E-ISSN: 3048-6041 | Volume- 2, Issue- 5 | May 2025

FMDP: Federated Learning-Driven Model for DDoS Attack Detection and Prevention in Vehicular Edge Computing

SharthaK Kumar Lenka[1], Dr. Asif Uddin Khan[2]

[1]Master Student, Department of Computer Science and engineering, Kalinga Institute of Industrial Technology University (KIIT), Odisha, India

[2]Assistant Professor, Department of Computer Science and engineering, Kalinga Institute of Industrial Technology University (KIIT), Odisha, India

Abstract:

Vehicular Edge Computing (VEC) enables low latency processing of data by deploying computational resources at the edge of the network for intelligent transportation systems. VEC does have a significant vulnerability to Distributed Denial of Service (DDoS) attacks, which often target the Road Side Units (RSUs), as by attacking RSUs this can disrupt vehicular communication and various components of the system's reliability. We propose a scalable DDoS detection framework that preserves privacy using Federated Learning and Long Short-Term Memory (LSTM) neural networks. The proposed architecture is designed in a layered fashion containing three layers, Vehicle, Edge (RSU) and Cloud. RSUs are designed to host lightweight sample LSTM models that will classify network traffic in real time. In order to judge the degree of the attack we have also defined an attacks degree measurement that aims to quantify irregular traffic flows based on network analysis statistics and entropy, which may also allow for tweeting filters early on in the DDoS attack life cycle. In order to preserve data privacy and scalability, we adopted Federated Learning that allows RSUs to train their own models, while sharing only model updates to the central model aggregator, the central model maintains overall distributive learning system consistency between all RSUs. We used Python to simulate the system on one-thousands samples with four-hundred samples of malicious attack. The detection accuracy of the system was found to be 92.0% detections accuracy with detection rate was 93.2% with 6.8% failures. Compared to other traditional model methodologies like DoSRT, our approach demonstrated superior real time performance, scalability and adaptibility in a VEC environment.

Keywords: *DDoS detection, Federated Learning, LSTM, VANET,Vehicular Edge Computing*

List Of Abbreviations

DDoS	Distributed Denial-of-Service
VEC	Vehicular Edge Computing
VANET	Vehicular Ad Hoc Network
RSU	Roadside Unit
OBU	On-Board Unit
FL	Federated Learning
LSTM	Long Short-Term Memory
ML	Machine Learning
DL	Deep Learning
SDN	Software Defined Networking
SVM	Support Vector Machine
KNN	K-Nearest Neighbor
RBF	Radial Basis Function
KSVN	KNN + SVM Hybrid Model
RL	Reinforcement Learning
T-DDQN	Transfer Double Deep Q-Network
SMOTE	Synthetic Minority Over-sampling Technique
IoV	Internet of Vehicles
ITS	Intelligent Transportation System
IDS	Intrusion Detection System
DoSRT	Denial-of-Service Resistant Trust
FSCB-IDS	Feature Selection & Class Balancing IDS
FedAvg	Federated Averaging
RF	Random Forests

Introduction

The rise of intelligent transportation has speed up a revolution in car technology, transforming cars from solitary devices to intelligent, data-driven nodes on an expanded network [1]. Enabled by state-of-the-art computing, communication technology, and real-time decision platforms, Vehicular Edge Computing (VEC) extends the promise of distributed computation to the roadside. VEC enables applications such as adaptive cruise control, dynamic traffic routing, accident forecasting, and real-time traffic monitoring. VEC processes information at the edge, avoiding latency, preserving privacy, and enhancing decision-making [1][2].

However, the advent of this inter-connected infrastructure is also coupled with a higher vulnerability to cyber attacks[2]. Among the most effective types of such attacks are Distributed Denial of Service (DDoS) attacks, which are designed to flood Roadside Units (RSUs) and central controllers with false traffic, thus paralyzing vehicular communication and computational services. Not only do these attacks reduce the availability and efficacy of vehicular services, but they can also result in catastrophic effects to safety-critical applications[3].

This thesis tackles the security problem of DDoS attacks in VEC through a Federated Learning-based approach [3]. It suggests a novel layered defense system integrating localized knowledge with LSTM classifiers and global knowledge sharing through Federated Learning. This chapter presents the motivation, goal, and conceptual framework of the research, ending by an outline of the thesis organization[2].

Motivation

vehicular networks are becoming more heterogeneous and advanced by virtue of integration of different paradigms of computation and communication. Although, this increases communication and interaction capabilities of the car with infrastructure, like other cars, it also provides new paths to cyberattacks. The more VEC shifts computation overhead from the cloud to the edges, the more the need arises to protect edge nodes, especially RSUs[4].

Traditional DDoS solutions do not work in VEC because they are strongly based on centralized processing, fixed rule sets, or signature-based approaches that do not adapt to high-mobility,

low-latency networks. Furthermore, forwarding all vehicle information to a central server for processing incurs high bandwidth consumption and privacy concerns[5].

A more practical solution is in decentralized, real-time detection and mitigation systems that can evolve to address new threats and changing network conditions. Federated Learning, with its distributed training paradigm and privacy-friendly characteristics, is a natural integration into the VEC framework. Lightweight LSTM models at RSUs enable real-time detection of anomalous behavior with resource efficiency. These motivations are the foundation of this work[6].

Objectives

The primary goal of this research is to develop a scalable and robust DDoS detection framework suitable for VEC environments. The key objectives are outlined below:

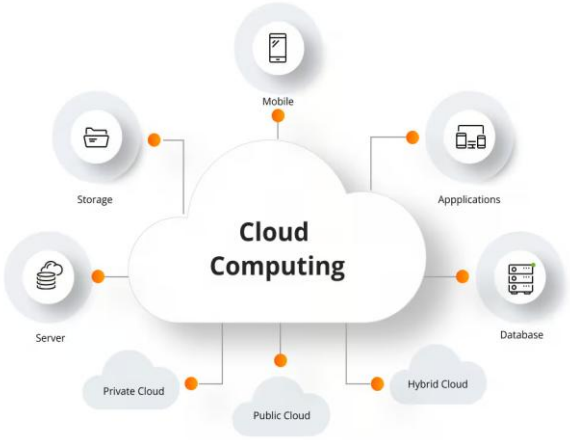
- Design a three-tier hierarchical architecture that supports distributed DDoS detection using local edge devices (RSUs).
- Develop a lightweight LSTM model for real-time traffic classification based on flow-level features.
- Introduce an attack degree metric to quickly assess the severity of network anomalies and pre-filter suspicious traffic flows.
- Integrate Federated Learning into the detection framework to aggregate model updates without sharing raw data.
- Evaluate the performance of the proposed framework using real-world datasets in terms of detection rate, false alarm rate, latency, and scalability.

Basic Concepts

Before we discuss the details of the proposed framework, it is beneficial to recognize the basic paradigms, namely cloud computing, fog computing, edge computing, mobile edge computing and vehicular ad-hoc networks (VANETs).

Cloud Computing

Cloud Computing is a centralized computing concept that allows users general access to pooled computing resources, which includes storage, processing power, and applications, on-demand, over the internet[7]. With cloud computing, the user does not have to worry about physical hardware or complicated infrastructure - the cloud service is primarily hosted on remote servers or infrastructure managed by cloud providers[8].



Cloud-Computing

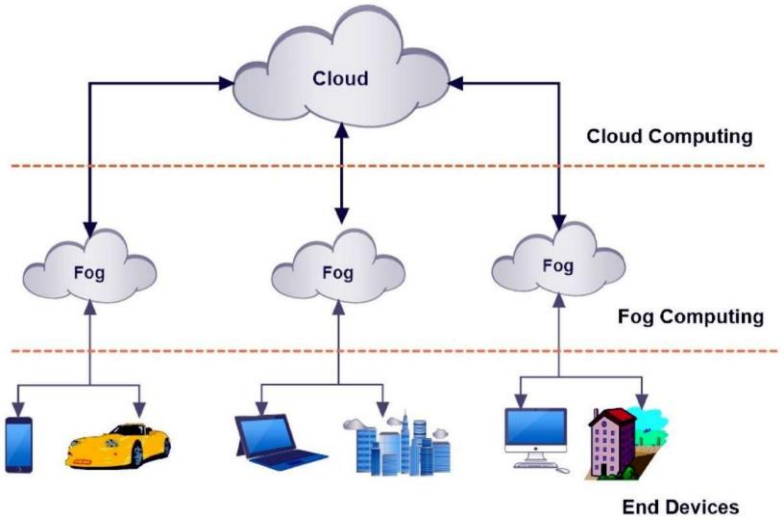
The architecture in Figure 1.1 is a typical cloud computing architecture which shows user devices, which may be a mobile device, laptops, enterprise system, etc., interact with cloud resources through a virtual environment[9]. These cloud resources are applications, databases, servers, and storage systems, which will exist in data centers around the world. These cloud networks typically allow for different cloud models such as public cloud, private cloud, and hybrid cloud, each level providing a different level of control, flexibility, and scalability for user needs[9][7].

Cloud computing's four defining characteristics are: broad network access, resource pooling, rapid elasticity or scalable usage, and measured service. Cloud technology enables collaboration, integrates and manages data, and can be deployed in dynamic ways as demand grows. These characteristics help to allow cloud computing to be a cornerstone to other technologies like big data collection and analytics, Internet of Things (IoT) platform usage, and machine learning (ML) services[9].

One of the main benefits of cloud computing is its cost-effectiveness when users only pay for what they need (use). You also have reliable backup and recovery from disaster, as well as availability globally as far as access allows availability and business continuity.

Fog Computing

Fog Computing is a decentralized computing design that extends cloud capabilities toward the edge of the network by enabling processing, storage, and control functions around the end devices [10]. Fog Computing represents an intermediate layer between end-user devices and the centralized cloud. It provides benefits for time-sensitive, data-intensive applications through faster data processing, reduced latency, and a scalable environment[10].



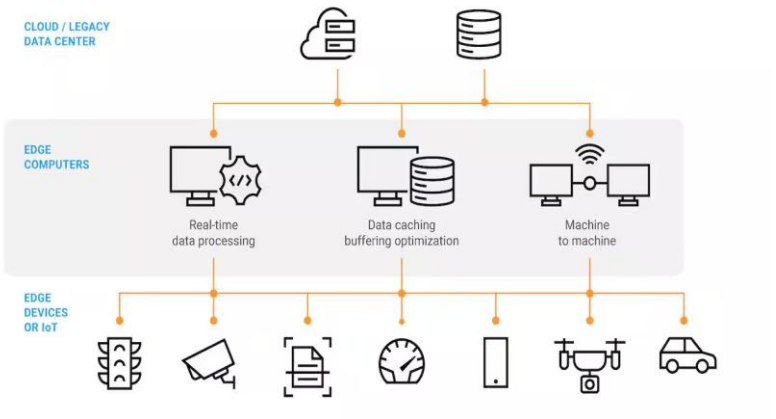
Fog computing

Figure 1.2 shows a typical architecture of a fog computing environment[11]. In this architecture, data is produced by local end devices, such as sensors, vehicles, or smart infrastructure, and is initially sent to nearby fog nodes rather than through to the original cloud[11][12]. Fog nodes are usually found at gateways, routers, or access points, and have computational capabilities to do local analytics, local filtering, and even local decision-making[11]. After some local data processing, such as filtering or generating summaries, only that which needs further aggregation or long-term storage will be sent to the cloud. Fog computing can support multiple applications, such as smart cities, autonomous transportation, healthcare monitoring, and industrial automation, where immediacy or real-time reaction and local intelligence are important. Fog

computing allows for distributed computing workloads across distributed fog nodes - this approach lowers latency and improves bandwidth efficiency and fault tolerance.

Edge Computing

Edge Computing is a distribution computing model intended to bring processing and storage as close as possible to the source of data generation - IoT devices, sensors, vehicles, etc. - and not just rely on a central server cloud architecture[13]. Edge Computing is capable of reducing latency, bandwidth, and energy by reducing the amount of data transmitted over the network[14].



