Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science

www.elsevier.com/locate/procedia

7th International Conference Futuristic Trends in Networks and Computing Technologies(FTNCT07) held in Uttarakhand, India

# A Survey On Security And Privacy In Deep Learning In Vehicular Ad Hoc Networks: A Review

Nayla .F.Othman[a]*,Shavan Askar[b],Hawkar Asaad[c],Media Ibrahim[d]Diana Hussein[e]

[a,b,c,d,e]*Erbil Polytechnic University, Technical College of Engineering, Department of Information System,Iraq*

**Abstract**

Recent advancements in telecommunications and deep learning (DL) have enabled the development of vehicle applications to improve road safety and environmental conditions. Vehicular ad hoc networks (VANETs) are a promising technology for improving traffic safety and efficiency. However, VANETs are also vulnerable to various security and privacy threats. Deep learning (DL) has the potential to address these challenges by providing new and innovative solutions for intrusion detection, authentication, authorization, privacy-preserving communication, and anomalous behavior detection. This paper reviews the state-of-the-art DL-based security and privacy solutions for VANETs. It also discusses the open challenges and future directions in this area. This study reviews papers published from 2015 (early publications on Deep Learning and VANETs) to 2023. This paper is a review of the latest works and techniques done in the field with the future trends and problems in security and privacy in deep learning vehicular ad hoc networks.



*Keywords:* Deep learning (DL); Vehicular ad hoc networks (VANET); Security; Networks.

## 1. Introduction

This section briefly introduces VANETs and DL. This review describes the characteristics of VANET security and thoroughly examines most of the challenges related to VANET security, along with the solutions that are currently available. By improving traffic flow, VANETs contribute to safer travel and fewer automobile accidents. Nevertheless, the modification of data in real-time may compromise security. The correct operation of the system needs to safeguard this information, for users' safety and trust. In VANETs, information is transmitted using wireless communication channels that are publicly accessible. The issue of security is of paramount significance in the context of VANETs[1]. The primary objective of VANET is to enhance driving safety and significantly reduce the occurrence of automobile accidents. The registration and administration processes are contingent upon specific agencies, namely roadside units

Corresponding author.
*E-mail address: Naila.othman@epu.edu.iq*

(RSUs) and on-board units (OBUs). To offer specialized services, Roadside Units (RSUs) are strategically distributed along the perimeters of roadways, while On-Board Units (OBUs) are installed within vehicles through the utilization of VANETs [2] [3]. VANETs possess several notable attributes, such as the presence of agile nodes, inherent self-organization capabilities, the existence of dispersed networks, and frequently fluctuating topologies. Despite recent advancements in VANETs, the issues surrounding attack prevention remain a subject of ongoing debate. Consequently, security, data integrity, and the protection of user private information remain significant concerns in this context[4]. The mitigation of security concerns can be effectively addressed through the utilization of machine learning and artificial intelligence inside road transport networks[5]. In addition, using DL in this field has played a significant role.
DL processes high-dimensional data effectively. Data that enable more precise detection. As stated by the writers who have used DL to choose the best path based on actively avoiding blackhole nodes. The fitness function values and accelerates the optimization process, which lowers latency and improves network functionality. Furthermore, given that DL is among the compact mapping functions, the skilled DL can determine how the input and output data relate to one another without extra procedures. It can therefore be modified to determine whether the subsequent node is a blackhole. strike the node or not. To maximize fitness values, an iteration-based technique is typically utilized [6].DSRC offers cost-effectiveness and a centralized communication system, hence presenting distinct advantages in inter-vehicle communication. The Dedicated Short-Range Communications (DSRC) technology has the potential to effectively cater to the need for the swift advancement in automotive network systems. However, given the characteristics of a vehicle node that exhibits rapid movement, irregular distribution, and continuous changes in network architecture, it is not feasible to employ V2V and V2I communication for comprehending the transmission of Intelligent Transportation Systems (ITS)[7]. As a result, nodes that require connection can establish a quick and inexpensive communication network. Numerous issues have been brought about by the extensive use of these networks and the rise in their node count. Among these issues are data transfer, traffic management, and routing. The mobility of several nodes in these networks has caused a rapid change in topology, which has pushed the quest for quicker and more effective fixes[8]. Various intrusion detection systems (IDSs) have been developed to safeguard VANET communications to address security problems. Different IDS architectures are available for automobiles in VANET, and they should be lightweight to satisfy the needs of intelligent monitoring in distributed systems[9]. The remaining review orders are as follows; section two explains the literature of the review paper, section three talks about the background and architectural communication of VANETS, section four goes over the security and privacy challenges in VANETS, section five explains the solutions to security and privacy problems of VANETS using DL, and finally section six concludes the review paper. In this paper, we aimed to find a balance between the approaches of these papers to get the best possible results. The models would leverage the advantages of the new transformer architecture for better prediction quality. As it was demonstrated, the first approach is focusing mainly on a bimodal architecture that takes into account video and audio inputs. In our approach, the videos for the training should showcase the facial expressions of the participants to get more precise predictions. Then, the architecture would need to include a scoring system to give the final output.

## 2. Literature Review

The literature used for the review paper comprises some research papers that elucidate the security and privacy aspects of DL VANETs. These papers were selected through an extensive search. This study is categorized by the year of publication. In 2016 performed investigations on these systems on the security risks and challenges associated with VANETs. from examined the key features of VANETs, including their design, security requirements, types of attackers, and potential assaults that can occur within VANETs [10]. In 2017, an in-depth analysis was given of the potential security risks that may emerge in vehicular network scenarios. An exhaustive compilation of the security obstacles encountered by VANETs is also provided. One of the challenges it would encounter. The implementation of alternative security solutions in VANETs is another area of inquiry. Security issue tendencies in vehicular networks; function as a reference for defining specific research topics[11]. A new RSU Deployment Problem Model (RDPM) was constructed in 2018 that integrated a profit model and road network. Proposed was a technique based on genetic algorithms that, in simulations, performed better than the conventional BEH method.[12].In 2019 research on these systems provided a detailed description of intelligent transportation system ITS and its progression to VANETs. have been describing VANETs, privacy and security assaults, and their uses and challenges. Architecture, privacy, and security challenges affect VANET and cloud computing efficacy. Each network layer's communication protocols and relevant attacks were analyzed—the benefits of the proposed VANET, application, and challenge methodologies.[13]. In 2020 The integration of two algorithms enabled the efficient detection of intrusive behavior and the learning of vehicle boundary behavior. By utilizing authentic vehicle data and

