UNIVERSITY OF TURKU

Deep Learning-Based Intrusion Detection Systems in VANETs: A systematic Literature Review

Cyber Security

Master's Degree Programme in Information and Communication Technology

Department of Computing, Faculty of Technology

Master of Science in Technology Thesis

Author:

Henok Bekele

Supervisors:

Jouni Isoaho

Petri Sainio

July 2025

Master of Science in Technology Thesis
Department of Computing, Faculty of Technology
University of Turku

Subject: Cyber Security
Programme: Master's Degree Programme in Information and Communication Technology
Author: Henok Bekele
Title: Deep Learning-Based Intrusion Detection Systems in VANETs: A systematic Literature Review
Number of pages: 50 pages, 5 appendix pages
Date: July 2025

Abstract

VANETs are key to intelligent transport, offering significant benefits for safety, efficiency, and self-driving cars. However, the wireless nature of VANETs makes them vulnerable to a variety of attacks. A robust security measure is a mandatory requirement. This paper provides a scientific literature review that examines deep learning (DL) methods applied to Intrusion Detection Systems (IDS) within VANETs.

We carefully reviewed recent research, identifying a range of deep learning architectures. Based on our findings, various DL models are implemented to enhance the security of VANETs, including Deep Belief Networks (DBNs), Recurrent Neural Networks (RNNs) like LSTMs and GRUs, and Convolutional Neural Networks (CNNs). The findings consistently show that these DL models achieve higher accuracy in detecting attacks than traditional machine learning models. Their performance is typically evaluated using confusion matrix metrics, accuracy, precision, recall and F1-score.

Regardless of their effective, some key challenges were discovered. DL models face challenges like large computational demands, privacy concerns, and a scarcity of quality training data. Also, we explore developing trends and future routes, for example Federated Learning (FL), Software-Defined Networking (SDN), and blockchain integration, which seem capable of addressing VANETs' challenges. In summary, this review indicates deep learning is crucial to strengthening IDS within VANETs. Implementing these advanced techniques is essential for safe and reliable intelligent transport system

Keywords: VANETs, Deep Learning, Intrusion Detection Systems, Cybersecurity, Road Safety, Systematic Literature Review, Machine Learning

Table of contents

1 Introduction 1

1.1 Related work 3

2 Overview of VANET 5

2.1 Wireless Connection 6

2.2 Routing Protocols 8

2.2.1 Topology-Based Routing Protocols 8

2.2.2 Position-Based Routing Protocols 9

2.2.3 Cluster-Based Routing Protocols 9

2.2.4 Broadcast Routing Protocols 10

2.2.5 Geocast/Multicast Routing Protocols 10

2.3 Positioning Systems 11

2.4 VANETs applications 12

3 Cybersecurity in VANET 15

3.1 Security Threats 15

3.1.1 Security Challenges 15

3.1.2 Security Requirements 16

3.2 Attack Taxonomy 17

3.3 Intrusion Detection Systems (IDS) 20

3.4 Machine Learning Applications in VANET Security 22

4 Research methodology 25

4.1 Literature review process 25

4.1.1 Defining Research Questions 26

4.1.2 Search Strategy 26

4.1.3 Inclusion and Exclusion Criteria 27

4.2 Finding research material and screening process 28

4.2.1 Initial Retrieval 29

4.2.2 Screening Procedure 30

4.3 Data Synthesis 33

4.4 Reporting the Review 33

5 Discussion of Findings 37

5.1 Different Deep Learning Approaches for IDS in VANETs 37
5.2 Challenges in Implementing Deep learning IDS in VANETs 39
5.3 Performance Evaluation Metrics 41
5.4 Emerging Trends and Future Directions 43
6 Discussions/Lessons learned 45
6.1 Challenges and Limitations of IDS in VANETs 45
6.1.1 Challenges 45
6.1.2 Limitation 46
6.2 Future directions 47
6.2.1 Blockchain-Based Security 47
6.2.2 Cloud-Based Architectures 47
6.2.3 Cluster-Based Routing 48
7 Conclusions 49
References 51
Appendices 60
Appendix 1. List of Reviewed Literature 60

1 Introduction

The primary goal of technology ethics is to enhance societal well-being by improving our quality of life. Road safety is a vital area ripe for technological advancements that can save lives and prevent injuries. Statistics Finland's 2024 report shows that 2,776 road accidents in Finland resulted in injuries (*Statistics Finland*, 2025). This results in 171 fatalities and 3,437 injuries from road traffic accidents in December 2024. As noted, these statistics cover only road accidents within Finland, a nation with a remarkably low accident rate. Based on this, a major global road safety problem demands the immediate implementation of smart technologies worldwide. Here, VANETs present a promising approach to enhance traffic safety and transportation efficiency substantially.

The fast development of wireless communication and the need for smart transport are leading to VANETs. VANETs, vehicular ad hoc networks, are a specialized MANETs. These networks allow vehicles and roadside infrastructure to communicate and share information. VANETs have the potential to revolutionize transportation by enabling real-time data sharing about traffic, accidents, and driver behaviour. This offers significant potential for accident prevention and traffic management, as well as various smart mobility and infotainment services (Hartenstein & Laberteaux, 2008). Because of their wireless connections, VANETs are extremely vulnerable. The growing use of VANETs in transport systems increases their emerging target to various cybersecurity threats. The security and reliability of this network are threatened by malicious activities such as data falsification, Sybil attacks, and denial-of-service attacks. Therefore, effective security is more than just useful but a must.

Intelligent intrusion detection systems (IDS) powered by machine learning are gaining traction as a solution to these security challenges. Furthermore, because of its ability to represent and learn from data, deep learning (DL) has had notable success in real-time detection of unknown and known attack patterns within its various subfields.

This thesis applies a systematic literature review (SLR) to study deep learning-based intrusion detection in VANETs. The goal is to understand current technologies and approaches. Additionally, identify their limitations and anticipated future research directions for this domain. For this literature review, we used the SLR methods of (Kitchenham & Charters, 2007) guidelines along with the PRISMA 2020 framework (Page et al., 2021).

This thesis aims to understand the fundamental area of deep learning (DL) applied to intrusion detection systems (IDS) for Vehicular Ad hoc Network (VANET). Four key research questions that define the scope and direction of this study will guide our research.

RQ1: What are the existing deep learning approaches applied in intrusion detection systems for VANETs?

RQ2: What are the current challenges and limitations of applying deep learning in intrusion detection?

RQ3: What is the comparative performance of deep learning models based on accuracy?

RQ4: What are the emerging trends and future directions in deep learning-based intrusion detection systems?

Besides VANET-specific studies, this literature review also includes a selection of works closely associated with VANET, such as literature on the Internet of Vehicles (IoV) and Intelligent Transportation System (ITS). Despite not focusing on VANET, these topics' common security concerns and IDS architectures offer helpful insights. And meaningfully contributing to the main topic.

To improve this thesis's readability and structure, Grammarly, an English writing software, was used to correct language and enhance quality. Editing, spell-checking, and grammar checks were done with its help for a better outcome.

To manage and organize collected literatures, Zotero was utilized as a reference management. Zotero is open source and free, research management tool (digital scholar, n.d.). This software enabled effective collection, annotation, and citation of studies.

The thesis progressively builds the reader's understanding of deep learning applications in VANET security. Besides the introduction, Chapter 1 contains a related work section. Chapter 2 establishes a foundation with a thorough explanation of VANET basics, covering communication, routing, and positioning. We will review the VANET security landscape in Chapter 3, covering major threats, attack categories, and IDS methods, with special attention to machine learning and deep learning, setting the context.

Chapter 4 describes the systematic approach used for the literature review, explaining the search, selection, and data extraction methods. Chapter 5 presents this review's findings,

directly addressing the research questions. This chapter expands on current deep learning methods for VANET intrusion detection, highlighting existing challenges and limitations, and suggesting future research directions.

Chapter 6 concludes by summarizing the key findings, highlighting important insights, and outlining areas for future research. Chapter 7 summarizes the thesis's main contributions and suggests ways to improve VANET security using advanced deep learning. Complete citations and appended supporting materials are included for all sources at the end of this document.

1.1 Related work

Lately, machine learning and deep learning have been increasingly used to improve VANET security, according to research. The growing importance of VANETs in intelligent transport systems requires robust, adaptive intrusion detection.

The evolving use of AI in vehicle networks has been examined in several literature reviews. The scope and depth of these studies are varied. Some reports broadly survey automotive cybersecurity, while others concentrate on specific attack types, protocol layers, or communication areas like V2I or V2V.

The (Christopoulou et al., 2023) survey, for example, generally reviews AI and machine learning applications in diverse V2X contexts. This study examines the use of learning algorithms to improve connectivity, spectrum efficiency, and real-time decision-making within vehicular networks. However, it gives limited attention to security-specific applications such as intrusion detection.

In contrast, (W. Wu et al., 2024) explicitly analyses deep transfer learning techniques in IoV intrusion detection systems. This review successfully emphasizes the rising interest in transfer learning to tackle data scarcity and model generalization within vehicular IDS. It also highlights the need for adaptable, lightweight models suited to VANETs' dynamic settings.

The (Nagarajan et al., 2023) paper offers a comprehensive survey of machine learning-based Intrusion Detection Systems. This litrature is specifilcay focused on on Connected and Autonomous Vehicles. Its primary aim is to review ML-based IDS solutions for both in-vehicle and inter-vehicle networks. In addition, the paper includes discussions on available datasets and testbed configurations. This survey distinguishes itself by its dedicated focus on ML-centric approaches and its holistic coverage of IDS solutions. Unlike similar papers, this

it is not restricted to network topics. It provides a thorough summary of relevant datasets, simulated environments, and various testbed categories. The comprehensive content makes it a valuable resource for researchers in CAV security and intelligent transportation in general.

(Belal et al., 2024) This survey examines Federated Learning (FL) applications in spatial-temporal (ST) mobility. Covering how FL enables private model training on devices for tasks like human mobility and traffic prediction. It addresses challenges such as data heterogeneity, model personalization, and privacy, and reviews existing FL frameworks. The paper concludes by outlining future research directions, including enhancing personalization. Also, it covers mitigating Byzantine attacks. Although the survey's focus is mobility and traffic prediction, it highlights intrusion detection as a crucial future application of federated learning within VANETs.

The existing literature highlights a growing trend in applying machine learning and deep learning to enhance the security of VANETs. This trend is driven by the critical need for effective IDS and VANETs popularity. While various studies have explored the roles of artificial intelligence and ML in vehicle networks, their scope varies. Despite their valuable contributions, we believe there is a gap in the DL application research survey. This paper aims to address that gap by focusing on advancements in deep learning-based intrusion detection systems for VANETs.

2 Overview of VANET

Vehicular Ad-hoc Networks in short VANETs, are a rapidly developing and crucial part of intelligent transport systems. VANETs, stemming from MANETs, adjust networking for the changing conditions of road travel. This section provides a foundational understanding of VANETs, covering their definition, evolution, architecture, key features, and varied purposes in modern transportation.

VANETs are specialized MANETs designed for communication between vehicles and roadside infrastructure(Jantosova et al., 2019). These networks are inherently self-organizing and wireless, with each participating vehicle functioning autonomously as a mobile node or router, transmitting and receiving data (Eze et al., 2014).

Although MANETs are the groundwork of VANETs, VANETs have unique characteristics. The main distinction is in how their nodes move. In comparison to the irregular node movement in MANETs, VANET vehicles usually follow organized paths due to roads, traffic rules, and fixed road networks. Furthermore, vehicle nodes have access to a virtually limitless power supply from the vehicle battery, enabling extensive communication and computation. VANETs are uniquely capable of robust, feature-rich solutions due to vehicles' powerful, self-contained computing and sensing, unlike power-constrained mobile devices (Eze et al., 2014).

VANETs are recognized as an essential and critical component of Intelligent Transportation Systems (Zeadally et al., 2012). They are key to creating "smart cities" by smoothly adding advanced communication technology to roads, vehicles, and people in urban areas. This integration is foundational to achieving the ambitious goals of modern transportation, from enhanced safety to optimized traffic flow.

The architecture of VANETs is carefully designed to support various communication types essential for intelligent transportation. Typically, VANETS network includes three main components, those are Road-Side Units, On-Board Units and the Application Unit (Gammaa et al., 2025).

On-board units (OBUs) vehicle electronic control units, are the key element for V2V, V2I, and other communication(Gammaa et al., 2025). OBUs are equipped with various sensors that continuously collect and process information about the vehicle's performance and its

surrounding environment (Hota et al., 2021). They also delivering different safety and other services to nodes in VANET.

Roadside Units (RSUs) they are fixed infrastructure components strategically deployed along roads. Typically, RSUs are at critical spots such as traffic signals, or intersections. RSUs play a crucial role in facilitating V2I communication. They can also establish direct connections to the Internet, extending network access to vehicles. Commonly, two types of network devices equip RSUs. The first one is dedicated to short-range communication such as DSRC. And another for communication with other infrastructure components such as cellular communication (G. Kumar et al., 2018).

Application Units (AUs) are devices within a vehicle that run VANET applications. They commonly offer services via OBUs to communicate with service providers for communication Field (Gammaa et al., 2025).

This chapter outlines the key elements that make up a VANET. The primary components include wireless technologies that enable communication between vehicles, routing protocols that control the flow of data through the network, and positioning systems that help vehicles identify and share their locations.

2.1 Wireless Connection

Wireless communication is the backbone of VANETs, allowing vehicles and infrastructure to exchange data in real time. This connectivity makes applications such as cooperative driving, collision avoidance, and intelligent traffic management possible. VANETs function in a decentralized, peer-to-peer manner, communicating without a central node, setting them apart from traditional networks.

Wireless Technologies in VANET

Dedicated Short Range Communication (DSRC) / IEEE 802.11p

DSRC uses IEEE 802.11p as a standard. DSRC facilitates V2E connections, both V2V and V2I communication within VANETs. Despite its wide use, DSRC has low reliability and several limitations that restrict its effectiveness for advanced applications. DSRC challenges are:

Frequent Collisions: High vehicle density can cause its contention-based access method to result in frequent data packet collisions.

Poor Non-Line-of-Sight (NLOS) Performance: A lack of a direct line of sight between communicating entities degrades DSRC's signals.

Bandwidth and Range Constraints: In overcrowded traffic scenarios, DSRC's available bandwidth can become insufficient. The limited communication range can impact its ability to exchange data.

These combined limitations present significant challenges to meeting a reliable connectivity demands of future V2X systems. (Stellwagen et al., 2023).

Cellular Vehicle-to-Everything (C-V2X) / LTE-V2X

C-V2X (LTE-V2X), based on 3GPP standards, became a DSRC alternative using 4G LTE and 5G networks. It is frequently in the 5.9 GHz range. It supports both device-to-network and device-to-device communication. C-V2X offers superior performance, extended range, and NLOS capabilities over DSRC. Limitations include privacy concerns due to cellular connectivity and scalability issues in very high traffic. While an improvement, current C-V2X still struggles with the extreme latency and bandwidth demands of highly automated driving (Stellwagen et al., 2023).

