Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.066306

REVIEW

A Comprehensive Survey of Deep Learning for Authentication in Vehicular Communication

Tarak Nandy[1,*] **and Sananda Bhattacharyya**[2]

[1]Institute of Computer Science and Digital Innovation (ICSDI), UCSI University, Kuala Lumpur, 56000, Malaysia
[2]Department of Information Technology, Maldives Business School, Malé, 20175, Maldives

*Corresponding Author: Tarak Nandy. Email: tarak@ucsiuniversity.edu.my

Received: 04 April 2025; Accepted: 04 July 2025; Published: 29 August 2025

ABSTRACT: In the rapidly evolving landscape of intelligent transportation systems, the security and authenticity of vehicular communication have emerged as critical challenges. As vehicles become increasingly interconnected, the need for robust authentication mechanisms to safeguard against cyber threats and ensure trust in an autonomous ecosystem becomes essential. On the other hand, using intelligence in the authentication system is a significant attraction. While existing surveys broadly address vehicular security, a critical gap remains in the systematic exploration of Deep Learning (DL)-based authentication methods tailored to these communication paradigms. This survey fills that gap by offering a comprehensive analysis of DL techniques—including supervised, unsupervised, reinforcement, and hybrid learning—for vehicular authentication. This survey highlights novel contributions, such as a taxonomy of DL-driven authentication protocols, real-world case studies, and a critical evaluation of scalability and privacy-preserving techniques. Additionally, this paper identifies unresolved challenges, such as adversarial resilience and real-time processing constraints, and proposes actionable future directions, including lightweight model optimization and blockchain integration. By grounding the discussion in concrete applications, such as biometric authentication for driver safety and adaptive key management for infrastructure security, this survey bridges theoretical advancements with practical deployment needs, offering a roadmap for next-generation secure intelligent vehicular ecosystems for the modern world.

KEYWORDS: Intelligent transportation systems; connected vehicles; cybersecurity; deep learning; authentication

1 Introduction

In the era of connected and autonomous vehicles, the landscape of vehicular communication is rapidly evolving, introducing both unprecedented opportunities and critical cybersecurity challenges. On the other hand, the number of road accident-related deaths in the United States in the first half of 2023 is only 3.3%, down from the 2022 first half, with a fatality rate of 1.24 per 100 Million Vehicle Miles Traveled (VMT), according to data supplied by the National Highway Traffic Safety Administration (NHTSA) [1]. Consequently, the demand for Intelligent Transportation Systems (ITS) is unparalleled and enormous. The ability of cars to monitor and record both internal and exterior events has grown over the past few decades, along with the usage of electronics in automobiles. The sharing of this data, especially with other connected vehicles, happens with the help of the internet. According to Statista's report, over 400 million connected automobiles are expected to be in use by 2025, up from about 237 million in 2021 [2]. On the other hand, the rapid development of ITS brings security concerns from different angles. The automotive and

mobility cybersecurity experienced nearly 50% increased large-scale incidents in 2023 over 2024, with 95% of remote attacks [3]. The serious security threats towards ITS have captured the government's and academia's attention to invest in ITS safety. Alternatively, Vehicular *Ad-hoc* Networks (VANETs), a key component of ITS, enable real-time data exchange between vehicles and infrastructure to support safer and more efficient transportation. However, the increased interconnectivity also makes these networks susceptible to a wide range of cyber threats, where authentication emerges as the first and most essential layer of defense.

Recent trends in authentication (see Fig. 1) on different security measures shows a significant uplift over the past few years, which ensures enhanced security and user convenience. In addition, the trends on the DL (see Fig. 2) on different AI methods proves that incremental research on DL has the highest jump compared to others. ITS represents a cutting-edge approach to enhancing transportation efficiency, safety, and sustainability through the integration of advanced technologies [4]. ITS enables real-time monitoring, management, and optimization of traffic flow, infrastructure utilization, and vehicle operations by leveraging interconnected networks, sensors, and data analytics. Key components of ITS include smart traffic management systems, connected vehicles, autonomous vehicles, and dynamic routing algorithms [5], and advanced traveler information systems [6]. These technologies facilitate proactive traffic management, congestion mitigation, accident prevention, and improved accessibility for all road users. Additionally, ITS plays a crucial role in supporting the transition towards sustainable transportation modes by promoting ride-sharing, public transit utilization, and the adoption of electric and alternative fuel vehicles. In order to establish communication between cars, the Vehicular *Ad-Hoc* Network (VANET) uses two different communication types, such as Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) [7]. V2V communication enables direct wireless communication between vehicles, facilitating the exchange of critical safety information such as speed, position, and direction. On the other hand, V2I communication facilitates the transfer of data between vehicles and roadside units (RSUs). The communication takes place with the help of Dedicated Short-Range Communication (DSRC) [8] radio and a couple of IEEE standards.

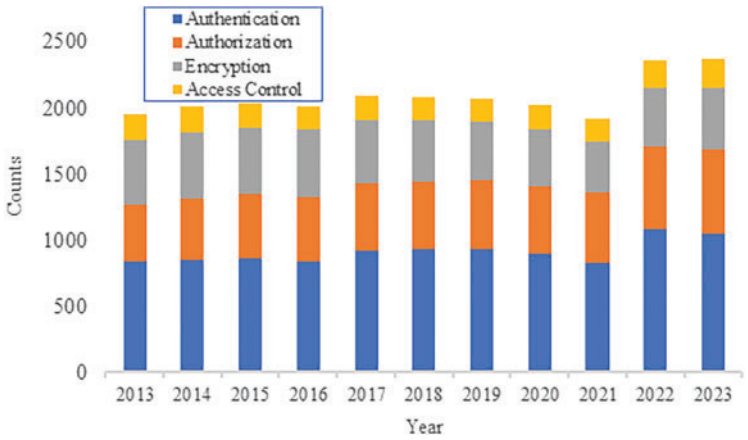

Figure 1: Trends of authentication in recent research [9]