employing self-iterative parameter updates, the model successfully detected anomalous behavior with an almost 96% success rate [14].In 2021 Deep neural networks (DNNs) are the foundation of VANETs, which employ a sequence reconstruction and thresholding algorithm. Roadside deployment of DNN architectures constitutes this framework. The receiver units (RSUs) of the transmitted vehicular data execute anomaly detection duties to categorize a specific message. sequence as authentic or anomalous. [15].In 2023 The field study demonstrated encouraging outcomes across multiple performance parameters, showcasing the potential of this technique in effectively assuring the safety of both passengers and drivers[16].In 2023 the 5G technology can efficiently route Emergency Safety Messages (ESMs) in the Internet of Vehicles (IoV) to prevent vehicle accidents. The Software-Defined Networking-based Collision Avoidance to achieve this goal. The SDNCA architecture has three main algorithms: Estimating risk severity Calculating QoS and Allocating Resources Scheduling and configuring ESM Schedule and configure ESM[17]. In 2023 the low-latency feature of 5G technology is important, especially in V2I communication for reliable and timely ESM transfer. Handling link and packet losses in 5G-V2X communication with D2D communication. Bayesian rule-based fuzzy logic and stable matching algorithms have been used to select QoS-enhancing forwarders. Other solutions include leveraging SDN and MEC to control ESM dissemination, regulating ESM transmitting rates depending on risk distances between cars, and federating k-means algorithms to cluster vehicles in SDN for efficient ESM transmission[18]. In 2023 an analysis of vehicular network clustering methods, techniques, and scenarios to improve clustering. The paper is divided into important sections on vehicular network clustering. Scott's technique may predict clusters for some highways, although complex layouts may not function as well. The claims that vehRxdBm, a communication-based metric, would have been better in such cases. The creating of a baseline for vehicular clustering is problematic due to data and dynamic differences[19][20]. In 2021VANETs are essential for traffic control, passenger safety, and travel convenience. VANETs and SDN are becoming key enablers of 5G technologies. This evaluation and overview of the publications considers their goals, challenges, and results[21].

## 3. Methodology

Vehicular ad hoc networks (VANETs) are a subset of mobile ad hoc networks (MANETs) wherein automobiles establish communication with one another in the absence of a permanent infrastructure. VANETs possess the capacity to significantly transform the field of transportation through the provision of a diverse range of applications for safety, traffic efficiency, and infotainment.

### *3.1. VANET Architecture and Communication Protocols*

The Internet of Vehicles uses a newly discovered generation of mobile communication technology to create a full-scale vehicle-to-person, vehicle-to-vehicle, vehicle-to-road, and vehicle-to-service platform network. Increasing automotive intelligence and self-driving capabilities created a new automotive and transportation service model. It improves traffic efficiency and car driving experience to offer intelligent, comfortable, safe, energy-saving, and efficient comprehensive services. Internet of Vehicles communication topology is presented in Fig. 1[22].

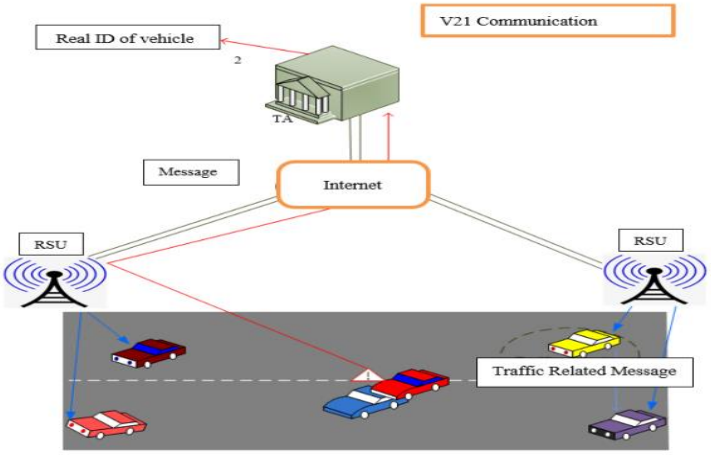


Fig. 1. Vehicle Architecture Design In VANET [22]

The major communication elements for road communication are the Road Side Unit (RSU), linked vehicles, pedestrians, and traffic authorities. In intelligent connected automobiles, components like the Telematic Box (T-Box), Electronic Control Units (ECU), and GPS aid in connection with other organizations. An intelligent connected vehicle uses the bus communication protocol to connect ECU nodes to form a bus network Fig. 2 simplifies the intelligent network communication schematic diagram, not only is ECU the core of vehicle communication but vital to in-vehicle communication. The node receives different bus messages to perform the command activity. ECU nodes must implement the bus to communicate Vehicle procedure, CAN is the most popular vehicle bus protocol, it's also an in-vehicle internal bus system standard that provides enough ECU communication data. A reliable and affordable vehicle network serial bus is the CAN bus. When ECU nodes compete to send data to the bus, the data frame priority domain determines the bus access control priority at this time. ECU nodes with low arbitration values will send messages first. Data and other nodes will compete again when the bus is idle[14].

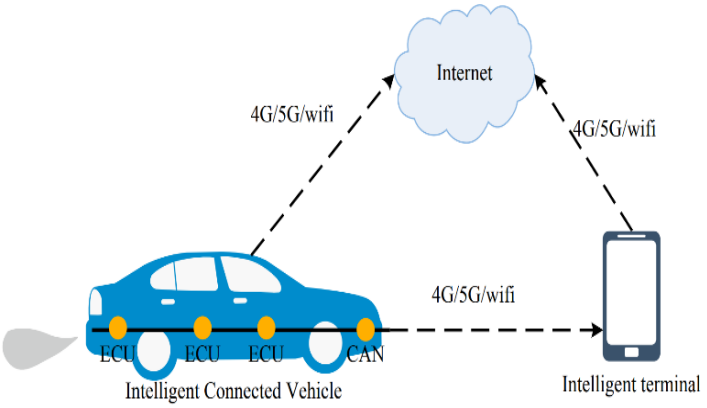


Fig. 2. ECU Nodes To Connect Bus Network [14]

### *3.2. Deep Learning Architectures and Algorithms*

A different domain within machine learning(ML), DL relies heavily on multilayer neural networks. Typically, a multilayer neural network comprises five to ten hidden layers shown in Fig 3. These layers are constructed through the learning of a deep nonlinear network structure, which enables the combination of low-level features into a higher-level representation that is more abstract and represents attribute categories or features. Neural networks contributed a significant role in numerous domains, including data fitting and object classification, through their robust self-learning and adaptability. Consider that there are DL employs numerous algorithms, including convolutional neural networks, recurrent neural networks, and extended short-term memory: deep Boltzmann machine, network, and Deep Belief Network. DL models employ numerous algorithms, whereas no single algorithm The network is deemed ideal. The exact algorithms are more suitable for carrying out particular [23].

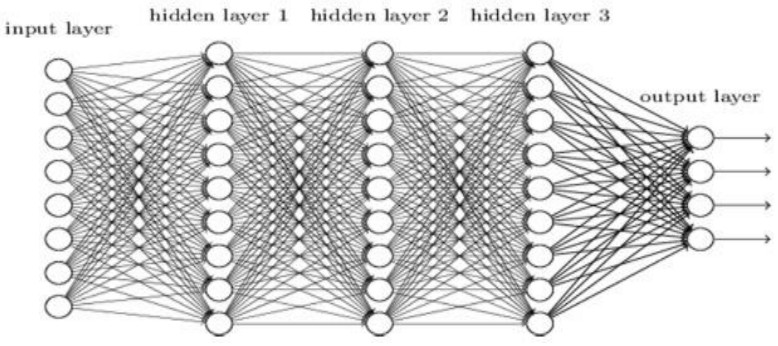


Fig. 3. Deep Learning Architectures [23]

## 4. Security and Privacy Challenges in VANETs

This section provides an analysis of the security and privacy concerns that are encountered in the context being discussed. VANET holds great potential as a technical innovation that can bring about substantial changes in the transportation industry. These networks offer a wide range of safety, traffic efficiency, and infotainment applications. However, it is important to note that VANETs have numerous security and privacy concerns.