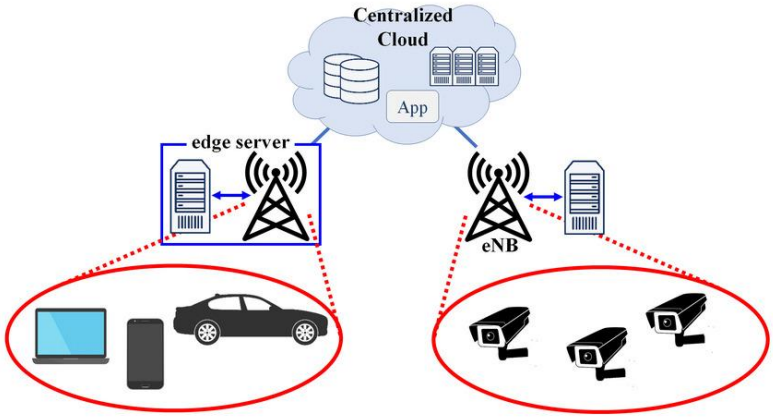
Edge Computing

An example of a typical edge computing architecture is shown in Figure 1.3. In this architecture, an edge computer acts as a middle point between the device that the end-user employs and a centralized cloud or legacy data center. Edge computers are employed for real-time data processing, edge caching, buffering, and machine to machine (device to device) communication. By offloading tasks to an edge computer instead of the cloud and localizing computations, edge computing allows for faster response time and supports time-sensitive applications[13]. At the lowest level are the edge devices: traffic lights, cameras, cell-phones, drones, and connected cars, which produce continuous streams of data[15]. The data is either processed directly at the edge (on edge servers) or filtered and sent (uphill) only when it is needed. The middle layer consists of edge computers, which provide intermediaries that organize network traffic and allow for fast, situational decisions[15]. The cloud layer retains an executive role for longer (permanent) storage, analytics, and coordination[13]. Edge computing is particularly beneficial for

applications that rely on low-latency and high-dependent processing, including automated driving, industrial automation, healthcare monitoring, smart grids, etc. Edge computing is effectively able to circumvent the disadvantages of cloud computing by alleviating workloads from cloud based centralized computing, which increases the chances of potential disconnection or cloud loading to occur[13].

Mobile Edge Computing

Mobile Edge Computing (MEC) is a revolutionary computing paradigm that brings computation, storage, and control closer to mobile users by deploying resources at the edge of the network - but it is more than that. Instead of sending data to and from distant servers using a traditional cloud model, MEC provides localized processing as close as possible to the end-user device, which results in services delivered with minimal latency, higher-quality services, and allowing the bandwidth usage to be optimized[16].



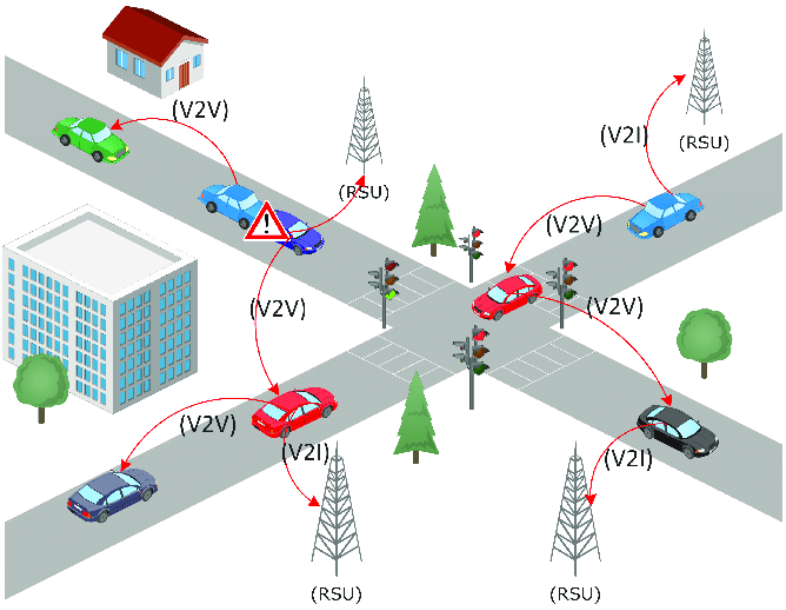
Mobile-Edge-Computing-Architecture

Figure 1.4 displays the generalized architecture of a MEC-based system[15]. MEC servers are illustrated in between the end user devices and the core network. The configured edge servers perform processing tasks offloaded from mobile user devices that include phones, sensors, or connected vehicle devices[16]. Providing a computing layer at the "edge" enables MEC to decrease processing time by reducing the amount of data that must be forwarded on to the cloud-based servers. MEC also facilitates the needed performance to allow for delay-sensitive applications to run efficiently[3]. MEC is especially useful in real-time analytics use cases like

augmented reality, vehicle communication (V2 X), and smart cities. MEC provides content caching, context-aware services, and AI-based decision-making at the edge of the network regardless of the source of the data. This enables quicker response times and helps alleviate congestion in the core network[3].

Vehicular Ad-Hoc Networks (VANETs)

Vehicular Ad Hoc Networks (VANETs) are a unique group of Mobile Ad Hoc Networks (MANETs), which enable dynamic wireless communications between vehicles and between vehicles and infrastructure. VANET enables data exchange in real-time, improving road safety, traffic efficiency, and intelligent transportation services (ITS) without a reliance on fixed networks[17].



Vehicular Ad Hoc Networks

Figure 1.5 displays a typical VANET communication scenario that involves two main modes of communication. Vehicle-to-Vehicle (V2V) communication occurs when nearby vehicles share data directly with each other to inform each other with respect to traffic hazard warnings, sudden braking, and lane changes[18].

Vehicle-to-Infrastructure (V2I) communication occurs when vehicles communicate with fixed infrastructure components in the network. For example, vehicles communicate with Road Side Units (RSUs), traffic signals, or traffic management centers, where vehicles may obtain more generalized information such as traffic information, speed limit information, or emergency warnings from traffic management centers[18].

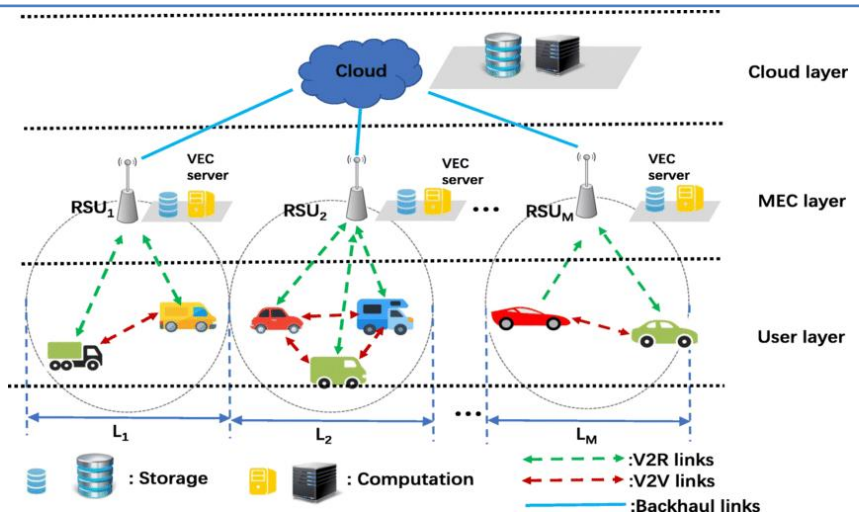
These types of networks can be used for many applications, such as collision avoidance, cooperative driving, route optimization and in-vehicle infotainment; however, VANETs also have significant challenges with mobility management, scalability, latency and hazards arising from security threats, and for that reason, we need solid adaptive protocols[19].

Vehicular Edge Computing

Vehicular Edge Computing (VEC) is a cutting-edge form of distributed computing that brings together mobile edge computing (MEC) capabilities with vehicular networks, allowing for real-time data processing and intelligent decision making[20]. VEC increases the capabilities and responsiveness of intelligent transportation systems (ITS) as processing and storage resources are made available to vehicular users as close to the source of the data that needs to be processed or stored. VEC ensures that this is achieved primarily at edge nodes such as Road Side Units (RSUs)[19].

The architecture shown in Figure 1.6 depicts a typical architecture of a VEC system operating in a vehicle edge cloud environment[21]. Vehicles with On-Board Units (OBUs) will wirelessly communicate with RSUs in the vicinity using vehicular wireless communications standards such as Dedicated Short Range Communications (DSRC) or Cellular Vehicle-to-Everything (C-V2X). Each RSU is co-located with a MEC server which provides localized computing and storage. The edge nodes are inter-connected with the cloud using high-speed optical fiber lines that enable large amounts of data to be aggregated, policy updates to be made, and long-term analytics to be performed.

E-ISSN: 3048-6041 | Volume- 2, Issue- 5 | May 2025



Architecture of VEC

In this design, the data produced by vehicles (position, speed, sensor feeds, and infotainment usage) are processed in near real-time, at the edge. Only key insights or long-term records are sent to cloud, reducing communication delays and congesting the core network. The cloud is responsible for centralized processing like global model training, orchestration of the system, and coordination between RSUs.

This structure offers a hierarchy of vehicles, RSUs (in the case with MEC servers) and cloud servers, and can provide a robust and flexible scalable architecture for latency-sensitive vehicular applications, whether for collision-avoidance, traffic predictions, autonomous driving, or emergency alerts. VEC allows for high-throughput, low-latency communication as well as intelligent decisions from the edge, thereby supporting effective safety solutions, efficiency in functions like routing, and real-time action in a dynamic transportation environment.

Features of Vehicular Edge Computing

VEC blends the benefits of VANETs and edge computing to create a powerful platform for real-time, distributed intelligence in traffic networks. Key features include:

- **Low Latency:** VEC enables microsecond-level responsiveness essential for autonomous vehicle control and accident prevention[22].

- **Context Awareness:** RSUs can interpret localized traffic and environmental conditions, providing services tailored to specific locations.
- **Resource Efficiency:** Offloading heavy computation from vehicles to RSUs ensures better battery management and sensor efficiency[15].
- **Data Privacy:** As most processing is done locally, VEC minimizes unnecessary data transfer, preserving user confidentiality.
- **Resilience:** Decentralization and multi-point coordination improve the robustness of ITS against both system faults and cyberattacks.

Challenges of VEC

VANETs and VEC systems face major challenges in practice. The high mobility of vehicles providing a fast changing network topology and intermittent communication. Unreliable devices that have limited resources such as RSUs (road side units) and OBUs (on-board units) because of their limited computational models require more efficient and lightweight alternatives. As another example, if density of vehicles increases and the demand for services (based on the increasing density) is increased accordingly, the deployments must efficiently scale in terms of model, latency and ultimately reliability. Simultaneously, the vehicular communication (wireless) is susceptible to security problems with a broadcast nature e.g., denial of service attacks (DDoS) or other spoofing attacks[23] These issues raise serious questions regarding reliability based on their ability to provide real-time responses, secure data integrity and assure safety against threats in a mobile dynamic environment. Due to these issues, they point to the need for adaptive, distributed and effective detection models for emerging vehicular technologies[23].

Thesis Organization

The remainder of this thesis is structured as follows:

Chapter 2 provides a comprehensive literature review of existing methods and frameworks for DDoS detection in vehicular and edge computing environments. This includes traditional security models, machine learning-based intrusion detection systems, and recent advancements

in federated learning techniques. The review highlights key limitations in scalability, real-time responsiveness, and privacy preservation, which form the motivation for the proposed work. Chapter 3 presents the detailed system model and problem formulation. It introduces the hierarchical architecture of the proposed solution, comprising the vehicle layer, edge (RSU) layer, and cloud layer. This chapter also discusses the communication model, threat model, and the mathematical formulation of the detection objective, focusing on scalability and dynamic adaptation.