5G New Radio (NR)

5G NR, the newest technology for vehicle communication, uses 5G and emphasizes ultra-low latency, high bandwidth, and better reliability. It allows for adaptable NR numerologies, functioning on sub-6 GHz and mmWave bands, greatly improving sidelink communication. 5G NR V2X aims to surpass LTE C-V2X for advanced applications like automated driving. Challenges include its lack of smooth compatibility with C-V2X, possible for interference, and the high cost. Researchers expect 5G NR V2X to coexist with C-V2X, where C-V2X handles basic applications and NR supports high-requirement advanced applications, leading to a heterogeneous VANET ecosystem Field (Nkenyereye et al., 2019).

DSRC/ IEEE 802.11p established VANET communication initially, but their limitations, as stated, are causing exploration of other connection options. Emerging technologies like 5G are being explored to address these issues, offering quality and robust connectivity. The

choice of wireless technology significantly influences the performance and reliability of VANET applications.

V2X Communication Modes

VANETs consists of various communication types, collectively named Vehicle-to-Everything (V2X).

Vehicle-to-Vehicle (V2V): is a communication enables nearby vehicles to exchange real-time data. Included in this data are speed, position, braking status, and hazard alerts. This helps vehicles anticipate and respond to the behaviour of traffic (Dutta et al., 2024).

Vehicle-to-Infrastructure (V2I): a communication connects vehicles with roadside units (RSUs) or traffic systems. It provides drivers with information about traffic, road conditions, roadway efficiency, and similar applications.(Dutta et al., 2024).

Vehicle-to-Pedestrian (V2P): a communication enhances safety by allowing vehicles to connect with pedestrians using smart devices. (Nkenyereye et al., 2019).

Vehicle-to-Network (V2N): a Communication involves interactions between vehicles and application servers, often utilizing cloud services. This communication typically occurs through RSUs or cellular networks (Nkenyereye et al., 2019).

2.2 Routing Protocols

Routing in VANETs is a challenging task because of VANETs' unique characteristics. such characteristics are high node mobility, dynamically changing network topology, and frequent network partitioning (Al Shugran, 2021) . There is no single routing protocol that can be considered the best for all scenarios in VANETs. Therefore, VANETs routing protocols are typically categorized based on their operational mechanisms and the type of information they utilize to make routing decisions.

2.2.1 Topology-Based Routing Protocols

These protocols rely on network topology, how vehicles/nodes are connected. They use node connection topology information to figure out the best path for sending data packets. In this case, every node maintains a routing table, each vehicle keeps a routing table, to identify the

best path to reach other nodes in the network. This protocol uses either proactive / table-driven, reactive / on-demand and hybrid approaches for routing (Al Shugran, 2021).

- **Proactive protocols** continuously collect and maintain up-to-date routing data by periodically distributing routing tables throughout the network.
- **Reactive or On-Demand Protocols** establish routes only when there is a need to transmit data. It generally discovers a path by overloading the network with Route Request packets.
- **Hybrid protocols** integrate reactive and proactive methods, in order to harness the strengths of both to improve efficiency.

2.2.2 Position-Based Routing Protocols

Position-based routing protocols in VANETs rely on nodes knowing their physical location, typically shared through periodic beacons, beacon a short message send by vehcles conatining idetificatio and location information. These protocols use the geographic position of nodes, rather than fixed routes, to make forwarding decisions. This makes them more scalable and adaptable in highly dynamic environments like vehicular networks.

Unlike topology-based routing , position-based routing uses GPS data and does not need route establishment or maintenance. Key components include beaconing, location services, and geographic forwarding. Examples include GPSR, DREAM, and newer approaches like CAR and geographical opportunistic routing. These protocols are particularly suited for VANETs due to their ability to handle frequent topology changes and high mobility (Zeadally et al., 2012).

2.2.3 Cluster-Based Routing Protocols

Cluster-Based Routing in VANETs groups nearby vehicles into clusters, each led by a cluster head. Cluster head is selected based on location, position etc, In recent research, cluster head selection is facilitated by machine learning too. This head manages communication within the cluster and with other clusters. Factors such as vehicle count, location, direction, and speed determine cluster formation. LORA-CBF, for example, employs cluster heads for beacon transmission and location requests in its routing management. It’s a reactive protocol, meaning it finds routes only when needed (Taleb, 2018).

2.2.4 Broadcast Routing Protocols

Considered a traditional, is a protocol floods packets throughout the network. All Node in the network will recive the message regardless of their position, location or any other factor. This protocol is useful for time-sensitive warnings like emergency braking alerts, but can cause network congestion due to redundancy.

2.2.5 Geocast/Multicast Routing Protocols

Multicast/Geocast Protocols facilitate communication among a specific group of vehicles, often within a defined area, which is particularly useful in situations like intersections or roadblocks(Taleb, 2018)

Given various challenges in VANETs, including issues of high mobility, scalability, stringent latency requirements, reliability concerns, and environmental variations, it is clear that there is no single “perfect” routing protocol that remains optimal. As this chapter has reported, each class of VANET routing protocol, whether topology-based, geographical, cluster-based, or broadcast-oriented, offers distinct advantages and disadvantages.

As summarized in Figure [Insert Figure Number Here, e.g., 3.5], the efficacy of a particular routing protocol is highly dependent on the specific scenario and desired outcome. Geographically based routing protocols, unlike others, scale better in dynamic networks by using location data; however, they have problems with service outages in sparsely populated areas. In contrast, topology-based protocols, despite their simplicity, are overwhelmed by the rapid link changes typical of highly mobile vehicular networks.

Protocol Type	**Characteristics**	**Best For**
Topology	Uses routing tables or route discovery	Stable or low-mobility networks
Position	Uses GPS/location info for forwarding	High-mobility, large-scale VANETs
Cluster	Groups vehicles to manage routing more efficiently	Dense or structured networks
Broadcast	Send data to all	Safety and emergency applications

Geocast	Sends data to specific regions or all nodes	Route Application, Accident warning for a affected area

Table 1. Summary of VANET Routing Protocol Types and Uses

2.3 Positioning Systems

Accurate positioning is one of the crucial needs for the effective application of VANETs, particularly for road safety applications and the fast-growing field of autonomous driving. (Chehri et al., 2020) Functionality like collision avoidance system, efficient traffic management, and the smooth integration of connected vehicle technologies are directly dependent on the precise position of vehicles in the VANET.

However, obtaining a high level of position accuracy in VANETs poses significant challenges. The constant movement of vehicles and changing network structures in VANETs make accurate localization challenging. Global Navigation Satellite Systems signals weaken in cities because of reflections from buildings, trees, and tunnels that block signals. More than Vanets, autonomous vehicle functionalities require centimeter-level accuracy, a precision that standard GPS systems (typically accurate to within 10 meters) cannot accurately achieve. These limitations of standalone GPS indicate the urgent need for more accurate and powerful positioning solutions in VANETs.

GPS technology serves as the huge part in the current vanet positioning, an American version of GNSS. Its widespread deployment in VANETs is largely attributable to its great accessibility and low implementation cost. (Günay et al., 2021) Created by the U.S. Department of Defence, GPS system locates an object's position on the Earth's surface by processing longitude, latitude, and altitude from signals. However, a challenge comes up from the relative motion between satellites and vehicles, leading to timing synchronization issues that can weaken accuracy. Differential GPS (DGPS) was developed to address this challenge by an enhanced system that combines ground-based stations to provide essential corrections, thereby minimizing synchronization errors and improving the reliability.

Other core positioning technologies include:

Dead Reckoning (DR): This technique estimates a vehicle's current position by calculating its position based on a known previous position, speed, and direction. The algorithms can

filter out unreasonable GPS positions by referencing travel history records, to improving overall accuracy(Günay et al., 2021) .

Cellular Localization: While less precise than GPS, cellular network signals can also be leveraged for localization, providing a fallback or complementary method, especially in areas where GPS signals are weak or unavailable. Key Positioning Technologies in VANETs (Günay et al., 2021).

Real-Time Kinematic (RTK) Positioning:- RTK offers centimeter level precision by analyzing phase measurements alongside correction data from a fixed base station (Günay et al., 2021). The high level of precision is especially beneficial for autonomous driving and cooperative manoeuvre. However, RTK systems are complicated and pricey, and they require uninterrupted communication with correction data.

Precise vehicle location is crucial for successful VANET applications, especially for application of road safety, self-driving cars, collision prevention and so on. However, achieving high accuracy is challenging due to vehicle mobility and signal obstructions in urban areas. Although standard GPS is widely used because os it's easily accessible and inexpensive. GPS's avarage accuracy of only 10 meters is not precise enough for certain applications.

To overcome these limitations, various technologies are developed. For instant DGPS enhances accuracy by using ground stations for signal corrections. Addionaly DR estimates position based on previous location, speed, and direction, helping to filter out inaccurate GPS readings. Cellular Localization provides a complementary or fallback option in areas with poor GPS. For greater precision, RTK uses phase measurements and correction data from a base station. However, RTK is complex, pricey and require constant communication. These varying technologies improve Vanet's positioning accuracy.

2.4 VANETs applications

In building ITS, VANETs play a vital role, offering numerous applications that improve road safety, traffic flow, and the overall driver and passenger experience. Vanet applications are commonly grouped into two main categories in most literature: safety and non safety services. However, we think a third category, Traffic Management and Efficiency Improvements or road efficency, sits between the two groups.

Safety applications:- This group includes applications mainly employed to eliminate or decrease the probability of road accidents and loss of life. This category is considered the main purpose of Vanet (Karagiannis et al., 2011). A few examples of road safety applications are listed below
Collision avoidance systems provide warnings of potential collisions.

- Head-on accident warning systems
- Emergency vehicle notification systems.
- Traffic signal violation warnings.
- head & rear-end collision warnings and slow vehicle indications.
- Blind spot monitoring and intersection management.

Traffic Management and Efficiency Improvements: leverage VANETs to optimize traffic flow and reduce congestion (Sadiq Alrubaye & Abdkhaleq, 2024). This category includes real-time traffic status updates, smart traffic insights, and adaptive route guidance. Here are a few examples:

- Navigation assistance / Recommending routes.
- Speed management/warning
- Remote diaglos

Infotainment and Comfort Services (often referred to as non-safety applications) help to enhance the driving experience and passenger comfort. Unlike safety applications, these applications typically need less strict latency but more bandwidth (Eze et al., 2014). This service can be sub-grouped into localized and global. Localized services include, for example include weather information, points of interest, or local commercials like restaurants and so on. In the other subgroup, services that are provided on a global or national scale, examples are streaming services or online games (Karagiannis et al., 2011).

To summarize, safety applications always need real-time communication, minimal latency, and maximum reliability. In compari, non-critical applications, despite their importance for user experience and convenience, typically have more flexible latency limits but often need higher bandwidth for content delivery. Optimizing a protocol for the demands of safety

messages (low latency, high reliability) may lead to bandwidth waste for infotainment applications, and vice versa. Because of this, a single communication or routing protocol is unlikely to be optimal across the range of VANET demands. To adapt, VANET systems will likely use flexible or combined strategies to dynamically manage resources based on transmitted data's type and urgency. This highlights the critical role of quality of service mechanisms in VANETs, prioritizing and reliably delivering safety messages despite heavy network loads from non-safety apps.son

3 Cybersecurity in VANET

The first chapter of the thesis that is given a number is the introduction. All text chapters are numbered. References and appendices are not numbered.

Intelligent Transportation Systems depend heavily on VANETs for real-time vehicle-to-everything communication to improve road safety and traffic flow. Nevertheless, the inherent characteristics, high mobility, dynamic topology, and reliance on open wireless communication, weaken the security of VANETs. Because traditional security measures are incompetent in this exceptional environment of Vanets, a robust IDS is crucial. This chapter examines the cybersecurity of VANETs, covering vulnerabilities, common attacks, the importance of IDS, and the growing use of machine learning/deep learning for improved network defense.

Since global VANET deployment is still in its early stages, our research has found no reports of officially documented, widespread, real-world VANET-specific attacks. Despite this, research using simulated and real attacks proves we desperately need proactive security.

3.1 Security Threats

The unique characteristics of VANETs, a subset of MANETs, lead to a complex set of security problems not found in traditional networks.

3.1.1 Security Challenges

High mobility is one of its most notable features. Rapid location changes are common for vehicles in VANETs due to their high speeds. The dynamic movement creates uncertain topology changes, causing challenges for accurate node position prediction and effective privacy protection. The characteristics of VANETs listed below pose a challenge to Security.

High-speed mobility Vanets nodes, which are vehicles that travel at high speed, making a location prediction very challenging (Quyoom et al., 2020).

Rapidly Changing Network Topology. The frequent and spontaneous arrivals and departures of vehicles, coupled with their varying speeds, cause the network's logical structure to change constantly and unpredictably. This unpredictability results in frequent link failures and network breaks. Which leads to message loss and communication overhead as nodes continuously update their positions within the network (Mejri et al., 2014).

Scalability presents another tough challenge. VANETs have the potential to cover large geographical regions, from single cities to whole countries, and can handle thousands or even millions of vehicles at a time (Engoulou et al., 2014). Although vehicle On-Board Units (OBUs) typically have expansive energy and computing power for robust cryptography (e.g., RSA, ECDSA). Some traditional key management methods remain unsuitable for resource-limited VANET security applications.

Time Criticality is perhaps the most defining security characteristic. Safety messages in VANETs need instant delivery for effective responses and accident avoidance. Delayed messages may cause catastrophic events, resulting in accidents.

Wireless communication: VANETs use wireless connectivity as their communication medium. While wireless transmission is a key benefit of Vanets, it introduces security vulnerabilities stemming from wireless transmission's inherent nature. And the use of open networks makes Vanets vulnerable to eavesdropping and jamming, common in open broadcast systems (Mejri et al., 2014).

The decentralized nature of these self-organizing networks makes managing them and enforcing security policies difficult. Intermittent connectivity and sparse vehicle distribution in certain scenarios can also lead to significant packet loss, impacting reliability.

Unique security issues in VANETs stem from high mobility, dynamic network structures, and time-sensitive needs. Rapidly changing environments are not compatible with traditional security tools built for static networks. Highly adaptive, real-time, and lightweight security solutions are necessary. OBUs possessing sufficient energy and computational resources are critically important. The main challenge lies in creating stable security systems that are quick and flexible to handle the rapidly evolving topology and connection periods.

3.1.2 Security Requirements

Human safety makes VANET security fundamentally different from and far more critical than traditional network security. Security is now a critical functional safety requirement, not just a technical issue; failures have severe implications.

To ensure the safety and reliability of VANETs, several fundamental security requirements must be rigorously met. The following are the main requirements of Vanet's security:

Authentication:- is crucial for all connections, particularly wireless. In VANETs, verifying node, sender identities, properties, and locations is critical. Secure vehicle authorization relies on authenticating network nodes and messages to prevent attacks. (Engoulou et al., 2014) suggested the ID and property authentication methods.

Confidentiality: To protect sensitive data such as driver profiles from unauthorized access, communication must be encrypted. Encryption isn't needed for all messages; safety messages, for instance, don't require (Engoulou et al., 2014). For For instance, a warning message about head-on traffic accidents does not need encryption to be available to everyone possible.

Non-repudiation involves preventing legitimate nodes from revoking their involvement. This principle provides clear evidence of sender accountability, essential for dispute resolution and exposing malicious actors unable to disavow their actions.