### *4.1. Sybil Attacks*

Concerning security, in particular, the imminent VANET technology presents both promising opportunities and significant obstacles. Its high susceptibility to security assaults is attributed to its distributed network and dynamic topology. Diverse approaches to detecting community-wide network intrusions have been suggested by the researchers. Nevertheless, VANET remains susceptible to several attacks, most notably the Sybil vulnerability. Fig. 4 shows that consisting of forged identities within the network to disrupt communication between network nodes, the Sybil Attack is among the most difficult assaults in VANETS. Possibly causing traffic congestion, this assault has a significant impact on transportation safety services[24].

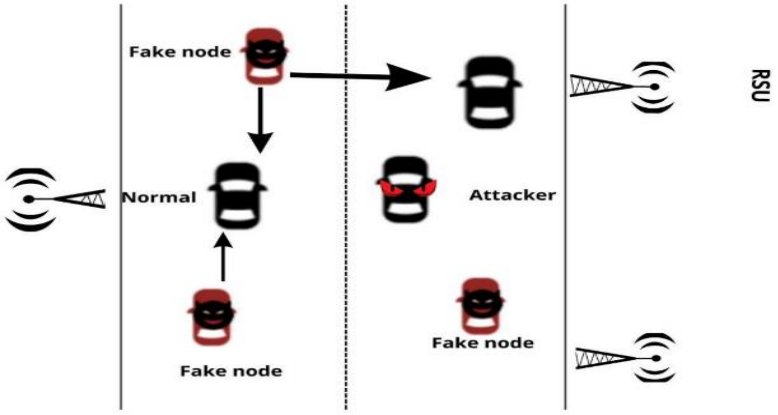


Fig. 1.Example Sybil Attacks [24]

### *4.2. Masquerade Attacks*

Masquerade attacks are regarded as one of the most dangerous in software-defined networks (SDN)VANETs. In such attacks, an unauthorized vehicle assumes the identity of more than a hundred vehicles through the use of numerous pseudonyms and confusion Fig 5. The purpose of this behavior is to deceive vehicles of varying types and request that they alter their itineraries. As the name suggests, disguise attacks involve a malicious vehicle assuming the identity of another vehicle in an attempt to deceive other vehicles by delivering bogus messages, modifying data, and replaying it[25].

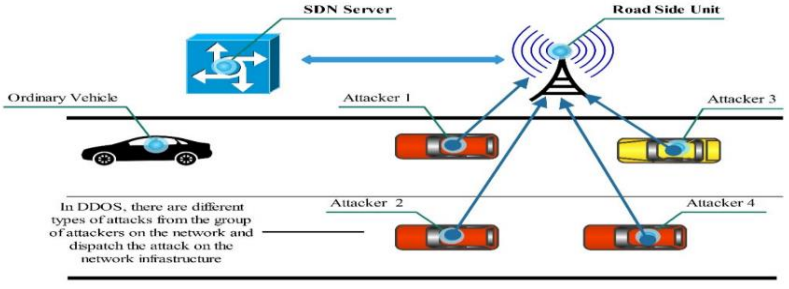


Fig. 2.Example Of Masquerade Attacks [25]

### 4.3. *Denial-of-service attacks*

DoS is used to slow down a network by introducing unnecessary traffic. The network is momentarily inaccessible or services of an internet-connected host are suspended. In a DoS attack, a malfunctioning node sends numerous unnecessary messages requesting network validation of requests with erroneous return addresses. When sending authentication approval, the network cannot search for the address of the defective node. This causes the network to maintain contact for longer before terminating it. When a network link is down, a defective node may send excessive messages with incorrect return addresses for authenticity. As a result, the server must wait for a lengthy period while the verification process is repeated, causing network delay to shut down[26]. A DoS attack is depicted below Fig. 6 depicts a DOS attack which shows a malicious vehicle closing the lane and stopping the RSU network [27].

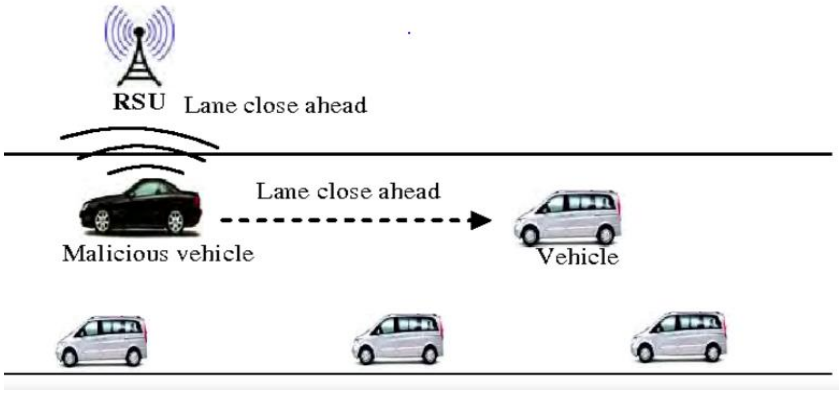


Fig.6.Denial-Of-Service Attacks [26]

### 4.4. *Message Tampering Attacks*

The dissemination of safety messages is a primary function of VANET. Users of VANET will receive safety-related alerts such as "Bump Ahead," "Traffic Congestion Details," "Blunish Turn Ahead," and "Decelerate Speed." The attacker will modify the message's content and deliver inaccurate information to the authorized recipient. Intruders may also modify non-safety application messages, such as those indicating the proximity of service stations, gas stations, hotels, and so forth. As shown in Fig 7, the gas station is near vehicle A. However, the assailant vehicle C will update the information and transmit the revised message that the petrol outlet is located 5 kilometers in the right-hand direction. This form of assault specifically targets the efficacy of VANET systems[27].

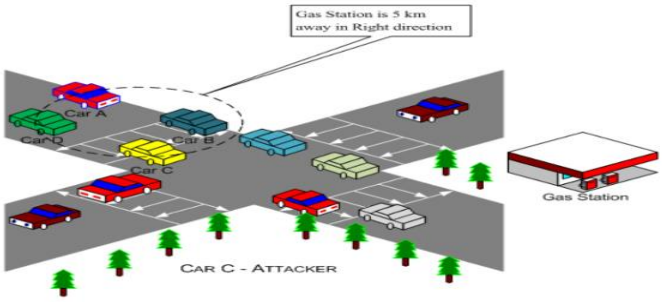


Fig.3.Message Tampering Attacks [27]

### 4.5. *Location Privacy Threats*

Another name for this type of attack is "position-faking attack." This form of attack involves an assailant attempting to alter the user's current geographic location and generate erroneous data from the GPS. The user

conceals his current whereabouts from the network and displays an incorrect position to others by employing this technique. The assault may be executed by an individual vehicle or a cluster of vehicles. Five vehicles are depicted in Fig 8 traversing Road ID-6; however, they are concealing their precise whereabouts and transmitting inaccurate data to the network. By obtaining such information, RSU could feign the absence of a vehicle on Road ID-6 at the moment[27].