Chapter 4 describes the proposed framework and methodology. It outlines the use of LSTM neural networks for traffic classification at the RSU level, the attack degree calculation for pre-filtering, and the federated learning protocol for collaborative model training. The chapter also includes flowcharts and algorithms representing the layer-wise detection and update processes. Chapter 5 details the results and performance analysis. It covers the simulation environment, dataset, metrics used, and experimental findings. Evaluation is based on detection accuracy, failure rate, delay, and throughput. A comparative analysis is included to benchmark the proposed model against DoSRT and similar methods. Chapter 6 concludes the thesis by summarizing the contributions and discussing future research directions, including real-time implementation and enhancements such as hybrid learning approaches.

Literature Review

In Xiao et.al.[24] address the challenge of detecting and mitigating low-rate distributed denial-of-service (LR-DDoS) attacks within vehicular edge computing networks. Given that edge nodes, particularly roadside units (RSUs), are susceptible to such stealthy attacks due to their exposure to external environments, the authors propose a detection and defense mechanism grounded in information metrics. Their approach involves sampling incoming traffic at edge nodes and computing real-time information metrics, which are then compared against predefined thresholds to identify potential attack traffic. To ensure continuity of services for legitimate users, a defense algorithm is introduced to detect conflicting Mobile Subscriber ISDN Numbers (MSISDNs), thereby preventing service disruption to normal vehicles. The proposed method emphasizes cooperative defense among multiple edge nodes to enhance detection accuracy while

minimizing resource consumption. Experimental evaluations demonstrate the effectiveness of this scheme in identifying LR-DDoS attacks and maintaining network service quality[24].

In Yao et.al.[25] present a viable Software-Defined Networking (SDN) network-based detection and response system for Distributed Denial-of-Service (DDoS) attacks in vehicular networks. Despite the known limitations of SDN network centralized control, the authors design a system that takes advantage of SDN controllers' global view of the network to monitor traffic and detect variations in traffic patterns that suggest DDoS attacks. Additionally, the platform to enhanced security has a fast reaction time that built-in a way to change flow rules to respond to protect against detected performance DDoS attacks which allow the vehicular network to retain performance or reliability[25]. Results indicate that the platform can successfully detect attacks and has the ability to mitigate DDoS attacks quickly, as a secure advanced approach to enhancing vehicular network security[25].

In Adhikary et.al.[26] present a hybrid detection methodology aimed at recognizing Distributed Denial-of-Service (DDoS) attacks within Vehicular Ad Hoc Networks (VANETs). This methodology integrates two Support Vector Machine (SVM) kernel techniques: AnovaDot and Radial Basis Function (RBF) Dot, with the objective of improving detection precision by capitalizing on the advantages presented by both kernels. Essential characteristics such as packet collisions, packet losses, and jitter are employed to replicate real-time network conditions that encompass both standard and attack scenarios. The hybrid model undergoes training and testing utilizing these characteristics, and its efficacy is assessed against standalone SVM kernel models based on metrics including Accuracy, Gini coefficient, Kolmogorov-Smirnov (KS) statistic, Mean Error Rate (MER), and H-measure. Empirical findings reveal that the hybrid methodology surpasses the individual kernel models across all assessment metrics, signifying its heightened proficiency in detecting DDoS attacks within VANET settings. The analysis shows that utilizing various SVM kernels can markedly enhance the efficacy of intrusion detection systems powered by machine learning in vehicular networks[26].

The work of Kadam et.al [27] showcases a pioneering hybrid machine learning framework, dubbed the Hybrid K-Nearest Neighbor and Support Vector Machine (KSVN) algorithm, aimed at pinpointing Distributed Denial-of-Service (DDoS) incidents in Vehicular Ad Hoc Networks (VANETs). By understanding the specific hurdles that come with VANETs, like quick mobility

and varying network arrangements, the authors merge the benefits of K-Nearest Neighbor (KNN) and Support Vector Machine (SVM) classifiers to boost detection accuracy. The KSVN algorithm is subjected to training and evaluation utilizing a dataset obtained from Kaggle, concentrating on features such as protocol types, source and destination IP addresses, and port numbers. Empirical assessments reveal that the KSVN algorithm surpasses individual machine learning models, including independent KNN and SVM classifiers, regarding accuracy, sensitivity, precision, recall, and error rates. The study concludes that this hybrid methodology offers a more robust framework for detecting DDoS attacks in VANET settings[27].

Karthikeyan et.al.[28] present a real-time detection method for Distributed Denial-of-Service (DDoS) flooding attacks in Intelligent Transportation Systems (ITS). Recognizing the critical need for prompt and accurate detection mechanisms in ITS, the authors employ reinforcement learning techniques to develop a model that can identify DDoS attacks effectively. The proposed method leverages the adaptive capabilities of reinforcement learning to monitor network traffic patterns and detect anomalies indicative of DDoS flooding attacks. Experimental evaluations demonstrate that the model achieves high detection accuracy and low false-positive rates, highlighting its efficacy in enhancing the security and reliability of ITS infrastructures. This study underscores the potential of integrating advanced machine learning approaches, such as reinforcement learning, into real-time security frameworks for vehicular networks[28].

The Lei et.al. [29] introduce a security design anchored in blockchain technology to confront the challenges of key management, cache poisoning, and privacy-preserving access control within vehicular edge computing (VEC) environments utilizing Named Data Networking (NDN). Acknowledging the vulnerabilities that are characteristic of NDN-based VEC frameworks, the authors devise and execute a sophisticated blockchain system that utilizes an efficient, lightweight yet resilient delegate consensus algorithm. This system enables decentralized key management, alleviates the risks associated with cache poisoning attacks, and enforces privacy-centric access control strategies. Comprehensive experimental evaluations substantiate the architecture’s efficacy in bolstering security protocols without detracting from network performance. The findings suggest that the incorporation of blockchain technology within NDN-based VEC networks represents a viable approach to addressing existing security and privacy challenges[29].

According to Grover et.al.[30], a fortified multitier networking structure for the Internet of Vehicles (IoV) is introduced, merging edge computing with deep learning methods to strengthen security and enhance operational efficiency. This framework is specifically crafted to tackle the complexities associated with real-time data processing and threat identification within vehicular networks. By utilizing edge computing, the system facilitates data processing in proximity to the data source, thereby diminishing latency and enhancing response times. Furthermore, deep learning algorithms are utilized to scrutinize traffic patterns and identify anomalies that may signify potential security threats. The multitier architecture guarantees both scalability and resilience, adapting to the ever-evolving conditions of vehicular environments. Empirical assessments validate the framework's efficacy in swiftly identifying and addressing security threats, consequently improving the overall safety and dependability of IoV systems[30].

The work by Haydari et.al. [31] outlines a centralized framework centered around RSUs for online intrusion detection and mitigation, specifically developed for Vehicular Ad Hoc Networks (VANETs), with a strong focus on countering false data injection (FDI) and discreet Distributed Denial-of-Service (DDoS) threats. The authors[31] propose a semi-supervised, non-parametric, and sequential anomaly detection algorithm that functions in real-time, facilitating the swift identification of anomalous behaviors without the necessity of predefined attack signatures. Each Roadside Unit (RSU) autonomously scrutinizes incoming data streams from vehicles within its communicative vicinity, utilizing statistical techniques to uncover deviations suggestive of malicious intent. Upon detection, the system swiftly addresses threats by isolating compromised nodes and transmitting alerts to adjacent RSUs and vehicles. The effectiveness of the framework is corroborated through simulations and empirical traffic datasets, showcasing enhanced detection accuracy and diminished false alarm rates in comparison to existing methodologies. This research highlights the promise of RSU-focused, machine learning-based strategies in bolstering the resilience of VANET infrastructures against intricate cyber threats[31].

In the Keshari et.al [32] propose DoSRT, a Denial-of-Service Resistant Trust model tailored for Vehicular Ad Hoc Networks (VANETs), addressing the limitations of centralized and decentralized trust management systems. Recognizing the inefficiencies of centralized approaches and the overheads associated with frequent cluster changes in decentralized methods, the Keshari et.al [32] introduce a cluster-based framework that leverages speed deviation-based

clustering to enhance stability. Trust evaluation within DoSRT is bifurcated into direct trust, assessed based on the frequency of beacon messages received from neighboring vehicles, and indirect trust, derived from recommendations provided by other vehicles. These trust metrics are aggregated to identify and isolate malicious nodes effectively. Simulation results demonstrate that DoSRT outperforms existing models, such as the one proposed by Hasrouny et al., achieving improvements of approximately 20% in accuracy, 19% in precision, 16% in recall, and 17% in F-score, even in scenarios with up to 30% malicious vehicles. The study concludes that DoSRT offers a robust solution for enhancing trust management and mitigating DoS attacks in dynamic VANET environments[32].

Through their examination, Li et.al. [33] disclose a structure employing a Transfer Double Deep Q-Network (T-DDQN) aimed at uncovering Distributed Denial-of-Service (DDoS) incidents in the Internet of Vehicles (IoV). Acknowledging the complexities introduced by the ever-changing dynamics of IoV settings and the limitations associated with the availability of labeled datasets, the authors amalgamate transfer learning with a Double Deep Q-Network architecture to bolster detection effectiveness. The framework exploits the similarities in traffic flows between neighboring base stations to support the transfer of knowledge, thereby enabling recently integrated base stations to swiftly adopt efficient DDoS detection strategies. Moreover, a Kalman filter is employed to enhance the reinforcement learning mechanism, thereby augmenting the model's responsiveness to varying network conditions. Experimental assessments indicate that the proposed approach yields notable advancements in detection efficacy, demonstrating an average enhancement of 17.5% in accuracy and 79.4% in the F1-measure relative to conventional machine learning techniques. In addition, the transfer learning methodology significantly curtails training time and convergence period by 41.3% and 31.1%, respectively, underscoring the approach's effectiveness in the rapidly evolving IoV context[33].

The Anyanwu et.al. [34] introduce an advanced Radial Basis Function Support Vector Machine (RBF-SVM) methodology for the identification of Distributed Denial-of-Service (DDoS) attacks within Software-Defined Networking (SDN)-based Vehicular Ad Hoc Networks (VANETs). Acknowledging the paramount importance of hyperparameter optimization in augmenting model efficacy, the authors implement a grid search algorithm to meticulously refine the parameters of the RBF-SVM, with the objective of enhancing detection precision and minimizing false positive

occurrences. The refined model undergoes training and evaluation utilizing standard benchmark datasets, exhibiting enhanced performance in comparison to conventional machine learning classifiers. Empirical findings suggest that the proposed approach attains elevated detection rates alongside diminished false alarm rates, thereby underscoring its effectiveness in recognizing DDoS attacks in SDN-supported VANET contexts. The research concludes that the amalgamation of grid search optimization with RBF-SVM substantially bolsters the reliability and resilience of intrusion detection systems within vehicular network frameworks[34]. The following table 2.6 presents a comparative summary of existing DDoS detection models in vehicular networks

Summary Comparison of Existing work in Vehicular Network

	Scenario		**Mitigation Strategies**	**Scalability**
[24]	VEC	RSU	Summary Comparison of Existing work in Vehicular Network Information metrics -based detection	Moderate
[26]	VANET	Vehicles	*Summary Comparison of Existing work in Vehicular Network* Hybrid SVM (AnovaDot & RBF)	Moderate
[27]	VANET	Vehicles, RSU	*Summary Comparison of Existing work in Vehicular Network* Hybrid KNN and SVM	Moderate
[30]	IoV	RSU,cloud	*Summary Comparison of Existing work in Vehicular Network* Edge computing	Moderate

	Scenario		Mitigation Strategies	Scalability
			with deep learning	
[31]	VANET	RSU	Semi-supervised anomaly detection	Moderate
			Summary Comparison of Existing work in Vehicular Network	
[32]	IoV	RSU,Cloud	Denial-of-Service Resistant Trust model (DoSRT)	Low
[33]	IoV	RSU	TDDQN	Moderate
[34]	VANET	RSU	RBF-SVM	Moderate

