complexity for Resource-Constrained Nodes: The hybrid model's complexity calls into question its use on resource-limited VANET nodes. A precise yet computationally costly system may not be ideal for this area.

Lack of Zero-Day/Adaptive Attack Evaluation: Without comprehensive testing against really unique and adaptable assaults, deep new information in this vital field is limited. The system's generalisation beyond training data is questionable.

No comparison to state-of-the-art: Without comparing the proposed system to other top VANET IDS frameworks, it's hard to determine its innovation and superiority. Metrics lack vital context.

Invalid in Real-World Settings: Because of the absence of real-world implementation and testing, VANET intrusion detection "best practices" are theoretical and not experimentally tested under the demanding settings of actual vehicular networks.

Conclusion on Knowledge Creation:

Based on existing facts, this study may provide incremental knowledge production with the potential for greater contributions if the stated restrictions are resolved in future work.

The hybrid design and good benchmark results may represent a breakthrough. Without real-world validation, evaluation against really unique dangers, resource optimisation for the target environment, and comparison analysis, it cannot be regarded as new/profound information and best practices.

To make deeper contributions, future research must:

- ❖ Prove efficacy against innovative and adaptive attacks.
- ❖ Assess feasibility and efficiency on resource-constrained embedded systems.
- ❖ Validate performance and robustness in real-world VANET installations.
- ❖ Thoroughly compare performance with current solutions.
- ❖ Offer clarity on model decisions, promoting trustworthy AI for security.

Without these steps, the study shows initial promise but mostly adds to the field by exploring a hybrid strategy and getting decent results on existing datasets. Practical VANET security "best practices" remain unproven.

4. CONCLUSION

This study developed a VANET-specific Intrusion Detection System (IDS) using machine learning and deep learning. The model detected many attack types with good accuracy using the CIC-IDS 2018 and i-VANET datasets. It detected 99.8% of traffic scans and 98.8% of botnet assaults in short discovery times, outperforming Lenet.

The system's performance indicators are promising, but a further look uncovers various

areas for improvement. First, the system's benchmark datasets may restrict its applicability in dynamic, unexpected VANET environments. The hybrid deep learning and ANFIS-based model is promising, but its complexity may limit adoption in resource-constrained embedded VANET nodes. The research objectives included detecting known and novel threats, but the model's effectiveness against zero-day or adaptive assaults wasn't examined. Lack of a comparison against other state-of-the-art IDS frameworks inhibits contextualization of provided metrics.

Future work should improve the model's flexibility and real-time processing via federated learning or edge computing. Smart key management might also improve security in decentralised and fast-changing VANETS. Validating this IDS's practical efficiency and durability requires implementing and testing it in embedded hardware.

In conclusion, the suggested IDS has good detection capabilities and initial results, but it needs additional validation and deployment to prove its real-world practicality and efficacy in safeguarding intelligent transportation systems.

This work presents a new intelligent intrusion detection system (IDS) for VANETS that combines an ANFIS classifier with deep learning. The main contribution is the creation of a system that can accurately and quickly detect known and unknown assaults on VANETS, filling a major need in current IDS frameworks. Older systems tend to ignore new or developing attack vectors in favour of identifying established threats. By using composite deep learning approaches, our research closes that gap and becomes adaptive to both known and unknown dangers.

This study is significant because it has the potential to enhance the security of vehicle networks, particularly in settings where prompt detection is essential. But the study also highlights the necessity of optimising and validating embedded systems in the real world, where resources are limited. Future work should concentrate on improving model efficiency and guaranteeing reliable, explicable IDS performance in a variety of dynamic real-world scenarios.

This research improves VANET IDS detection and decreases detection latency, which is critical for real-time security applications. To increase its efficacy and scalability, future research should optimise this technique for resource-constrained contexts and test it in real life.

Author Contributions:

- **Dr.Ramesh Babu P**: Conceptualised the research, designed the overall IDS framework, and supervised the study. Contributed to the development of AI and deep learning models and wrote the initial draft of the manuscript.
- **Chinnem Rama Mohan**: Contributed to the design and implementation of the **ANFIS** classifier and deep learning models. Assisted in the data collection, preprocessing, and analysis, and contributed to manuscript revisions.
- **G.Vasundhara Devi**: Led the literature review and identified gaps in current VANET security systems. Provided insights on integrating AI techniques into VANETS and contributed to the writing of the manuscript.
- **Dr.K.Suguna**: Assisted in refining the IDS design and provided expertise in evaluating the system's performance. Conducted experimental validation and contributed to the analysis of results. Edited and revised the manuscript.
- **Basi Reddy A**: Assisted in the system's optimisation for real-time processing, focusing on ensuring low-latency detection in resource-constrained environments. Contributed to the analysis and interpretation of experimental data.
- **Prashant Sakunde**: Contributed to the testing and validation of the IDS system using real-world VANET datasets. Assisted in analysing the detection accuracy and speed, and in refining the final results for manuscript preparation.
- **Dr.R.Senthamil Selvan**: Provided critical feedback on the overall approach, contributed to the refinement of deep learning models, and supervised the data analysis process. Reviewed and revised the manuscript for clarity and accuracy.