Availability:- Applications must remain functional despite faults or attacks, which requires robust, fault-tolerant, and volatile designs. Efficient delivery routes and access to resources, like successful key exchange, are included in this. Many VANET applications, especially safety-critical ones, need real-time or near-real-time responses; thus, mechanisms are needed to guarantee information access despite unreliable application layers.

Accessibility: Restrict access to sensitive communications. For example , Police communication should be available to the appropriate receiver or sender.(R. Kaur et al., 2018).

Scalability:- Communication quality should be consistent despite varying node density across locations (cities vs. remote areas). Communication flow in VANETs is expected to remain unaffected by density differences (R. Kaur et al., 2018).

Besides the requirements mentioned above, we consider time constraints to be another security concern. Time, as previously noted, is critically important. Thus, authenticating messages and verifying nodes need to be done in the shortest time possible.

3.2 Attack Taxonomy

The wireless and dynamic nature of VANETs exposes them to a wide range of attacks. Understanding this multi-layered threat model is essential for designing effective Intrusion Detection Systems that can operate across various layers of the VANET architecture. VANET attacks can be systematically categorized into multiple forms. These classification approaches

are crucial for developing targeted defense strategies. Common categorization methods include:

Classification based on target security requirements: Attacks are often grouped by the specific security goals they aim to compromise. Few examples of this classification method are:-

- Authentication and identification: Attacks compromise the verification process used in authentication and identification (Krishna K & Reddy K, 2022). Examples include a Sybil attack, where multiple pseudonymous identities are used to manipulate network perception.
- Confidentiality and non-repudiation: are threatened by attempts to access sensitive data without authorization. Examples include eavesdropping
- Availability attacks:- stop legitimate users from accessing network services or resources (Krishna K & Reddy K, 2022). Common examples include jamming, DoS and DDoS.

Categorization depends on their network position or actions. This includes a discussion of "Inside the Network vs. Outside the Network," where authenticated insiders pose a greater threat due to their intimate knowledge of network configurations.

Classification based on VANET Layers: Or, originally proposed by (Sumra et al., 2011), VANET attacks can also be categorized into five classes based on their characteristics. Those are, Network attacks, Application attacks, Timing Attacks, Social Attacks and Monitoring attacks. Network attacks are classified as the top priority class, with the priority reducing for the remaining classes accordingly.

1. **First Class: Network Attacks:** Network attacks constitute a high-priority class of threats within VANETs, directly impacting the entire communication infrastructure (Sumra et al., 2011). This class of attacks affects all parties in the network vehicles and RSUs by disrupting their normal operations. These attacks disrupt network services, manipulate routing, and severely impact legitimate users.

Examles of network attacks include:

- **Denial of Service and Distributed Denial of Service Attacks:** DoS and DDoS attacks are the most serious and famous network attacks (R. Kaur et al., 2018). They make systems or network services unusable by overwhelming them with traffic.
- **Black Hole Attack:** A malicious node uses routing algorithms to falsely advertise the shortest path to a destination, exploiting the system (Krishna K & Reddy K, 2022). This deceptive tactic causes other nodes to send their data packets to the attacker, who discards them, thus creating a network "black hole".
- **Wormhole attack:** attacks when two hostile vehicles secretly communicate to change routing algorithms. Their connection is prioritized by the network as the best route to any location, similar to a Black Hole attack.
- **A Gray Hole attack**: a more advanced black hole attack, involves nodes initially advertising a valid path before disrupting it**.** (Krishna K & Reddy K, 2022) However, in a later phase, they selectively discard captured packets probabilistically, thus making detection harder than a full black hole attack.

2. **Second Class: Application Attacks :-** Application attacks specifically target the various software applications running within Vanets. These attacks usually manipulate application messages and data to trick, disrupt, or exploit the system logically, not just the network connection.Examples of application attacks include:

   - **Broadcast Tampering Attack:** An attacker changes or inserts improper safety messages into the network. The consequences of this could be severe, potentially causing road accidents by hiding real traffic warnings and disrupting traffic flow.
   - **Greedy Drivers:** These are those who initiate attacks for personal gain, often causing overload problems for RSUs. False traffic congestion data may be generated by them to reroute nearby nodes from their preferred paths. Their actions lead to delays in service for authorized users.

3. **Third Class: Timing Attack:- In** a timing attack, a deliberately delays a message by inserting extra time slots. But the attacker does not alter the original message's content (Sumra et al., 2011). This type of attack is extremely dangerous for safety-critical applications, which rely on timely information.

4. **Forth Class: Social Attack:-** Disrupting networks is done by sending emotionally charged or "immoral" messages in a social attack (R. Kaur et al., 2018). By provoking user anger, attackers indirectly manipulate user behavior and network activity. An insulting message could, for example, cause a driver to speed, thus disturbing other vehicles.

5. **Fifth Class: Monitoring Attack:- This** attack centers on observing and tracking vehicles and their communications (R. Kaur et al., 2018). Attackers listen to network traffic (V2V and V2I) to gather sensitive information, like police operation details, and pass it on. The attacks use unique vehicle IDs for location tracking, which is a major privacy concern. Some advanced forms involve infecting neighboring vehicles to steal data from a target.

Because VANETs are inherently wireless, effective security requires a deep understanding of their varied attack landscape. Classifying attacks according to their target's security requirements, network location, and the affected VANET layers (network, application, timing, social, and monitoring layers) is critical. A structured approach to classification is necessary for building comprehensive intrusion detection and prevention systems ensuring Vanets

3.3 Intrusion Detection Systems (IDS)

Protecting VANETs requires IDS, which offers strong protection from constantly changing threats. VANET security necessitates that IDSs detect both known and unknown attack types (Azad & Jha, 2013). A system like VANETs, which is life-critical, is becoming increasingly vulnerable to sophisticated cyberattacks. This makes it essential to adopt a proactive and comprehensive approach to security stability that starts with thoroughly identifying potential threats.

Real-time threat identification is critical in VANETs due to the time sensitivity and the potentially catastrophic effects of delays. A quick and accurate action is vital for network operational integrity and accident prevention. IDSs are crucial for reducing the vulnerabilities that come from VANETs' unique features. Because VANETs are so dynamic, with vehicles

constantly moving and changing connections, and their wireless communication is open and broadcast-based, they're especially vulnerable to attacks. IDSs help mitigate these risks by actively monitoring for suspicious activity.

Based on detection techniques IDUs fall into two categories (Azad & Jha, 2013):

- Anomaly Detection: This method identifies patterns in data that deviate from established "normal" behavior. These deviations, or anomalies (also called outliers, deviations, intrusions, etc.), signal potential threats.
- Signature Detection/ Misuse Detection : Similar to antivirus software, this technique compares collected network information against a database of known attacks database. It looks for specific, documented attacks.

Also based on architectures, IDUs can be deployed as (V. Kumar et al., 2005):

- Distributed: A distributed IDS analyzes data gathered from various systems. In the Vanets structure, collected data is analyzed and classified for all parties (Vehicle or RSU)
- Centralized: A centralized IDS uses a single system to collect and analyze data. For example, RSUs function as the central system.

Centralized and distributed IDUs may use host-based, network-based, or a combination of data collection approaches.

Regarding responses, (Azad & Jha, 2013) categorizes IDUs into two types.

- Active: They directly respond to intrusions (e.g., by shutting down services, logging users out).
- Passive: Alarms or notifications are generated without their direct intervention.

Vanets require IDSs with low false alarm rates for successful deployment(Althunayyan et al., 2024). Conversely, a high False Negative Rate , where actual attacks are missed, can result in severe, safety-critical incidents(Althunayyan et al., 2024). Developing lightweight IDS solutions, even with complex Deep Learning, remains a significant engineering challenge due to resource constraints in vehicles and time constraints.

3.4 Machine Learning Applications in VANET Security

Vast network traffic data allows ML algorithms to effectively learn complex patterns, leading to the identification of known and unknown malicious activities. IDS leverages ML mainly for feature selection/extraction and classification. Feature extraction involves automatically identifying and isolating the most relevant characteristics from raw network traffic, a process that reduces the complexity of the data. Afterwards, ML models then use these extracted features to classify network traffic or events as either normal or malicious.

A typical ML model operates in three phases (N & Patil, 2023) :

- **Training Phase:** Raw data is preprocessed to extract relevant features. The information is used to train ML models to learn patterns and categories.
- **Test Phase:** The model's categorization abilities are tested on a new dataset to assess its learned knowledge.
- **Forecasting (or Estimation) Phase:** The operational effectiveness of the ML scheme is assessed based on various quality criteria such as false negatives, false positives, and accuracy.

ML approaches are mainly categorized into two groups: supervised learning and unsupervised learning (N & Patil, 2023). Supervised/controlled learning, where models are trained on labeled datasets containing examples of both normal and attack traffic. The training process allows the model to learn the complex relationships between input and output data. However, the effectiveness of ML models is heavily reliant on the availability of high-quality data for training. This requirement presents a notable challenge for VANETs, given the scarcity of realistic and appropriately labelled datasets.

Unsupervised learning, however, is an ML technique that processes input data without predefined labels or tags. Its primary goal is to uncover hidden patterns and structures within unlabeled datasets. This process leads to the grouping of similar data points into categories. Consequently, unsupervised algorithms are generally more efficient and expedient for data processing, as they don't require the time-consuming process of labeling data (N & Patil, 2023).

Common Machine Learning Techniques for VANET IDS:

Support Vector Machine (SVM): is a supervised learning model. it is a powerful algorithm that builds linear classifiers by employing margin maximization. Essentially, SVM works by finding the optimal hyperplane a decision boundary that most effectively separates data into two distinct classes. This approach allows SVM to deliver better performance and handle complex datasets with ease (Chaymae et al., 2022).

Decision Tree (DT): supervised learning method, forms a model by extracting features from data. It then predicts the value of a target variable by using a simple decision rules. This method is effective in both classification and regression problems. (Singh et al., 2023).

Random Forest (RF): a supervised learning method, it combines multiple decision trees. For classification, it employs a majority vote. RF is simple and fast, achieving success in numerous fields. (Singh et al., 2023).

K-Nearest Neighbor (KNN): a simple supervised learning algorithm. It also functions effectively for both classification and regression. KNN calculates the distance between a new data point and existing and selects the ‘k’ closest data points. For classification, it uses a majority vote to determine the label (Singh et al., 2023).

It is essential to acknowledge that achieving high-performance detection in IDS is not entirely dependent on the choice of algorithm. Other critical parameters, such as the computational power and the characteristics of the dataset used for training, play a significant role. As highlighted here, creating reliable intrusion detection systems for VANETs needs an integrated approach.

Deep Learning

Deep learnin in short DL, which is a subset of machine learning, proven to enhance IDS effectiveness and outperforms conventional ML (Liu & Lang, 2019). DL offers a significant advantage by systematically learning high-level features from raw data through hierarchical layers. This capability eliminates the need for manual feature engineering, particularly in environments like VANETs. The nature of DL helps streamline the development of IDS and enhances real-time performance.

Various DL architectures have been implemented for IDS in VANETs, with each algorithm leveraging its unique strengths to tackle different aspects of network security (Singh et al., 2023):-

Convolutional Neural Network (CNN): A versatile and highly efficient deep learning algorithm that excels in image recognition and feature extraction. CNNs use convolutional and pooling layers to better generalize features. These effectively prevent and detect attacks, including Denial of Service, Black Hole, and Gray Hole.

Deep Neural Network (DNN): powerful method for real time analysis of large datasets. DNN is particularly effective at identifying unexpected and unpredictable attacks. These qualities make them ideal for intrusion detection systems in VANETs.

ANN: A neural network that mimics the human brain, featuring multiple fully connected layers. It has an input layer, plus one or more hidden layers, and finally an output layer.

Recurrent Neural Network (RNN): A neural network specialized in handling temporal or sequential data. It includes internal loops that allow data to be stored within the network, making it effective for tasks involving discrete and sequential information.

Long Short-Term Memory (LSTM): A sophisticated RNN architecture incorporates feedback connections. LSTMs differ from standard neural networks by processing both individual data points and entire sequences, thus excelling at retaining information over extended timeframes.

Deep Belief Network (DBN): A deep neural network using multiple layers of Restricted Boltzmann Machines (RBMs). Deep Belief Networks were created to overcome the difficulties in training DNN.

Hybrid Deep Learning Models are currently a noticeable trend. These methods boost performance and create more robust detection by using multiple DL algorithms or combining DL with other ML techniques. Combining different methods enhances the ability to counter complex and zero-day attacks.

4 Research methodology

This chapter explains the method used in the selection and analysing of literatures. A systematic and structured approach was followed to ensure quality and relevant material that directly addresses the research questions. The process involved several key stages searching, selection, analysing and synthesis of research findings.

A systematic literature review in short SLR, and often referred to as a systematic review, is a means of identifying, evaluating and interpreting available materials relevant to a particular research question, proposed topic or aspect of interest (Kitchenham & Charters, 2007). Thus, to address the principal topic detailed, a systematic literature review was adopted as a guideline of research. We think adopting this method diminishes bias, improves repeatability, and provides a summary of the field's current position. The review process was guided by a standards by Kitchenham Guidelines (Kitchenham & Charters, 2007). Additionally, supported by Preferred Reporting Items for Systematic Reviews and Meta-Analyses in short PRISMA framework (Page et al., 2021). These methods ensure the review process is clear, accurate, and academically acceptable.

The SLR conducted in this study was followed the Kitchenham Guidelines, a well-recognized framework designed specifically for conducting evidence-based systematic reviews in software engineering and related disciplines (Kitchenham & Charters, 2007). Developed by Barbara Kitchenham, the guidelines emphasize a structured process that includes clear planning, execution, and reporting phases. Key elements of this approach include designing research questions, creating a review protocol, systematic inclusion and exclusion, assessing study quality, and using standardized data extraction.

In the following sections, the steps of the literature review process, including question formulation, search strategy, study selection, data extraction, and synthesis are described in detail to illustrate how the research methodology was applied.

4.1 Literature review process

The main purpose of this thesis is to gather and critically analyze current research on the main topic. The review used a structured multi phase process to meet the SLR accurate. It started with creating specific research questions. Followed by a search strategy, and strict inclusion and exclusion criteria. Finally, systematic data extraction, and the synthesis of results. To

secure reliable, transparent, and academically acceptable results, all phases were meticulously planned and executed.

4.1.1 Defining Research Questions

The first and foundational step in the SLR is the formulation of clear and focused research questions. These questions were created for the purpose of addressing main research topic. Their explicitness was helpful in establishing the boundaries of the literature search, promoting consistency and focus in the process.

The research questions were crafted to direct the systematic review by emphasizing the study area's critical points. The questions focused on finding out the deep learning models often used in IDS for VANETs. Furthermore, their goals included evaluating the models' effectiveness and applicability in practice, assessing current challenges and limitations in implementation, and highlighting present research gaps. The review's final intention was to investigate rising patterns and potential directions in the evolution of deep learning-based IDS for VANETs, in order to guide scholarly studies and promote hands-on implementations within the domain.

Research Questions:

RQ1: What are the existing deep learning approaches applied in intrusion detection systems for VANETs?

RQ2: What are the current challenges and limitations of applying deep learning in intrusion detection?

RQ3: What is the comparative performance of deep learning models based on accuracy and evaluation metrics?

