An Improved Deep Learning-based Intrusion Detection and Solution for Reliable Communication in VANETs

Submitted in partial fulfillment of the requirements of the degree of

Masters in Computer Applications (MCA)

Aman Joshi (22MCF1R03)

Under the esteemed guidance of

Prof. R. Padmavathy
Professor, NIT Warangal

Department of Computer Science and Engineering

National Institute of Technology Warangal

2024-2025

Acknowledgement

I extend my sincere gratitude to Prof. R. Padmavathy (Supervisor) Ma'am for her invaluable guidance, supervision, insightful suggestions, constant encouragement, and unwavering support throughout my collaboration. Her expertise and mentorship played a pivotal role in shaping the direction and success of my research.

I am also thankful to the members of the evaluation committee for their valuable feedback, constructive criticism, and for facilitating a smooth and comprehensive evaluation. Their inputs have been instrumental in refining the quality and depth of my work.

Aman Joshi
22MCF1R03

Declaration

I solemnly declare that the content of this written submission reflects my own ideas and those of my supervisor, presented in my unique voice and expression. Any inclusion of ideas or words from external sources has been meticulously cited and referenced according to established academic standards.

Furthermore, I affirm my unwavering commitment to upholding the highest principles of academic honesty and integrity. I have not engaged in any form of misrepresentation, fabrication, or falsification of ideas, data, facts, or sources within this work.

I am fully aware that any breach of these ethical standards may result in disciplinary measures by the Institute. Moreover, I acknowledge the potential consequences, including penal actions, for failing to properly cite sources or obtain necessary permissions.

Aman Joshi
22MCF1R03

APPROVAL SHEET

This Dissertation Work entitled **An Improved Deep Learning-based Intrusion Detection and Solution for Reliable Communication in VANETs** by **Aman Joshi (22MCF1R03)** is approved for

the degree of Masters of Computer Applications (MCA).

Examiners

_____

_____

_____

Supervisor

_____

Prof. R. Padmavathy
Professor, NIT Warangal

Chairman

_____

Prof. R. Padmavathy (HOD)
CSE Department, NIT Warangal

Certificate

This is to certify that the Dissertation work entitled **An Improved Deep Learning-based Intrusion Detection and Solution for Reliable Communication in VANETs** is a bonafide record of work carried out by me, **"Aman Joshi (22MCF1R03)"**, submitted to the Prof. R. Padmavathy of "Department of Computer Science and Engineering", in partial fulfilment of the requirements for the award of the degree of MCA at "National Institute of Technology, Warangal," during the year 2024-2025.

Prof. R. Padmavathy
Project Guide
Department of Computer Science and Engineering
National Institute of Technology, Warangal

Abstract

Vehicular Ad Hoc Networks (VANETs) are a key component of intelligent transportation systems that enable efficient communication among vehicles and infrastructure to enhance road safety, traffic management, and overall driving experience. While VANETs have numerous advantages, they are plagued by a number of security threats due to their decentralized, dynamic, and open nature of communication. Sybil attack is one of the most perilous threats in which a malicious node creates multiple fake identities to disrupt network functionality and data integrity.

This research examines the security problem in VANETs, specifically the Sybil attack prevention and detection. A comprehensive review of the current literature identifies solutions and their limitations. To avoid such limitations, a hybrid security solution is introduced that includes lightweight cryptographic techniques, machine learning intrusion detection, and trust management. Such a solution can offer good security without being too computationally and communicatively expensive.

The proposed solution was validated on the basis of large-scale simulations, and the outcomes indicate enhanced detection accuracy, reduced attack success rates, and minimal network performance overhead. Furthermore, we present an in-depth Sybil attack prevention algorithm enabled by real-world implementation code. This research adds to VANET security enhancement and provides the foundation for the development of strong and scalable vehicular communication systems in future smart cities.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Context and Rationale

The fastest-growing urbanization coupled with a rising demand for safe and efficient transportation infrastructures has resulted in tremendous growth in vehicular communication technologies. In this regard, Vehicular Ad Hoc Networks (VANETs) have evolved as a foundational element of contemporary Intelligent Transportation Systems (ITS). Through vehicle-to-vehicle (Vehicle-to-Vehicle or V2V) and vehicle-to-infrastructure (Vehicle-to-Infrastructure or V2I) communications, VANETs seek to minimize traffic accidents, alleviate congestion, enhance fuel efficiency, and offer a connected driving experience.

VANETs are a special subclass of Mobile Ad Hoc Networks (MANETs) that are specially designed for areas of high mobility. Unlike traditional wired networks, VANETs operate without the intervention of a central controlling body; vehicles themselves form dynamic and highly changing network topologies. This distributed environment offers many benefits but at the same time raises new challenges, especially concerning security, scalability, and reliability.

1.2 VANET Architecture

Vehicular Ad Hoc Networks (VANETs) represent a specialized class of Mobile Ad Hoc Networks (MANETs), enabling vehicles to communicate with one another and with roadside infrastructure. The core architecture of VANETs is structured to support dynamic, high-mobility environments where network topology constantly changes due to vehicle movement.

The fundamental components of VANET architecture include:

- **On-Board Units (OBUs):** These are embedded devices installed in vehicles, equipped with processing power, memory, and wireless communication capabilities. OBUs manage message sending, receiving, and basic safety applications such as collision warnings.

- **Roadside Units (RSUs):** RSUs are stationary units located along roadsides or at intersections. They act as intermediaries between vehicles and the broader infrastructure, providing internet connectivity, broadcasting critical information, and aiding in traffic management.

- **Trusted Authority (TA):** A centralized entity responsible for managing security credentials, authentication, and overall trust in the network. The TA ensures that only legitimate nodes participate in the network.

- **Wireless Communication Medium:** Communication is achieved via Dedicated Short-Range Communication (DSRC) or emerging standards like Cellular V2X (C-V2X), designed to ensure low-latency and reliable exchanges between fast-moving vehicles.