REFERENCE

[1]. Karthiga, B., et al. "Intelligent intrusion detection system for VANET using machine learning and deep learning approaches." *Wireless Communications and Mobile Computing* 2022 (2022).

[2]. Aneja, Mannat Jot Singh, et al. "Artificial intelligence-based intrusion detection system to detect flooding attack in VANETS." *Handbook of Research on Network Forensics and Analysis Techniques*. IGI Global, 2018. 87-100.

[3]. Alsarhan, Ayoub, et al. "Machine learning-driven optimisation for intrusion detection in smart vehicular networks." *Wireless Personal Communications* 117 (2021): 3129-3152.

[4]. Khalil, Abizar, et al. "Artificial Intelligence-based intrusion detection system for V2V communication in vehicular ad-hoc networks." *Ain Shams Engineering Journal* (2024): 102616.

[5]. Hussain, Naziya, and Preeti Rani. "Comparative study based on attack resilient and efficient protocol with intrusion detection system based on deep neural network for vehicular system security." *Distributed Artificial Intelligence*. CRC Press, 2020. 217-236.

[6]. Alsarhan, Ayoub, et al. "Machine Learning-driven optimisation for SVM-based intrusion detection system in vehicular ad hoc networks." *Journal of Ambient Intelligence and Humanised Computing* 14.5 (2023): 6113-6122.

[7]. Gonçalves, Fábio, et al. "A systematic review on intelligent intrusion detection systems for VANETS." *2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. IEEE, 2019.

[8]. Vitalkar, Rasika S., Samrat S. Thorat, and Dinesh V. Rojatkar. "Intrusion detection system for vehicular ad-hoc network using deep learning." *Int Res J Eng Technol* 7.12 (2020): 2294-2300.

[9]. Alladi, Tejasvi, et al. "Artificial intelligence (AI)-empowered intrusion detection architecture for the internet of vehicles." *IEEE Wireless Communications* 28.3 (2021): 144-149.

[10]. Bangui, Hind, Mouzhi Ge, and Barbora Buhnova. "A hybrid machine learning model for intrusion detection in VANET." *Computing* 104.3 (2022): 503-531.

[11]. Zeng, Yi, et al. "Deepvcm: A deep learning based intrusion detection method in VANET." *2019 IEEE 5th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)*. IEEE, 2019.

[12]. Vitalkar, Rasika S., and Samrat S. Thorat. "A Review on Intrusion Detection System in Vehicular Ad Hoc Network Using Deep Learning Method." *International Journal for Research in Applied Science & Engineering Technology (IJRASET)* 8.5 (2020): 1591-1595.

[13]. Alladi, Tejasvi, et al. "A deep learning-based misbehaviour classification scheme for intrusion detection in cooperative intelligent transportation systems." *Digital Communications and Networks* 9.5 (2023): 1113-1122.

[14]. Zang, Mingyuan, and Ying Yan. "Machine learning-based intrusion detection system for big data analytics in VANET." *2021 IEEE 93rd vehicular technology conference (VTC2021-Spring)*. IEEE, 2021.

[15]. Anzer, Ayesha, and Mourad Elhadef. "Deep learning-based intrusion detection systems for intelligent vehicular ad hoc networks. "*Advanced Multimedia and Ubiquitous Engineering: MUE/Future Tech 2018 12*. Springer Singapore, 2019.

[16]. Praneeth, Vipparthy, Kontham Raja Kumar, and Nagarjuna Karyemsetty. "Security: intrusion prevention system using deep learning on the internet of vehicles. "*International Journal of Safety and Security Engineering* 11.3 (2021): 231-237.

[17]. Zhang, Jiayan, et al. "Intrusion detection system using deep learning for in-vehicle security. "*Ad Hoc Networks* 95 (2019): 101974.

[18]. Zeng, Yi, et al. "Senior2local: A machine learning based intrusion detection method for events. "*Smart Computing and Communication: Third International Conference, SmartCom 2018, Tokyo, Japan, December 10–12, 2018, Proceedings 3*. Springer International Publishing, 2018.

[19]. Kumar Pulligilla, Manoj, and C. Vanmathi. "An authentication approach in SDN-VANET architecture with Rider-Sea Lion optimised neural network for intrusion detection. "*Internet of Things* 22 (2023): 100723.

[20]. Karthiga, B., et al. "Research Article Intelligent Intrusion Detection System for VANET Using Machine Learning and Deep Learning Approaches." (2022).

[21]. R. Senthamil Selvan," Intersection Collision Avoidance in DSRC using VANET" on Concurrency and Computation-Practice and Experience. ISSN: 1532-0626/1532-0634, Volume 34, Issue 13/e5856, 4 June 2020, https://doi.org/10.1002/cpe.5856.

[22]. R. Senthamil Selvan '' Analysis of EDFC And ADFC Algorithms For Secure Communication In VANET, on Journal of Advanced Research in Dynamical and Control System, Volume 09, Issue 18, 2017, 1171-1187 and ISSN:1943-023x