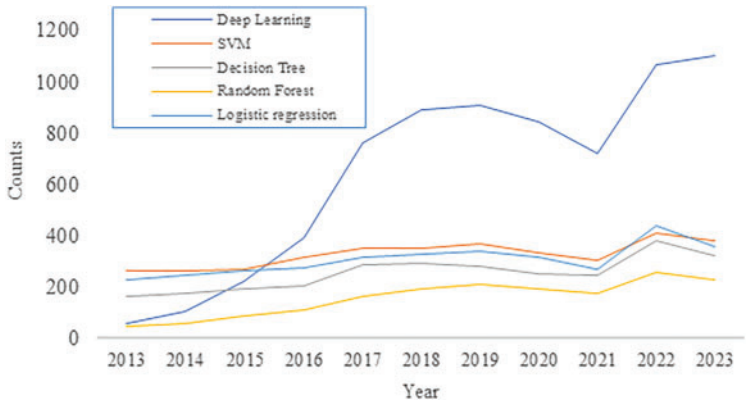

Figure 2: Trends of DL in recent research [9]

The unique features of VANET make it more vulnerable to internal and external attacks. These challenges have caused the main concern in designing security for VANETS, such as authentication, authorization, and access control. On the other hand, authentication in the VANET is the backbone of other security measures, which makes authentication more popular among security designers. In short, privacy protection and identity authentication are the main problems with VANET security protection, but they still encounter great challenges.

1.1 Comparison with Related Work

A plethora of excellent surveys have been published regarding the security of vehicular networks, which have covered the overview, requirements, characteristics, challenges, and solutions against attacks. The different research works provide their points and contributions (See Table 1). The survey of this research is fully based on the authentication mechanism of vehicular communication; therefore, the discussion of the related research is covered in this section.

Ali et al. [10] presented a survey on the privacy schemes and authentication in the VANET. Moreover, the security requirements, limitations, attacks, and efficiency of performance are shown in this research. In 2020, Farooq et al. [11] reviewed different authentication techniques in VANET. Additionally, they showed comparisons of several authentication protocols in the context of privacy preservation, batch verification, signature, attack mitigation, and communication. In 2021, Abbas et al. [12] proposed a complete review of authentication based on the blockchain in the Internet of Vehicles (IoV) and VANET. To emphasize clearly, the detailed discussion on blockchain, attacks, and mitigation to vehicular networks is discussed in this research. Moreover, the research shows a thorough comparative study of the technique used, authentication scheme, evaluation tools, network models, and attack prevention. In the same year, Al-Shareeda et al. [13] emphasized a survey on VANET's different authentication and privacy schemes. Azam et al. [14] presented a detailed discussion on the taxonomy of authentication schemes on VANET. The scalability requirements, security, and privacy were compared with the existing research. Additionally, recent technologies such as 5G, blockchain, and 5 G-SDN were discussed to develop low-cost, low-overhead, and low-communication-powered authentication. In the same context, Muhammad et al. [15] reviewed a few DL-based authentications in autonomous vehicles. In 2022, Jenefa and Mary Anita [16] presented the broad classification of VANET authentication based on message signing and verification methods. Moreover, the security attacks, performance parameters, and requirements are compared with other research. In 2023, Dong et al. [17] proposed a survey on security challenges and properties with respect to attacks and builders. Furthermore, this research

discussed the availability of systems, the authenticity of nodes, integrity, confidentiality, and non-repudiation of information. Sripathi Venkata Naga et al. [18] presented the classification of certificate authentication and features of the VANET in their research. The classifications were further extended based on the attacks addressed, security requirements, type of authentication, and the technique used. The review showed the complete performance analysis with the existing VANET authentication. In 2024, Sutradhar et al. [19] surveyed vehicular communication on the basis of privacy preservation. Alternatively, Shawky et al. [20] proposed a review of PHY-layer, cross-layer, and crypto-based authentication on VANET. Alternatively, Soujanya and Azam [21] discuss the problems in general authentication in vehicular networks in their studies. On the other hand, Aljehane [22] studied the roles and challenges of DL in autonomous vehicles; however, the research was not very comprehensive. In the same context, Zhang et al. [23] reviewed the application of ML and DL in ITS. However, the discussion on authentication was neglected in both of the studies. In 2025, Yang et al. [24] studied privacy concerns of Vehicular Cloud Computing (VCC) on the basis of ML-based approaches.

Table 1: Comparison of recent related surveys on vehicular authentication

Related research	Year	VANET Overview	Deep learning approaches	Deep learning-based authentication in VANET	Current challenges and Future directions	Theme	Features
Abbas et al. [12]	2021	-✕-	×	×	-✕-	Investigation on Blockchain-based authentication	- Taxonomy of Blockchain in authentication. - Discussion on privacy-preservation. -Attacks and their mitigation.
Al-Shareeda et al. [13]	2021	-✕-	×	×	-✕-	Investigation of a few security concerns on VANET authentication	- Public key infrastructure-based privacy scheme. - Group signature-based privacy scheme. - Identity-based privacy scheme.
Azam et al. [14]	2021	✓	×	×	-✕-	Investigation on general authentication in VANET.	- Taxonomy of authentication in VANET. - Recent advancements in VANET.
Muhammad et al. [15]	2021	-✕-	✓	-✕-	-✕-	Investigation on Deep Learning for Safe Autonomous Driving	- DL-based authentication (not all DLs are covered). - Challenges on DL-based authentication (not sufficient).
Jenefa and Mary Anita [16]	2022	×	×	×	-✕-	Investigation of authentication is based on message signing and verification methods.	- Classification on message signing-based authentication. - Classification on verification method.
Dong et al. [17]	2023	✓	×	×	-✕-	Investigation on authentication and attack detection in VANET.	- VANET architecture - Classification of authentication scheme.