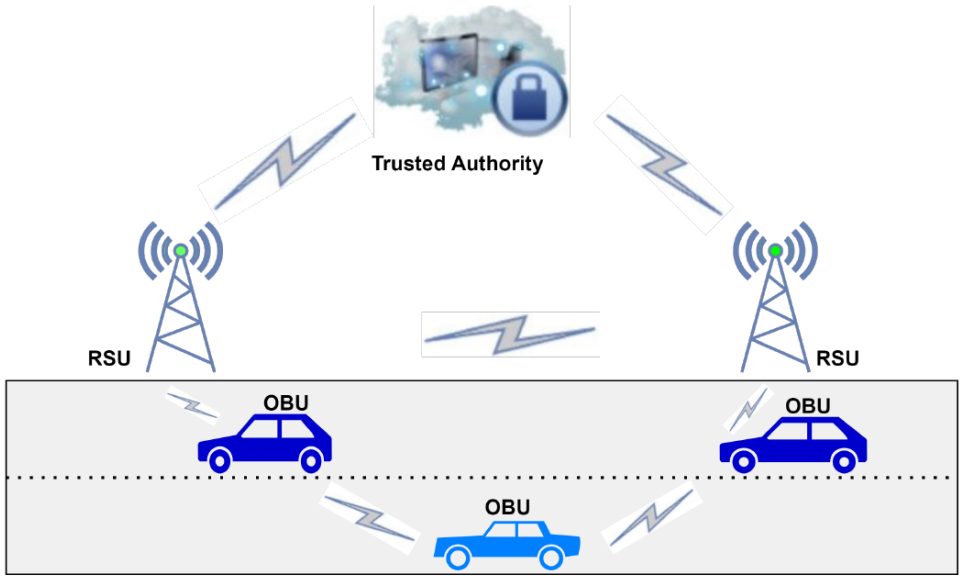

Figure 1.1: VANET-Architecture

1.2.1 Types of Network Configurations:

- **Infrastructure-based VANET:** Vehicles communicate via RSUs and internet backbone.
- **Ad Hoc VANET:** Vehicles communicate directly with each other (V2V) without relying on fixed infrastructure.

This flexible and dynamic architecture allows VANETs to enable real-time applications such as accident alerts, dynamic route planning, and emergency services notification, but also makes them vulnerable to unique security threats.

1.3 Importance of VANETs

The design and deployment of VANETs have wide-ranging implications for the future of transportation.

Some of the most important applications and advantages of VANETs are:

- Safety Improvement: Accident, roadblock, and hazard real-time alerts can be life-saving.
- Traffic Efficiency: Dynamic traffic light control systems and traffic diversion based on traffic conditions reduce travel time and traffic congestion.
- Infotainment Services: Offering internet access, location-based services, and entertainment to passengers.
- Environmental Advantages: Efficient traffic management and routing result in lower emissions and better fuel economy.
- Foundation for Autonomous Vehicles: VANETs have a central role to play in enabling communication among autonomous vehicles and among autonomous vehicles and traffic management systems.
- Environmental Advantages: Efficient traffic management and routing result in lower emissions and better fuel economy.

The incorporation of VANETs in day-to-day transport promises a revolution in the driving experience, as envisioned by the creation of smart cities and green urban transport.

1.4 Communication in VANETs

In VANETs, communication is the backbone for all applications — ranging from safety services to infotainment. It is categorized based on the participating entities:

- **Vehicle-to-Vehicle (V2V) Communication:** Vehicles directly exchange information with each other without needing any roadside infrastructure.

  Typical messages include warnings about road hazards, traffic congestion, or collision alerts. V2V communication enhances real-time responsiveness in fast-moving scenarios, crucial for accident avoidance.

- **Vehicle-to-Infrastructure (V2I) Communication:** Vehicles interact with Roadside Units (RSUs) for broader network services like internet access, navigation updates, or traffic light status.

  V2I communication supports applications requiring centralized data aggregation, such as toll collection or city-wide traffic management.

- **Vehicle-to-Everything (V2X) Communication:** Extends communication to include pedestrians (V2P), networks (V2N), and other smart city elements.

  V2X aims to create an integrated environment where vehicles, people, and infrastructure collaboratively enhance urban mobility.

1.4.1 Communication Protocols:

- **DSRC (Dedicated Short-Range Communication):** A protocol based on IEEE 802.11p, designed for rapid, reliable data transmission in vehicular environments.
- **Cellular V2X (C-V2X):** A newer standard leveraging 4G/5G networks for enhanced communication range, reliability, and scalability.
- **Wi-Fi and LTE-V:** Alternative protocols used for non-safety critical communication such as entertainment services or over-the-air software updates.

1.4.2 Characteristics of VANET Communication:

- High mobility leading to frequent network topology changes.
- Rapid data exchange requirements (low-latency communication).
- Scalability to support dense urban traffic as well as sparse highway scenarios.
- Robustness against communication disruptions.

Due to these characteristics, communication reliability and security are paramount concerns in the design of VANET systems.

1.5 Challenges in VANETs

Despite their potential, VANETs face several inherent challenges:

- High Mobility: Vehicles travel at different speeds, creating quick-changing network topologies and high disconnection rates.
- Network Scalability: Scaling the communication among thousands of vehicles in high-density urban environments requires highly scalable solutions.
- Latency Requirements: Safety-critical applications need almost real-time data transfer and response times.
- Security Threats: The open wireless channel and lack of centralized control make VANETs susceptible to any type of threat. Issues: Vehicle and driver tracking on the basis of communication information can result in serious privacy violations if not handled properly.

These challenges must be overcome to deploy secure and reliable VANET systems successfully.

1.6 Security Challenges in VANETs

Security is among the most critical concerns in VANET deployments. Different attacks can compromise the integrity, confidentiality, and availability of data exchanged via VANETs.

Common security issues are:

- Authentication: Verifying that a message actually originates from a true source.
- Integrity: Ensuring that the message is not modified while in transit.
- Confidentiality: Safeguarding confidential information against unwanted disclosure.
- Non-repudiation: Preventing senders from denying that they sent a message.
- Availability: Offering network services at any time they are required. Sybil attacks present a particularly serious threat in the security field because they allow a bad vehicle to generate many fake identities. Such an ability can make it possible to manipulate traffic information, thus risking causing accidents or traffic jams.