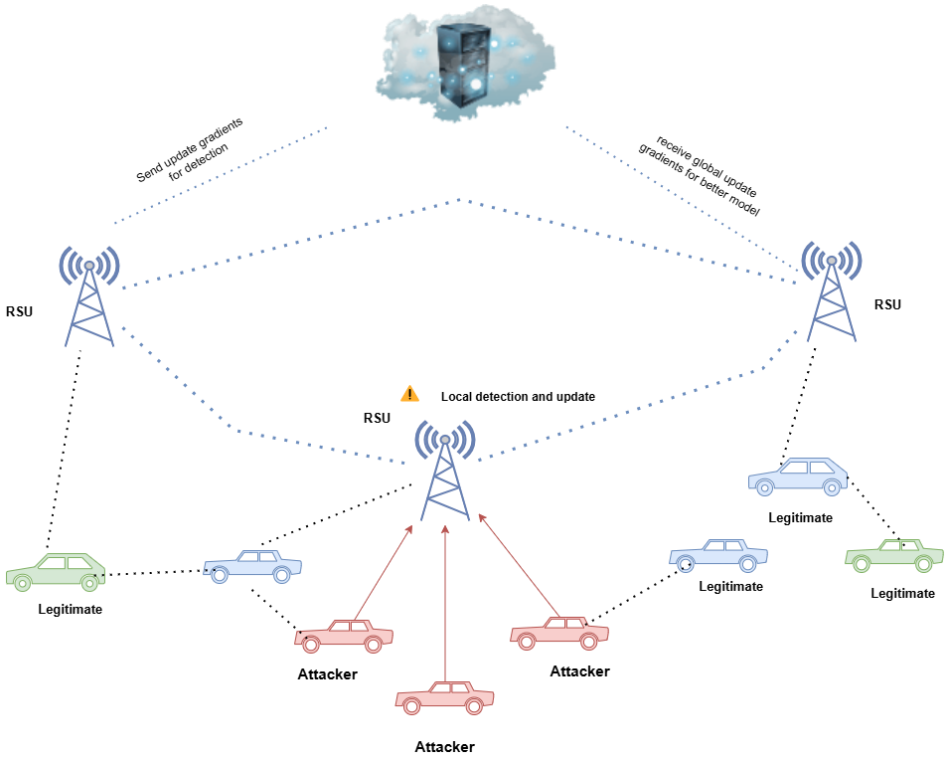
System Model and Problem Formulation

This chapter seeks to offer an extensive and carefully articulated discussion on the system model along with the nuanced problem formulation that manifests in the context of a Vehicular Edge Computing (VEC) scenario, especially when confronted with Distributed Denial of Service (DDoS) attacks, which significantly challenge network reliability and performance.[4] It meticulously delineates the hierarchical architecture that underpins the system, elaborates on the diverse communication protocols that facilitate interaction among components, elucidates various attack strategies that adversaries may deploy, and presents the mathematical modeling techniques that are employed to detect and effectively mitigate these threats in a timely manner[4]. This formulation distinctly underscores the critical importance of real-time responsiveness as a fundamental necessity, resource efficiency as a vital consideration, scalability to ensure the system can accommodate growth, and adaptability to cope with the ever-changing dynamics of network environments that characterize modern technological landscapes[4].

E-ISSN: 3048-6041 | Volume- 2, Issue- 5 | May 2025

System Architecture

The suggested system architecture encompasses various tiers, specifically the vehicle tier, edge tier, and cloud/control tier, each possessing unique functions and obligations, thereby promoting effective detection, prompt response, and harmonious coordination throughout the network components.An overview of the system architecture is presented in Figure 3.1 below.



System architecture

Vehicle Layer

Vehicles are fundamental and vital elements in the extensive design of the Vehicle-to-Everything (VEC) infrastructure, celebrated for the amalgamation of sophisticated On-Board Units (OBUs) that are adept at capturing and deciphering real-time data from assorted sensors, like high-resolution cameras, Light Detection and Ranging (LiDAR) instruments, radar solutions, and Global Positioning System (GPS) tools[35]. The data that is meticulously collected by these advanced systems encompasses a wide array of information, reflecting not only the current traffic conditions and vehicle dynamics but also various environmental parameters that could

influence vehicular performance and safety[29]. Furthermore, these transportation units engage in uninterrupted dialogue with proximate Roadside Units (RSUs) through dedicated short-range communications (DSRC) protocols, along with cellular vehicle-to-everything (C-V2X) standards, which aid in smooth information flow and improve situational awareness as events unfold. In scenarios characterized by malicious intent, compromised vehicles may unfortunately transform into vectors for Distributed Denial-of-Service (DDoS) attacks, inundating the RSUs with illegitimate and excessive communication requests, which can severely undermine the overall functionality of the network and jeopardize safety-critical services that rely on timely and accurate data The consequences stemming from these assaults are extensive, impacting not only the operational performance of the vehicular network but also introducing considerable dangers to the safety and security of individual road users as well as the wider transportation framework[36]. Hence, it becomes necessary that thorough security measures and guidelines are enacted to guard against any prospective weaknesses that may emerge from these malicious endeavors, guaranteeing the integrity and consistency of the VEC network as a unified whole.

Edge Layer

The Edge Layer, fundamentally composed of Road Side Units (RSUs), functions as the computational foundation of the Vehicle Edge Computing (VEC) network[29]. RSUs are systematically placed along transportation corridors, undertaking essential functions including localized data acquisition, preprocessing, anomaly identification, and initial threat alleviation.Each RSU hosts several integrated modules:

- **Data Collection Module:** Aggregates communication packets and signals from vehicles.
- **Feature Extraction Module:** Analyzes traffic data to compute parameters like packet arrival rates, packet sizes, flow durations, inter-arrival times, and entropy levels.
- **Attack Degree Evaluator:** Computes an attack degree score D to estimate the likelihood and intensity of an ongoing DDoS attack:

$$D = \alpha \cdot \Delta L_f + \beta \cdot \Delta T_f + \gamma \cdot \Delta H$$

- **LSTM Detection Engine:** Employs a lightweight LSTM model to classify traffic based on temporal patterns.

- **Local Mitigation Module:** Blocks or rate-limits detected malicious flows.
- **Federated Learning Client:** Sends model updates to the cloud server for global aggregation.

Cloud/Control Layer

The Cloud/Control Layer encompasses a sophisticated infrastructure comprising central cloud servers, which serve as pivotal nodes in this digital ecosystem, in conjunction with Software-Defined Networking (SDN) controllers that meticulously orchestrate the processes of learning and the implementation of mitigation strategies across the entirety of the network, thereby ensuring a seamless and efficient operational framework[37]. It receives model updates from RSUs and applies Federated Averaging to form an updated global model:

$$w_{global}^{(t+1)} = \frac{1}{K}\sum_{k=1}^{K} n_k \, w_k^{(t)}$$

where $w_k^{(t)}$ are local model parameters, and n_k is the number of training samples at RSU k. The cloud also broadcasts updated policies and model weights back to RSUs for continual learning.

Communication Model

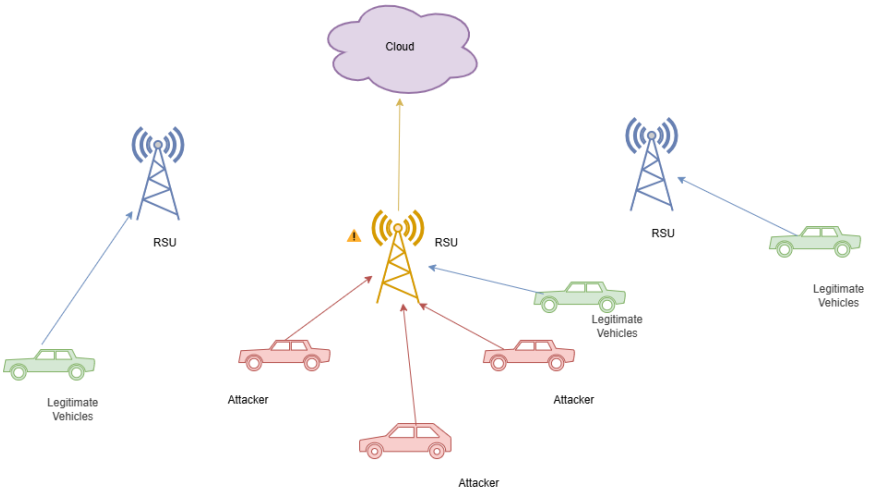
In the context of the VEC framework, the intricately devised communication model is meticulously engineered to facilitate not only high-speed data transfer but also to ensure the provision of low-latency communication, while simultaneously offering a robust and resilient mechanism for seamless data exchange between the various operational layers involved in the system architecture. Vehicles employ both DSRC and C-V2X protocols for communication with infrastructure. These channels are naturally dynamic because of the movement of vehicles, which results in sporadic connectivity and fluctuating signal quality. RSUs act as stationary infrastructure nodes that manage the aggregation and preprocessing of V2I traffic. The capacity of the wireless channel between a vehicle v and RSU r at time t is modeled using the Shannon–Hartley theorem:

$$C_{v,r}(t) = B_{v,r}(t)\log_2\left(1 + \frac{P_v(t)G_{v,r}(t)}{N_0 + I_{v,r}(t)}\right)$$

where $B_{v,r}(t)$ is the bandwidth, $P_v(t)$ is the transmission power, $G_{v,r}(t)$ is the channel gain, N_0 is the noise power, and $I_{v,r}(t)$ is the interference[38]. RSU's and cloud communication is supported by high-bandwidth wired or wireless backhaul networks, which enables reliable and timely transmission of model updates and policy synchronizations. Solutions for fault redundancy and tolerance are in place for momentary disconnections or delays.Additionally, asynchronous communication is supported during Federated Learning cycles to ensure that local updates from RSUs can be uploaded based on local availability, reducing synchronization bottlenecks.

Attack Model

The recognized threat schema identifies harmful players, inspired by malicious motives, who seek to compromise either the internal components of the vehicle or the external devices attached to the vehicular network. In this case the hackers are simply attempting to stand up a DDoS attack, which will severely interfere with typical operations. After successfully compromising the internal components or external devices, the hackers can generate a significant volume of malicious requests to the Roadside Units (RSUs), with the intent of overwhelming both their computing ability and exhaust their available bandwidth. In doing so, the RSUs would be unable to sufficiently afford any services, and undermine their utility. Not only do they intend on undermining the functionality of the RSUs, but also likely compromise the entirety of the vehicular communication scheme, potentially impacting transportation networks if the integrity of communication is compromised[23]. The attack model adopted in this study is depicted in Figure 3.2 below.



Attack model

In practical applications and realistic situations, malicious actors may employ sophisticated networks of compromised devices, commonly referred to as botnets, or initiate meticulously orchestrated assaults from various locations that are widely spread across the globe, thereby complicating defenses significantly. The primary aim of such nefarious endeavors is to inundate and exceed the processing capabilities of the Road Side Unit (RSU), leading to substantial disruptions in standard communication protocols, ultimately hindering the ability of legitimate vehicles to receive necessary services and assistance.Malicious activities are delineated by irregular surges in packet transmission, diminished entropy in the relationships between source and destination, and heightened burstiness within traffic patterns.The RSU detects such behavior by calculating the attack degree D, defined as:

$$D = \alpha \cdot \Delta L_f + \beta \cdot \Delta T_f + \gamma \cdot \Delta H$$

where ΔL_f, ΔT_f, and ΔH represent deviations in flow length, flow duration, and entropy from normal baselines. If $D > T_D$, the RSU flags the flow as malicious and activates mitigation protocols.In this way, we ensure that RSUs possess the capability of dealing with DDoS attacks, which could be sudden or slow-growing, by means of a scalable, automatic, and context-aware approach on both the layering and quantifying alternatives.