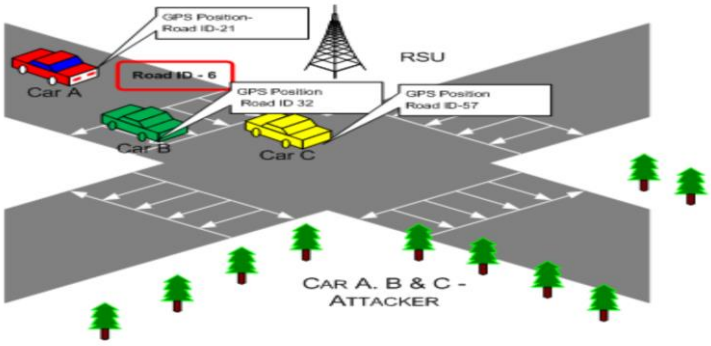


Fig.4.Location Privacy Threats [27]

## 5. Deep Learning for Security and Privacy in VANETs

This section reviews the following DL-based solutions for security and privacy in VANETs. DL-based solutions can also be used to protect the privacy of VANET users. For example, DL-based privacy protection mechanisms can be used to anonymize vehicle identifiers and other sensitive data before it is transmitted over the network. This can help to prevent attackers from tracking vehicles or identifying individual users. An Intrusion Detection System (IDS) that precisely identifies attacks with a minimal False Positive Rate (FPR). Moreover, the findings indicate that the framework could derive advantages from employing diverse algorithm types at various hierarchical levels. Specifically, employing more precise, accurate, and complex algorithms in nodes higher in the hierarchy would be preferable to selecting light and fast processing algorithms at lower levels, which may compromise accuracy[28]. An intrusion prevention system (IPS) refers to a network security apparatus that diligently observes and evaluates network traffic to identify any potentially malicious behavior, subsequently implementing measures to obstruct or alleviate the impact of such hazardous traffic. In practice, Intrusion Prevention Systems (IPSs) are commonly implemented alongside firewalls to augment the existing security measures. The phrase "intrusion detection and prevention system" (IDPS) is commonly employed to encompass both intrusion detection systems (IDS) and intrusion prevention systems (IPS), as they are frequently deployed in conjunction to offer a full security framework[29]. An IDS can detect VANET attacks. An (IDS) detects suspicious or anomalous network or host activity. It shows intrusion successes and failures. IDS is suggested for internal attack detection. Cryptographic solutions cannot detect these attacks. Indeed, infected nodes launch internal attacks. IDSs are commonly employed as a second defense following cryptographic systems. A typical intrusion detection system includes three phases: data gathering, analysis, and response to prevent or mitigate the attack. Monitor nodes contain IDS. How these nodes are deployed depends on the IDS protocol and architecture[30]. The IDS technique employs machine and DL approaches. The method being presented comprises two components, namely Known Intrusion Detection Systems (KIDS) and Unknown Intrusion Detection Systems(UIDS). The UIDS modules are capable of detecting both known and unknown entities—acts of aggression. The KIDS module employs a machine learning algorithm to identify and discern recognized harmful assaults. The Universal Identification System The module employs a DL algorithm to identify unfamiliar entities. The topic of discussion pertains to assaults in VANETs. The comprehensive algorithm or workflow of The illustrated Intrusion Detection System (IDS) for VANET is presented in Fig 9[31].

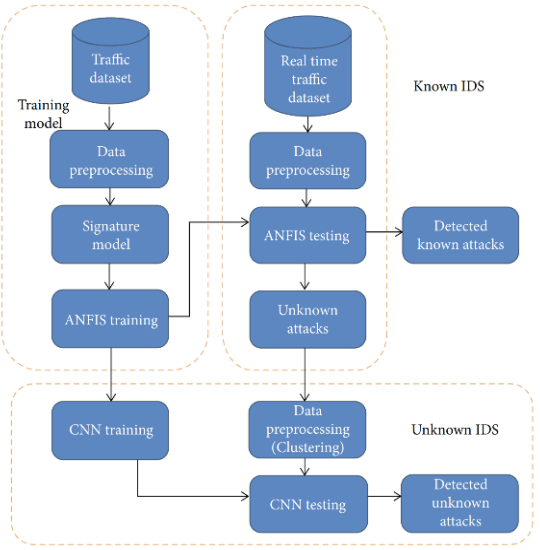


Fig.5.Hybrid Deep Learning Model For IDS In VANET [31]

As shown in Table 1. In the context of driver fingerprinting, it is of utmost importance to preserve the privacy of driver data and prevent adversaries from tracking the vehicle by linking it to the driver's identification. To enable this, DL techniques are used by researchers to authenticate the true identification and fingerprinting of a user/driver to make vehicles resilient to theft without hiding the true identity of drivers. Also note that DL is the most widely used technique for driver fingerprinting, as shown in Table 1.

Table 1. Deep Learning Techniques Applied To Vehicular Security

| Author(s) | Title | Year | Learning Technique | Security Application |
|---|---|---|---|---|
| Alheeti, Khattab M Ali Gruebler, Anna Mcdonald-maier, KlausD [32] | An Intrusion Detection System Against Black Hole Attacks on the Communication Network of Self-Driving Cars | 2015 | Deep learning | detect black hole attacks |
| Kwak, Byung Il Kim, Huy Kang[33] | Know Your Master: Driver Profiling-based Anti-theft Method | 2016 | Deep learning | Driver fingerprinting, passwords. |
| Dong, Weishan [34] | Characterizing Driving Styles with Deep Learning | 2017 | Deep learning | Driving style feature learning directly from GPS data. |
| Loukas, George Vuong, Tuan Heartfield, Ryan Sakellari, Georgia Yoon, Yongpil Gan, Diane [35] | Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning | 2018 | Deep learning | Intrusion detection system (IDS) |
| Askar, Shavan Jameel Hamad, Zhala Wahhab Kareem, Shahab [36] | Deep Learning and Fog Computing: A Review | 2021 | Deep learning | DDoS attacks |

| | | | | |
|---|---|---|---|---|
| Jeong, Daun<br>Kim, Minseok<br>Kim, Kyungtaek<br>Kim, Taewang<br>Jin, Jihun<br>Lee, Chungsu[37] | Real-time Driver Identification using Vehicular Big Data and Deep Learning | 2018 | Deep learning | real-time driver detection |
| Tangade, Shrikant [38] | A Deep Learning Based Driver Classification and Trust Computation in VANETs | 2019 | Deep learning | driver classification and trust computation (DL-DCTC) |
| Rasheed, Iftikhar<br>Hu, Fei<br>Zhang, Lin[39] | Deep reinforcement learning approach for autonomous vehicle systems for maintaining security and safety using LSTM-GAN | 2020 | Deep learning | Data manipulation attack detection |
| Wang, Tian<br>Cao, Zhihan<br>Wang, Shuo<br>Wang, Jian Huang<br>Qi, Lianyong<br>Liu, Anfeng<br>Xie, Mande<br>Li, Xiaolong [40] | Privacy-Enhanced Data Collection Based on Deep Learning for Internet of Vehicles | 2019 | Deep learning,<br>Federated learning | The protection of user privacy |
| Jiang, Yanna<br>Ma, Baihe<br>Wang, Xu<br>Yu, Ping<br>Yu, Guangsheng<br>Wang, Zhe<br>Ni, Wei<br>Liu, Ren Ping[41] | Block chained Federated Learning for Internet of Things: A Comprehensive Survey | 2023 | Federated learning | Privacy protection |
| Lu, Yunlong<br>Huang, Xiaohong<br>Dai, Yueyue<br>Maharjan, Sabita<br>Zhang, Yan [42] | Federated Learning for Data Privacy Preservation in Vehicular Cyber-Physical Systems | 2020 | Federated learning | Privacy protection and safety of vehicles |
| Tariq, Shahroz<br>Lee, Sangyup<br>Woo, Simon [43] | CANTransfer – Transfer Learning based Intrusion Detection on a Controller Area Network using Convolutional LSTM Network | 2020 | Transfer learning | Intrusion detection system (IDS) |
| Lu, Xiaozhen<br>Xiao, Liang<br>Member, Senior<br>Xu, Tangwei<br>Zhao, Yifeng<br>Tang, Yuliang[44] | Reinforcement Learning Based PHY Authentication for VANETs | 2020 | Transfer learning | spoofing signals to attack VANETs. |