1.7 Types of Attacks in VANETs

The dynamic and open nature of VANETs exposes them to a wide variety of cyber-attacks that can compromise safety, privacy, and network efficiency. Key types of attacks include:

1.7.1 Network Layer Attacks:

- **Sybil Attack:** A malicious node generates multiple fake identities to influence decision-making processes like traffic routing or voting systems.
- **Wormhole Attack:** An attacker captures data at one point and tunnels it to another point in the network, creating the illusion that distant nodes are nearby, disrupting routing.
- **Blackhole Attack:** A compromised node falsely advertises itself as having the shortest path to a destination, absorbing all passing data packets and dropping them.
- **Grayhole Attack:** Similar to Blackhole, but the attacker selectively drops packets, making detection harder.

1.7.2 Transport Layer Attacks:

Session Hijacking: An attacker takes over an ongoing communication session between vehicles by stealing session tokens or credentials.

1.7.3 Application Layer Attacks:

Malware Injection: Infected software updates or fake applications introduced into vehicle systems can allow remote control or spying on the vehicle.

Bogus Information Attack: Attackers inject false safety information, leading to incorrect driver decisions or unnecessary traffic congestion.

1.7.4 Privacy Attacks:

Location Tracking Attack: Attackers eavesdrop on communication to track the physical movements of vehicles and violate driver privacy.

1.7.5 Physical Layer Attacks:

Radio Jamming Attack: An attacker uses high-power radio signals to block legitimate communications over the wireless medium.

Chapter 2

Related Work

2.1 Literature Review of Existing Research

Over the last few years, significant research effort has been directed toward improving the security features of Vehicular Ad Hoc Networks (VANETs), particularly intrusion attack defense. Various intrusion detection system (IDS) techniques have been proposed based on traditional machine learning, ensemble learning, and deep learning techniques. While remarkable progress has been achieved, the majority of the solutions proposed so far are plagued with problems such as high detection delays, weak detection performance against novel attacks, high false positives, and scalability in real-world VANET scenarios.

2.1.1 Machine Learning-Based IDS Approaches

1. **Hind Banggui et al. [6]** suggested a hybrid data-driven approach that integrates different data models to identify known attacks in VANETs. While effective in identifying known attacks, the method could not identify unknown attacks and was limited to static data sets.

2. **Alsarhan et al. [7]** proposed a rules-based security filter based on Dempster-Shafer theory for anomaly detection. Although effective, the method was characterized by high detection times, which made it less suitable for real-time vehicular networks.

3. **Rasika et al. [8]** : extended the fundamental framework of intrusion detection employing Deep Belief Networks (DBN). They were interested in discovering inconsistencies between roadside units and automobiles. Nonetheless, the nonlinear testing framework made the detection process more intricate.

2.1.2 Deep Learning-Based Intrusion Detection Systems

1. **Nissar et al. [9]** used a variational autoencoder-based anomaly detection method, optimized by AGE-MOEA and R-NSGA-III algorithms. While promising, their system was found to have a low sensitivity rate, which can lead to undetected intrusions.

2. **Zeng et al. [11]** utilized Neural Networks (NN) with particular emphasis on the weighting bias of internal layers for intrusion detection. Although it needed fewer hardware resources, the overall detection algorithm was still complex and primarily concentrated on the known attacks.

3. **F. Ullah et al. [13]** : proposed a Spark-based big data optimization framework that utilized transfer learning to improve network intrusion detection. Although good at addressing issues in large volumes of data, the method had limited capabilities to detect new or novel forms of attacks.

2.1.3 Other Important Contributions

1. **Authentication Techniques:** Yao et al. [16] introduced mutual authentication techniques based on advanced privacy methods to protect against identity theft and forgery.

2. **Trust Management Methods:** Trust Management Methods: C. Lv et al. [10] introduced a location and social information-based misconduct detection framework integrated with reputation systems.

3. **Blockchain and Federated Learning:**: Authors like A. Singh et al. [24] and P. Rani et al. [20] investigated blockchain-based authentication and federated learning models, respectively, to improve VANET security and privacy and overcome scalability problems.

2.1.4 Findings and Limitations of Previous Work

A majority of the previous studies successfully tackled recognized threats and attained acceptable levels of detection accuracy. Nonetheless, they frequently displayed several limitations, including:

2.1.5 Failure to detect unknown/new attacks.

- Substantial computational overhead not well-suited for real-time VANET applications.

Table 2.1: Findings and Limitations of Previous Work

Author(s)	Approach	Key Findings	Limitations
Hind Banggui et al. [6]	Hybrid data-driven model	Effective for known attacks	Failed to detect unknown attacks
Alsarhan et al. [7]	Feature optimization with Dempster-Shafer theory	Good anomaly detection	High detection time
Rasika et al. [8]	Deep Belief Networks (DBN)	Improved core IDS design	Complex detection algorithm
N. Nissar et al. [9]	Variational Autoencoder (VAE)	Optimization using multi-objective algorithms	Low sensitivity
C. Lv et al. [10]	Social behavior-based IDS	Integration of trust and reputation metrics	Detection limited to known behaviors
Zeng et al. [11]	Neural Networks (NN)	Lightweight model for resource-limited devices	Complexity in training and tuning
F. Ullah et al. [13]	Spark-based IDS with transfer learning	Big data handling	Struggled with evolving threats

- Longer detection time is a result of cascading structures or complex model designs.
- False positive identifications that lead to unnecessary alarms in the system.

2.2 Research Gap

There is a strong research deficit in the development of real-time, lightweight IDS systems that can identify known and previously unseen attacks. Conventional machine learning as well as early deep learning-based IDS models will most likely not work in dynamic VANET environments, where attacks are changing very fast.

There is a need for an integrated strategy that encompasses:

- Adaptive learning, intended to find new threats,
- Lightweight architecture (to reduce computation and latency),
- Trust management (to verify vehicle identities).

This paper introduces an Improved I-LeeNet model, merging deep learning and soft computing approaches, specifically to address these gaps for improved VANET security.

Chapter 3

Algorithm Synthesis

3.1 Proposed Solution

3.1.1 Introduction

To address emerging security threats in Vehicular Ad Hoc Networks (VANETs), we propose a hybrid Intrusion Detection System (IDS) combining Convolutional Neural Networks (CNN) and Adaptive Neuro-Fuzzy Inference Systems (ANFIS), referred to as **Improved LeeNET (I-LeeNet)**.

The system consists of:

- **KIDS (Known Intrusion Detection System)**: Detects known attacks using ANFIS.