RQ4: What are the emerging trends and future directions in deep learning-based intrusion detection systems?

4.1.2 Search Strategy

A comprehensive and structured search strategy was developed to ensure the identification of relevant literature. The search was conducted across multiple academic databases, listed below:

- IEEE Xplore
- ACM Digital Library
- SpringerLink
- ScienceDirect

We mainly concentrated on the studies that came out between January 1, 2020, and April 30, 2025. Keywords, along with Boolean operators, used in finding the relevant materials.

Keywords: VANET, deep learning, intrusion detection system, IDS, cybersecurity, anomaly detection, machine learning in VANETs

Generalized search query: `(VANET OR "Vehicular Ad Hoc Network") AND ("Intrusion Detection" OR IDS) AND ("Deep Learning")`

This research was draw upon materials gathered from the databases previously mentioned. It is important to note that access to some content on these databases is restricted. As such, this literature review is limited to materials that are openly accessible or available through the University of Turku's student credentials.

The following steps were taken to filter and refine the results:

1. **Initial Retrieval** :- Articles were gathered using the specified keywords across selected databases. Focusing on publications dated between January 1, 2020, and April 30, 2025.
2. **Duplicate Removal**:- Redundant entries were identified and excluded.
3. **Title Screening**:- Studies were filtered based on relevance reflected in the title.
4. **Abstract Screening**:- Abstracts were reviewed to determine whether each study met the inclusion criteria.
5. **Full-Text Review**:- Selected articles underwent in-depth analysis for final inclusion. And few literatures were removed during this stage.

4.1.3 Inclusion and Exclusion Criteria

To ensure relevance and quality, studies were screened based on the following criteria:

Inclusion Criteria:

- Peer-reviewed journal or conference papers
- Studies directly related to deep learning based IDS in VANETs
- Articles published between 01 January 2020 and 31 April 2025
- English language publications

Exclusion Criteria:

- Non-peer-reviewed articles (e.g., blog posts, newsletters)
- Non-English publications
- Short abstracts, posters, or editorials
- Duplicates publications

By applying these steps and criteria, the search strategy ensured a focused and quality selection of literature relevant to the research questions.

4.2 Finding research material and screening process

Relevant literature was collected from the previously listed databases using a set of predefined keywords. The keywords are built on topics related to VANETs, IDS, and deep learning. The initial search results were compiled into a reference management system, and duplicate entries were removed to ensure the uniqueness of each study. Zotero, open source reference management, makes removing duplicate items simple and fast.

Following duplicated items removal, the titles and abstracts of the remaining studies were reviewed to assess their initial relevance to the research questions. Studies that met the preliminary inclusion criteria were then moved to a full text review. Full text review determine their suitability for final inclusion in the findings of this paper.

These sections elaborate on the screening, its criteria, and the methods used for each stage.

4.2.1 Initial Retrieval

A systematic search was performed across four major academic databases: IEEE Xplore, ACM Digital Library, SpringerLink, and ScienceDirect. The search was limited to specific publications dated between January 1, 2020, and April 30, 2025. The search queries were developed using a combination of Boolean operators and keywords related to the core concepts of VANETs, intrusion detection, and deep learning. The details of the search queries and results are summarized in Table 1.

Downloaded records were converted to a uniform format to ensure the accessibility and consistency of metadata across platforms. While SpringerLink and IEEE Xplore allowed for CSV exports, results from ACM and ScienceDirect were exported in BibTeX format. These were subsequently converted to CSV using JabRef for integration and further processing.

Database	Search Query	Filters Applied	Total Results	Downloaded Format	Converted Format
IEEE Xplore	(VANET OR "Vehicular Ad Hoc Network") AND ("Intrusion Detection" OR IDS) AND ("Deep Learning")	Years: 2020–2025	43	CSV	NA
ACM DL	[[All: vanet] OR [All: "vehicular ad hoc network"]] AND [[All: "intrusion detection"] OR [All: ids]] AND [All: "deep learning"] AND [E-Publication Date: (01/01/2020 TO 03/31/2025)]	Years: 2020–2025	119*	BibTeX	CSV (via JabRef)
SpringerLink	("Vehicular Ad Hoc Network" OR VANET) AND ("Intrusion Detection	Years: 2020–2025,	266*	CSV	NA

	System" OR IDS OR "Intrusion Detection") AND ("Deep Learning")	Language : English			
ScienceDirect	(VANET OR "Vehicular Ad Hoc Network") AND ("Intrusion Detection" OR IDS) AND ("Deep Learning")	Years: 2020–2025, Open Access & Archive	577	BibTeX	CSV (via JabRef)

Table 2. Summary of Literature Collection

*Manually excludes studies published after April 30, 2025.

The combined search result was 1,007. Following the removal of non-research content (e.g., book chapters, editorials, and incomplete metadata), the dataset was refined to 1,006 entries for further screening.

4.2.2 Screening Procedure

Before initiating the screening process, essential information from all collected literature was retrieved to ensure easier access, organization, and evaluation during subsequent review stages. This preparatory step facilitated efficient filtering and analysis by consolidating key details from each source.

From each retrieved article, the following metadata were extracted:

- Title of the Document
- Author(s)
- Year of Publication
- Source/Publisher
- Link to Full Text

This metadata formed the foundation for tracking, sorting, and referencing articles throughout the review process.

4.2.2.1 Duplicate Removal

During the initial retrieval phase, redundant entries were identified and removed, and duplicate materials eliminated. Non-research materials, including editorial board listings, indexing information, and table of contents pages, which were mistakenly included, were also excluded at this stage. As a result, 970 relevant literature items were retained and moved forward to the next screening phase.

4.2.2.2 Title Screening

In this stage, studies were filtered by assessing their titles against the topic. Screening was performed by identifying titles that contained keywords or closely related terms to the main topic. For instance, studies mentioning "machine learning" or "vehicular communication" in their titles were considered potentially relevant and proceeded to the next stage. Out of the 970 items, 110 studies passed this title screening phase and were selected for the next evaluation stage.

4.2.2.3 Abstract screening

The remaining literature from the previous title screening underwent abstract screening. This stage aimed to further refine the selection by focusing on studies that are precisely relevant to the core research topic. In this stage we examine the abstract if it is related to IDS in VANETs. During this stage a great attention was given to ensuring that machine learning literature included was specifically based on deep learning algorithms, rather than traditional machine learning methods. This step was crucial to maintaining alignment with the research scope.

Out of the initial 110 studies, 75 publications met the inclusion criteria and were selected to proceed to the next stage of the review process.

4.2.2.4 Full text review

Following the abstract screening, 75 publications were identified for full-text review. Additional evaluation was done to ensure the remaining literature's were relevance and contribution to the research topic. This phase focused on a detailed examination of the methodologies, models, and findings of each study, with a specific emphasis on the deep

learning techniques employed for IDS in VANETs. A carefully chosen set of literature was picked from this stage.

Upon the conclusion of the abstract review, four articles from by SpringerNature data base were identified as highly related to this study. However, they were excluded from the full review phase. This exclusion was a direct result of access limitations, as these four publications were not available through open access or the University of Turku's student credential. The literatures included in the final findings, are materials only attainable through open access or institutional licenses, as per criteria.

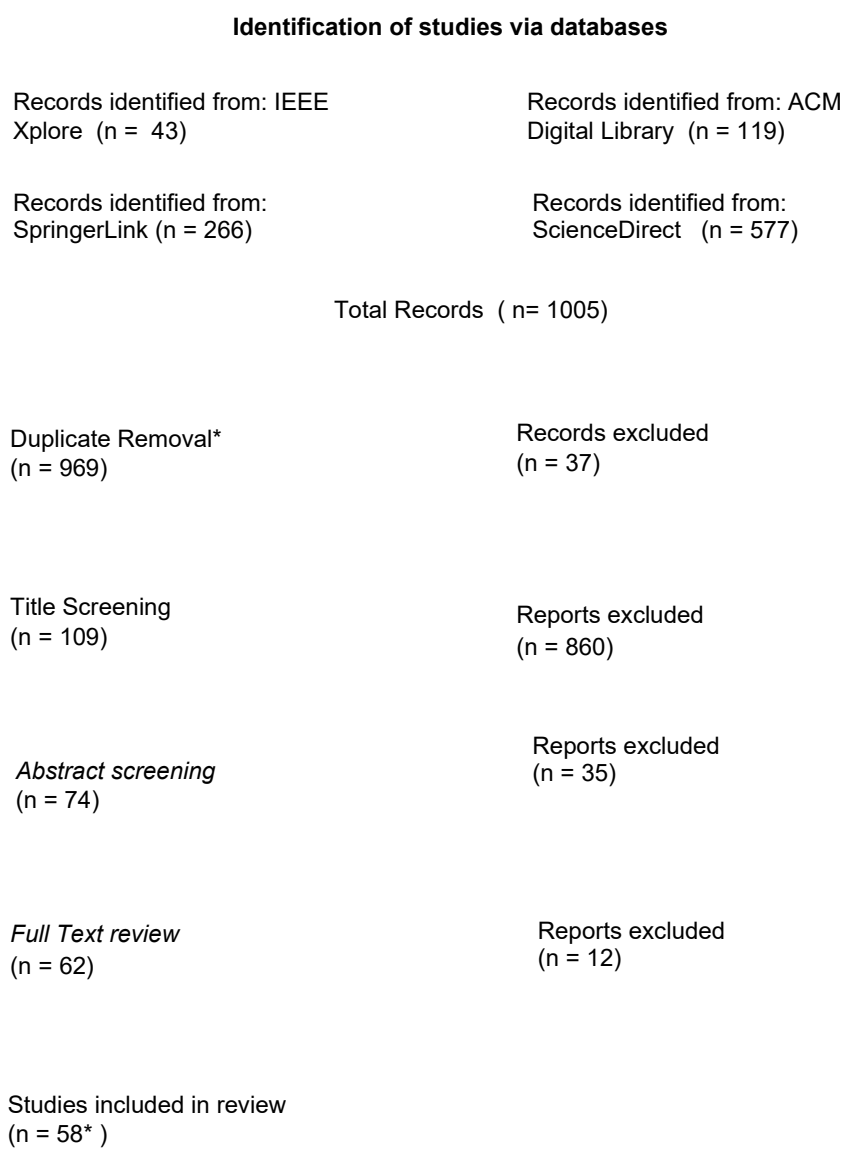

*Figure 1 PRISMA Flow diagram (*PRISMA 2020 Flow Diagram — PRISMA Statement*, n.d.)*

*Four litratures exclusion due to access limitations.

To provide a comprehensive overview of the data collection process and result, Figure 1. illustrates the detailed findings at each stage. Every step added significant value, ensuring the quality, topic focused literature directly relevant to this thesis topic.

4.3 Data Synthesis

The synthesis phase focused on identifying how the included studies addressed the main research topic and questions. This involved analysing patterns related to the algorithms employed, reported limitations, and proposed future research directions.

Data synthesis in this review involved systematically collating and summarizing the findings of the selected primary studies. According to Kitchenham and Charters (2007), synthesis can be descriptive (non-quantitative), though it may be complemented by quantitative summaries when feasible.

For this review, a thematic analysis approach was applied to extract and organize insights related to the core areas of interest, including:

- Deep learning algorithms used in VANET intrusion detection systems
- Key challenges and limitations highlighted by the studies
- Commonly addressed attack types
- Emerging trends and future research directions

Where applicable, quantitative data aggregation was also conducted—particularly in relation to performance metrics (e.g., accuracy, precision, recall) and datasets used. This helped to supplement the descriptive synthesis with measurable insights, enhancing the overall analysis of patterns across the literature.

4.4 Reporting the Review

The literature gathered spans from 2020 to 2025, reflecting a growing interest and evolving research. A total of 58 litratures were review at last, as year distribution shown in the Figure 2 below. A trend shows a steady increase in research activity, peaking in 2024 and 2025. The recent focus on 2024 and 2025 publications indicates a continued push toward real-time,

secure, and scalable IDS in VANETs. Thus VANETs are close to being a standard system used in on the roads.

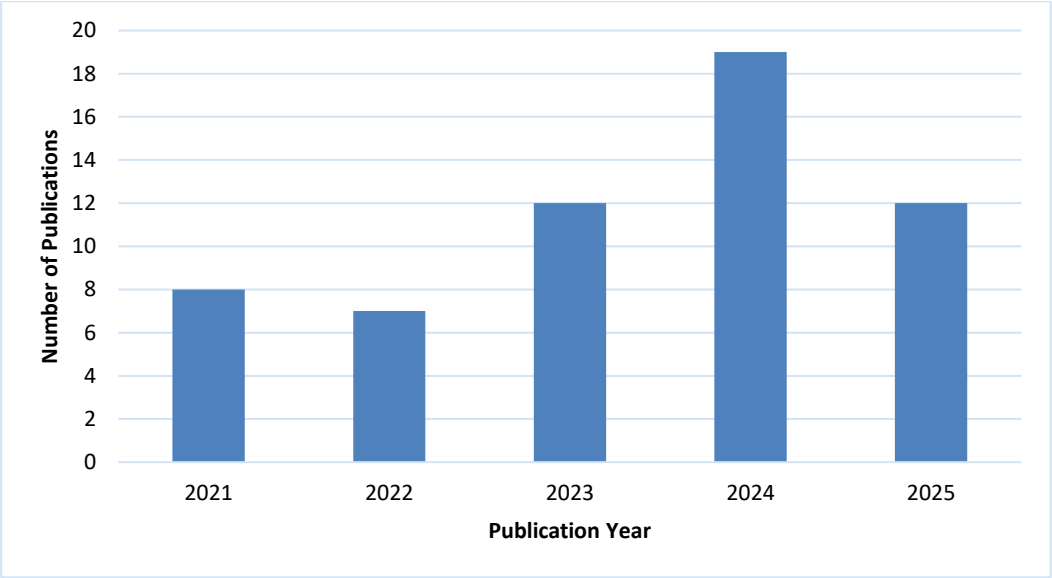

Figure 2. Publication Year Distribution of Reviewed Literature

Furthermore, in this chapter of the literature review focuses on the datasets utilized in the examined studies, deferring detailed discussion of research questions to the next chapter. A variety of datasets were identified, as presented in figure 3. VeReMi and NSL-KDD emerging as the most frequently employed, as illustrated in the accompanying figure 3.