(Continued)

Table 1 (continued)

Related research	Year	VANET Overview	Deep learning approaches	Deep learning-based authentication in VANET	Current challenges and Future directions	Theme	Features
							- Classification of attack and detection scheme.
Sripathi Venkata Naga et al. [18]	2023	×	×	×	×	Investigation on certificateless authentication scheme in ITS.	- Certificateless authentication. - Performance comparison on certificateless authentication.
Sutradhar et al. [19]	2024	✓	×	×	-×-	Classification of various cryptographic authentication techniques in vehicular communication.	- Discussion on authentication schemes on the basis of cryptographic techniques such as blockchain, pseudonyms, signatures, elliptic curve, certificateless, public key, and symmetric key.
Shawky et al. [20]	2024	✓	×	×	-×-	Investigation on PHY layer-based, cross-layer, and crypto-based authentication in VANET.	- Performance analysis matrix. - Authentication on three mentioned techniques.
Soujanya and Azam [21]	2024	✓	×	×	-×-	Investigation on vehicular authentication challenges and attack detection.	- Overview of authentication techniques. - Taxonomy of authentication scheme. - Challenges in authentication.
Aljehane [22]	2024	-×-	✓	×	-×-	Investigation on DL-based authentication; however, a few techniques were discussed.	- A few deep learning approaches in authentication are discussed. - Key challenges (not sufficient to the recent scenario).
Zhang et al. [23]	2024	×	✓	×	×	Investigation on the application of ML and DL in intelligent transport	- Scientific metric analysis. - Publication trends. - Qualitative discussion.
Yang et al. [24]	2025	✓	×	×	×	Investigation of security and privacy concerns in Vehicular Cloud Computing (VCC)	- Security and privacy challenges in VCC. - ML based approaches in VCC.
							- Security services of VANET and their challenges. - Most recent Deep Learning methods.

(Continued)

Table 1 (continued)

Related research	Year	VANET Overview	Deep learning approaches	Deep learning-based authentication in VANET	Current challenges and Future directions	Theme	Features
Ours	2025	✓	✓	✓	✓	Investigation of Deep learning-based authentication in detail in vehicular communication	- A detailed taxonomy of DL-based authentication in VENET. - A complete trend analysis on Deep Learning based authentication in VANET. - Detailed discussion on current challenges. - Detailed future research directions.

Note: ✓ Available, ✕ not available, -✕- Not sufficient information.

Traditional authentication mechanisms—such as certificate-based schemes and symmetric key cryptography—struggle to meet the real-time, scalable, and adaptive demands of highly dynamic vehicular environments. Deep Learning (DL), with its powerful pattern recognition capabilities, has recently gained attention as a promising tool to enhance the robustness and intelligence of authentication protocols. However, despite the broad interest in DL across ITS applications, its application in vehicular authentication remains underexplored. The research, as mentioned earlier, contributed to the knowledge of VANET information, which is respectable. Although there are few surveys on autonomous vehicle security [25], security issues in IoV [26], motion control security on road vehicles [27], and context-aware specified [28] cyber-physical security [29] in recent days, our research has been completely based on the recent advancements in deep learning for authentication in vehicular networks. This survey aims to bridge this critical research gap by offering a comprehensive overview of DL-based authentication techniques tailored for VANETs. While previous surveys have reviewed general security protocols or specific technologies such as blockchain or cryptography, a focused and up-to-date review on DL techniques for authentication is notably missing. Addressing this deficiency is vital, not only to consolidate current knowledge but also to guide future innovations towards building secure, scalable, and intelligent vehicular networks. To show the unique contribution of our research, the comparisons are shown with the existing related research in Table 1. The indicators '✓' and '✕' show if the specified factors are discussed in the mentioned review. Moreover, '-✕-' represents if the specified factors are discussed by providing sufficient knowledge of content.

1.2 Contribution

This survey focuses on topics that are not covered comprehensively in any of the research, as far as we know. Most importantly, the main focus of this survey is to investigate various DL methods in vehicular authentication. The main contributions are discussed as follows:

- To provide independent information, this survey discussed the overview of VANET in detail, along with the architecture and communication standards in VANET.
- To highlight the importance of discussion on DL, recent trends in DL on other related terms are shown.
- To make a unique yet essential survey, a comprehensive discussion on DL-based authentication in VANET communication is discussed. Moreover, a complete taxonomy of DL methods on vehicular authentication is shown.
- The survey objectively summarized some important points on current challenges, open issues, and possible future directions for the research on the authentication of vehicular communication.

The survey highlights the potential of DL in enhancing the security and efficiency of authentication mechanisms in vehicular networks. It underscores the need for robust, adaptive models to address evolving threats and ensure reliable communication in dynamic vehicular environments.

The organization of the rest of the paper (see Fig. 3) are as follows. In Section 1, the introduction, and the contribution towards vehicular authentication are discussed. Section 2 shows the overview of the vehicle network, including the architecture and communication standards in VANET. A detailed discussion on DL-based authentication in vehicular communication is shown in Section 3. In addition, the challenges, open issues, and future directions on the DL method-based vehicular authentication are discussed in Section 4. Finally, the survey is concluded in Section 5.