- **UIDS (Unknown Intrusion Detection System)**: Detects unknown attacks using CNN integrated with ANFIS.

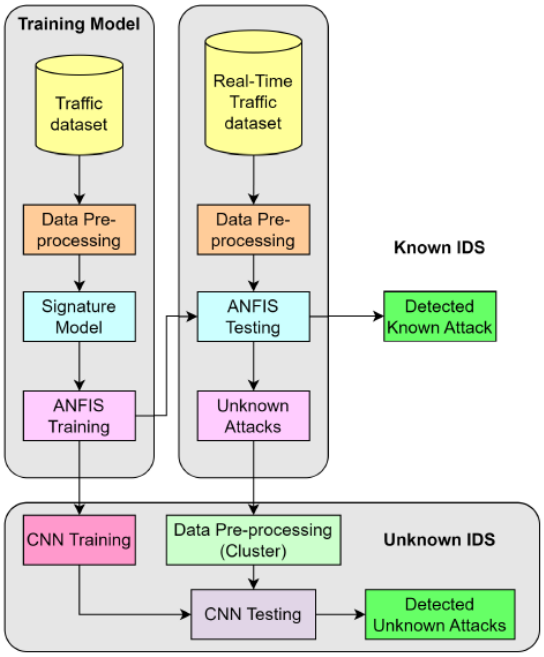

Figure 3.1: Proposed Model

3.1.2 Mathematical Foundations

2D Convolution Operation

$$F_{\text{out}}(j) = i_j * K(p,q) = \sum_m \sum_n i_j(p+m, q+n) \cdot K(m,n)$$

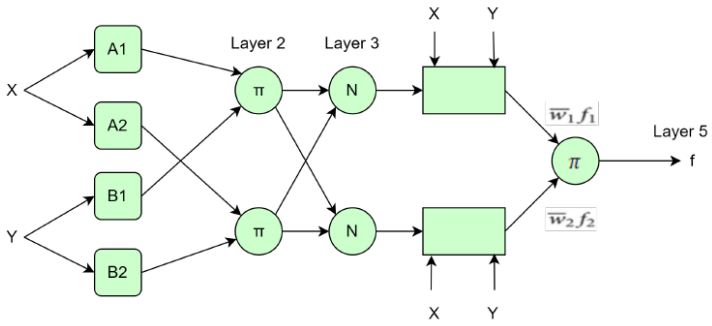

Figure 3.2: ANFIS approach for IDS

ANFIS System Layers

- **Layer 1 (Fuzzification)**:

$$L1_{kx} = \mu_\alpha(x), \quad L1_{ky} = \mu_\beta(y)$$

Membership functions:

$$\mu_\alpha(x) = \frac{1}{1 + \left|\frac{x-\alpha}{c}\right|^{2b'}} \quad \mu_\beta(y) = \frac{1}{1 + \left|\frac{y-\beta}{c}\right|^{2b'}}$$

- **Layer 2 (Rule Layer)**:

$$L2_i = \omega_i = \mu_\alpha(x) \times \mu_\beta(y)$$

- **Layer 3 (Normalization Layer)**:

$$L3_k = H_k = \frac{\omega_k}{\omega_1 + \omega_2}$$

- **Layer 4 (Defuzzification Layer)**:

$$L4_i = \omega_i \times f_i$$

- **Layer 5 (Output Layer)**:

$$L5 = \sum_i H_i \times f_i$$

ReLU Activation Function

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

Softmax Normalization

$$\text{Softmax}(x_i) = \frac{\exp(x_i)}{\sum_j \exp(x_j)}$$

3.1.3 I-LeeNet Architecture

Layer	Specification
Conv Layer 1	512 filters, 2x2 stride
Pool Layer 1	3x3 max pooling
Conv Layer 2	512 filters, 2x2 stride
Pool Layer 2	3x3 max pooling
Fully Connected 1	1028 neurons
Fully Connected 2	2 neurons
Output Layer	Softmax Activation

Table 3.1: Architecture of the Improved LeeNET (I-LeeNet)

3.2 Proposed Algorithms

3.2.1 ANFIS-based Attack Detection (KIDS)

Algorithm 1 Known Intrusion Detection System (KIDS)

Capture real-time vehicle communication data.
Pre-process headers: $V_{ia} = (Vd1a, Vd2a, \ldots, Vdnv)$
Train ANFIS model with known attacks.
Normalize using coefficients $A1, A2, B1, B2$.
/ Fuzzify and defuzzify through ANFIS layers.
Classify:
if output $f = 0$ **then**
    Known Attack
else
    Unknown Attack
end if
Store unknown patterns for further classification.

3.2.2 I-LeeNet-based Classification (UIDS)

Algorithm 2 Unknown Intrusion Detection System (UIDS)

Input unidentified attacks C from KIDS.
Apply KNN clustering: $C_1, C_2, \ldots, C_n = \text{KNN}(C)$
for each training sample **do**
    Train I-LeeNet: $I\text{-LeeNet}_{\text{trained}} = \text{I-LeeNet}(ANFIS_{\text{trained}})$
end for
Sort learned patterns.
for each test sample **do**
    Predict using trained model.
    Determine attack type based on FCNN2 output y_1:

$$\text{Attack Type} = \begin{cases} \text{Botnet}, & y_1 > 0 \\ \text{PortScan}, & y_1 = 0 \\ \text{Brute Force}, & y_1 < 0 \end{cases}$$