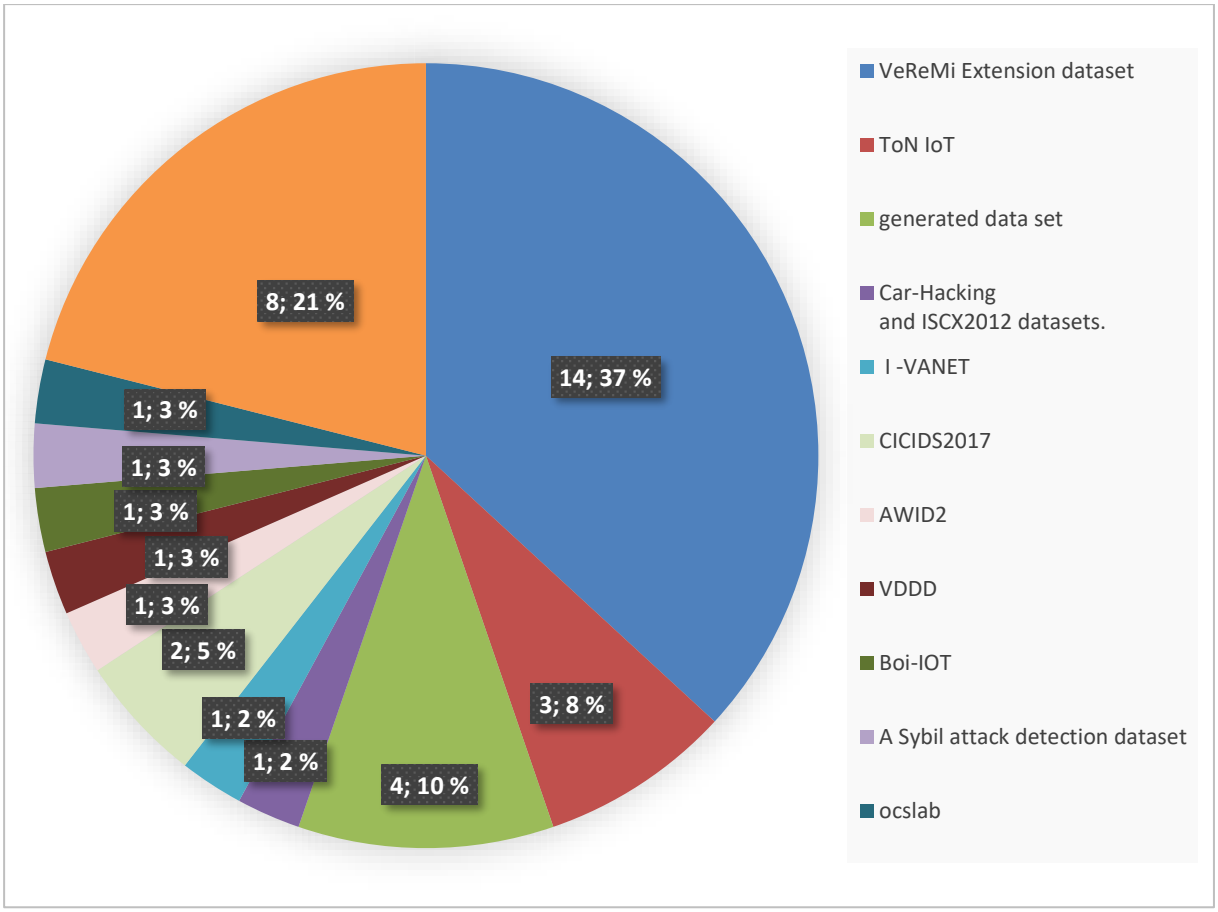

Figure 3. Distribution of datasets used in reviewed studies.

The VeReMi (Vehicular Reference Misbehavior) dataset is a crucial resource specifically designed for evaluating misbehavior detection mechanisms in Vehicular Ad hoc Networks (VANETs). It is a simulation-based dataset, generated using tools like Luxembourg SUMO Traffic (LuST) and VEINS, and provides comprehensive message logs from on-board units, including GPS data and Basic Safety Messages (BSM) (*VeReMi Dataset*, n.d.). This dataset is particularly valuable because it includes malicious messages that simulate various attack types (e.g., position falsification, noise injection) across different traffic and attacker densities, making it suitable for anomaly detection and vehicular security research.

Conversely, the NSL-KDD dataset serves as a benchmark for general network intrusion detection systems, building upon and improving the limitations of its predecessor, the KDD Cup 1999 dataset (*NSL-KDD | Datasets | Research | Canadian Institute for Cybersecurity | UNB*, n.d.). Its enhancements include the removal of redundant training records and duplicate test records, which helps prevent bias and ensures more consistent and comparable evaluation results for machine learning models. NSL-KDD comprises network connection records with numerous features, categorized as either normal traffic or one of four main attack types:

Denial of Service (DoS), Remote to Local (R2L), User to Root (U2R), and Probing. Its design, especially the inclusion of novel attack types in the test set, offers a more realistic scenario for assessing the effectiveness of intrusion detection algorithms.

5 Discussion of Findings

This section covers the key findings from the reviewed literature. We will first explore the deep learning approaches and architectures that have been proposed to enhance detection capabilities. Proceeding, the challenges and limitations encountered in implementing DL techniques within VANET. Following this, an overview of the performance evaluation metrics utilized in the literature will be presented. The performance evaluation also includes an analysis of reported model performances. Finally, we will cover the emerging trends and future directions that are expected to shape VANET systems.

5.1 Different Deep Learning Approaches for IDS in VANETs

This section discusses type deep learning (DL) algorithm that have been proposed in the literatures. With the increasing complexity of VANETs and the threat of cyberattacks, as the literatures have proposed a range of deep learning architectures. The diversity of the proposed DL algorithms is illustrated in Figures 4. According to figure 4, CNN, DBN, DNN, and hybrid DL models are the most proposed methods to enhance detection in dynamic vehicular environments.

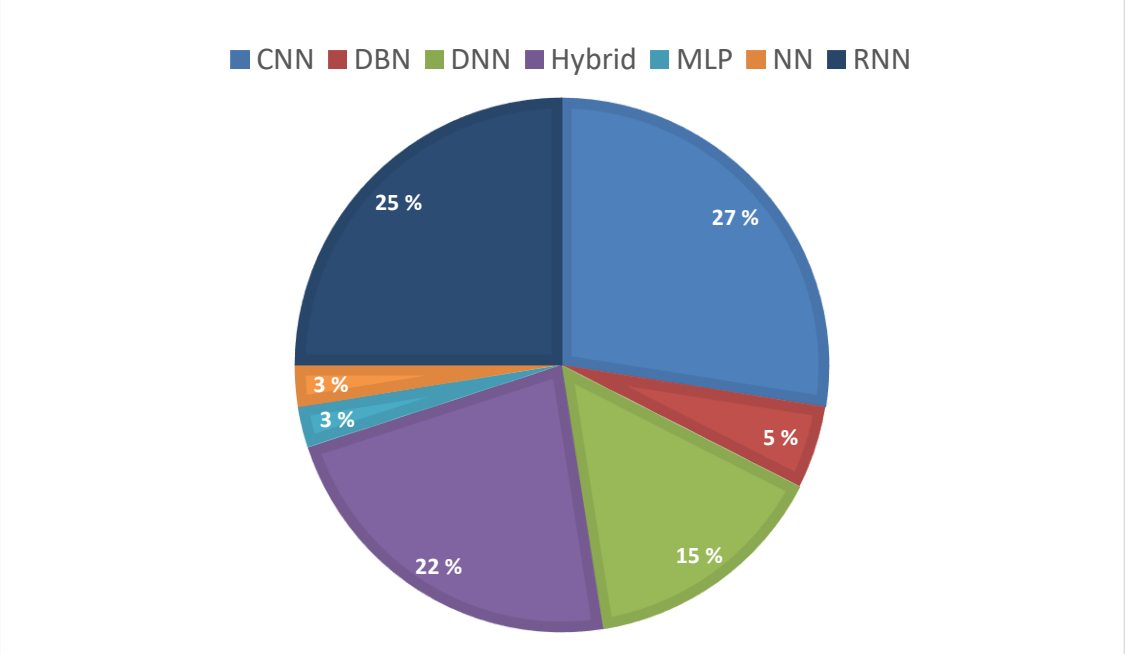

Figure 4 Percentage of Algorithm Types Used Across Selected Studies

The comprehensive review of recent literature highlights the increasing adoption and diverse application of deep learning (DL) models for enhancing intrusion detection capabilities within Vehicular Ad Hoc Networks (VANETs). A variety of architectural paradigms and hybrid

approaches have been explored to address the unique security challenges posed by dynamic vehicular environments.

Foremost utilized DL architectures are Deep Belief Networks (DBNs). These models are frequently employed for their effectiveness in unsupervised feature learning. Additionally, DBN are known for dimensionality reduction and efficient classification tasks (El-Dalahmeh & Adeel, 2023; Sarathkumar et al., 2024a; Shu et al., 2021; Tripathi et al., 2022). These DBNs are often integrated with conventional machine learning algorithms. For instance, Decision Trees or Backpropagation Neural Networks to refine the final classification of malicious activities. Another significant models proposed are Recurrent Neural Networks (RNNs) and their specialized variants, particularly Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) networks. These are particularly suited for processing sequential data, making them ideal for analyzing time series network traffic patterns. LSTM networks have been proposed to identify false messages from internal attackers (Yu et al., 2022)(and to detect Sybil attacks (Sultana et al., 2024). Advanced RNN configurations, such as BiLSTM and hybrid models like CNN-LSTM and CNN-BiLSTM, have shown success in Sybil attack detection (Sultana et al., 2024). (ALMahadin et al., 2024) introduced SEMI-GRU, a semi-supervised hybrid, which offers increased capabilities in managing imbalanced datasets in IDS. Convolutional Neural Networks (CNNs) are also proposed, especially for their network data feature extraction. The utilization of both 1D and 2D CNNs has been explored for the purpose of detecting DDoS attacks (Parfenov et al., 2021). Parfenov findings showed 1D CNNs tend to show a performance advantage over 2D. It has been demonstrated that detection accuracy and generalization can be improved using transfer learning with pre-trained CNNs on time-series imaging of network data (Shahid et al., 2024).

Beyond individual model types, a significant trend involves the development of hybrid DL solutions. This involves integrating various DL techniques or combining them to improve performance. Notable examples include the GC-LSTM-GhostNet model, which incorporates Graph Convolutional Networks, LSTMs with an attention mechanism, and a lightweight CNN for accurate attack detection (Jayakrishna & Prasanth, 2025). I-leeNet is another implemented model mentioned in the literature (Suman et al., 2024). Furthermore, neural network architectures like RideNN, optimized through algorithms such as the Rider Optimization Algorithm and Jellyfish Chimp Optimization Algorithm, are deployed within SDN-based VANETs for attack identification (Kaur et al., 2024; Pulligilla & Vanmathi, 2023). Deep Maxout Networks (DMNs) are also utilized for attack classification, with their parameters

fine-tuned by advanced optimization algorithms like Fractional Aquila Spider Monkey Optimization (FASMO) (G. Kaur & Kakkar, 2022, 2025). Other proposed hybridizations include the combination of Stacked Auto Encoders and Capsule Networks for attack detection (Tanati & Ponnusamy, 2025).

We also noticed that few studies are proposing DL based on a VANET architecture. For instance, many studies recommend SDN based solutions in VANETs. SDN leverages centralized control capabilities to facilitate collaboration and distributed in security (El-Dalahmeh & Adeel, 2023; Pulligilla & Vanmathi, 2023; Setitra & Fan, 2024; Shu et al., 2021; Wei et al., 2025). Federated Learning (FL) represents another solid framework, addressing privacy and latency by decentralizing the learning process across individual vehicles (Gurjar et al., 2025; Mansouri et al., 2025). Within FL environments, hybrid models such as RNN-LSTM have demonstrated high accuracy (Gurjar et al., 2025). The efficacy of these deep learning models is reinforced by the integration of metaheuristic optimization algorithms. Examples of these optimization techniques include the Improved Weight Optimization with Energy-Efficient Clustering (IWOEEC) and Adaptive Bald Eagle Search Optimization (ABESO)(Ajin & Shaji, 2025). The reviewed literatures highlighting the importance of continuous model updates in response to evolving attack vectors (Wei et al., 2025), and the strategic application of blockchain technology for secure network (Mansouri et al., 2025).

Deep learning is becoming an essential tool to secure VANETs. Based on the review, a wide range of applications are applied in the literatures. DL models, from DBNs that learn patterns on their own to LSTMs that are great at spotting attacks in real time data. Often, we observed that researchers are focusing on developing hybrid models and using optimization algorithms to make them even better.

The future of this field seems to be in hybrid DL models. These helps tackle challenges of VANETs, such as limited computational power and time constraint. All literatures shows a strong push to create security systems that are not only powerful but also adaptable and scalable enough to handle VANETs requirements.

5.2 Challenges in Implementing Deep learning IDS in VANETs

Apart from performance of DL in IDS for VANET, limitations in the literatures were raised. These issues appear due to technical limitations also VANET's decentralized, dynamic nature.

One of the most notable limitations is the requirement for computational resources. Deep learning models, particularly convolutional neural networks (CNNs), are computationally intensive and often demand high performance hardware. As highlighted by (S et al., 2023), the CNN-based method they proposed required significant data preprocessing resource. Furthermore, it demands significant computing resources, making it unsuitable for environments with limited resources, like VANETs. Similarly, (ALMahadin et al., 2024) raised concerns regarding the processing power required by their MLB-GRU (RNN-based) model, which presents scalability challenges when deploying such models across large scale VANET infrastructures.

Besides computational costs, security and privacy concerns continue to pose challenges in VANETs. According to (Patil & Adhiya, 2025), VANETs face numerous unresolved security issues. As listed in the literature, including authentication, availability, confidentiality, pseudonymity, data integrity, key management, access control, and non-repudiation. These concerns are intensified by the high dynamic topology of VANETs. This adds complexity to security and intrusion detection in VANETs. The integration of DL techniques into VANETs systems must account for these security demands, which are often beyond the capabilities of conventional deep learning models.

A key research challenge is the shortage of real-world, high-quality datasets to train and validate deep learning models. As (Aboelfottoh & Azer, 2022) pointed out, the performance of DL-based IDSs heavily depend on the availability of clean and real world representative datasets. Many existing datasets are manufactured and outdated, which affect the performace of proposed models in real VANETs environment. Without verifying the models on more realistic training dataset, models are likely to underperform when exposed to unknown and upscale attack patterns.

Furthermore, VANETs are dynamic and distributed, involving frequent topology changes and short lived communicatio. This complicates the deployment of centralized or static deep learning models, as they may struggle to adapt in real time to changing traffic patterns and attacker strategies. To stay effective in a rapid network, models require accuracy, efficiency, and adaptability.

In conclusion, while deep learning holds significant potential for enhancing intrusion detection in VANETs, current implementations face great obstacles. These include high computational demands, security and privacy integration, and the limited availability of

prosperous datasets. Addressing these limitations is critical to advancing the practical adoption of DL-based IDSs in vehicular networks.

5.3 Performance Evaluation Metrics

Several studies in the literature have adopted performance evaluation metrics based on the confusion matrix to assess the effectiveness of machine learning classification models. The confusion matrix is a standard approach in machine learning to compare predicted classifications with actual labels, providing a basis for calculating key metrics such as accuracy, precision, recall, and F1-score Among these, accuracy widely reported metric due to its simplicity, especially in balanced datasets where the costs of different error types are similar.

A confusion matrix consists of four key components:

	Predicted Positive	**Predicted Negative**
Actual Positive	True Positive (TP)	False Negative (FN)
Actual Negative	False Positive (FP)	True Negative (TN)

Table 3 confusion matrix the four components

The comment performance evaluation metrics from the revied literatures are: -

$$Precision = \frac{TP}{TP + FP}$$

Precision: - shows the proportion of correctly identified positive instances out of all instances predicted as positive. High precision is important to minimize false positives. High false positive can lead to unnecessary alerts, resource waste, or even the false accusation of legitimate vehicles (Sultana et al., 2024).

$$Recall = \frac{TP}{TP + FN}$$

Recall: - measures the proportion of actual positive instances that were correctly identified. Preventing undetected abnormal vehicles or malicious actions is crucial because of potential safety repercussions (Sultana et al., 2024).