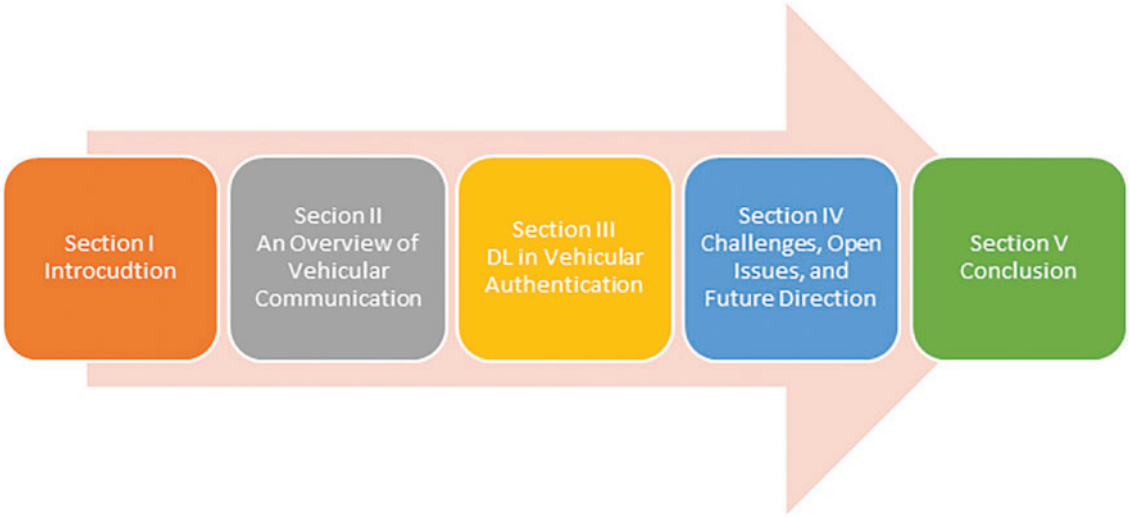

Figure 3: Organization of the paper

2 An Overview of Vehicle Communication

Vehicle communication encompasses various technologies and protocols enabling communication between vehicles and infrastructure, forming the backbone of VANETs. These systems utilize wireless communication technologies to exchange critical safety messages, traffic information, and other data. Vehicle communication systems play a pivotal role in enhancing road safety, improving traffic management, and optimizing transportation efficiency in smart and connected transportation ecosystems. The detailed discussion on the overview of vehicle communication is explored as follows:

2.1 VANET Architecture

VANETs are a specialized form of Mobile *Ad-hoc* Networks (MANETs) designed to facilitate communication among vehicles and between vehicles and roadside infrastructure. The architecture of VANETs typically involves several key components. The architecture of the vehicular network is shown in Fig. 4.

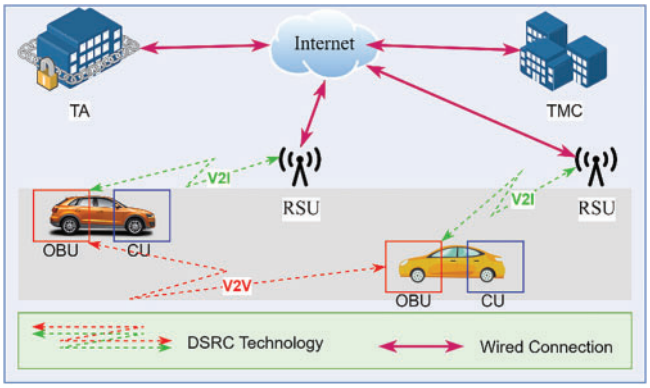

Figure 4: The architecture of the vehicular network

2.1.1 On-Board Units (OBUs)

OBUs are essential components within VANETs, embedded within vehicles to facilitate seamless communication and interaction within the network ecosystem. Equipped with wireless transceivers operating on DSRC frequencies [8], OBUs enable both V2V and V2I communication [30], which is crucial for exchanging real-time traffic and safety-related data. OBUs integrate Global Positioning System (GPS) receivers for precise vehicle location determination [31] alongside additional sensors for measuring speed [32], acceleration, and environmental conditions. Computational capabilities within OBUs support local data processing, executing algorithms for collision avoidance, route planning, and other ITS functions. With secure storage, power management, and user interfaces, OBUs ensure efficient and secure operation, enhancing overall road safety, traffic management, and transportation efficiency within VANETs [33].

Alternatively, OBUs are responsible for enabling V2V and V2I communication and play a pivotal role in collecting rich vehicular and environmental data that can be leveraged for deep learning-based authentication. Embedded with GPS, sensors, and communication modules, OBUs gather critical real-time data such as driver behavior, vehicle dynamics, and contextual surroundings. Deep learning models—particularly CNNs, RNNs, and hybrid architectures—can process this high-dimensional sensor data to generate unique authentication signatures or detect anomalies indicative of spoofing or unauthorized access attempts. For instance, an OBU can use locally stored DL models to identify behavioral biometrics that distinguish one driver from another. Furthermore, OBUs can serve as edge nodes to perform lightweight DL inference, thereby reducing reliance on centralized cloud infrastructure and supporting faster, context-aware decision-making in vehicular authentication protocols.

2.1.2 Roadside Units (RSUs)

RSUs are integral elements in VANETs, strategically positioned along roadways and intersections to facilitate seamless communication between vehicles and the surrounding infrastructure [34]. Equipped with powerful transceivers and antennas, RSUs serve as access points and relays, extending the communication range and providing connectivity to vehicles within their vicinity. RSUs support V2I communication, enabling the dissemination of traffic information, road conditions, and safety messages [33]. These units play a crucial role in enhancing traffic management, enabling applications such as traffic signal control [35], congestion detection, and route optimization. With their robust networking capabilities and integration into the transportation infrastructure, RSUs contribute to improving road safety and reducing congestion within VANET environments [36].

On the other hand, RSUs strategically deployed along roadways are crucial not only for extending communication range but also for acting as intelligent intermediaries in DL-enabled vehicular authentication systems. These units can function as edge computing nodes, hosting and executing deep learning models closer to the data source to ensure real-time authentication. For example, RSUs can collect encrypted identity data from nearby vehicles and utilize lightweight convolutional or recurrent neural networks to validate legitimacy before granting access to services such as dynamic traffic routing or secure intersection control. This localized decision-making process significantly reduces communication latency and the burden on centralized servers. Moreover, RSUs can participate in federated learning setups by aggregating model updates from vehicles without compromising raw data privacy, which is essential in training adaptive DL models that continuously learn from diverse driving environments. By integrating deep learning directly into RSU operations, the system becomes more resilient, scalable, and capable of responding swiftly to evolving cyber threats in vehicular networks.

2.1.3 Application Units (AUs)

AUs are pivotal components within VANETs and are responsible for executing various ITS applications and services [37]. AUs are typically software-based modules running on vehicles' OBUs or RSUs, leveraging the network's infrastructure for data exchange and processing. These software modules can embed DL algorithms to process contextual data, such as driving patterns, voice commands, or biometric inputs, for real-time identity verification. For instance, an AU could employ an LSTM network to monitor temporal patterns in driver behavior, flagging any significant deviation that might indicate spoofing or unauthorized vehicle access. These units support a diverse range of applications, including collision avoidance systems, intersection collision warnings, lane change assistance, traffic congestion detection, route optimization, and traffic signal control. By utilizing real-time data collected from vehicles and infrastructure, AUs enable informed decision-making to enhance road safety, improve traffic flow, and optimize transportation efficiency within VANET. On the other hand, by embedding DL capabilities directly into AUs, the authentication process becomes more adaptive, personalized, and responsive to dynamic vehicular environments, enhancing both security and user experience in connected vehicle systems.