| | | | | |
|---|---|---|---|---|
| Li, Xinghua<br>Hu, Zhongyuan<br>Xu, Mengfan<br>Wang, Yunwei<br>Ma, Jianfeng [45] | Transfer Learning-based Intrusion Detection Scheme for Internet of Vehicles | 2021 | Transfer learning | Intrusion detection systems (IDS) |
| Dezheen H. Abdulazeez and Shavan K. Askar[46] | A Novel Offloading Mechanism Leveraging Fuzzy Logic and Deep Reinforcement Learning to Improve IoT Application Performance in a Three-Layer Architecture Within the Fog-Cloud Environment | 2023 | Deep Reinforcement Learning, Fuzzy Logic | IoT and fog computing |
| Media Ali Ibrahim and Shavan Askar[47] | An Intelligent Scheduling Strategy in Fog Computing System Based on Multi-Objective Deep Reinforcement Learning Algorithm | 2023 | Multi-Objective Deep Reinforcement Learning (MODRL) | Scheduling in fog computing |

### *5.1. Authentication and Authorization Protocols*

The identification and communication of a legitimate user is a crucial concern in the context of VANET. The privacy of a car is an additional significant concern. In an open location, an assailant can engage in eavesdropping on the communication that occurs between automobiles. The establishment of authenticated communication has emerged as a fundamental necessity within the realm of VANET[48]. Nonetheless, the process of authenticating has the potential to expose sensitive personal data, including the user's identity and location. Consequently, it becomes imperative to safeguard the privacy of an honest user. To address this concern, an authentication protocol that incorporates conditional privacy preservation measures can be used to bolster the security of the VANET. The majority of existing protocols employ either pseudonym-based methods with certificate revocation lists (CRL), which result in substantial communication and storage burdens, or group signature-based methods that are computationally demanding Hence, the disclosure of such information could potentially compromise the user's privacy. The objective is to verify the identity of a user while ensuring the preservation of their privacy. In the event of a malevolent action, Once detection occurs, the technique should possess the capability to accurately identify the malevolent user[49].

### *5.2. Privacy-Preserving Communication Scheme*

The proposed communication technique, known as the VANET-based privacy-preserving communication scheme (VPPCS), is a secure VANET-based system that aims to preserve privacy. The suggested approach employs signatures for identity verification that are based on pseudonyms. Furthermore, the utilization of batch verification is employed to enhance the computational efficiency of the technique. The act of introducing counterfeit messages into a broadcast, hence creating ambiguity for the attacker in determining the authenticity of the sent message. The proposed Virtual Private Pseudonym Communication System (VPPCS) utilizes a predetermined set of pseudonyms to digitally sign the message, hence rendering the attacker incapable of discerning the true origin of the communication. A thorough examination of security and privacy is conducted to illustrate the resilience of the proposed scheme against different types of assaults and to meet the security and privacy criteria of the Vehicular Ad hoc Network (VANET). This paper presents a comprehensive security analysis of the proposed VPPCS system, employing BAN logic, the random oracle model, security of proof, and security attributes. The research reveals that the VPPCS system is resilient against a range of attacks, including replay attacks, impersonation attacks, modification attacks, and man-in-the-middle attacks[50].

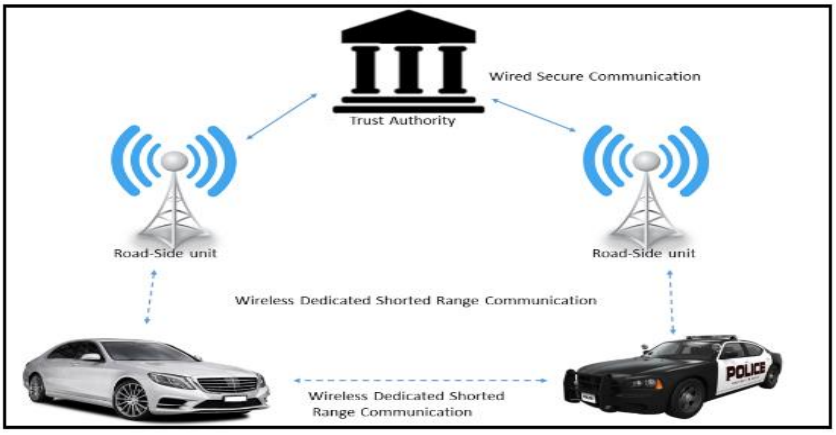


Fig.6. Example Privacy-Preserving Communication Scheme [50]

### 5.3. *Anomalous Behavior Detection Systems* to thank

The notion of distributed ensemble learning. In this context, vehicles employ the random forest algorithm to independently train local intrusion detection system (IDS) classifiers. These locally trained classifiers are then shared with other vehicles as needed, resulting in a reduction of communication overhead. Upon reception, the performance of the classifiers is assessed by utilizing the local testing dataset within the receiving vehicle. The evaluation values serve as a metric of trustworthiness and are utilized to establish a ranking among the received classifiers. Classifiers that exhibit significant deviation from the lower boundary of the box-and-whisker plot are deemed ineligible for inclusion in the collection of collaborators. Subsequently, every individual vehicle generates a collection of weighted random forest classifiers that incorporate both the classifiers trained locally and those trained remotely. A robust weighted voting mechanism is employed to aggregate the outputs of the classifiers[51].