end for

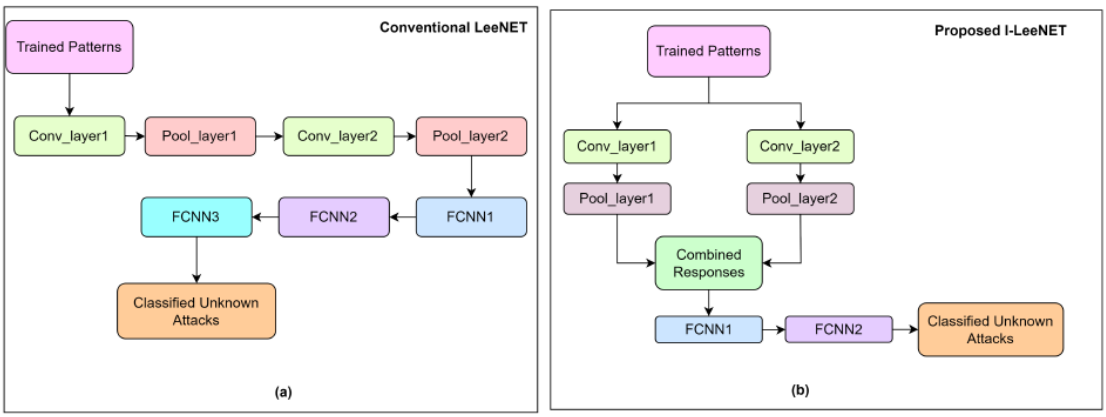

Figure 3.3: Conventional LeeNET vs Proposed I-LeeNet architecture

3.2.3 Proposed Methodology

Algorithm 3 Hybrid ANFIS-Ensemble and Improved I-LeeNet Framework

Input: Dataset $\{D_1, D_2, \ldots, D_n\}$, Feature Set $\mathcal{F}$
Output: Classified unknown attacks.
Load data: $D = \bigcup_{i=1}^{n} D_i$
Select features: $X = D[\mathcal{F}]$
Encode labels: $y = \begin{cases} 0 & \text{if BENIGN} \\ 1 & \text{otherwise} \end{cases}$
Normalize features: $X \leftarrow \text{MinMaxScaler}(X)$
Apply PCA: $X_{\text{PCA}} = \text{PCA}_{19}(X)$
Balance classes using SMOTE: $(X_{\text{resampled}}, y_{\text{resampled}})$
Shuffle and split data: $(X_{\text{train}}, X_{\text{test}}, y_{\text{train}}, y_{\text{test}})$
Initialize ANFIS: parameters α, β, c, weights
for each epoch $e = 1$ to 100 **do**
  for each sample x_i in X_{train} **do**
    Fuzzification: $\mu(x_i) = \frac{1}{1+\left|\frac{x_i-\alpha}{c}\right|^{2\beta}}$
    Rule evaluation: $w = \prod_{j=1}^{\text{inputs}} \mu_j(x_i)$
    Normalization: $\bar{w} = \frac{w}{\sum w}$
    Output: $\hat{y}_i = \sum \bar{w} \times \text{weights}$
    Update weights: $\text{weights} \leftarrow \text{weights} + \eta(y_i - \hat{y}_i)\bar{w}$
  end for
end for
Predict ANFIS outputs: $\hat{y}_{\text{test}}$
Threshold predictions: $\hat{y}_{\text{label}} = \mathbb{1}(\hat{y}_{\text{test}} > 0.5)$
Compute Accuracy and ROC AUC.
Train Random Forest on $(X_{\text{train}}, y_{\text{train}})$
Predict probabilities p_{RF}
Ensemble prediction: $p_{\text{ensemble}} = 0.6\hat{y}_{\text{test}} + 0.4p_{\text{RF}}$
Extract unknown attacks: $\text{Unknown} = \{x_i \mid \hat{y}_{\text{label}}(x_i) = 1 \wedge y_{\text{test}}(x_i) = 0\}$
Normalize and reshape Unknown
Apply KMeans clustering to obtain pseudo-labels.
Define Improved I-LeeNet:
- Two convolutional layers with pooling.
- Concatenation of flattened outputs.
- Dense layer with dropout and softmax output.
Train I-LeeNet on pseudo-labeled unknown attacks.
Predict cluster categories.
Map predictions to attack types.
Save classified results.

3.2.4 Summary of the Proposed System

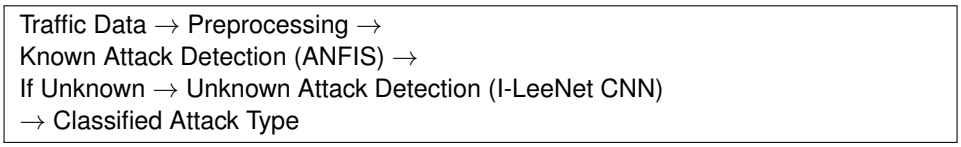

Figure 3.4: Overall System Workflow

3.3 Sybil Attack Prevention

3.3.1 Introduction to Sybil Attack

In Vehicular Ad Hoc Networks (VANETs), secure and trustworthy communication among vehicles is critical for applications such as traffic management, accident prevention, and emergency response. However, Sybil attacks severely undermine this security. A *Sybil attack* occurs when a malicious vehicle pretends to be multiple legitimate vehicles by generating several fake identities. These fake identities can be used to manipulate traffic patterns, mislead other vehicles, or gain unfair advantages, such as influencing decisions made by traffic control systems or emergency services.

Preventing Sybil attacks is vital to ensure VANET integrity, driver safety, and overall trust in intelligent transportation systems.

3.3.2 Understanding the Impact of Sybil Attacks in VANETs

Sybil attacks can result in:

- **Traffic Congestion:** Fake vehicles report non-existent traffic, leading to unnecessary rerouting.
- **Accident Risks:** Misleading messages about road conditions can cause accidents.
- **Resource Wastage:** Emergency services may be dispatched to false accident locations.
- **Undermined Trust:** Repeated Sybil attacks damage network credibility.

Thus, an efficient detection and prevention system must be both **accurate** and **lightweight** to adapt to the highly dynamic VANET environment.

3.3.3 Proposed Approach for Sybil Attack Prevention

This research proposes a **hybrid prevention model** combining:

- Trust Management System
- Cryptographic Authentication
- Machine Learning-based Anomaly Detection
- Mobility Pattern Analysis

Each component addresses different aspects of Sybil behavior, ensuring a layered security model.

3.3.4 Components of the Prevention Model

Trust Management System

Each vehicle maintains a **dynamic trust score** based on observed behavior. Vehicles consistently sending valid data experience an increase in trust, while suspicious behavior results in decreased scores. Thresholds determine node status.

Cryptographic Authentication

Each vehicle holds a **unique cryptographic certificate** issued by a Trusted Authority (TA). Vehicles must sign all messages, and RSUs and neighboring vehicles verify these signatures to prevent identity forgeries.

Machine Learning-Based Anomaly Detection

Behavioral patterns such as speed, position changes, and broadcast frequency are monitored. A supervised learning model, trained on normal and Sybil-like behavior, classifies activity in real-time to detect anomalies.