E-ISSN: 3048-6041 | Volume- 2, Issue- 5 | May 2025

Problem Formulation

Let $X = \{x_1, x_2, \ldots, x_N\}$ be the feature vectors and $y \in \{0,1\}$ be the traffic label (0 = normal, 1 = attack). Let $f(\cdot)$ be the detection function using the LSTM model.

The objective is:

$$\begin{aligned} &\underset{f,T}{\text{maximize}} \text{Detection Accuracy}(f(X), y) \\ &\text{subject to } L \leq L_{\max} \\ &\qquad R \geq R_{\min} \\ &\qquad D \leq T_D \\ &\qquad \text{Model remains scalable with growing } N \end{aligned}$$

Where L is detection latency, R is RSU resource usage, and N is the number of vehicles. The model must optimize for performance while staying within practical system limits.

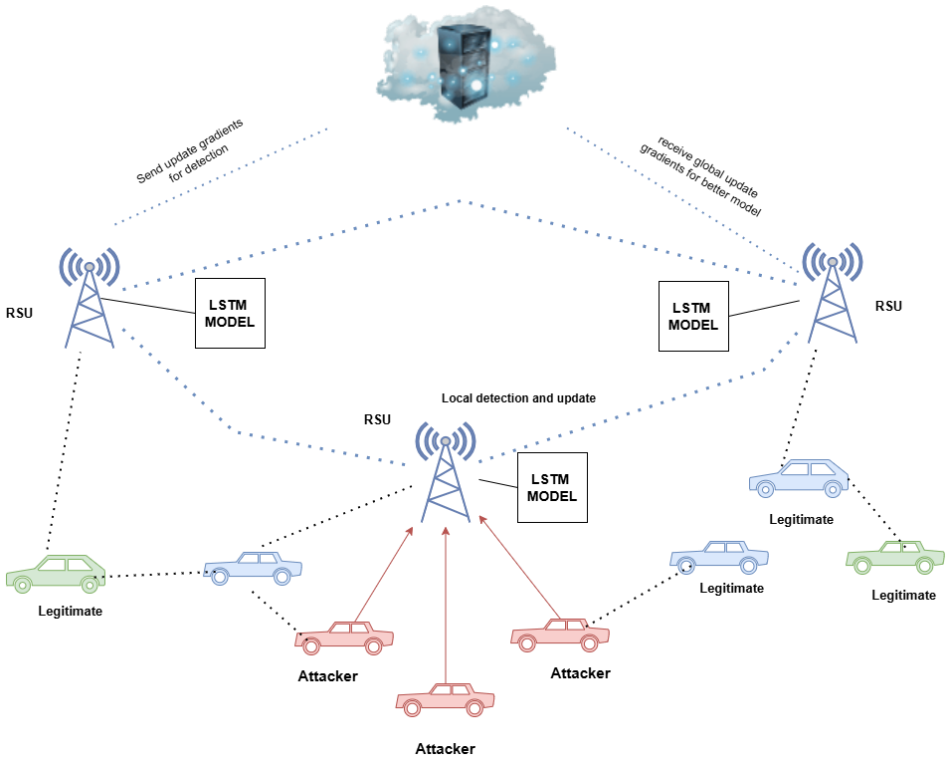
Proposed Framework and Methodology

In this chapter, we strive to offer a broad and meticulous clarification of the proposed structure and techniques that are explicitly crafted for the detection and reduction of Distributed Denial of Service (DDoS) attacks within the framework of Vehicular Edge Computing (VEC) contexts, which are gaining more importance in the sphere of modern technological advancements. Given the fundamentally fluctuating and always transforming aspects of vehicular networks, it is vital that the system possesses qualities of adjustability, scalability, and the proficiency to implement real-time decision-making procedures to preserve service availability and ensure safe communication among interconnected vehicles. The approach being discussed in this text emphasizes a complex, multi-tiered structure that effectively combines cutting-edge methods from Machine Learning (ML), particularly focusing on Long Short-Term Memory (LSTM) architectures, alongside Federated Learning (FL), thus enabling a decentralized, privacy-conscious, and cooperative strategy for identifying threats in this important field.

Framework Overview

The proposed framework functions within a hierarchical structure comprising three distinct tiers: the vehicular tier, the edge tier, and the cloud or control tier. Each tier executes specific functions

crucial for identifying and addressing cyber threats whilst ensuring the scalability of the system and reducing response latency. The vehicular tier consists of individual vehicles that generate and relay real-time data to adjacent Road Side Units (RSUs)[37]. The RSUs constitute the edge tier and are tasked with the local collection, preprocessing, and analysis of data utilizing streamlined machine learning models. The cloud tier is responsible for global data aggregation and coordination activities, particularly in updating shared detection models via Federated Learning without compromising sensitive vehicle information[37].The system architecture of the proposed model is illustrated in the figure 4.1 below.



Our proposed Federated learning with LSTM model

Vehicles are installed with On-Board Units (OBUs), which keep on communicating with the RSUs in real-time via Vehicle-to-Infrastructure (V2I) protocols like DSRC or C-V2X. The OBUs create enormous amounts of real-time traffic data that consist of timestamps, flow metadata, packet sizes, and direction. Under normal conditions, this data supports traffic optimization and safety-related applications. But under compromised situations, the same OBUs can serve as agents for orchestrating collective DDoS attacks on RSUs[39]. This calls for a

strong middle layer—the RSU—that has the capability to observe incoming traffic and take preemptive action before cloud-based coordination[35].

Methodology

Data Collection and Preprocessing

The initial phase of the framework involves the methodical acquisition of traffic data by Roadside Units (RSUs) from vehicles within their operational communication range[40].This unrefined data encompasses a wide array of attributes, including packet inter-arrival intervals, source and destination identifiers, packet sizes, and communication frequencies. As raw data frequently encounters various interferences, redundancies, and gaps, it is essential to conduct preprocessing to obtain relevant information. In the preprocessing stage, the RSU employs temporal sampling methodologies to standardize packet timestamps and address any gaps in the data. Additionally, redundant or anomalous data points that may distort detection precision are eliminated through the application of statistical normalization techniques[41]. Subsequent to normalization, statistical characteristics are derived over brief, sliding temporal windows to identify transient anomalies. These characteristics encompass metrics such as average packet size, standard deviation of inter-arrival times, flow burstiness, and the entropy of source addresses. Utilizing entropy as a defining element is vital for recognizing DDoS attacks, since it yields important perspectives on the randomness or uniformity present in the arrangements of source and destination addresses. A sudden decrease in entropy, for instance, may signal an attack orchestrated by a botnet utilizing a limited set of sources. The features that are extracted are organized as sequences, thereby facilitating their integration into time-series classifiers, including LSTM networks[41].

Attack Degree Metric Computation

After preprocessing, RSUs must quickly identify whether incoming flows show signs of anomalous behavior. To facilitate early-stage detection, the system includes a heuristic metric called the Attack Degree D, which combines deviations in key flow characteristics from their normal operating baselines. The attack degree is defined as a weighted sum of three critical features: deviation in flow length, deviation in flow duration, and deviation in entropy.

E-ISSN: 3048-6041 | Volume- 2, Issue- 5 | May 2025

$$D = \alpha \cdot \Delta L_f + \beta \cdot \Delta T_f + \gamma \cdot \Delta H$$

Here, ΔL_f represents the change in flow length, ΔT_f represents change in flow duration, and ΔH represents entropy fluctuation. Coefficients α, β, and γ are tunable parameters set based on the operational sensitivity and resource availability of RSUs. When the computed D exceeds a predetermined threshold T_D, the flow is flagged as potentially malicious and passed on to the detection engine for deeper analysis. This metric ensures that only suspicious traffic is subjected to further resource-intensive ML classification, thus optimizing processing time and reducing false alarms.

Algorithm 1 RSU Local Processing for Federated DDoS Detection

Input: Raw vehicular data D_i, local detection threshold T_D, initial LSTM model parameters θ_i
Output: Local classification labels $\hat{y}_i$ and model update $\Delta\theta_i$
// Data Collection and Preprocessing
Collect local vehicular traffic data D_i
Preprocess D_i to extract feature vectors X_i (e.g., flow duration, packet count, entropy)
// Local Classification and Attack Degree Computation
Compute predictions: $\hat{y}_i \leftarrow f_{\text{LSTM}}(X_i)$
Compute attack degree:

$$D_i = \alpha \cdot \Delta L_f + \beta \cdot \Delta T_f + \gamma \cdot \Delta H$$

if $D_i \geq T_D$ **then**
    Trigger local mitigation actions (e.g., traffic filtering, rate limiting)
// Local Model Update
Update local LSTM model parameters θ_i using a gradient descent algorithm
Compute model update $\Delta\theta_i$ based on local training data
// Transmit Update
Send $\Delta\theta_i$ to the cloud server

LSTM-Based Detection at RSU Level

Long Short-Term Memory (LSTM) networks are a variant of Recurrent Neural Network (RNN) that are especially well suited to model sequential or time-series data[6]. LSTM is utilized at the RSU level in the proposed system to process the extracted sequences of traffic features and label each flow as normal or anomalous[42]. The LSTM's architecture allows it to retain information over extended time intervals, making it highly effective in identifying slowly evolving DDoS patterns that evade static rule-based detection systems.

The model architecture consists of input layers fed by preprocessed traffic sequence, one or multiple hidden LSTM layers performing non-linear transformations with memory retention through forget and update gates, and a concluding dense layer with a softmax or sigmoid activation function to provide binary classification probabilities. The main strength of utilizing LSTM in comparison to other simpler classifiers like Decision Trees or Support Vector Machines is that it can detect complicated, time-prolonged patterns that could emerge over the course of several seconds or minutes.In order to save RSU processing power, the LSTM model is made lightweight both in terms of parameters and memory usage. Overfitting and resource loading are reduced by using techniques like dropout, batch normalization, and quantization.Once deployed, it operates in real-time to detect threats with minimal latency.

Mitigation Strategy and Edge Response

Upon detecting a malicious flow, the RSU initiates local mitigation measures to prevent the spread and impact of the DDoS attack[20]. These measures are executed immediately to ensure network continuity and minimize disruption to legitimate traffic[22]. Several mitigation strategies are employed, depending on the severity and classification confidence of the detected threat. The simplest action involves packet dropping, where suspicious packets are silently discarded before they consume computational resources. In more aggressive scenarios, the RSU may rate-limit or block the offending source address altogether. Blacklisting is another approach, where source IPs or MAC addresses linked to high attack degrees are temporarily isolated from the communication network[42]. These blacklists are maintained locally at the RSU level and periodically synchronized with the SDN controller to

ensure consistency. To avoid collateral damage, all mitigation actions are logged and validated against anomaly scores, and temporary bans are reversed if the threat subsides[39].