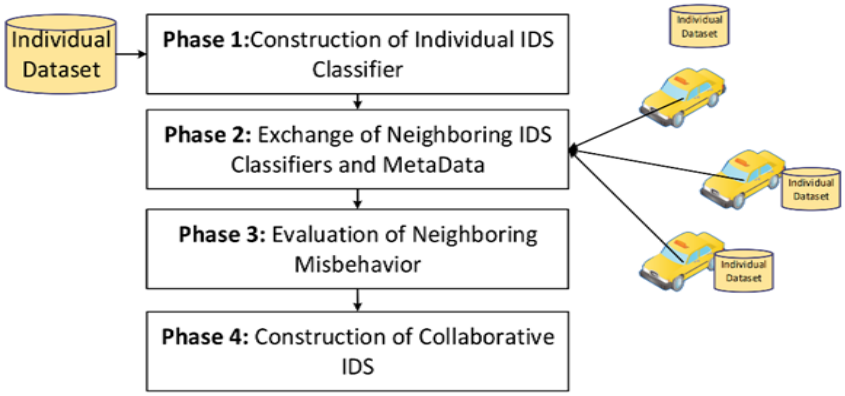


Fig. 7. Example Anomalous Behavior Detection Systems[51]

### 5.4. *Evolution of Deep Learning-Based VANETs Technology*

Several detection approaches based on DL models have been developed in the literature by the research community to protect VANETs from various cyber-attacks. This section contains an understanding development of this technology, highlighting the primary evolution from one work to the next for the most relevant and recent investigations. Machine learning and DL use in vehicular networks is gaining significant attention to address multiple challenges. Several survey works exist in the literature that cover different security problems in vehicular networks and discuss challenges with solutions proposed in the literature.

Table 2 summarizes and analyzes the works under consideration from several perspectives.

| Author(s) | Focused Area | Type of Network | ML & DL context | Service | Algorithms | Security Requirements |
|---|---|---|---|---|---|---|
| Nova, Kannan A, Umaamaheshvari Jacob, Suma Sira Banu, G. Balaji, M. Sundar Prakash S, Srithar[4] | Security and Privacy | VANET | No | Detection mechanism | No | Integrity |
| Arif, Muhammad Wang, Guojun Zakirul Alam Bhuiyan, Md Wang, Tian Chen, Jianer[13] | Security and Privacy in VANET Applications | VANET | Limited | Detection | No | accessibility of ubiquitous availability |
| Member, Wang Tong Hussain, Azhar Bo, Wang X I[52] | Safety, Congestion, Demand and Supply Applications, Navigations, Security and Vehicle Platoons | VANET and IoV | ML& DL | Detection | AI Algorithms | Integration |
| Hossain, Mohammad Asif Noor, Rafidah Yau, Kok-lim Alvin[53] | Cognitive Radio-based Vehicular Applications | Vehicular Networks and all of its Variants | ML& DL | Detection | ML Algorithms | integrated with CR-VANET |
| Liu, Xiao-yang[54] | Autonomous Driving, Energy Management, Road Control and other Applications | ITS | DRL | Detection | Deep Q-Networks (DQN) | Availability |
| Sharma, Vishal You, Ilsun Andersson, Karl Palmieri, Francesco Rehmani, Mubashir Husain Lim, Jaedeok[55] | Security, Trust and Privacy in Mobile-IoT Applications | M-IoT | Limited | Prevention | No | security, privacy |
| Stoyanova, Maria Nikoloudakis, Yannis Panagiotakis, Spyridon Pallis, Evangelos Markakis, Evangelos K[56] | Security Attacks | IOT | Limited | Prevention | No | Secure the evidence integrity |
| Al-garadi, Mohammed AliMohamed, Amr Al-ali, Abdulla Du, Xiaojiang | Security Threats Types and Threats Surface | IOT | ML & DL | Detection | ML/DL to IoT Algorithms | Authentication, integrity nonrepudiation, |

| | | | | | | |
|---|---|---|---|---|---|---|
| Guizani, Mohsen[57] | | | | | | confidentiality availability and authorization |
| Hussain, Fatima Hussain, Rasheed Hassan, Syed Ali Hossain, Ekram Mar, C R[58] | Authentication and Security Attacks | IOT | ML & DL | Detection | ML & DL Algorithms | Authentication |
| Uprety, Aashma Rawat, Danda B Li, Jiang[59] | Perception, Networking, Computing and Security | Vehicular-IoT | Federated Learning | Detection | FL protocols and algorithms | Privacy, security & incentive, Collaborative Intelligence |
| Kuutti, Sampo Bowden, Richard Jin, Yaochu Barber, Phil Fallah, Saber[60] | Lateral and Longitudinal Vehicle Control System | Autonomous Vehicle Network | ML & DL | segmentation and object detection | ML & DL Algorithms | Availability |
| Askar, Shavan Aziz, Glena Rashid, Tarik A[61] | SDN Based VANET security and challenges | SDN-VANET | Not specified | Addressing security attacks | Not specified | Session hijacking, identity revealing, position tracking, eavesdropping, Denial of Service |
| Kosrat Dlshad Ahmed & Shavan Askar [62] | Cybersecurity in IoT networks; Deep learning models for cybersecurity | IoT Networks | Deep Learning (DL) | Improved user experience, privacy and security | MLP, CNN, LSTM, Hybrid of CNN and LSTM | Ensuring privacy and security |
| Dezheen H. Abdulazeez and Shavan K. Askar[46] | Task offloading in IoT applications | Fog-Cloud Computing Environment | Application performance optimization in IoT | Task offloading service | Fuzzy Logic-based Task Scheduler, Deep Q Network (DQN) | Secure task allocation and processing |
| Media Ali Ibrahim and Shavan Askar[47] | Task scheduling in fog computing | Fog Computing System | Resource management and task scheduling | Intelligent scheduling service | Multi-Objective Deep Reinforcement Learning (MODRL), DQN | Secure task processing and allocation |

## 6. Conclusion

This sums up everything that has been stated so far about the main points of the paper and highlights the potential of DL to improve security and privacy in VANETs. They hold countless potential as a technical revolution that can bring about considerable changes in the transportation business. These networks offer a wide range of safety, traffic efficiency, and infotainment applications. However, it is important to note that VANETs have numerous security and privacy concerns. By improving the security and privacy of VANETs the roads will be safer and more accident-free for drivers and pedestrians. All vehicles that use VANET have OBUs installed in the car which is connected to the RSUs alongside the roads. De technique helps VANET security and makes it stronger against hackers. Intrusion Detection System (IDS) precisely identifies attacks with a minimal False Positive Rate The Internet of Vehicles uses a recently revealed generation of mobile communication technology to generate a full-scale vehicle-to-person, vehicle-to-vehicle, vehicle-to-road, and vehicle-to-service podium system, ECU, and GPS help in linking with other establishments (VANETs) are a subset of mobile ad hoc networks (MANETs) where vehicles launch communication with one another in the absence of an everlasting organization.


## Acknowledgements

I want to thank my supervisor and the teachers at EPU for all the help and knowledge they gave me over the past few years. This paper is dedicated to my family for all the love, support, and encouragement that they gave me and have allowed me to do what I love. And lastly, I would also like to thank my friends that have helped me.


## References


[1] Z. Afzal and M. Kumar, "Security of Vehicular Ad-Hoc Networks (VANET): A survey," J. Phys. Conf. Ser., vol. 1427, no. 1, 2020, doi: 10.1088/1742-6596/1427/1/012015.

[2] H. A. Hassan, "Review Vehicular Ad hoc Networks Security Challenges and Future Technology," no. 1, pp. 1–14, 2022.

[3] F. A. Ghaleb, W. Ali, B. A. S. Al-Rimy, and S. J. Malebary, "Intelligent Proof-of-Trustworthiness-Based Secure Safety Message Dissemination Scheme for Vehicular Ad Hoc Networks Using Blockchain and Deep Learning Techniques," Mathematics, vol. 11, no. 7, 2023, doi: 10.3390/math11071704.