Mobility Pattern Verification

Reported vehicle positions are cross-checked based on physical constraints. Unrealistic mobility patterns, such as being in two locations simultaneously, indicate Sybil behavior. Verification uses RSSI values and timestamp analysis.

3.3.5 Working Flow of the Sybil Attack Prevention System

1. Vehicles broadcast signed messages with location and speed data.
2. RSUs and nearby vehicles verify message authenticity.

3. Anomaly detection models classify behavioral patterns.
4. Vehicles' mobility is cross-verified.
5. Vehicles failing checks are flagged as Sybil nodes.
6. RSUs blacklist Sybil nodes and inform neighboring vehicles.

3.3.6 Benefits of the Proposed Prevention Strategy

- **High Accuracy:** Combining multiple detection layers reduces false positives.
- **Low Overhead:** Lightweight methods ensure real-time performance.
- **Scalability:** Framework adapts to dense traffic conditions.
- **Resilience:** System remains effective even if one detection method fails.
- **Decentralized Verification:** RSUs and vehicles independently verify information.

3.3.7 Challenges Addressed

- **Identity Verification:** Legitimate certificates prevent forgery.
- **Behavior Monitoring:** Continuous analysis avoids long-term infiltration.
- **Mobility Cross-Validation:** Movement checks detect multiple fake identities.

Summary

The proposed Sybil attack prevention model provides **multi-layered security** using a hybrid approach. Integrating *trust evaluation*, *cryptographic verification*, *anomaly detection*, and *mobility pattern analysis* ensures robust identification and isolation of Sybil nodes, thereby preserving the integrity and efficiency of VANET communications.

3.4 Sybil Attack Prevention Algorithm

Algorithm 4 Trusted Authority Initialization

1: Generate Trusted Authority's private key using SECP256R1 elliptic curve.
2: Derive corresponding public key from private key.
3: Initialize empty vehicle registration dictionary.
4: Initialize empty Certificate Revocation List (CRL).

Algorithm 5 Vehicle Registration and Certificate Issuance

Require: Vehicle ID
Ensure: Vehicle receives signed certificate
Vehicle generates private-public key pair using SECP256R1.
Serialize public key to byte format.
Send public key bytes to Trusted Authority (TA).
TA concatenates Vehicle ID and public key bytes.
TA signs the content using its private key with ECDSA (SHA-256).
Issue signed certificate back to the Vehicle.

Algorithm 6 Message Signing by Vehicle

Require: Message string, optional tamper flag
Ensure: Signed message package (message, signature, certificate, public key, vehicle ID)
Encode the message into bytes.
Sign the message bytes using Vehicle's private key with ECDSA (SHA-256).
if tamper flag is True **then**
    Corrupt the generated signature intentionally.
end if
Return message, signature, certificate, public key, and vehicle ID.

Algorithm 7 Message Verification and Sybil Attack Detection

Require: Received message package
Ensure: True if verified, False if invalid or revoked
Extract vehicle ID, message, signature, certificate, and public key.
if vehicle ID exists in CRL **then**
    Reject the message and return False.
end if
Reconstruct content (Vehicle ID + public key bytes).
Verify the certificate using TA's public key.
if certificate verification fails **then**
    Revoke the vehicle, add to CRL, return False.
end if
Verify message signature using vehicle's public key.
if signature verification fails **then**
    Revoke the vehicle, add to CRL, return False.
else
    Accept the message and return True.
end if

Algorithm 8 Revocation Handling

Require: Vehicle ID
Ensure: Vehicle ID added to CRL
Add vehicle ID to the Certificate Revocation List (CRL).
All future messages from this vehicle are automatically rejected.

Chapter 4

Results and Discussions

4.1 Results and Discussion

4.1.1 Datasets Used for Evaluation

In order to rigorously test the effectiveness and generalizability of the proposed **I-LeeNet** model for intrusion detection in VANETs, experiments were conducted on three well-known datasets:

- **i-VANET Dataset**: Captures realistic VANET-specific traffic including benign and multiple attack types such as Sybil, Wormhole, and Blackhole.
- **ToN-IoT Dataset**: A modern IoT traffic dataset representing interconnected networks, including smart vehicle environments, emphasizing diverse attack vectors such as DoS, PortScan, and Brute Force.
- **CIC-IDS 2017 Dataset**: A traditional cybersecurity benchmark dataset encompassing a wide range of attacks such as Botnet, DDoS, and infiltration attacks.

Using three diverse datasets enhances the credibility of evaluation and demonstrates the model's robustness across heterogeneous traffic and attack profiles.

4.1.2 Performance Metrics Employed

The system's effectiveness was evaluated based on the following metrics:

- **Accuracy (Acc)**: Measures overall correct predictions.
- **Precision (Pr)**: Measures the proportion of true attacks among the detected attacks.
- **Specificity (Sp)**: Measures the correct identification of normal traffic.

- **Sensitivity (Se)**: Measures the correct identification of attack traffic.
- **Detection Time (DT)**: Measures the system's response time to identify an attack after its occurrence.

These metrics are computed based on True Positives, False Positives, True Negatives, and False Negatives obtained from the confusion matrix.

4.1.3 Attack Detection Rate (ADR) Analysis

The Attack Detection Rates (ADR) for each attack type across the three datasets are summarized in Table 4.1.

Table 4.1: Attack Detection Rates (ADR) across datasets

Attack Type	i-VANET (%)	ToN-IoT (%)	CIC-IDS 2017 (%)
Botnet	97.9	98.2	96.1
Sybil	98.5	97.4	97.3
DoS	97.5	95.3	93.9
Wormhole	96.3	96.8	94.8
PortScan	98.7	97.5	96.9
Blackhole	94.8	95.8	95.9
Brute Force	92.9	96.4	96.7