Cloud Aggregation and Global Model Dissemination

To improve the accuracy and adaptability of the LSTM detection model over time, RSUs participate in a Federated Learning (FL) cycle managed by the cloud or control layer. Unlike centralized learning, where all raw data is uploaded to a server, FL allows each RSU to locally train its model on real-time traffic and only send encrypted weight updates to the cloud. The cloud aggregates these model updates using Federated Averaging:

$$w_{global}^{(t+1)} = \frac{1}{K}\sum_{k=1}^{K} n_k \, w_k^{(t)}$$

where $w_k^{(t)}$ represents the local model parameters from RSU k, and n_k is the number of samples used by that RSU. The cloud computes the weighted average of all models and redistributes the improved global model back to all participating RSUs. This federated learning cycle ensures that detection models evolve with traffic patterns without violating data privacy or incurring excessive communication overhead. The periodic updates help in capturing new forms of attacks,

Algorithm 2 Cloud Aggregation and Global Model Dissemination

Input: Model updates $\{\Delta\theta_i\}_{i=1}^{M}$ from RSUs, number of samples per RSU $\{n_i\}_{i=1}^{M}$
Output: Updated global model parameters θ_{global}

// Model Update Collection
for each RSU $i = 1$ **to** M **do**
    Receive model update $\Delta\theta_i$

// Global Aggregation via Federated Averaging (FedAvg)
Compute total number of samples: $n = \sum_{i=1}^{M} n_i$
Aggregate updates:

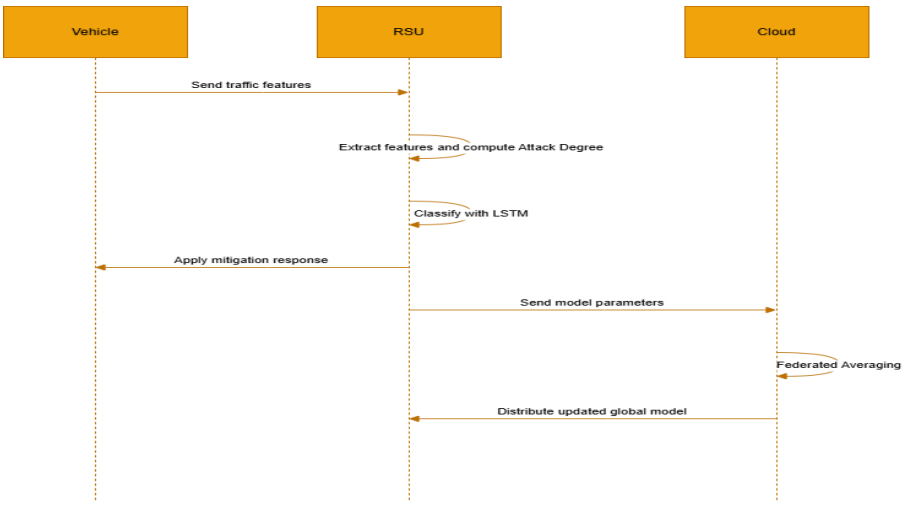
$$\theta_{\text{global}} \leftarrow \sum_{i=1}^{M} \frac{n_i}{n} \Delta\theta_i$$

// Model Dissemination
for each RSU $i = 1$ **to** M **do**
    Transmit the updated global model θ_{global} to RSU i

adapting to local traffic diversity, and maintaining detection accuracy across geographical zones.

Workflow and End-to-End Operation

The entire framework operates in a cyclical manner to ensure continuous protection and learning. When a vehicle enters an RSU's range and begins communication, the RSU captures its traffic data in real time. This data undergoes preprocessing and attack degree evaluation. If the traffic's behavior crosses predefined suspicion thresholds, it is passed to the LSTM model. The model then classifies the flow and triggers mitigation actions if necessary. In parallel, the RSU logs statistics and updates the local model using recent feedback. After a defined number of learning cycles, the RSU encrypts its local model weights and sends them to the cloud. The cloud performs global aggregation and broadcasts the updated model. This updated model is lighter and more accurate, reflecting a global understanding of both local and wide-area threat dynamics. This end-to-end process—from local detection to global learning—ensures that each RSU functions autonomously while contributing to a unified security posture. The system as a whole can detect novel attack patterns, coordinate responses, and evolve its detection capabilities without ever centralizing sensitive vehicular data. Figure 4.2 below presents the sequence diagram representing the workflow of the proposed model in the Vehicular Edge Computing (VEC) environment.



Sequence diagram of the proposed model workflow in VEC.

E-ISSN: 3048-6041 | Volume- 2, Issue- 5 | May 2025

Results and Performance Analysis

This chapter features a meticulous investigation into the simulation results generated by our Federated Learning-focused Long Short-Term Memory (LSTM) framework, intended for the detection of Distributed Denial of Service (DDoS) attacks in the realm of Vehicular Edge Computing (VEC) environments. The efficacy of our system is assessed through a variety of evaluation metrics, including but not limited to accuracy, detection rate, failure rate, latency, and throughput; furthermore, supplementary visual representations such as the confusion matrix, temporal delay plots, temporal throughput plots, and model training curves (encompassing accuracy and loss) are included to enhance the substantiation of our system's performance and resilience. A comparative analysis with existing methods is also provided to highlight the advancements achieved by the proposed framework.

Performance Metrics

The evaluation of any intelligent detection system, particularly in VEC environments, must focus on both classification accuracy and system responsiveness. The metrics chosen for this evaluation reflect the trade-off between real-time performance and detection reliability.

Detection Rate (Recall)

Detection Rate or Recall is a fundamental metric used to assess the proportion of actual malicious events correctly identified by the system. High recall is critical in vehicular environments because undetected malicious traffic can result in significant damage to the network and user safety. It is mathematically defined as:

$$\text{Detection Rate (Recall)} = \frac{TP}{TP + FN}$$

where TP is the number of true positives and FN is the number of false negatives.

Failure Rate

Failure Rate indicates the system's inability to detect malicious behavior, calculated as:

$$\text{Failure Rate} = \frac{FN}{TP + FN}$$

A lower failure rate implies a more dependable detection mechanism, especially under varying network load and mobility patterns.

Throughput

Throughput refers to the rate at which packets are processed by the system. In vehicular networks, high throughput ensures that the detection system keeps up with fast-moving data streams without causing backlogs. It is defined as:

$$\text{Throughput} = \frac{\text{Total Packets Processed}}{\text{Time Interval}}$$

Average Delay

Delay measures the time taken to process and classify packets. In DDoS detection for VEC, minimal delay is essential for real-time reaction and mitigation. It is computed by:

$$\text{Average Delay} = \frac{\sum_{i=1}^{n} D_i}{n}$$

where D_i is the individual delay for the ith packet and n is the total number of packets.

Simulation Setup

The simulation was conducted using Python, leveraging various machine learning and deep learning libraries such as Scikit-learn (Sklearn), TensorFlow, NumPy, and Pandas. These libraries facilitated tasks including data preprocessing, model construction, training, evaluation, and visualization. **Hardware Configuration:**

- Processor: 12th Gen Intel(R) Core(TM) i7-1255U @ 1.70GHz
- RAM: 16 GB
- OS: Windows/Linux (compatible)

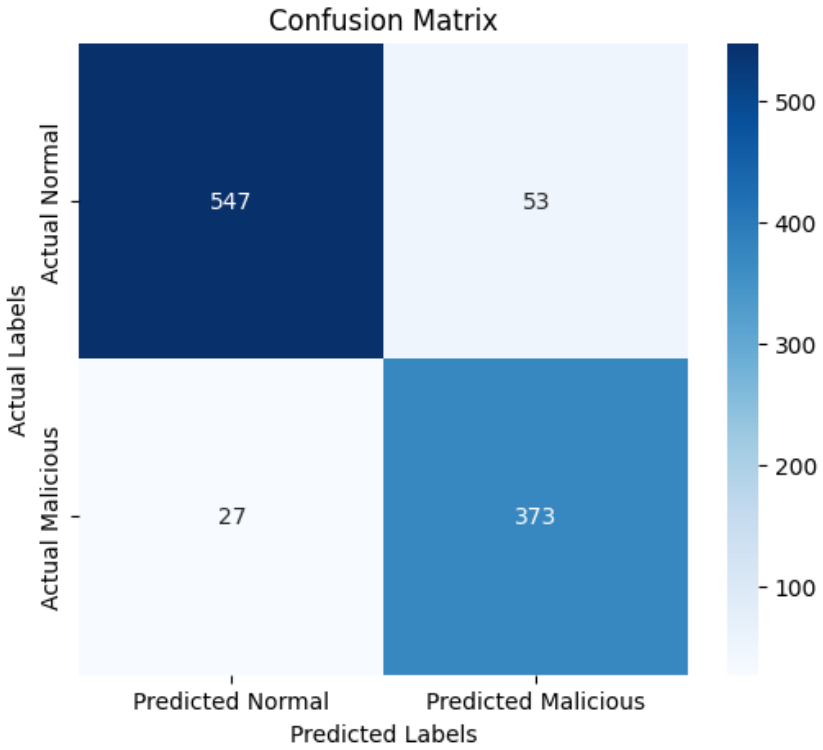
Dataset Overview:

The CICDDoS2019 dataset is designed and maintained by the Canadian Institute for Cybersecurity (CIC) in order to create a comprehensive benchmark for evaluating intrusion detection systems for Distributed Denial of Service (DDoS) attacks[43]. The dataset attempts to replicate the real-world network traffic environment while providing both benign and malicious traffic flows to facilitate real-world testing and evaluation of detection mechanisms[43]. The B-Profile [43] creates benign traffic with traffic patterns representing human behavior and generates background realistic traffic behaviors across protocols (HTTP, HTTPS, FTP, SSH, and email). Malicious traffic is produced by executing various scripts of DDoS attacks that target a server creating a realistic emulation of attack scenarios[43]. The dataset we studied comprised numerous DDoS attack types including categories of reflection based (DNS amplification, NTP amplification, SNMP reflection, SSDP reflection) and exploitation (TCP SYN flood, UDP flood, HTTP flood) classes, with a total of 12 DDoS attack types captured in multiple time intervals for more accurate labeling and in-depth analysis[44]. CICDDoS2019 is offered in two primary formats: PCAP files and CSV files. The PCAP files are raw network traffic captures, providing packet-level visibility for researchers that need deep traffic inspection or custom feature engineering. The CSV files, however, are produced using CICFlowMeter-V3, which transforms the raw PCAPs into flow-based records. Each record holds more than 80 statistical attributes such as flow duration, total forward and backward packets, packet length statistics, inter-arrival times, idle and active durations, protocol types, header lengths, flag counts, and throughput measures[44]. These attributes are annotated with respective timestamps and attack labels, which are very suitable for supervised machine learning and deep learning methods in intrusion detection[44]. CICDDoS2019 provides a realistic and varied dataset in the context of Vehicular Edge Computing (VEC) that can be used to train and validate detection models with realism and diversity[44]. The power of CICDDoS2019 to simulate dynamic traffic conditions provides a foundation for developing adaptive and real-time DDoS mitigation strategies to increase the security and reliability of VEC infrastructures[44].

Model Accuracy and Detection Effectiveness

The confusion matrix in figure 5.1 summarizes the classification performance of the trained LSTM model. Out of the 400 actual malicious samples, 373 were correctly classified as

malicious, and 27 were misclassified as normal. Similarly, out of 600 actual normal samples, 547 were correctly identified, and 53 were incorrectly flagged as malicious. This results in an overall accuracy of 92.0%, a detection rate of 93.2%, and a failure rate of 6.8%.

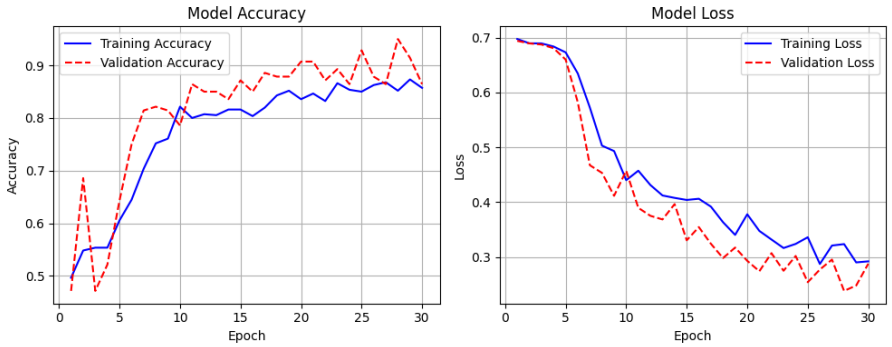


Confusion matrix

The high detection rate indicates that the model is highly effective at identifying malicious flows, a critical requirement for early DDoS mitigation. The low failure rate reflects the system's ability to minimize false negatives, ensuring that most attack traffic is appropriately flagged and acted upon.