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

F1-Score: - is the combination of precision and recall, providing a single metric that balances both.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Accuracy: - measures the proportion of correctly identified instances out of the total number of instances in a dataset.

$$Specificity = \frac{TN}{TN + FP}$$

Specificity measures the proportion of actual negative instances that were correctly identified.

Other measurements:-

False Positive Rate is shows the proportion of normal instances incorrectly classified as attacks. A low False Positive Rate is critical for VANETs to avoid disrupting communication, which could lead to user distrust or system overload (ALMahadin et al., 2024; Sultana et al., 2024).

Average Detection Time: In VANETs, the speed at which an intrusion is detected is as important as its accuracy. Low detection time is essential to enable timely prevent attacks and avoid accidents (Sarathkumar et al., 2024; Suman et al., 2024).

Relying solely on accuracy can disguise performance implications (Jacob; Kavlakpglu, 2024). Particularly in safety applications, where the cost of a false negative is high. A missed attack with potentially safety implications,is far higher than the cost of a false positive, a false alarm that might cause inconvenience or minor resource waste. At the very least, an examination of accuracy, precision, recall, and F1-score is vital for a reliable assessment of model efficacy. Therefore, to truly understand the system effectiveness, we must consider a balanced set of metrics.

Several studies included in this review employ confusion matrix based evaluation metrics. Such as accuracy, precision, recall, and F1-score to assess model performance. For example, (Suman et al., 2024) introduced a hybrid deep learning model named IleeNet, which integrates Convolutional Neural Networks (CNNs) with an Adaptive Neuro-Fuzzy Inference

System (ANFIS). The model was evaluated using three datasets: I-VANET, ToN-IoT, and CICIDS2017, achieving impressive average accuracy scores of 97.21%, 97.75%, and 96.66%, respectively. These results indicate that hybrid architectures can deliver robust performance when trained on rich and diverse datasets.

In contrast, (Parfenov et al., 2021) explored the use of 1D and 2D CNNs on generated datasets targeting DDoS attacks. Their findings showed a notable decrease in performance compared to IleeNet, with accuracy values of 89.08% for CNN-1D and 83.96% for CNN-2D. Similarly, (Al-Jawahry et al., 2024) implemented a Deep Belief Network (DBN) using the NSL-KDD dataset, achieving a respectable accuracy of 96.32%.

Further comparisons reveal interesting performance differences between models. (Sarathkumar et al., 2024b) applied a DBN model and reported the following results: Accuracy: 97.45%, Precision: 86.70%, Recall: 80.64%, and F1-score: 81.24%. In comparison, Barve and Patheja (Barve & Patheja, 2024) proposed a hybrid model and achieved superior metrics, as follows Accuracy: 99.65%, Precision: 99.3%, Recall: 99.21%, and F1-score: 99.02%. These outcomes suggest that hybrid approaches offer improved detection success. In another part, (Sarathkumar et al., 2024a) demonstrate the remarkable computational efficiency using their proposed model. They demonstrated lowest computation time (CT) of 1.24 seconds, outperforming other models in terms of processing speed.

Overall, these findings highlight two key insights. Deep learning based IDS can attain high accuracy across various model architectures and datasets. More critically, the characteristics of the dataset particularly its diversity and representativeness, play a role in determining the model's performance, as also emphasized by (Suman et al., 2024).

5.4 Emerging Trends and Future Directions

Recent advancements in network architecture are paving the way for more robust IDS in VANETs. Among these,

Federated Learning (FL) has gained significant attention due to its ability to train models collaboratively across multiple vehicles. FL has the extra advantage of not needing to share raw data. By doing so, FL addresses one of the security requirement of VANETs privacy. However, FL introduces new security challenges, exploited to malicious actors. This issue is addressed in (Mansouri et al., 2025) , by integrating blockchain and smart contracts to ensure data integrity and secure collaboration across distributed nodes.

Software Defined Networking (SDN) SDN provides centralized control and flexible network management This facilitates the ease of implementing and updating IDS policies dynamically (El-Dalahmeh & Adeel, 2023; Pulligilla & Vanmathi, 2023; Shu et al., 2021).

5G networks supports low latency data exchange, and enables faster threat detection and response (Thorat et al., 2024). With the arrival of 5G networks and their cutting-edge technologies, creating sustainable VANETs is possibility. 5G boasts faster data speeds, quicker communication, and can efficiently handle traffic from countless devices.

We anticipate that FL, SDN, blockchain, and 5G will serve as cornerstones in the widespread adoption of VANETs. VANET will be improved by these new technologies to be intelligent, scalable and secure. For future IDS models, this integration will probably be crucial for addressing the performance, privacy, and adaptability requirements of quickly changing vehicular networks.

6 Discussions/Lessons learned

In this section, we will first examine the challenges and limitations faced by existing Intrusion Detection Systems (IDS) solutions discussed in the reviewed literatures. And, providing a summary of issues that impede their effective deployment. Following this, we will explore promising future directions and proposed solutions aimed at overcoming these obstacles. Furthermore, highlighting advancements that could shape the next generation of secure VANETs.

6.1 Challenges and Limitations of IDS in VANETs

The effective implementation of IDS in VANETs is crucial for ensuring the security and reliability of vehicular communication. Yet, VANETs has a distinct set of problems and constraints. VANET environments' behavior characteristics such as dynamic, resource-constrained, and open nature causes these issues. Understanding these issues are base for developing effective IDS solutions.

6.1.1 Challenges

Computational limitation: - IDS in VANETs faces several notable issues. A primary concern is the computational constraint. Especially for our paper topic, DL required a lot of computational resources. Mostly DL computational need are more that the current on board power or on board units will struggle to perform in a urban envirument.

Scarcity of real world dataset to train DL models:- We noticed a common problem in VANET research, the challenge of finding real datasets. (Tanati & Ponnusamy, 2025)found evaluations using actual data are often skipped in studies. regardelss of perfoming well on training dataset, method they presented didn't perform well in real world situations. The reason for this is real world data are more noisey, incompleteness, or inconsistency versus training dataset.

Infrastructure readiness:- Another key challenge is infrastructure readiness. VANETs require robust deployments of roadside units (RSUs), reliable connectivity, and interoperability standards, all of which are still evolving globally. Without a fully deployed infrastructure, the scalability and real-time applicability of IDS solutions often remain theoretical.

6.1.2 Limitation

Currently, VANET security systems have some clear limitations. A primary concern is the resource intensiveness of deep learning based IDS. As we discussed previously, DL based IDS demand significant computational resources and power that are often scarce in VANET environments (Aboelfottoh & Azer, 2022). The dependency also applies to RSUs, which could raise initial expenses and create implementation obstacles in areas with limited internet access or inadequate RSU infrastructure. Moreover, deep learning models demand hefty computing power and extensive data preparation, particularly for actual traffic data.

(Tanati & Ponnusamy, 2025) observed that the dynamic nature of cyberattacks, for instance DDoS attacks in real-world scenarios, leads to lower detection accuracy. Even if their model was performance was outstanding in the NSL-KDD dataset. This requires detailed testing environments and powerful dataset frameworks to manage uncertain behavior and real-time needs. Following Tanati & Ponnusamy's experiment, this issue could appear in more samples, despite lacking documented evidence.

Scalability remains a significant issue, as many proposed VANET solutions are not practical for larger systems and have only undergone limited evaluations (Sultana et al., 2024). The computational overhead associated with feature processing and multi-level classifications can be substantial, particularly in high-density and large-scale networks. This can lead to issues such as overloading edge computing servers when fake identities are created.

Specific attack types also present unique difficulties. The detection of complex attacks, such as those involving Sybil nodes, is particularly challenging due to the lack of extensive datasets for these specific threats (Shahid et al., 2024). Even within existing models, factors like low vehicle density can impact feature calculation and subsequently lower detection performance. Some pre-trained models may not generalize well to attack types not present in their initial training data. Issues like statistical attacks and the unintentional propagation of fake messages by authenticated nodes can further compromise system efficiency and security.

In summary, the key limitations in securing VANETs revolve around the demanding resource requirements of deep learning models. Particularly in resource constrained VANET environments. And the other challenges is associated with acquiring and processing large, clean, and real-world datasets for effective training. The dynamic and evolving nature of cyber threats frequently leads to high false positive and negative rates in existing IDS, and

many current solutions lack the scalability and generalizability needed for large-scale, real-world deployments. Also, detecting complex and new attacks, like Sybil attacks, is still hard because of limited data and difficulty differentiating malicious actions from regular traffic. These limitations collectively highlight the need for continued research into more robust, efficient, and adaptable security mechanisms for VANETs.

6.2 Future directions

Looking ahead, several promising directions can help overcome the current challenges. As computational power in vehicles continues to increase, there's greater potential for deploying advanced AI models directly at the edge. This will enable real-time detection and response capabilities without over-reliance on cloud infrastructure.

6.2.1 Blockchain-Based Security

For instance, (Zhang et al., 2023) proposed a blockchain-based security framework that utilizes On-Board Units (OBUs) and RSUs as nodes within an alliance blockchain to secure traffic information and enhance trust in data exchange. Their approach integrates computing on local processing and leverages blockchain mechanisms. For example, Merkle trees and smart contracts, to ensure data is reliable and flexible using deep reinforcement learning.

6.2.2 Cloud-Based Architectures

(Y. Wu et al., 2023) proposed a comprehensive vehicle road cloud architecture. This method drafting a communication model between vehicles, roadside units, and cloud services. This model not only facilitates more structured data sharing but also supports scalable IDS deployment.

Additinaly (Alladi et al., 2023) also proposed a cloud-based architecture where base servers are connected to cloud servers via high-speed wired backhaul links. In this framework, DL models for misbehavior detection are trained in the cloud, while prediction and interfering tasks are executed on base servers. This design offers two key advantages, first it enables efficient real-time detection at the network base. And secondly, it effectively addresses the computational limitations typically associated with VANETs.

6.2.3 Cluster-Based Routing

Literature has demonstrated that implementing cluster-based routing protocols can significantly improve security. (G. Kaur & Kakkar, 2022) introduced an approach to enhance security and reliable routing in VANETs. Their core contribution is a hybrid optimization and deep learning model, specifically using a Deep Maxout Network (DMN), designed to detect malicious activity and optimize the selection and routing of Cluster Heads. This system employs an ensemble machine learning approach with a fuzzy ranking model to identify hostile actions. They documented a significant improvements in accuracy, recall, energy efficiency, and routing trust.

Similarly, (M et al., 2023) introduced the IWOEEC-DWNN method to address energy constraints in VANETs. This approach uses an Improved Weight Optimization with Energy-Efficient Clustering (IWOEEC) technique to form clusters by selecting optimal cluster heads. For intrusion detection, a Deep Weighted Neural Network (DWNN) model classifies network behavior as either normal or malicious. This method consistently outperformed existing algorithms in detection accuracy and energy efficiency.

Finally, despite their importance to VANET security, IDSs encounter significant deployment issues. Challenges include computational limits in vehicle hardware, limited realistic data, varying infrastructure readiness, and the complex, adaptive nature of attacks. Despite these challenges, the future of VANET security looks bright, thanks to promising new approaches. The combination of blockchain security, and cloud-based architectures allows for the deployment of distributed, and highly secure IDS. Furthermore, optimized routing, like cluster-based methods, presents a a system to detect attacks better and make networks more study. To unlock the full potential of secure and dependable VANETs, we need a concentrated effort in building comprehensive strengthening adaptable, lightweight models, and integrating cross-layer security.

7 Conclusions

This systematic literature review investigated deep learning based intrusion detection systems (IDS) in Vehicular Ad-Hoc Networks (VANETs). Recognizing the crutial need to enhance global road safety and while reducing cybersecurity threats in these dynamic networks. This thesis aimed to provide a foundational understanding of the current state, limitations, and future research directions on DL based IDS in VANETs. The review highlighted DL's significant potential for safe, smart VANET.

We recognized the global road safety problem and suggested VANETs are key for enhancements. However, we also aim to highlight VANETs' vulnerability to cyber threats such as data forgery, Sybil attacks, and DoS attacks. We suggest an intelligent IDS, leveraging deep learning is vital defense mechanisms. This SLR evaluated current approaches, and try to identified areas for further attention.

To ensure credibility, the SLR methodology developed by (Kitchenham & Charters, 2007) used as a guidelines and furthermore the PRISMA 2020 framework (Page et al., 2021) used to improve the conclusions quality. The method used involved defining research questions, systematic searching, applying stringent selection criteria, and synthesizing data, ensuring an unbiased and thorough examination.

The systematic review yielded significant insights. A predominant finding is the demonstrated efficacy of various deep learning architectures (e.g., CNNs, RNNs, LSTMs, Autoencoders) in detecting a wide array of cyberattacks targeting VANETs. These models generally achieve high accuracy, precision, recall, and F1-scores, often outperforming traditional machine learning due to their ability to process complex, high-dimensional data and learn intricate patterns.

However, the review also underscored persistent challenges and limitations. Data availability and quality are significant hurdles, often necessitating simulated data that may not capture real-world complexities. Computational overhead and latency are critical concerns for real-time deployment in resource-constrained VANET environments. The "black-box" nature of many deep learning models poses challenges for explainability and interpretability, hindering trust and debugging. The vulnerability to adversarial attacks is a growing concern. Finally, a lack of standardized evaluation metrics and benchmarks across the literature made direct comparisons challenging.

While specific research questions were not explicitly detailed, this SLR effectively addressed the core inquiries. It elucidated what deep learning techniques are currently applied for IDS in VANETs, and how these techniques are implemented and evaluated. Crucially, it identified the key challenges and limitations impeding widespread deployment, thus laying a solid foundation for mapping out future research directions.

To sum it up, we think deep learning is a strong tool to improve VANET cybersecurity, as shown by our literature review. Findings consistently demonstrate deep learning models' superior capabilities in detecting cyber threats. Intelligent IDS integration is a fundamental requirement for secure and reliable future intelligent transportation systems. While significant progress exists, identified limitations in data, computational efficiency, explainability, and adversarial robustness highlight the field's nascent stage of practical deployment. Overcoming these challenges is crucial for translating theoretical advancements into tangible improvements in road safety and transportation efficiency globally.

Future research should prioritize: large-scale, realistic, and publicly accessible VANET datasets; lightweight and efficient deep learning models suitable for resource-constrained environments; hybrid IDS architectures combining deep learning with other security mechanisms; robust deep learning models and adversarial training techniques against adversarial attacks; Explainable AI (XAI) for VANET security; real-world deployment and validation in testbeds; and standardization of evaluation metrics and benchmarks. Addressing these critical areas will significantly advance VANET security, paving the way for secure, efficient, and life-saving intelligent transportation systems.