2.1.4 Traffic Management Center (TMC)

TMC serves as a centralized hub for aggregating authentication data from multiple vehicles and RSUs, enabling large-scale training and refinement of deep learning models and monitoring and controlling traffic VANETs, overseeing roadways and intersections to optimize transportation efficiency and enhance road safety [38]. Equipped with advanced traffic monitoring systems and data analysis tools, the TMC collects real-time traffic data from vehicles, roadside RSUs, and other sensors deployed throughout the transportation network [39]. Using this data, the TMC can detect traffic congestion, accidents, and other incidents, allowing for proactive management strategies such as adjusting traffic signal timings, rerouting vehicles, and deploying emergency services as needed. By analyzing network-wide patterns using DL, TMCs can detect coordinated cyber threats or anomalies in authentication behavior, enhancing the overall security and intelligence of the vehicular ecosystem. Moreover, by facilitating coordinated responses to traffic events and providing actionable insights to transportation authorities, the TMC plays a vital role in improving traffic flow and reducing congestion within VANET environments [40].

2.1.5 Trusted Authority (TA)

TAs are foundational in managing authentication credentials and can leverage deep learning to enhance trust evaluation and anomaly detection. Acting as a central entity or a distributed system, the TA is

responsible for managing security credentials, distributing cryptographic keys, and authenticating vehicles and RSUs within the network [33]. By integrating DL models, TAs can intelligently analyze behavioral patterns or authentication requests across the network to identify fraudulent activities, adapt trust scores, and dynamically update authentication policies in response to emerging threats. The TA establishes trust relationships, verifies the identities of participants, and enforces security policies to prevent unauthorized access, data tampering, and malicious attacks. By maintaining the trustworthiness of the VANET infrastructure, the TA contributes to the overall reliability and resilience of the network, enhancing road safety and protecting against cybersecurity threats [37].

Overall, the architecture of VANET inherently supports deploying deep learning models for intelligent authentication due to its distributed and layered structure. Each architectural component, from OBUs and RSUs to TMCs and TAs, can serve as a data source or computational node for deep learning tasks. For instance, the decentralized nature of VANET allows for edge deployment of DL models at OBUs and RSUs, enabling real-time authentication based on local sensor data. Meanwhile, central entities such as TMCs and TAs can aggregate data across the network to train more robust behavior profiling and threat detection models. This synergy between the VANET architecture and deep learning frameworks creates a scalable foundation for building adaptive, context-aware, and secure authentication mechanisms tailored to the dynamic environment of vehicular networks.

2.2 Communication Standard

Vehicular networks rely on several communication standards to facilitate efficient and reliable communication among vehicles and between vehicles and roadside infrastructure. The primary communication standards in VANETs are discussed as follows.

2.2.1 Dedicated Short-Range Communication (DSRC)

DSRC is a wireless communication standard designed specifically for vehicular communication systems, including VANETs. DSRC operates in the 5.9 GHz frequency band and follows a channel allocation scheme defined by regulatory authorities, such as the Federal Communications Commission (FCC) in the United States, for transportation-related applications. It is based on the IEEE 802.11p standard, a variant of the Wi-Fi protocol optimized for low-latency and high-reliability communication. The DSRC band is divided into seven 10 MHz channels. Control Channel (CCH) is reserved for control purposes, facilitating the coordination and management of VANET communications [8]. CCH is primarily used for exchanging safety-critical messages, such as collision avoidance warnings and traffic management information. On the other hand, the remaining channels are designated as Service Channels (SCH) and are used for non-safety-critical communication and application-specific data exchange. These channels support various VANET applications, such as infotainment services, road tolling, and commercial services. Moreover, DSRC enables low-latency data exchange, making it ideal for deploying real-time deep learning-based authentication models at the vehicular edge. DL algorithms can leverage the consistent and reliable DSRC channels to authenticate vehicles quickly during safety-critical interactions, such as intersection crossing or lane merging, where rapid trust decisions are essential.

2.2.2 Cellular Vehicle-to-Everything (C-V2X)

C-V2X is an advanced communication technology that allows vehicles to communicate with each other, with roadside infrastructure, with pedestrians, and with networks using cellular networks. Operating in both direct communication mode (PC5) and network-based communication mode, C-V2X leverages existing cellular infrastructure, such as LTE and 5G networks, to enable low-latency, high-reliability communication.

This technology offers extended communication range, higher data rates, seamless integration with cellular networks, and flexibility to support a wide range of applications, making it a crucial enabler for connected and autonomous vehicles, advanced driver assistance systems, and intelligent transportation solutions aimed at enhancing road safety, improving traffic management [41]. Moreover, C-V2X supports high-speed, low-latency communication and seamless connectivity to cloud infrastructure, enabling vehicles to offload deep learning-based authentication tasks to more powerful remote servers. This facilitates advanced DL applications such as federated learning or real-time behavioral analysis for scalable and adaptive authentication in dynamic traffic environments.

2.2.3 Wireless Access in Vehicular Environments (WAVE)

WAVE constitutes a comprehensive framework for communication within VANETs, leveraging IEEE 802.11p as its backbone standard. WAVE encompasses protocols and standards tailored to the unique challenges of dynamic vehicular environments, including the Physical Layer (PHY) and Medium Access Control (MAC) layers, management services, security mechanisms, networking protocols, and application support. Its PHY layer defines radio parameters for reliable communication in the 5.9 GHz band [42]. In contrast, the MAC layer includes enhancements such as priority-based access and multi-channel operation to prioritize safety-critical messages and optimize channel utilization. WAVE ensures network initialization, synchronization, and authentication through management services, while robust security measures safeguard data integrity and privacy, including message authentication and encryption. Furthermore, WAVE, making it highly compatible with real-time deep learning-based authentication, facilitates interoperability among diverse devices and systems, enabling seamless communication between vehicles and infrastructure. DL models deployed at the edge can leverage WAVE's multi-channel support to process and verify authentication data efficiently, enabling quick responses to identity spoofing or intrusion attempts during V2V and V2I interactions. Overall, WAVE serves as a foundational framework within VANETs, fostering enhanced road safety, efficient traffic management, and improved transportation efficiency [43].