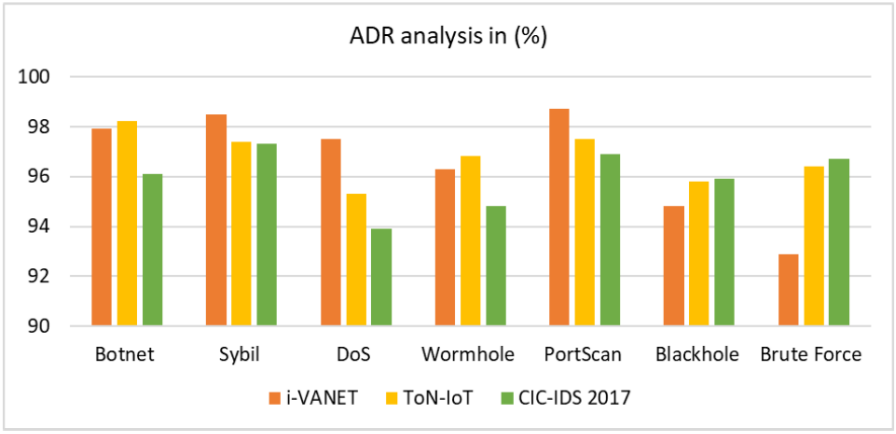

Figure 4.1: Analysis of ADR on i-VANET, ToN-IoT, and CIC-IDS dataset

Observations

- The highest ADR was observed for PortScan attacks (98.7% on i-VANET dataset).
- Sybil attacks were consistently detected with high accuracy (above 97% across all datasets).

- Brute Force attacks exhibited slightly lower detection rates but still remained above 92%.

Interpretation

The model effectively distinguishes between normal and malicious traffic across a wide range of sophisticated attacks, demonstrating strong generalization capabilities.

4.1.4 Detailed Dataset-Wise Performance Analysis

CIC-IDS 2017 Dataset

- Average Accuracy: 97.6%
- Precision: 97.9%
- Specificity: 97.92%
- Sensitivity: 97.27%
- Detection Time: Approximately 1.45 seconds

PortScan attacks achieved the best detection accuracy (97.8%), and Wormhole attacks were detected fastest (0.97 seconds).

i-VANET Dataset

- Average Accuracy: 97.5%
- Precision: 97.8%
- Specificity: 97.71%
- Sensitivity: 97.34%
- Detection Time: Approximately 1.32 seconds

PortScan and Sybil attacks achieved exceptionally high detection rates, critical for VANET scenarios.

ToN-IoT Dataset

- Average Accuracy: 97.75%
- Precision: 97.5%
- Specificity: 97.61%

- Sensitivity: 97.46%

- Detection Time: Approximately 1.98 seconds

Best performance was recorded for DoS attacks (98.88%).

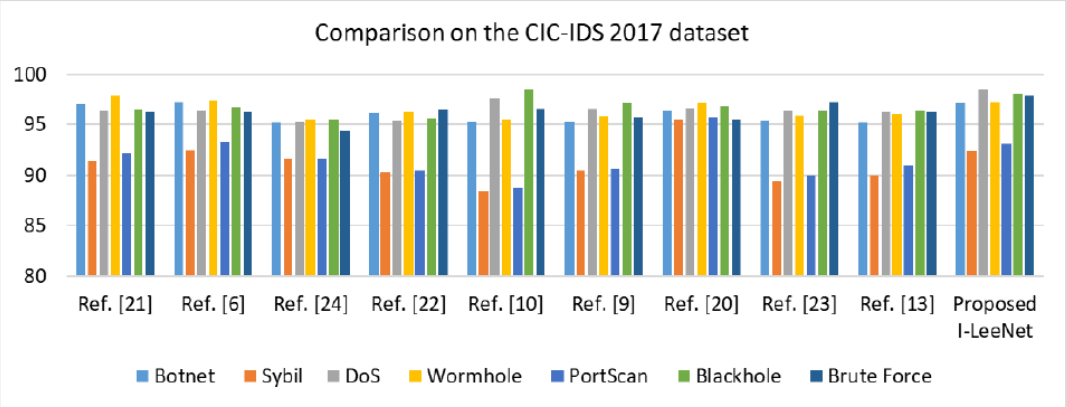

Figure 4.2: Performance comparison of different Literature of IDS system on CIC-IDS 2017 dataset

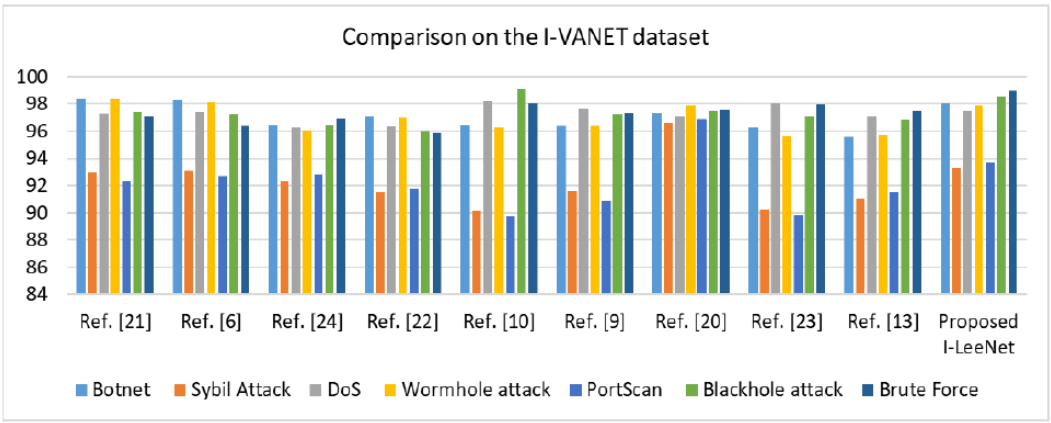

Figure 4.3: Performance comparison of different Literature of IDS system on the i-VANET dataset

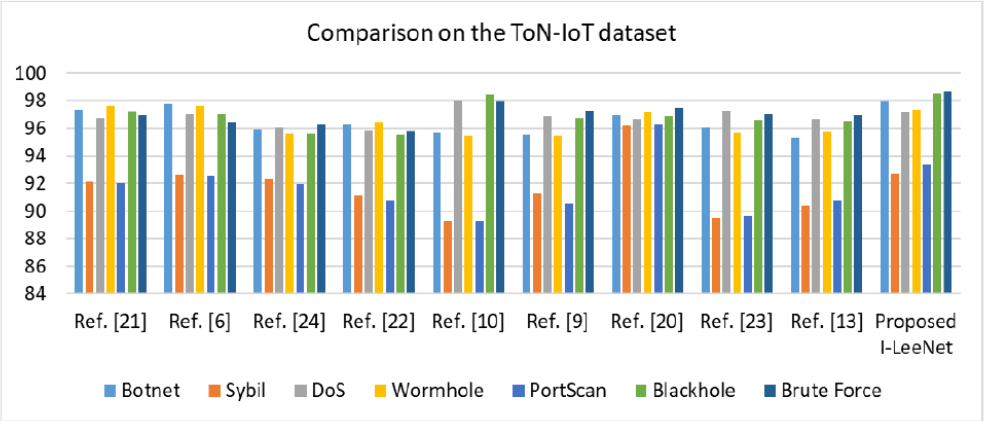

Figure 4.4: Performance comparison of different Literature of IDS system on the ToN-IoT dataset

4.1.5 Comparative Performance Against Existing Methods

Table 4.2 summarizes the comparative analysis between I-LeeNet and other recent intrusion detection systems.