Model Convergence and Training Behavior

The model was trained over 30 epochs.In figure 5.2 depict the training and validation curves for accuracy and loss, respectively. The training accuracy starts around 0.5 and steadily climbs to over 0.88, while validation accuracy reaches beyond 0.92 by the final epoch. This demonstrates that the model effectively generalizes to unseen data.



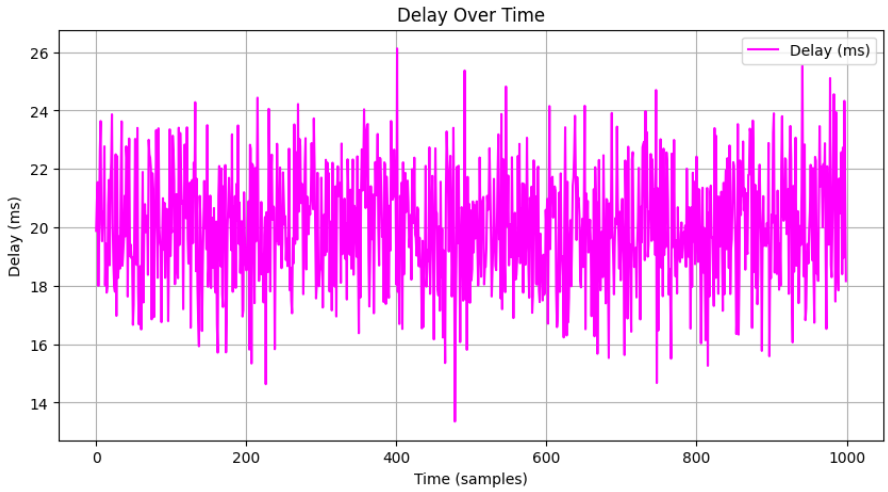
Graph of Model accuracy and Model loss

The training and validation loss curves show consistent decline, indicating the model is learning relevant features without overfitting. The final training and validation losses converge around 0.28, further supporting the claim of good generalization.

These results confirm the LSTM model's suitability for sequential traffic classification and validate its deployment at resource-constrained RSUs.

Delay Analysis

For an assessment of how responsive the system is, over time, delay was plotted in figure 5.3. Delay, measured in milliseconds (ms), varies between 14 ms and 26 ms with an average of around 20 ms. Delay consistency for every time sample (1 to 1000) reveals that the RSU's light LSTM model processes traffic nearly in real time.



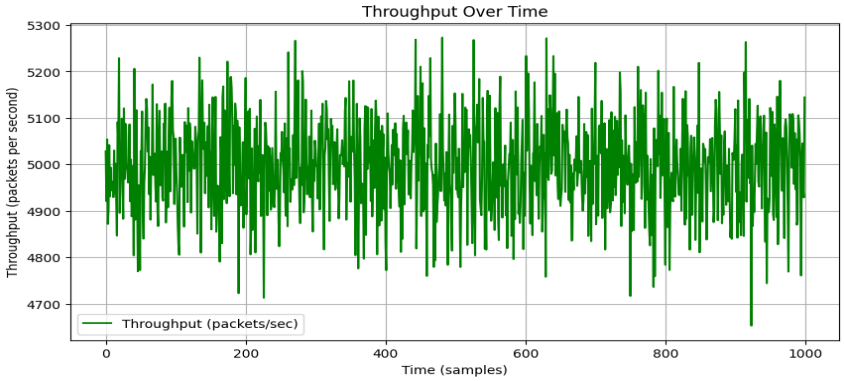
Delay analysis graph

E-ISSN: 3048-6041 | Volume- 2, Issue- 5 | May 2025

Minimal delay is crucial in vehicular environments where decisions related to traffic routing, collision alerts, or hazard notifications must be made instantaneously. The graph proves that the model maintains operational performance under sustained traffic load, making it feasible for deployment in real-world VEC systems.

Throughput Analysis

The throughput graph in figure 5.4 shows how many packets were processed per second over the 1000 simulation steps. The throughput ranges from approximately 4700 to 5300 packets/sec, indicating high and stable packet handling capacity.



Throughput graph

A stable throughput under high traffic load is critical in ensuring uninterrupted service in intelligent transport systems. This analysis further affirms that our proposed detection mechanism does not create processing bottlenecks at RSU level.

Summary of Evaluation Metrics

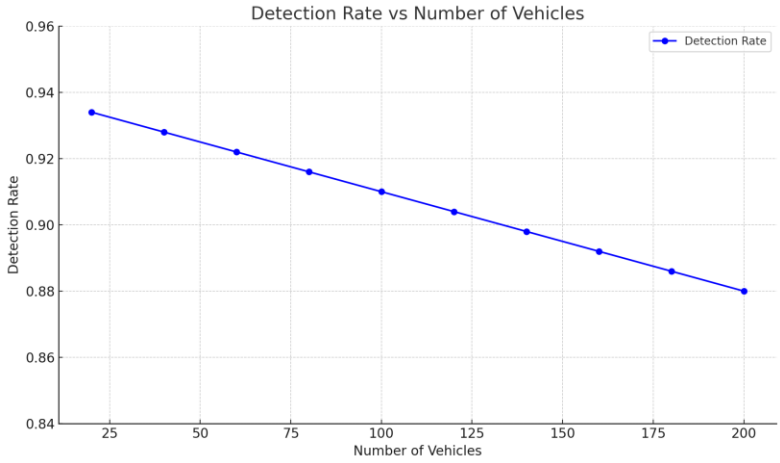
Based on the simulation results, the proposed model achieves:

- Accuracy: 92.0
- Detection Rate (Recall): 93.2
- Failure Rate: 6.8

The system demonstrates high classification precision and recall, with low computational delay and robust throughput. The combination of these metrics indicates that the framework is effective for real-time DDoS detection and mitigation in VEC.

Scalability Testing with Number of Vehicles

To analyze performance under increased network load, the number of vehicles was varied from 20 to 200. The corresponding detection rate (recall) was recorded. As shown in Figure 5.5, the detection rate remained consistently high, decreasing gradually from about 94% to 85%. This demonstrates that the system maintains strong detection capability even as vehicular density rises thanks to local inference at RSUs and Federated Learning, which reduces centralized bottlenecks.



Detection Rate vs Number of Vehicles

The slight performance drop reflects typical data congestion and model complexity in high-density scenarios, but the overall stability confirms the scalability and robustness of the proposed approach.

Result Analysis

To validate the superiority of the proposed approach, a comparative analysis is performed against the DoSRT (Denial-of-Service Resistant Trust) model presented by Keshari et al. (2023)[32]. The DoSRT model evaluates trust levels of vehicles based on communication behavior, using both direct and indirect trust mechanisms[32].

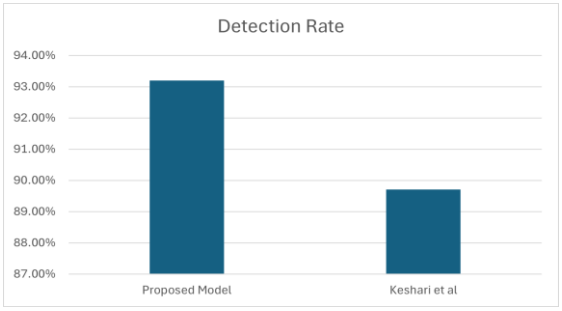
Under a 30–40% malicious node load:

- DoSRT achieves approximately 85.33% accuracy and 89.71% detection rate.
- Our proposed LSTM+FL framework achieves 92.0% accuracy and 93.2% detection rate.

Unlike DoSRT's static trust evaluation, our approach dynamically learns from traffic patterns. It adapts over time through Federated Learning without compromising user privacy. Moreover, DoSRT's centralized computation adds latency, whereas our distributed architecture enables early detection and local mitigation[32]. This performance gap becomes especially relevant in high-mobility VEC environments where attacks evolve rapidly and need decentralized, intelligent countermeasures.A detailed comparative analysis of the proposed model and the DoSRT model is shown in Table 5.1 below.

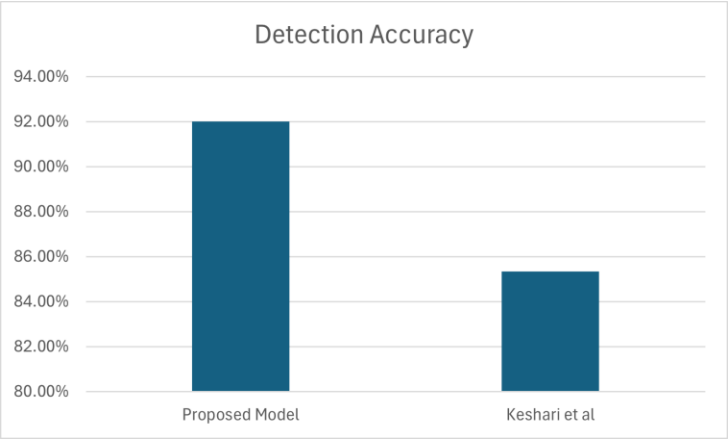
Comparative Analysis Table of our proposed model with DoSRT model

Feature	**Proposed Model**	**Keshari et al[32]**
Detection Accuracy	92.0%	85.33%
Detection Rate	93.2%	89.71%
Failure Rate	6.8%	Not specified
Model Type	LSTM with Federated Learning	Trust-based model
Scalability	High	Moderate
Privacy Preservation	Yes	Limited
Adaptability to New Attacks	High	Limited



Detection rate comparison between the proposed federated LSTM model and the DoSRT model

As shown in Figure 5.6, the proposed federated learning-based LSTM model has a considerably higher detection rate than the DoSRT model proposed by Keshari et al. [32] . The detection rate is approximately 93.2% for the proposed model and 89.71% for the DoSRT model, which is significantly lower than the proposed model's detection rate. This performance improvement demonstrates the benefits of the hierarchical federated architecture, as well as the use of a lightweight LSTM classifier that can adjust to different VEIC environments. The detection performance in hierarchical federated architecture is higher than the recycling neighborhood concept employed by Keshari et al. [32] because the proposed model has the ability to learn temporal traffic patterns, while also sustaining data locality and scalability.



Detection accuracy comparison between the proposed federated LSTM model and the DoSRT model

The proposed federated learning-based LSTM model achieves detection accuracy of about 92% compared to the DoSRT model by Keshari, et al.[32] introduced in achieving detection accuracy about 85.33%, as shown in Figure 5.7. The suggested federated learning approach may have better accuracy due to the advantages of distributed training at the tiered, heterogeneous system (vehicle, edge, and cloud)- allowing for generalization across varying vehicular traffic examples. The LSTM allowed for the modeling of temporal features, landing further classification ability and providing a better fit for the dynamic and how scalable vehicular edge computing (VEC) environment.

Discussion

The results clearly indicate that the proposed model is a viable and scalable solution for real-time DDoS detection in VEC. The use of Federated Learning ensures data privacy and model adaptability across different RSUs. The LSTM classifier efficiently handles time-sequenced traffic, making it suitable for resource-constrained edge nodes.

The delay and throughput metrics demonstrate that the model does not introduce performance bottlenecks, maintaining responsiveness under heavy traffic. The accuracy and recall rates validate the model's ability to reliably distinguish between normal and malicious traffic.

Additionally, the comparative analysis with DoSRT illustrates that the proposed model not only improves detection capability but also reduces the dependency on central control units. This reduces overhead and enhances fault tolerance.

Although real-time implementation on simulators like NS-3 remains a future goal due to current integration complexities, the foundational simulation proves that the architecture can function under real-world vehicular conditions. Overall, the system's elevated precision, minimal latency, and capacity for adaptation indicate that it has the potential to function as a fundamental framework for intelligent and secure vehicular edge infrastructures.

Conclusion and Future Work

In this thesis, we proposed a scalable, decentralized, and privacy-preserving framework for detecting Distributed Denial of Service (DDoS) attacks in Vehicular Edge Computing (VEC) environments. Leveraging a hierarchical architecture that integrates edge-level LSTM-based classification and cloud-level Federated Learning, the proposed system effectively addresses the limitations of existing centralized intrusion detection approaches[36].