The aforesaid communication standards play a crucial role in enabling various intelligent transportation applications and cooperative driving. By facilitating the exchange of real-time data and enabling seamless communication within VANETs, these standards contribute to improving overall performance and enhancing the driving experience.

3 Comprehensive Analysis of Deep Learning in Vehicular Authentication

Deep learning has arisen as a formidable instrument in vehicular authentication [44], enhancing security and access control in ITS. By leveraging Deep Neural Networks (DNNs), authentication mechanisms can effectively analyze biometric data [45], vehicular signals, and contextual information to distinguish between legitimate and unauthorized users. Supervised Deep Learning, Unsupervised Deep Learning, Deep Reinforcement Learning, and Hybrid Deep Learning have been widely applied to process visual and sequential data for driver identification and anomaly detection. Additionally, deep learning enables high accuracy of real-time authentication, reducing vulnerabilities associated with traditional key-based systems. The taxonomy of deep learning in vehicular authentication is shown in Fig. 5.

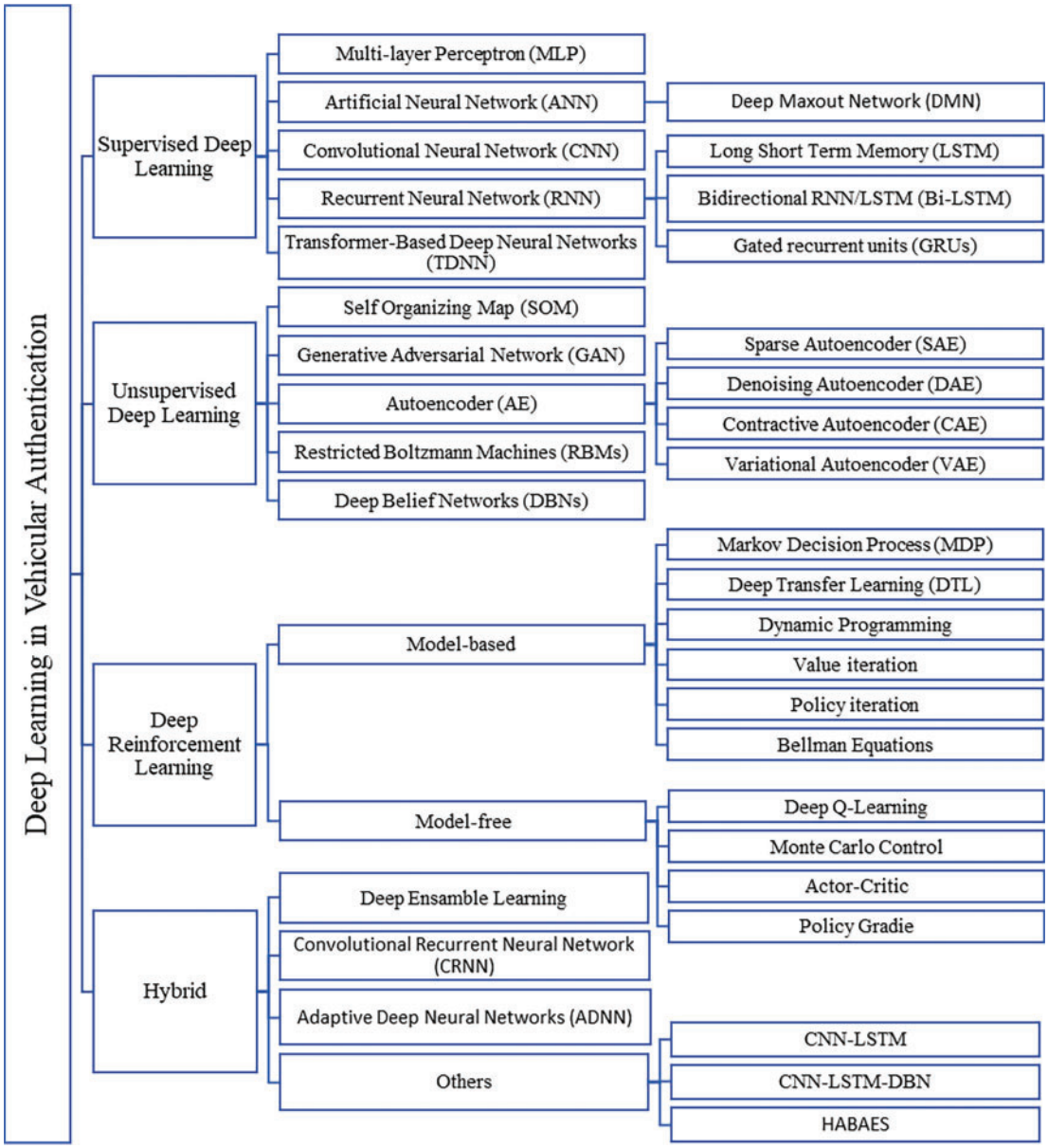

Figure 5: Taxonomy of deep learning in vehicular authentication

3.1 Supervised Deep Learning

Supervised deep learning has emerged as a powerful approach for enhancing authentication in vehicular communication systems, addressing the growing need for robust security in Vehicle-to-Everything (V2X) networks. By leveraging hierarchical neural architectures, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), deep supervised learning models can analyze complex patterns in heterogeneous data sources, including sensor data, communication logs, and behavioral patterns, to distinguish between legitimate and malicious entities.