References

Aboelfottoh, A. A., & Azer, M. A. (2022). Intrusion detection in VANETs and ACVs using deep learning. In *Proceedings of the 2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC)* (pp. 241–245). **IEEE**. https://doi.org/10.1109/MIUCC55081.2022.9781691

Ajin, M., & Shaji, R. S. (2025). Enhancing security in vanVANETs: Adaptive Bald Eagle Search Optimization based multi-agent deep Q neural network for Sybil attack detection. *Vehicular Communications*, *54*, 100928. https://doi.org/10.1016/j.vehcom.2025.100928

Al Shugran, M. A. (2021). Applicability of Overlay Non-Delay Tolerant Position-Based Protocols in Highways and Urban Environments for VANET. *International Journal of Wireless & Mobile Networks*, *13*(2), 9–24. https://doi.org/10.5121/ijwmn.2021.13202

Al-Jawahry, H. M., Bai B G, M., Veena, T., Ramesh, V., & Indupalli, T. (2024). Deep Belief Network Based Intrusion Detection in Vehicle Ad Hoc Network. *2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT)*, 1–4. https://doi.org/10.1109/ICDCOT61034.2024.10515496

Alladi, T., Kohli, V., Chamola, V., & Yu, F. R. (2023). A deep learning based misbehavior classification scheme for intrusion detection in cooperative intelligent transportation systems. *Digital Communications and Networks*, *9*(5), 1113–1122. https://doi.org/10.1016/j.dcan.2022.06.018

ALMahadin, G., Aoudni, Y., Shabaz, M., Agrawal, A. V., Yasmin, G., Alomari, E. S., Al-Khafaji, H. M. R., Dansana, D., & Maaliw, R. R. (2024). VANET Network Traffic Anomaly Detection Using GRU-Based Deep Learning Model. *IEEE Transactions on Consumer Electronics*, *70*(1), 4548–4555. https://doi.org/10.1109/TCE.2023.3326384

Althunayyan, M., Javed, A., & Rana, O. (2024). *A Robust Multi-Stage Intrusion Detection System for In-Vehicle Network Security using Hierarchical Federated Learning* (No. arXiv:2408.08433). arXiv. https://doi.org/10.48550/arXiv.2408.08433

Azad, C., & Jha, V. K. (2013). Data Mining in Intrusion Detection: A Comparative Study of Methods, Types and Data Sets. *International Journal of Information Technology and Computer Science*, *5*(8), 75–90. https://doi.org/10.5815/ijitcs.2013.08.08

Barve, A., & Patheja, P. S. (2024). A hybrid deep learning based enhanced and reliable approach for VANET intrusion detection system. *Cluster Computing*, *27*(9), 11839–11850. https://doi.org/10.1007/s10586-024-04634-w

Belal, Y., Mokhtar, S. B., Haddadi, H., Wang, J., & Mashhadi, A. (2024). Survey of Federated Learning Models for Spatial-Temporal Mobility Applications. *ACM Transactions on Spatial Algorithms and Systems*, *10*(3), 1–39. https://doi.org/10.1145/3666089

Christopoulou, M., Barmpounakis, S., Koumaras, H., & Kaloxylos, A. (2023). Artificial Intelligence and Machine Learning as key enablers for V2X communications: A comprehensive survey. *Vehicular Communications*, *39*. https://doi.org/10.1016/j.vehcom.2022.100569

Communication and Localization Techniques in VANET Network for Intelligent Traffic System in Smart Cities. (2020). In *Smart Transportation Systems 2020* (1st ed., Vol. 185, pp. 167–177). Springer Singapore. https://doi.org/10.1007/978-981-15-5270-0_15

digital scholar. (n.d.). *Zotero | About*. About. Retrieved July 29, 2025, from https://www.zotero.org/about/

Dutta, A., Samaniego Campoverde, L. M., Tropea, M., & De Rango, F. (2024). A Comprehensive Review of Recent Developments in VANET for Traffic, Safety & Remote Monitoring Applications. *Journal of Network and Systems Management*, *32*(4). https://doi.org/10.1007/s10922-024-09853-5

El-Dalahmeh, M., & Adeel, U. (2023). Intrusion Detection System for SDN based VANETs Using A Deep Belief Network, Decision Tree, and ToN -IoT Dataset. *2023 IEEE IAS Global Conference on Emerging Technologies (GlobConET)*, 1–6. https://doi.org/10.1109/GlobConET56651.2023.10150188

Engoulou, R. G., Bellaïche, M., Pierre, S., & Quintero, A. (2014). VANET security surveys. *Computer Communications*, *44*, 1–13. https://doi.org/10.1016/j.comcom.2014.02.020

Eze, E. C., Zhang, S., & Liu, E. (2014). Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward. *2014 20th International Conference on Automation and Computing*, 176–181. https://doi.org/10.1109/iconac.2014.6935482

Gammaa, A., Khaleghian, S., Tran, T., & Sartipi, M. (2025). *Improving VANET Simulation Channel Model in an Urban Environment via Calibration Using Real-World Communication Data* (No. arXiv:2502.07954). arXiv. https://doi.org/10.48550/arXiv.2502.07954

Günay, F. B., Öztürk, E., Çavdar, T., Hanay, Y. S., & Khan, A. U. R. (2021). Vehicular Ad Hoc Network (VANET) Localization Techniques: A Survey. *Archives of Computational Methods in Engineering*, *28*(4), 3001–3033. https://doi.org/10.1007/s11831-020-09487-1

Gurjar, D., Grover, J., Kheterpal, V., & Vasilakos, A. (2025). Federated learning-based misbehavior classification system for VANET intrusion detection. *Journal of Intelligent Information Systems*, *63*(3), 807–830. https://doi.org/10.1007/s10844-025-00920-0

Hartenstein, H., & Laberteaux, K. P. (2008). A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine*, *46*(6), 164–171. https://doi.org/10.1109/mcom.2008.4539481

Hota, L., Nayak, B. P., Kumar, A., Ali, G. G. Md. N., & Chong, P. H. J. (2021). An Analysis on Contemporary MAC Layer Protocols in Vehicular Networks: State-of-the-Art and Future Directions. *Future Internet*, *13*(11), 287. https://doi.org/10.3390/fi13110287

Jacob; Kavlakpglu, E. M. (2024, January). *What is a confusion matrix? | IBM*. https://www.ibm.com/think/topics/confusion-matrix

Jantosova, A., Dolnak, I., & Dado, M. (2019, November). An overview of vehicular ad hoc networks. *2019 17th International Conference on Emerging eLearning Technologies and Applications (ICETA)*. 2019 17th International Conference on Emerging eLearning Technologies and Applications (ICETA), Starý Smokovec, Slovakia. https://doi.org/10.1109/iceta48886.2019.9040098

Jayakrishna, N., & Prasanth, N. N. (2025). Detection and mitigation of distributed denial of service attacks in vehicular ad hoc network using a spatiotemporal deep learning and reinforcement learning approach. *Results in Engineering*, *26*, 104839. https://doi.org/10.1016/j.rineng.2025.104839

Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., & Weil, T. (2011). Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. *IEEE Communications Surveys & Tutorials*, *13*(4), 584–616. https://doi.org/10.1109/surv.2011.061411.00019

Kaur, G., & Kakkar, D. (2022). Hybrid optimization enabled trust-based secure routing with deep learning-based attack detection in VANET. *Ad Hoc Networks*, *136*, 102961. https://doi.org/10.1016/j.adhoc.2022.102961

Kaur, G., & Kakkar, D. (2025). A secure lightweight authentication model with interference aware routing and attack detection approach in VANET. *Cluster Computing*, *28*(2), 109. https://doi.org/10.1007/s10586-024-04772-1

Kaur, R., Singh, T. P., & Khajuria, V. (2018). Security Issues in Vehicular Ad-Hoc Network(VANET). *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, 884–889. https://doi.org/10.1109/icoei.2018.8553852

Kaur, U., Mahajan, A. N., Kumar, S., & Dutta, K. (2024). Jellyfish Search Chimp Optimization Enabled Routing and Attack Detection in SDN based VANETs. *Wireless Personal Communications*, *138*(2), 819–859. https://doi.org/10.1007/s11277-024-11525-1

Kitchenham, B., & Charters, S. M. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering* (No. EBSE-2007-01). Keele University, UK. https://www.researchgate.net/publication/302924724

Krishna K, V., & Reddy K, G. (2022). VANET Vulnerabilities Classification and Countermeasures: A Review. *Majlesi Journal of Electrical Engineering*, *16*(3). https://doi.org/10.30486/mjee.2022.696508

Kumar, G., Saha, R., Rai, M. K., & Kim, T.-H. (2018). Multidimensional Security Provision for Secure Communication in Vehicular Ad Hoc Networks Using Hierarchical Structure and End-to-End Authentication. *IEEE Access*, *6*, 46558–46567. https://doi.org/10.1109/access.2018.2866759

Kumar, V., Srivastava, J., & Lazarevic, A. (Eds.). (2005). *Managing cyber threats: Issues, approaches, and challenges*. Springer.

M, M. V. B. M. K., Ananth, C. A., & Krishnaraj, N. (2023). Detection of intrusions in clustered vehicle networks using invasive weed optimization using a deep wavelet neural networks. *Measurement: Sensors*, *28*, 100807. https://doi.org/10.1016/j.measen.2023.100807

Mansouri, F., Tarhouni, M., Alaya, B., & Zidi, S. (2025). A distributed intrusion detection framework for vehicular Ad Hoc networks via federated learning and Blockchain. *Ad Hoc Networks*, *167*, 103677. https://doi.org/10.1016/j.adhoc.2024.103677

Mejri, M. N., Ben-Othman, J., & Hamdi, M. (2014). Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Communications*, *1*(2), 53–66. https://doi.org/10.1016/j.vehcom.2014.05.001

N, J., & Patil, R. (2023). Enhanced Machine Learning Based Techniques for Security in Vehicular Ad-Hoc Networks. *2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, 386–393. https://doi.org/10.1109/incacct57535.2023.10141791

Nagarajan, J., Mansourian, P., Shahid, M. A., Jaekel, A., Saini, I., Zhang, N., & Kneppers, M. (2023). Machine Learning based intrusion detection systems for connected autonomous vehicles: A survey. *Peer-to-Peer Networking and Applications*, *16*(5), 2153–2185. https://doi.org/10.1007/s12083-023-01508-7

Nkenyereye, L., Nkenyereye, L., Islam, S. M. R., Choi, Y.-H., Bilal, M., & Jang, J.-W. (2019). Software-Defined Network-Based Vehicular Networks: A Position Paper on Their Modeling and Implementation. *Sensors*, *19*(17), 3788. https://doi.org/10.3390/s19173788

NSL-KDD | Datasets | Research | Canadian Institute for Cybersecurity | UNB. (n.d.). Retrieved July 29, 2025, from https://www.unb.ca/cic/datasets/nsl.html

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, *372*, n71. https://doi.org/10.1136/bmj.n71

Parfenov, D., Grishina, L., Zhigalov, A., & Bolodurina, I. (2021). Applying Convolutional Neural Networks for Security in VANET. *2021 International Conference Engineering and Telecommunication (En&T)*, 1–4. https://doi.org/10.1109/EnT50460.2021.9681796

Patil, M. J., & Adhiya, K. P. (2025). Secured VANET: An improved COOT-algorithm-based optimal routing protocol with multiple authentication and fake message detection for secure data transmission. *Wireless Networks*, *31*(4), 3315–3342. https://doi.org/10.1007/s11276-025-03941-3

PRISMA 2020 flow diagram—PRISMA statement. (n.d.). https://www.prisma-statement.org/prisma-2020-flow-diagram

Pulligilla, M. K., & Vanmathi, C. (2023). An authentication approach in SDN-VANET architecture with Rider-Sea Lion optimized neural network for intrusion detection. *Internet of Things*, *22*, 100723. https://doi.org/10.1016/j.iot.2023.100723

Quyoom, A., Mir, A. A., & Sarwar, Dr. A. (2020). Security Attacks and Challenges of VANETs: A Literature Survey. *Journal of Multimedia Information System*, *7*(1), 45–54. https://doi.org/10.33851/jmis.2020.7.1.45

S, A., A, R., & Maheswari, G. U. (2023). Improved IDS for Vehicular Ad-Hoc Network using Deep Learning Approaches. *2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS)*, 341–346. https://doi.org/10.1109/ICACRS58579.2023.10404805

Sadiq Alrubaye, J., & Abdkhaleq, M. H. G. (2024). A Comprehensive Review for different perspectives in Ad-Hoc/ Cellular VANET Networks: Taxonomy, Challenges, Routing, Future Directions. *Wasit Journal for Pure Sciences*, *3*(4), 78–104. https://doi.org/10.31185/wjps.594

Sarathkumar, K., Sudhakar, P., & Kanmani, A. C. (2024a). Enhancing intrusion detection using coati optimization algorithm with deep learning on vehicular Adhoc networks. *International Journal of Information Technology*, *16*(5), 3009–3018. https://doi.org/10.1007/s41870-024-01827-9

Sarathkumar, K., Sudhakar, P., & Kanmani, A. C. (2024b). Enhancing intrusion detection using coati optimization algorithm with deep learning on vehicular Adhoc networks. *International*

Journal of Information Technology, *16*(5), 3009–3018. https://doi.org/10.1007/s41870-024-01827-9

Setitra, M. A., & Fan, M. (2024). Detection of DDoS attacks in SDN-based VANET using optimized TabNet. *Computer Standards & Interfaces*, *90*, 103845. https://doi.org/10.1016/j.csi.2024.103845

Shahid, M. A., Jaekel, A., Zhang, N., & Allsopp, T. (2024). DoS Attack Detection in VANET using Transfer Learning Approach for BSM Data. *2024 International Wireless Communications and Mobile Computing (IWCMC)*, 748–753. https://doi.org/10.1109/IWCMC61514.2024.10592612

Shu, J., Zhou, L., Zhang, W., Du, X., & Guizani, M. (2021). Collaborative Intrusion Detection for VANETs: A Deep Learning-Based Distributed SDN Approach. *IEEE Transactions on Intelligent Transportation Systems*, *22*(7), 4519–4530. https://doi.org/10.1109/TITS.2020.3027390

Singh, P. A., Kamboj, V., & Kaur, R. (2023). Role of VANETs in Machine Learning and Deep Learning. *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)*, 306–312. https://doi.org/10.1109/ic3i59117.2023.10397957

Statistics Finland. (2025, January 28). Road Traffic Accidents Claimed 12 Lives in December 2024. https://stat.fi/en/publication/cm160x9wv3ua107vzqc193naj?utm_source=chatgpt.com

Stellwagen, J., Deegener, M., & Kuhn, M. (2023). Hybrid Vehicle-to-X Communication Network by Using ITS-G5 and LTE-V2X. *IEEE Access*, *11*, 30783–30795. https://doi.org/10.1109/access.2023.3260980

Sultana, R., Grover, J., Tripathi, M., Sachdev, M. S., & Taneja, S. (2024). Detecting Sybil Attacks in VANET: Exploring Feature Diversity and Deep Learning Algorithms with Insights into Sybil Node Associations. *Journal of Network and Systems Management*, *32*(3), 51. https://doi.org/10.1007/s10922-024-09827-7

Suman, P., Padhy, S., Kumar, N., Suman, A., Singh, A., Singh, K. K., Castilla, Á. K., & AL-Zahrani, T. S. S. (2024). An Improved Deep Learning-Based Intrusion Detection for Reliable

Communication in VANET. *IEEE Transactions on Consumer Electronics*, 1–1. https://doi.org/10.1109/TCE.2024.3475823