[4] K. Nova, U. A, S. S. Jacob, G. Banu, M. S. P. Balaji, and S. S, "Floyd–Warshalls algorithm and modified advanced encryption standard for secured communication in VANET," Meas. Sensors, vol. 27, no. March, p. 100796, 2023, doi: 10.1016/j.measen.2023.100796.

[5] M. H. Junejo, A. A. H. Ab Rahman, R. A. Shaikh, K. M. Yusof, D. Kumar, and I. Memon, "Lightweight Trust Model with Machine Learning scheme for secure privacy in VANET," Procedia Comput. Sci., vol. 194, pp. 45–59, 2021, doi: 10.1016/j.procs.2021.10.058.

[6] B. An, "Blackhole Attacks in VANETs †," pp. 1–28, 2023.

[7] K. Giridhar, C. Anbuananth, and N. Krishnaraj, "Energy efficient clustering with Heuristic optimization based Ro/uting protocol for VANETs," Meas. Sensors, vol. 27, no. January, p. 100745, 2023, doi: 10.1016/j.measen.2023.100745.

[8] S. MUTİ and E. E. ÜLKÜ, "A Review on Machine Learning Techniques Used in VANET and FANET Networks," Bilecik Şeyh Edebali Üniversitesi Fen Bilim. Derg., vol. 9, no. 2, pp. 1150–1165, 2022, doi: 10.35193/bseufbd.1102897.

[9] H. Bangui, M. Ge, and B. Buhnova, "A hybrid machine learning model for intrusion detection in VANET," Computing, vol. 104, no. 3, pp. 503–531, 2022, doi: 10.1007/s00607-021-01001-0.

[10] R. Mishra, A. Singh, and R. Kumar, "VANET security: Issues, challenges and solutions," Int. Conf. Electr. Electron. Optim. Tech. ICEEOT 2016, pp. 1050–1055, 2016, doi: 10.1109/ICEEOT.2016.7754846.

[11] A. M. S. Abdelgader, F. Shu, W. Zhu, and K. Ayoub, "Security challenges and trends in vehicular communications," Proc. - 2017 IEEE Conf. Syst. Process Control. ICSPC 2017, vol. 2018-Janua, no. December, pp. 105–110, 2017, doi: 10.1109/SPC.2017.8313030.

[12] Z. Gao, D. Chen, N. Yao, Z. Lu, and B. Chen, "A Novel Problem Model and Solution Scheme for Roadside Unit Deployment Problem in VANETs," Wirel. Pers. Commun., vol. 98, no. 1, pp. 651–663, 2018, doi: 10.1007/s11277-017-4888-6.

[13] M. Arif, G. Wang, M. Zakirul Alam Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," Veh. Commun., vol. 19, p. 100179, 2019, doi: 10.1016/j.vehcom.2019.100179.

[14] F. Li, J. Zhang, E. Szczerbicki, J. Song, R. Li, and R. Diao, "Deep learning-based intrusion system for vehicular ad hoc networks," Comput. Mater. Contin., vol. 65, no. 1, pp. 653–681, 2020, doi: 10.32604/cmc.2020.011264.

[15] T. Alladi, B. Gera, A. Agrawal, V. Chamola, and F. R. Yu, "Deepadv: A deep neural network framework for anomaly detection in vanets," IEEE Trans. Veh. Technol., vol. 70, no. 11, pp. 12013–12023, 2021, doi: 10.1109/TVT.2021.3113807.

[16] M. Thirumalaisamy and M. George, "Unlocking the Potential of VANETs : Trust-Based Authentication and Deep Learning for Enhanced Security and E ciency," 2023.

[17] D. H. Hussein and S. Askar, "Federated Learning Enabled SDN for Routing Emergency Safety Messages (ESMs) in IoV Under 5G Environment," IEEE Access, vol. 11, pp. 141723–141739, 2023, doi: 10.1109/ACCESS.2023.3343613.

[18] D. H. Abdulazeez and S. K. Askar, "Offloading Mechanisms Based on Reinforcement Learning and Deep Learning Algorithms in the Fog Computing Environment," IEEE Access, vol. 11, no. January, pp. 12554–12585, 2023, doi: 10.1109/ACCESS.2023.3241881.

[19] F. E. F. Samann and S. Askar, "Estimating The Optimal Cluster Number For Vehicular Network Using Scott's Formula," in 2022 4th International Conference on Advanced Science and Engineering (ICOASE), 2022, pp. 136–141. doi: 10.1109/ICOASE56293.2022.10075588.

[20] F. Samann and S. Askar, "Examining the Use of Scott's Formula and Link Expiration Time Metric for Vehicular Clustering," Comput. Model. Eng. Sci., vol. 138, no. 3, pp. 2421–2444, 2024, doi: 10.32604/cmes.2023.031265.