In the realm of deep learning for vehicular authentication, a Multi-Layer Perceptron (MLP) serves as a foundational neural network architecture that can be leveraged to address the challenges of secure

and efficient vehicle identity verification. The architecture of authentication using MLP is shown in Fig. 6. Recently, Zhang and Li [46] proposed an automatic irrigation system with authentication features in VANET using a neural network. They used MLP to analyze sensor data to reduce water waste. Alternatively, Artificial Neural Networks (ANNs), inspired by the structure and function of biological neural networks, consist of interconnected layers of nodes that process input data to extract meaningful patterns and make decisions. ANN can learn to recognize unique signatures, such as cryptographic keys, vehicle-specific sensor data, or driving behavior, to authenticate vehicles in real-time scenarios [41]. Islam et al. [47] proposed a license plate authentication in a barrier access control tailoring with ANN to recognize characters in license plates. In addition, ANN can further use the maxout layer to extract features for authentication in a Deep Maxout Network (DMN). Recently, Kaur and Kakkar [34] used the Fractional Aquila Spider Monkey Optimization (FASMO) algorithm to train the bias and weights of DMN for attack detection. Alternatively, Convolutional Neural Networks (CNNs) have emerged as a highly effective architecture for processing structured and spatial data, such as images, sensor inputs, or communication patterns, to enhance security. CNNs leverage convolutional layers to automatically extract hierarchical features from input data, followed by pooling layers to reduce dimensionality and fully connected layers for decision-making. In vehicular authentication, CNNs can be employed to analyze visual data from cameras, such as license plate recognition or driver behavior monitoring, to verify vehicle identity and detect anomalies. In their research, Xun et al. [48] proposed an authentication scheme by leveraging the secure driver fingerprint using CNN and support vector domain description. On the other hand, Borra et al. [40] proposed biometric authentication for transport users using Multilayer CNN (ML-CNN) and Deep Hashing Component Analysis (DHCA) to extract high-level and low-level features. In addition, Qiu et al. [49] proposed a signal enhancement-based authentication using a deep convolutional generative adversarial network (DCGAN). On the other hand, Recurrent Neural Networks (RNNs) offer a powerful framework for addressing the dynamic and sequential nature of data in ITS. Unlike traditional feedforward networks, RNNs are designed to process sequential data by maintaining a hidden state that captures temporal dependencies, making them particularly suitable for tasks involving time-series data. Additionally, advanced recurrent architectures such as Long Short-Term Memory (LSTM), Bidirectional RNN/LSTM (Bi-LSTM), and Gated Recurrent Units (GRUs) have gained prominence in authentication due to their ability to model complex temporal dependencies and sequential data. LSTM networks address the limitations of traditional RNNs by incorporating memory cells and gating mechanisms that enable them to capture long-term dependencies and mitigate the vanishing gradient problem [50]. Alternatively, Bi-LSTM extends the capabilities of LSTMs by processing sequential data in both forward and backward directions, allowing the network to capture contextual information from past and future states simultaneously. GRUs [51], on the other hand, offer a simplified yet powerful alternative to LSTMs by combining the forget and input gates into a single update gate and reducing the number of parameters. In recent research, Shen et al. [52] proposed batch-based authentication using LSTM to predict workflow. Alternatively, Transformer-Based Deep Neural Networks (TDNNs) have emerged as a cutting-edge approach for addressing the challenges of secure and efficient identity verification in VANETs by leveraging the self-attention mechanism to capture global dependencies within sequential data, enabling them to process long-range interactions and complex patterns more effectively [53].

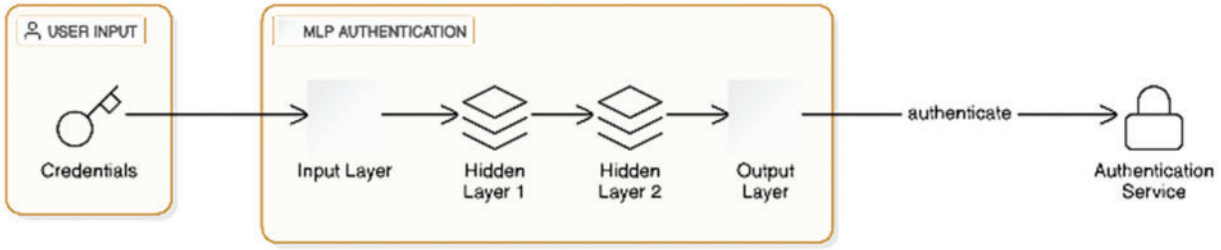

Figure 6: MLP in authentication

In contrast, the deep supervised learning models are trained using labeled datasets to minimize loss functions, such as cross-entropy, enabling accurate and real-time authentication while mitigating threats such as spoofing and replay attacks. However, challenges such as the need for large labeled datasets, computational overhead, and vulnerability to adversarial attacks remain, prompting research into techniques such as transfer learning and ensemble methods to improve robustness and scalability. Deep supervised learning thus offers a promising solution for securing vehicular communication systems, ensuring the integrity and reliability of intelligent transportation networks. A critical analysis of strengths, weaknesses, and limitations of supervised learning in the context of vehicular authentication has been shown in Table 2.

Table 2: Critical analysis of supervised deep learning in vehicular authentication

Model	Strengths	Weaknesses	Limitations
MLP	- Simple & easy to implement. - Works well for small feature sets. - Good for static authentication tasks.	- Struggles with high-dimensional data. - Not suitable for sequential or spatial data. - Prone to overfitting.	- Limited ability to handle real-time sensor data. - Poor performance with dynamic authentication (e.g., behavioral biometrics).
ANN	- Flexible architecture. - Can model non-linear relationships. - Works for structured data (e.g., IDs, PINs).	- Requires large datasets. - Computationally expensive for deep architectures. - Black-box nature reduces interpretability.	- Not optimized for temporal or spatial patterns in vehicular data. - Vulnerable to adversarial at tacks in authentication.
CNN	- Excellent for image & spatial data (e.g., license plates, facial recognition). - Robust to translation invariance. - Feature extraction is automated.	- Overkill for non-image data. - Requires significant computational power. - Struggles with sequential data.	- Limited applicability if authentication relies on non-visual data (e.g., RF signals, behavioral patterns). - High latency in real-time systems.