Sumra, I. A., Ahmad, I., Hasbullah, H., & Bin Ab Manan, J. (2011). Classes of attacks in VANET. *2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC)*, 1–5. https://doi.org/10.1109/siecpc.2011.5876939

Taleb, A. A. (2018). VANET Routing Protocols and Architectures: An Overview. *Journal of Computer Science*, *14*(3), 423–434. https://doi.org/10.3844/jcssp.2018.423.434

Tanati, M. K., & Ponnusamy, M. (2025). Dense capsule stacked auto-encoder model based DDoS attack detection and hybrid optimal bandwidth allocation with routing in VANET environment. *Vehicular Communications*, *52*, 100888. https://doi.org/10.1016/j.vehcom.2025.100888

Thorat, S. S., Rojatkar, D. V., & Deshmukh, P. R. (2024). A Deep Learning Approach for Sustainable Ad Hoc Vehicular Network. In T. Senjyu, C. So–In, & A. Joshi (Eds.), *Smart Trends in Computing and Communications* (Vol. 946, pp. 429–443). Springer Nature Singapore. https://doi.org/10.1007/978-981-97-1323-3_37

Tripathi, K. N., Yadav, A. M., & Sharma, S. C. (2022). Fuzzy and Deep Belief Network Based Malicious Vehicle Identification and Trust Recommendation Framework in VANETs. *Wireless Personal Communications*, *124*(3), 2475–2504. https://doi.org/10.1007/s11277-022-09474-8

VeReMi dataset. (n.d.). VeReMi-Dataset.Github.Io. Retrieved July 29, 2025, from https://veremi-dataset.github.io/

Wei, L., Yang, J., Jin, H., Cui, J., Li, J., & He, D. (2025). Sustainable Learning-Based Intrusion Detection System for VANETs. *IEEE Transactions on Intelligent Transportation Systems*, 1–12. https://doi.org/10.1109/TITS.2025.3562226

Wu, W., Joloudari, J. H., Jagatheesaperumal, S. K., Rajesh, K. N. V. P. S., Gaftandzhieva, S., Hussain, S., Rabih, R., Haqjoo, N., Nazar, M., Vahdat-Nejad, H., & Doneva, R. (2024). Deep Transfer Learning Techniques in Intrusion Detection System-Internet of Vehicles: A State-of-the-Art

Review. In *Computers, Materials and Continua* (Vol. 80, Issue 2, pp. 2785–2813). Tech Science Press. https://doi.org/10.32604/cmc.2024.053037

Wu, Y., Wu, L., & Cai, H. (2023). A deep learning approach to secure vehicle to road side unit communications in intelligent transportation system. *Computers and Electrical Engineering*, *105*, 108542. https://doi.org/10.1016/j.compeleceng.2022.108542

Yu, Y., Zeng, X., Xue, X., & Ma, J. (2022). LSTM-Based Intrusion Detection System for VANETs: A Time Series Classification Approach to False Message Detection. *IEEE Transactions on Intelligent Transportation Systems*, *23*(12), 23906–23918. https://doi.org/10.1109/TITS.2022.3190432

Zeadally, S., Hunt, R., Chen, Y. S., Irwin, A., & Hassan, A. (2012). Vehicular ad hoc networks (VANETS): Status, results, and challenges. *Telecommunication Systems*, *50*(4), 217–241. https://doi.org/10.1007/s11235-010-9400-5

Zhang, B., Wang, X., Xie, R., Li, C., Zhang, H., & Jiang, F. (2023). A reputation mechanism based Deep Reinforcement Learning and blockchain to suppress selfish node attack motivation in Vehicular Ad-Hoc Network. *Future Generation Computer Systems*, *139*, 17–28. https://doi.org/10.1016/j.future.2022.09.010

Appendices

Appendix 1. List of Reviewed Literature

1	Improved IDS for Vehicular Ad-Hoc Network using Deep Learning Approaches	A. S; R. A; G. U. Maheswari	2021	IEEE
2	usion Detection in VANETs d ACVs using Deep Learning	A. A. Aboelfottoh; M. A. Azer	2021	IEEE
3	An Improved Deep Learning-Based Intrusion Detection for Reliable Communication in VANET	P. Suman; S. Padhy; N. Kumar; A. Suman; A. Singh; K. K. Singh; Á. K. Castilla; T. S. S. AL-Zahrani	2021	IEEE
4	Sustainable Learning-Based Intrusion Detection System for VANETs	L. Wei; J. Yang; H. Jin; J. Cui; J. Li; D. He	2021	IEEE
5	Collaborative Intrusion Detection for VANETs: A Deep Learning-Based Distributed SDN Approach	J. Shu; L. Zhou; W. Zhang; X. Du; M. Guizani	2021	IEEE
6	Intrusion Detection System for SDN based VANETs Using A Deep Belief Network, Decision Tree, and ToN -IoT Dataset	M. El-Dalahmeh; U. Adeel	2021	IEEE
7	Collaborative Intrusion Detection System for SDVN: A Fairness Federated Deep Learning Approach	J. Cui; H. Sun; H. Zhong; J. Zhang; L. Wei; I. Bolodurina; D. He	2021	IEEE
8	LSTM-Based Intrusion Detection System for VANETs: A Time Series Classification Approach to False Message Detection	Y. Yu; X. Zeng; X. Xue; J. Ma	2021	IEEE
9	Applying Convolutional Neural Networks for Security in VANET	D. Parfenov; L. Grishina; A. Zhigalov; I. Bolodurina	2022	IEEE
10	Deep Belief Network Based Intrusion Detection in Vehicle Ad Hoc Network	H. M. Al-Jawahry; M. Bai B G; T. Veena; V. Ramesh; T. Indupalli	2022	IEEE
11	VANET Network Traffic Anomaly Detection Using GRU-Based Deep Learning Model	G. ALMahadin; Y. Aoudni; M. Shabaz; A. V. Agrawal; G. Yasmin; E. S. Alomari; H. M. R. Al-Khafaji; D. Dansana; R. R. Maaliw	2022	IEEE
12	Transfer Learning Based Intrusion Detection System Using Gramian Angular Field for Connected Vehicles	M. A. Shahid; A. Jaekel; N. Zhang; T. Allsopp	2022	IEEE
13	Deep Neural Networks for Securing IoT Enabled Vehicular Ad-Hoc Networks	T. Alladi; A. Agrawal; B. Gera; V. Chamola; B. Sikdar; M. Guizani	2022	IEEE

14	Securing VANETs: Multi-Objective Intrusion Detection With Variational Autoencoders	N. Nissar; N. Naja; A. Jamali	2022	IEEE
15	DoS Attack Detection in VANET using Transfer Learning Approach for BSM Data	M. A. Shahid; A. Jaekel; N. Zhang; T. Allsopp	2022	IEEE
16	DeepADV: A Deep Neural Network Framework for Anomaly Detection in VANETs	T. Alladi; B. Gera; A. Agrawal; V. Chamola; F. R. Yu	2023	IEEE
17	Edge Computing and Deep Learning Enabled Secure Multitier Network for Internet of Vehicles	H. Grover; T. Alladi; V. Chamola; D. Singh; K. -K. R. Choo	2023	IEEE
18	Detection and Classification of Anomalies in Internet of Vehicles using Convolutional Neural Networks	P. Hade; K. Waghmare	2023	IEEE
19	A Deep Learning-Based Integrated Algorithm for Misbehavior Detection System in VANETs	Hsu, Hsiao-Yuan; Cheng, Nai-Hsin; Tsai, Chun-Wei	2023	ACM
20	Secured VANET: an improved COOT-algorithm-based optimal routing protocol with multiple authentication and fake message detection for secure data transmission	Mayur Jagdish PatilKrishnakant P. Adhiya	2023	SpringerLink
21	Intrusion detection in smart grids using artificial intelligence-based ensemble modelling	Amjad AlsirhaniNoshina TariqMamoona HumayunGhadah Naif AlwakidHassan Sanaullah	2023	SpringerLink
22	An efficient privacy-preserving authentication scheme for internet of vehicles based on blockchain technology with hybrid adaptive network	R. LoganathanS. SelvakumaraSamy	2023	SpringerLink
23	Cost-Sensitive Detection of DoS Attacks in Automotive Cybersecurity Using Artificial Neural Networks and CatBoost	Nabil NissarNajib NajaAbdellah Jamali	2023	SpringerLink
24	Federated learning-based misbehavior classification system for VANET intrusion detection	Dayanand GurjarJyoti GroverVanisha KheterpalAthanasios Vasilakos	2023	SpringerLink
25	Trust-based secure federated learning framework to mitigate	D. S. Bhupal NaikVenkatesulu Dondeti	2023	SpringerLink

	internal attacks for intelligent vehicular networks			
26	A secure and efficient blockchain enabled federated Q-learning model for vehicular Ad-hoc networks	Huda A. AhmedHend Muslim JasimAli Noori GateaAli Amjed Ali Al-AsadiHamid Ali Abed Al-Asadi	2023	SpringerLink
27	A secure lightweight authentication model with interference aware routing and attack detection approach in VANET	Gurjot KaurDeepti Kakkar	2023	SpringerLink
28	Jellyfish Search Chimp Optimization Enabled Routing and Attack Detection in SDN based VANETs	Upinder KaurAparna N. MahajanSunil KumarKamlesh Dutta	2024	SpringerLink
29	A hybrid deep learning based enhanced and reliable approach for VANET intrusion detection system	Atul BarvePushpinder Singh Patheja	2024	SpringerLink
30	Detecting Sybil Attacks in VANET: Exploring Feature Diversity and Deep Learning Algorithms with Insights into Sybil Node Associations	Rukhsar SultanaJyoti GroverMeenakshi TripathiManhar Singh SachdevSparsh Taneja	2024	SpringerLink
31	Enhancing intrusion detection using coati optimization algorithm with deep learning on vehicular Adhoc networks	K. SarathkumarP. SudhakarA. Clara Kanmani	2024	SpringerLink
32	A Deep Learning Approach for Sustainable Ad Hoc Vehicular Network	Samrat Subodh ThoratDinesh Vitthalrao RojatkarPrashant R. Deshmukh	2024	SpringerLink
33	A Hybrid Few-Shot Learning Based Intrusion Detection Method for Internet of Vehicles	Yixuan ZhaoJianming CuiMing Liu	2024	SpringerLink
34	Machine Learning-Based Systems for Intrusion Detection in VANETs	Hala Eldaw IdrisInes Hosni	2024	SpringerLink
35	Machine Learning based intrusion detection systems for connected autonomous vehicles: A survey	Jay NagarajanPegah MansourianMuhammad Anwar ShahidArunita JaekelIkjot SainiNing ZhangMarc Kneppers	2024	SpringerLink
36	False Data Injection Attack Detection in VANET Using Upgraded Grey Wolf Optimization Algorithm Using LSTM Classifier	M. S. Bennet PrabaR. Rathna	2024	SpringerLink

37	Enhanced Dragonfly-Based Secure Intelligent Vehicular System in Fog via Deep Learning	Anshu DeviRamesh KaitVirender Ranga	2024	SpringerLink
38	Physical Layer Parameters for Jamming Attack Detection in VANETs: A Long Short Term Memory Approach	Yassin El JakaniAbdellah BoulouzSaid El Hachemy	2024	SpringerLink
39	A federated learning framework for cyberattack detection in vehicular sensor networks	Maha DrissIman AlmomaniZil e HumaJawad Ahmad	2024	SpringerLink
40	Fuzzy and Deep Belief Network Based Malicious Vehicle Identification and Trust Recommendation Framework in VANETs	Kuldeep Narayan TripathiAshish Mohan YadavS. C. Sharma	2024	SpringerLink
41	Intrusion Detection for Vehicular Ad Hoc Network Based on Deep Belief Network	Rasika S. VitalkarSamrat S. ThoratDinesh V. Rojatkar	2024	SpringerLink
42	Sybil attack detection and secure data transmission in VANET using CMEHA-DNN and MD5-ECC	Nitha C. VelayudhanA. AnithaMukesh Madanan	2024	SpringerLink
43	Deep Learning Approaches for IoV Applications and Services	Lina Elmoiz AlatabaniElmustafa Sayed AliRashid A. Saeed	2024	SpringerLink
44	Intrusion Detection Technology of Internet of Vehicles Based on Deep Learning	Rongxia Wang	2024	SpringerLink
45	DeepSecDrive: An explainable deep learning framework for real-time detection of cyberattack in in-vehicle networks	Ding, Weiping; Alrashdi, Ibrahim; Hawash, Hossam; Abdel-Basset, Mohamed	2024	ScienceDirect
46	A deep learning technique to detect distributed denial of service attacks in software-defined networks	Gadallah, Waheed G.; Ibrahim, Hosny M.; Omar, Nagwa M.	2024	ScienceDirect
47	Dense capsule stacked auto-encoder model based DDoS attack detection and hybrid optimal bandwidth allocation with routing in VANET environment	Tanati, Murali Krishna; Ponnusamy, Manimaran	2025	ScienceDirect
48	Enhancing security in vanets: Adaptive Bald Eagle Search Optimization based multi-agent deep Q neural network for Sybil attack detection	Ajin, M.; Shaji, R. S.	2025	ScienceDirect

49	A distributed intrusion detection framework for vehicular Ad Hoc networks via federated learning and Blockchain	Mansouri, Fedwa; Tarhouni, Mounira; Alaya, Bechir; Zidi, Salah	2025	ScienceDirect
50	A deep learning approach to secure vehicle to road side unit communications in intelligent transportation system	Wu, Yun; Wu, Liangshun; Cai, Hengjin	2025	ScienceDirect
51	Detection and mitigation of distributed denial of service attacks in vehicular ad hoc network using a spatiotemporal deep learning and reinforcement learning approach	Jayakrishna, Naramalli; Prasanth, N. Narayanan	2025	ScienceDirect
52	A reputation mechanism based Deep Reinforcement Learning and blockchain to suppress selfish node attack motivation in Vehicular Ad-Hoc Network	Zhang, Bowei; Wang, Xiaoliang; Xie, Ru; Li, Chuncao; Zhang, Huazheng; Jiang, Frank	2025	ScienceDirect
53	A deep learning based misbehavior classification scheme for intrusion detection in cooperative intelligent transportation systems	Alladi, Tejasvi; Kohli, Varun; Chamola, Vinay; Yu, F. Richard	2025	ScienceDirect
54	An authentication approach in SDN-VANET architecture with Rider-Sea Lion optimized neural network for intrusion detection	kumar Pulligilla, Manoj; Vanmathi, C.	2025	ScienceDirect
55	Vehicular network anomaly detection based on 2-step deep learning framework	Kushardianto, Nur Cahyono; Ribouh, Soheyb; El Hillali, Yassin; Tatkeu, Charles	2025	ScienceDirect
56	Detection of DDoS attacks in SDN-based VANET using optimized TabNet	Setitra, Mohamed Ali; Fan, Mingyu	2025	ScienceDirect
57	Intelligent defense strategies: Comprehensive attack detection in VANET with deep reinforcement learning	Sultana, Rukhsar; Grover, Jyoti; Tripathi, Meenakshi	2025	ScienceDirect
58	Detection of intrusions in clustered vehicle networks using invasive weed optimization using a deep wavelet neural networks	M.V.B. Murali Krishna, M.; Ananth, C. Anbu; Krishnaraj, N.	2025	ScienceDirect