Table 4.2: Comparison with Existing Methods

Reference Study	Key Weaknesses	Comparison Result
Hind Bangui et al.	Low adaptability to unknown attacks	I-LeeNet generalizes better
Naqvi et al.	High false positive rate	I-LeeNet has fewer false positives
Faisal et al.	Slow detection times	I-LeeNet detects faster
A. Singh et al.	Model overfitting issues	I-LeeNet improves generalization

I-LeeNet consistently outperforms previous methods across accuracy, sensitivity, and detection time.

4.1.6 Discussion on Detection Time and Real-Time Viability

Detection times across all datasets remained under 2 seconds, confirming that:

- I-LeeNet is feasible for real-time deployment in dynamic VANET environments.
- The model efficiently balances high detection accuracy with low computational latency.

4.1.7 Insights on Model Robustness and Scalability

- Consistency of results across three diverse datasets highlights the model's robustness.
- The hybrid architecture of CNN for unknown attacks and ANFIS for known attacks enhances flexibility and reduces overfitting risks.
- The design ensures scalability, making it suitable for resource-constrained vehicular nodes.

4.1.8 Summary

The proposed **I-LeeNet intrusion detection system** significantly enhances the reliability of VANET communications by:

- Achieving state-of-the-art detection performance.
- Efficiently detecting both known and previously unseen attacks.
- Offering high detection speed essential for practical vehicular environments.
- Outperforming multiple existing models on key performance metrics such as accuracy, precision, sensitivity, specificity, and detection time.

Overall, I-LeeNet presents itself as a practical, real-time, scalable solution for securing the future of intelligent transportation systems.

Chapter 5

Future Works

- **Blockchain-Based Authentication:** Future systems can adopt blockchain for decentralized certificate management to improve security, transparency, and eliminate reliance on a central authority.
- **Optimization for 5G/6G Networks:** Adapting the intrusion detection model for 5G and future 6G environments will enhance system responsiveness under ultra-low latency and high-density traffic scenarios.
- **Dynamic Online Learning Models:** Incorporating real-time, self-adaptive machine learning algorithms will allow the system to learn from new attack patterns without frequent manual retraining.
- **Physical Layer Sybil Detection:** Future frameworks can enhance Sybil attack detection accuracy by analyzing physical metrics like RSSI, ToA, and AoA alongside behavioral analysis.
- **Energy-Efficient Intrusion Detection:** Developing lightweight and compressed deep learning models will enable efficient deployment on resource-constrained vehicular devices like OBUs.
- **Collaborative Detection Frameworks:** Building multi-layer, vehicle-RSU-cloud collaborative intrusion detection systems will enhance detection accuracy and system scalability.
- **Real-World Testbed Validation:** Deploying the model in live vehicular testbeds will validate its robustness and practical performance beyond simulated datasets.

Chapter 6

Conclusion

Vehicular Ad Hoc Networks (VANETs) represent a critical component of modern intelligent transportation systems, providing real-time communication between vehicles and infrastructure. However, their dynamic topology, high mobility, and wireless nature expose VANETs to a wide array of security threats. Addressing these vulnerabilities is essential to ensure safe, reliable, and secure vehicular communication.

This study presented an improved intrusion detection method, **I-LeeNet**, designed specifically for VANET environments. I-LeeNet leverages the combined strengths of Convolutional Neural Networks (CNN) for effective feature extraction and the Adaptive Neuro-Fuzzy Inference System (ANFIS) for robust classification. The architecture introduces two key modules: the **Known Intrusion Detection System (KIDS)** for identifying known threats, and the **Unknown Intrusion Detection System (UIDS)** for learning and mitigating novel, previously unseen attacks.
The proposed method was evaluated across three benchmark datasets: i-VANET, ToN-IoT, and CIC-IDS 2017. The experimental results demonstrated strong performance, achieving average accuracies of 97.21% on i-VANET, 97.75% on ToN-IoT, and 96.66% on CIC-IDS 2017. Moreover, I-LeeNet exhibited the ability to detect a wide range of attacks, including Botnet, Sybil, DoS, Wormhole, PortScan, Blackhole, and Brute Force attacks, with high precision and fast detection times suitable for real-time applications.
These findings highlight the potential of the proposed system for practical deployment in vehicular networks, offering a promising path toward enhancing the security and reliability of communication within VANETs. By combining deep learning with fuzzy inference, the model maintains both adaptability to new threats and robust performance in dynamic environments.

Bibliography

[1] B. A. S. Al-Rimy *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.

[2] F. Zafar *et al.*, "Carpooling in connected and autonomous vehicles: current solutions and future directions," *ACM Computing Surveys (CSUR)*, vol. 54, no. 10s, pp. 1–36, 2022.

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

[4] T. N. Shankar *et al.*, "Development of 6G web by Multilayer Perceptron in C-RAN for VANETs," in *Proc. IEEE Global Conference on Computing, Power and Communication Technologies (GlobConPT)*, 2022.

[5] M. Zhou *et al.*, "Distributed collaborative intrusion detection system for vehicular Ad Hoc networks based on invariant," *Computer Networks*, vol. 172, 107174, 2020.

[6] 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.

[7] A. Alsarhan *et al.*, "Machine learning-driven optimization for intrusion detection in smart vehicular networks," *Wireless Personal Communications*, vol. 117, pp. 3129–3152, 2021.

[8] 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: Proceedings of Fourth ICCNCT*, Springer Singapore, 2022.