[21] S. Askar, G. Aziz, and T. A. Rashid, “SDN Based 5G VANET : A Review,” Int. J. Sci. Bus., vol. 5, no. 6, pp. 148–162, 2021, doi: 10.5281/zenodo.5221874.
[22] S. Sulthana and B. N. R. Manjunatha Reddy, “Machine learning algorithms for privacy preserving in vehicular ad hoc network,” Indones. J. Electr. Eng. Comput. Sci., vol. 30, no. 2, pp. 1021–1028, 2023, doi: 10.11591/ijeecs.v30.i2.pp1021-1028.
[23] R. S. Vitalkar, “A Review on Intrusion Detection System in Vehicular Ad- hoc Network Using Deep Learning Method,” Int. J. Res. Appl. Sci. Eng. Technol., vol. 8, no. 5, pp. 1591–1595, 2020, doi: 10.22214/ijraset.2020.5258.
[24] S. Azam, M. Bibi, R. Riaz, S. S. Rizvi, and S. J. Kwon, “Collaborative Learning Based Sybil Attack Detection in Vehicular AD-HOC Networks (VANETS),” Sensors, vol. 22, no. 18, 2022, doi: 10.3390/s22186934.
[25] M. Arif et al., “applied sciences and Challenges,” Appl. Sci., vol. 10, no. 9, 2020.
[26] D. Rampaul, “Detection of DoS Attack in VANETs,” Indian J. Sci. Technol., vol. 9, no. 1, pp. 1–6, 2016, doi: 10.17485/ijst/2016/v9i47/106865.
[27] A. N. Upadhyaya and J. Shah, “Attacks on VANET Security,” Int. J. Comput. Eng. Technol. (IJCET, vol. 9, no. 1, pp. 8–19, 2018.
[28] F. Gonçalves, J. Macedo, and A. Santos, “An intelligent hierachical security framework for vanets,” Inf., vol. 12, no. 11, 2021, doi: 10.3390/info12110455.
[29] H. G. Shahabi and S. Soni, “SECURITY AND PRIVACY CHALLENGES IN VEHICULAR AD-HOC NETWORKS : THREATS , COUNTERMEASURES,” vol. 8, no. 1, 2023.
[30] S. Sharma and A. Kaul, “A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud,” Veh. Commun., vol. 12, no. April, pp. 138–164, 2018, doi: 10.1016/j.vehcom.2018.04.005.
[31] B. Karthiga, D. Durairaj, N. Nawaz, T. K. Venkatasamy, G. Ramasamy, and A. Hariharasudan, “Intelligent Intrusion Detection System for VANET Using Machine Learning and Deep Learning Approaches,” Wirel. Commun. Mob. Comput., vol. 2022, 2022, doi: 10.1155/2022/5069104.
[32] K. M. A. Alheeti, A. Gruebler, and K. D. Mcdonald-maier, “An Intrusion Detection System Against Black Hole Attacks on the Communication Network of Self-Driving Cars,” 2015, doi: 10.1109/EST.2015.10.
[33] B. Il Kwak and H. K. Kim, “Know Your Master : Driver Profiling-based Anti-theft Method”.
[34] W. Dong, “Characterizing Driving Styles with Deep Learning”.
[35] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, “Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning,” pp. 3491–3508, 2018.
[36] S. Askar, Z. Jameel Hamad, and S. Wahhab Kareem, “Deep Learning and Fog Computing: A Review,” Papers.Ssrn.Com, pp. 197–208, 2021, doi: 10.5281/zenodo.5222647.
[37] D. Jeong, M. Kim, K. Kim, T. Kim, J. Jin, and C. Lee, “Real-time Driver Identification using Vehicular Big Data and Deep Learning,” pp. 123–130, 2018.
[38] S. Tangade, “A Deep Learning Based Driver Classification and Trust Computation in VANETs,” 2019 IEEE 90th Veh. Technol. Conf., pp. 1–6, 2019.
[39] I. Rasheed, F. Hu, and L. Zhang, “Deep reinforcement learning approach for autonomous vehicle systems for maintaining security and safety using LSTM-GAN,” Veh. Commun., vol. 1, p. 100266, 2020, doi: 10.1016/j.vehcom.2020.100266.
[40] T. Wang et al., “Privacy-Enhanced Data Collection Based on Deep Learning for Internet of Vehicles,” IEEE Trans. Ind. Informatics, vol. PP, no. 8, p. 1, 2019, doi: 10.1109/TII.2019.2962844.
[41] Y. Jiang et al., “Blockchained Federated Learning for Internet of Things: A Comprehensive Survey,” vol. 1, no. 1, pp. 1–30, 2023.
[42] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, “CYBER SECURITY BASED ON ARTIFICIAL INTELLIGENCE FOR CYBER-PHYSICAL SYSTEMS Federated Learning for Data Privacy Preservation in Vehicular Cyber-Physical Systems,” no. June, pp. 50–56, 2020.
[43] S. Tariq, S. Lee, and S. S. Woo, “CANTransfer – Transfer Learning based Intrusion Detection on a Controller Area Network using Convolutional LSTM Network,” pp. 1048–1055, 1985.
[44] X. Lu, L. Xiao, S. Member, T. Xu, Y. Zhao, and Y. Tang, “Reinforcement Learning Based PHY Authentication for VANETs,” vol. 9545, no. c, pp. 1–13, 2020, doi: 10.1109/TVT.2020.2967026.
[45] X. Li, Z. Hu, M. Xu, Y. Wang, and J. Ma, “Transfer Learning based Intrusion Detection Scheme for Internet of Vehicles,” Inf. Sci. (Ny)., 2020, doi: 10.1016/j.ins.2020.05.130.
[46] D. H. Abdulazeez and S. K. Askar, “A Novel Offloading Mechanism Leveraging Fuzzy Logic and Deep Reinforcement Learning to Improve IoT Application Performance in a Three-Layer Architecture within the Fog-Cloud Environment,” IEEE Access, vol. 12, no. March, pp. 39936–39952, 2024, doi: 10.1109/ACCESS.2024.3376670.
[47] M. A. Ibrahim and S. Askar, “An Intelligent Scheduling Strategy in Fog Computing System Based on Multi-Objective Deep Reinforcement Learning Algorithm,” IEEE Access, vol. 11, no. November, pp. 133607–133622, 2023, doi: 10.1109/ACCESS.2023.3337034.
[48] U. Rajput, F. Abbas, H. Eun, R. Hussain, and H. Oh, “A two level privacy preserving pseudonymous authentication protocol for VANET,” 2015 IEEE 11th Int. Conf. Wirel. Mob. Comput. Netw. Commun. WiMob 2015, pp. 643–650, 2015, doi: 10.1109/WiMOB.2015.7348023.
[49] U. Rajput, F. Abbas, and H. Oh, “A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET,” IEEE Access, vol. 4, no. XX, pp. 7770–7784, 2016, doi: 10.1109/ACCESS.2016.2620999.
[50] M. A. Al-Shareeda, M. Anbar, S. Manickam, and A. A. Yassin, “VPPCS: VANET-Based Privacy-Preserving Communication Scheme,” IEEE Access, vol. 8, pp. 150914–150928, 2020, doi: 10.1109/ACCESS.2020.3017018.
[51] F. A. Ghaleb et al., “Misbehavior-aware on-demand collaborative intrusion detection system using distributed ensemble learning for VANET,” Electron., vol. 9, no. 9, pp. 1–17, 2020, doi: 10.3390/electronics9091411.
[52] W. T. Member, A. Hussain, and W. X. I. Bo, “Artificial Intelligence for Vehicle-to-Everything : a Survey,” IEEE Access, vol. PP, no. c, p. 1, 2019, doi: 10.1109/ACCESS.2019.2891073.
[53] M. A. Hossain, R. Noor, and K. A. Yau, “Comprehensive Survey of Machine Learning Approaches in Cognitive Radio-based Vehicular Ad Hoc Networks,” no. May, 2020, doi: 10.1109/ACCESS.2020.2989870.
[54] X. Liu, “Transportation Systems,” no. Nips, 2018.
[55] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, “Security , Privacy and Trust for Smart Mobile-Internet of Things ( M-IoT ): A Survey”.
[56] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, “A Survey on the Internet of Things ( IoT ) Forensics : Challenges , Approaches and Open Issues,” IEEE Commun. Surv. Tutorials, vol. PP, p. 1, 2019, doi: 10.1109/COMST.2019.2962586.
[57] M. A. Al-garadi, A. Mohamed, A. Al-ali, X. Du, and M. Guizani, “A Survey of Machine and Deep Learning Methods for Internet of Things ( IoT ) Security,” pp. 1–42, 2020.

[58] F. Hussain, R. Hussain, S. A. Hassan, E. Hossain, and C. R. Mar, "Machine Learning in IoT Security : Current Solutions and Future Challenges," pp. 1–23.
[59] A. Uprety, D. B. Rawat, and J. Li, "Privacy Preserving Misbehavior Detection in IoV using Federated Machine Learning," pp. 1–6, 2021.
[60] S. Kuutti, R. Bowden, Y. Jin, P. Barber, and S. Fallah, "Autonomous Vehicle Control," pp. 1–23.
[61] G. Aziz and S. Askar, "Software Defined Network Based VANET," Int. J. Sci. Bus., vol. 5, no. 3, pp. 83–91, 2021, doi: 10.5281/zenodo.4497640.
[62] K. D. A. & S. Askar, "Deep Learning Models for Cyber Security in IoT Networks: A Review," Int. J. Sci. Bus., vol. 5, no. 3, pp. 2588–2593, 2021