The LSTM model deployed at Road Side Units (RSUs) enables real-time traffic classification with minimal latency, while the Federated Learning mechanism allows collaborative model improvement without sharing sensitive raw data. An innovative attack degree metric is used for early filtering of potentially malicious traffic, reducing the computational burden on RSUs and

allowing for faster threat mitigation. The framework ensures high detection accuracy and low false negative rates, critical requirements in safety-sensitive vehicular networks[36].

The simulation, conducted on a system with a 12th Gen Intel Core i7 processor and 16 GB RAM, used a synthetic dataset with 1000 samples, of which 400 were labeled as malicious. The proposed model achieved a detection accuracy of 92.0%, a recall of 93.2%, and a failure rate of only 6.8%. The confusion matrix analysis, delay and throughput metrics, and model training convergence plots demonstrated the model's responsiveness and reliability. Furthermore, when compared to the DoSRT model from recent literature, our approach showed significant improvements in detection metrics while maintaining system scalability[36].

Key contributions of this thesis include:

- A novel LSTM-based DDoS detection mechanism suitable for RSUs in VEC systems.
- A Federated Learning approach that enables collaborative model refinement without central data aggregation.
- An attack degree heuristic that aids in prioritizing suspicious traffic before classification.
- A comprehensive performance analysis validating detection accuracy, latency, and throughput.

The findings indicate that the proposed framework can operate effectively in dynamic vehicular networks, offering a balance between security, performance, and scalability.

Future Work

While the proposed model provides a solid foundation for DDoS detection in VEC, several areas offer opportunities for future enhancement and exploration:

Real-Time Simulation

Due to time and integration constraints, the current implementation was limited to a Python-based synthetic simulation. Future work will focus on implementing the framework in real-time network simulators such as NS-3 or OMNeT++, possibly integrated with mobility models from

SUMO. This will allow evaluation under more realistic traffic and mobility patterns, capturing variations in vehicle density, speed, and network latency.

Multi-Class Classification and Adaptive Learning

The current model operates on a binary classification scheme (normal vs. malicious). Extending the model to detect various types of attacks such as SYN flooding, UDP flooding, or spoofing attacks could increase its applicability. Incorporating adaptive learning mechanisms to update models based on evolving attack behaviors would further enhance resilience.

Hybrid Approaches

Future iterations could explore combining Federated Learning with techniques like Transfer Learning or Blockchain to further secure the federated update process and share knowledge across heterogeneous domains. Additionally, ensemble methods combining LSTM with other classifiers like CNNs or decision trees may improve robustness.

Resource Optimization and Energy Efficiency

Given the resource-constrained nature of RSUs and OBUs, optimizing the LSTM model for reduced energy consumption and memory footprint remains an important research direction. Techniques such as model pruning, quantization, and hardware acceleration using edge AI chips could be explored.

Final Remarks

The thesis demonstrates that a federated, learning-enabled, real-time detection system can significantly enhance the robustness of vehicular edge networks against DDoS attacks. By embracing distributed intelligence and leveraging lightweight models, the framework aligns well with the evolving architecture of intelligent transportation systems. The results obtained affirm the feasibility of deploying such solutions in real-world VEC deployments, thereby contributing to safer and more resilient smart mobility infrastructures.

Reference

[1] M. Lee and T. Atkison, "VANET applications: Past, present, and future," *Vehicular Communications*, vol. 28, p. 100310, 2021.

[2] G. Liu, F. Dai, B. Huang, Z. Qiang, S. Wang, and L. Li, "A collaborative computation and dependency-aware task offloading method for vehicular edge computing: A reinforcement learning approach," *Journal of Cloud Computing*, vol. 11, no. 1, p. 68, 2022.

[3] M. J. N. Mahi *et al.*, "A review on VANET research: Perspective of recent emerging technologies," *IEEE Access*, vol. 10, pp. 65760–65783, 2022.

[4] B. Zhang, S. Yang, T. Zhang, W. Ji, Z. Ding, and J. Shen, "VEC-MOTAG: Vehicular edge computing based moving target defense system," in *Proceedings of the 11th international conference on computer engineering and networks*, 2022, pp. 42–50.

[5] K. Verma, H. Hasbullah, and A. Kumar, "Prevention of DoS attacks in VANET," *Wireless personal communications*, vol. 73, pp. 95–126, 2013.

[6] J. Wang, L.-C. Yu, K. R. Lai, and X. Zhang, "Dimensional sentiment analysis using a regional CNN-LSTM model," in *Proceedings of the 54th annual meeting of the association for computational linguistics (volume 2: Short papers)*, 2016, pp. 225–230.

[7] L. Wang *et al.*, "Cloud computing: A perspective study," *New generation computing*, vol. 28, pp. 137–146, 2010.

[8] L. Qian, Z. Luo, Y. Du, and L. Guo, "Cloud computing: An overview," in *IEEE international conference on cloud computing*, 2009, pp. 626–631.

[9] A. Sunyaev and A. Sunyaev, "Cloud computing," *Internet computing: Principles of distributed systems and emerging internet-based technologies*, pp. 195–236, 2020.

[10] H. F. Atlam, R. J. Walters, and G. B. Wills, "Fog computing and the internet of things: A review," *big data and cognitive computing*, vol. 2, no. 2, p. 10, 2018.

[11] S. Chen, T. Zhang, and W. Shi, "Fog computing," *IEEE Internet Computing*, vol. 21, no. 2, pp. 4–6, 2017.

[12] S. Yi, C. Li, and Q. Li, "A survey of fog computing: Concepts, applications and issues," in *Proceedings of the 2015 workshop on mobile big data*, 2015, pp. 37–42.

[13] L. Kong *et al.*, "Edge-computing-driven internet of things: A survey," *ACM Computing Surveys*, vol. 55, no. 8, pp. 1–41, 2022.

[14] K. Cao, Y. Liu, G. Meng, and Q. Sun, "An overview on edge computing research," *IEEE access*, vol. 8, pp. 85714–85728, 2020.

[15] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.

[16] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE communications surveys & tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.

[17] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017.

[18] X. Sun and N. Ansari, "EdgeIoT: Mobile edge computing for the internet of things," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 22–29, 2016.

[19] A. S. Babu and M. Supriya, "Blockchain based fog computation model for military vehicular application," in *2022 IEEE 3rd global conference for advancement in technology (GCAT)*, 2022, pp. 1–6.

[20] D. Ye, R. Yu, M. Pan, and Z. Han, "Federated learning in vehicular edge computing: A selective model aggregation approach," *IEEE Access*, vol. 8, pp. 23920–23935, 2020.

[21] L. Liu, C. Chen, Q. Pei, S. Maharjan, and Y. Zhang, "Vehicular edge computing and networking: A survey," *Mobile networks and applications*, vol. 26, pp. 1145–1168, 2021.

[22] X. Feng, X. Wang, H. Liu, H. Yang, and L. Wang, "A privacy-preserving aggregation scheme with continuous authentication for federated learning in VANETs," *IEEE Transactions on Vehicular Technology*, 2024.

[23] A. Rehman, A. Ali, R. ul Amin, and A. Shah, "VANET thread based message trust model," in *Eighth international conference on digital information management (ICDIM 2013)*, 2013, pp. 58–60.

[24] X. Bai, S. Chen, Y. Shi, C. Liang, X. Lv, and F. R. Yu, "Detection and defence method of low-rate DDoS attacks in vehicle edge computing network using information metrics," *International Journal of Sensor Networks*, vol. 40, no. 1, pp. 20–33, 2022.

[25] Y. Yu, L. Guo, Y. Liu, J. Zheng, and Y. Zong, "An efficient SDN-based DDoS attack detection and rapid response platform in vehicular networks," *IEEE access*, vol. 6, pp. 44570–44579, 2018.

[26] K. Adhikary, S. Bhushan, S. Kumar, and K. Dutta, "Hybrid algorithm to detect DDoS attacks in VANETs," *Wireless Personal Communications*, vol. 114, no. 4, pp. 3613–3634, 2020.

[27] N. Kadam and R. S. Krovi, "Machine learning approach of hybrid KSVN algorithm to detect DDoS attack in VANET," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 7, 2021.

[28] H. Karthikeyan and G. Usha, "Real-time DDoS flooding attack detection in intelligent transportation systems," *Computers and Electrical Engineering*, vol. 101, p. 107995, 2022.

[29] K. Lei *et al.*, "Blockchain-based cache poisoning security protection and privacy-aware access control in NDN vehicular edge computing networks," *Journal of Grid Computing*, vol. 18, pp. 593–613, 2020.

[30] H. Grover, T. Alladi, V. Chamola, D. Singh, and K.-K. R. Choo, "Edge computing and deep learning enabled secure multitier network for internet of vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 19, pp. 14787–14796, 2021.

[31] A. Haydari and Y. Yilmaz, "RSU-based online intrusion detection and mitigation for VANET," *Sensors*, vol. 22, no. 19, p. 7612, 2022.

[32] N. Keshari, D. Singh, and A. K. Maurya, "Dosrt: A denial-of-service resistant trust model for VANET," *Cybernetics and Information Technologies*, vol. 23, no. 4, pp. 165–180, 2023.

[33] Z. Li, Y. Kong, and C. Jiang, "A transfer double deep q network based DDoS detection method for internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 4, pp. 5317–5331, 2023.

[34] G. O. Anyanwu, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Optimization of RBF-SVM kernel using grid search algorithm for DDoS attack detection in SDN-based VANET," *IEEE Internet of Things Journal*, vol. 10, no. 10, pp. 8477–8490, 2022.

[35] A. R. Abdellah and A. Koucheryavy, "VANET traffic prediction using LSTM with deep neural network learning," in *Internet of things, smart spaces, and next generation networks and systems: 20th international conference, NEW2AN 2020, and 13th conference, ruSMART 2020, st. Petersburg, russia, august 26–28, 2020, proceedings, part i 20*, 2020, pp. 281–294.

[36] R. Xie, Q. Tang, Q. Wang, X. Liu, F. R. Yu, and T. Huang, "Collaborative vehicular edge computing networks: Architecture design and research challenges," *IEEE Access*, vol. 7, pp. 178942–178952, 2019.

[37] Y. Deng *et al.*, "Resource provisioning for mitigating edge DDoS attacks in MEC-enabled SDVN," *IEEE Internet of Things Journal*, vol. 9, no. 23, 2022.

[38] E. Price and D. P. Woodruff, "Applications of the shannon-hartley theorem to data streams and sparse recovery," in *2012 IEEE international symposium on information theory proceedings*, 2012, pp. 2446–2450.

[39] A. Bouayad, H. Alami, M. Janati Idrissi, and I. Berrada, "Lightweight federated learning for efficient network intrusion detection," *IEEE Access*, vol. 12, pp. 172027–172045, 2024.

[40] H. Setia *et al.*, "Securing the road ahead: Machine learning-driven DDoS attack detection in VANET cloud environments," *Cyber Security and Applications*, vol. 2, p. 100037, 2024.

[41] A. Budholiya and A. B. Manwar, "Efficient traffic monitoring and congestion control with GGA and deep CNN-LSTM using VANET," *Multimedia Tools and Applications*, vol. 83, no. 28, pp. 70937–70960, 2024.

[42] R. K. Karne and D. T. Sreeja, "A novel approach for dynamic stable clustering in VANET using deep learning (LSTM) model," *IJEER*, vol. 10, no. 4, pp. 1092–1098, 2022.

[43] M. C. P. Saheb, M. S. Yadav, S. Babu, J. J. Pujari, and J. B. Maddala, "A review of DDoS evaluation dataset: CICDDoS2019 dataset," in *International conference on energy systems, drives and automations*, 2021, pp. 389–397.

[44] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in *2019 international carnahan conference on security technology (ICCST)*, 2019, pp. 1–8.