(Continued)

Table 2 (continued)

Model	Strengths	Weaknesses	Limitations
RNN	- Ideal for sequential data (e.g., time-series sensor data, driving patterns). - Can model temporal dependencies. - Useful for behavioral biometrics.	- Suffers from vanishing/exploding gradients. - Computationally intensive. - LSTM/GRU variants help but add complexity.	- Slow training & inference times. - Vulnerable to adversarial time-series attacks. - Difficult to deploy on edge devices in vehicles.
DNN	- High accuracy with sufficient data. - Can integrate multiple layers for complex feature learning. - Versatile (can combine CNN/RNN).	- Requires massive labeled datasets. - High computational cost. - Prone to overfitting without regularization.	- May be excessive for simple authentication tasks. - Lack of interpretability raises security concerns. - Energy-intensive for in-vehicle deployment.

3.2 Unsupervised Deep Learning

From the perspective of deep learning for vehicular authentication, unsupervised deep learning plays a pivotal role in addressing the challenges of secure and efficient identity verification in ITS. Unlike supervised methods that require labeled datasets, unsupervised learning techniques leverage unlabeled data to discover hidden patterns, structures, and anomalies, making them highly suitable for real-world vehicular environments where labeled data may be scarce or costly to obtain. Techniques such as autoencoders, Restricted Boltzmann Machines (RBMs), Deep Belief Networks (DBNs), and Self-Organizing Maps (SOMs) enable the extraction of meaningful features and the detection of anomalies by learning low-dimensional representations of high-dimensional vehicular data, such as sensor readings, communication logs, or driving patterns. By leveraging unsupervised deep learning, vehicular authentication systems can achieve greater adaptability, scalability, and robustness, ensuring secure and reliable operation in dynamic and evolving connected and autonomous vehicle ecosystems.

Self-Organizing Maps (SOMs), a type of unsupervised neural network, excel in clustering and visualizing high-dimensional data by mapping it onto a low-dimensional space while preserving topological relationships [54]. In vehicular authentication, SOMs are utilized to identify patterns and anomalies in vehicle behaviour, sensor data, or communication logs, enabling the detection of unauthorized access or spoofing attempts by clustering normal and abnormal activities. Alternatively, Generative Adversarial Networks (GANs), which consist of a generator and a discriminator network engaged in a competitive learning process, are particularly effective in generating synthetic data and enhancing anomaly detection capabilities [55]. Subsequently, GAN can be represented by a generator $G(z)$ which maps a random noise vector $z \sim p_z(z)$ to a generated sample $G(z)$ and a discriminator $D(x)$ which is a classifier that outputs the probability that an input x is real from the true data distribution $data(x)$ rather than fake from $G(z)$ as per (1).

$$G{:}\, z \to G(z), D{:}\, x \to [0,1] \tag{1}$$

where $D(x)$ should be close to 1 for real data and 0 for generated (fake) data, and $G(z)$ aims to fool D into predicting 1 for fake data.

Additionally, GANs can be employed to create realistic synthetic datasets for training robust authentication models [56], as well as to improve intrusion detection systems by learning the distribution

of legitimate data and identifying deviations indicative of cyberattacks [42]. In their recent studies, Fei et al. [57] used a Deep Convolution Generative Adversarial Network (DCGAN) to utilize the pseudo-random number generator for entropy-stopping method-based training in vehicular networks. On the other hand, autoencoders (AEs) and their variants, such as Sparse Autoencoder (SAE), Denoising Autoencoder (DAE), Contractive Autoencoder (CAE), and Variational Autoencoder (VAE) provide powerful frameworks for feature extraction, anomaly detection, and data reconstruction, which are critical for ensuring secure and reliable vehicle identity verification in the domain of deep learning for vehicular authentication [39]. In this context, the architecture of AE-based vehicular authentication is shown in Fig. 7. Eventually, Sparse Autoencoders (SAEs) introduce sparsity constraints during training, encouraging the network to activate only a small subset of neurons, which enhances feature selection and improves the interpretability of learned representations. Hemavathi et al. [58], in their studies, used a deep stacked sparse autoencoder unsupervised algorithm for authentication in HetNet. On the other side, Denoising Autoencoders (DAEs) are trained to reconstruct clean data from corrupted or noisy inputs, making them robust to noise and perturbations in sensor data or communication logs. Likewise, Saponara et al. [59] utilized SAE for reconstructing fingerprints to use it for authentication. In 2024, Chen et al. [60] proposed a physical layer authentication by utilizing DAE to reduce noise and feature dimension from the vehicular data. On the other hand, Contractive Autoencoders (CAEs) add a regularization term to the loss function that penalizes sensitivity to small input variations, resulting in more robust and stable feature representations. Azri et al. [61] used CAE for capturing robust and effective features of user and item to build a temporal recommender system. On the other hand, Variational Autoencoders (VAEs) introduce a probabilistic approach by learning a distribution over the latent space, enabling the generation of new data samples and improving anomaly detection by modeling the likelihood of observed data. In 2023, Meng et al. [62] used the VAE model to improve the representational ability of Channel Impulse Responses (CIR) for an Industrial Internet of Things (IIoT) physical layer authentication. In 2024, Qiu et al. [63] proposed a hardware fingerprint authentication utilizing VAE on optical spectra and trained the model for feature extraction. In the same year, Li et al. [64] used VAE for data augmentation and data reduction for mobile user authentication. Recently, Wang et al. [65] proposed a CNN-based authentication for digital therapeutics and used VAE for data augmentation. In the other aspects, Restricted Boltzmann Machines (RBMs) excel in learning probabilistic representations of input data by modeling the joint distribution between visible and hidden layers as generative stochastic neural networks [66,67]. Furthermore, multiple RBMs stack and construct Deep Belief Networks (DBNs) [68], which further enhance feature extraction by learning hierarchical representations of data. Eventually, DBNs can capture complex, non-linear relationships in vehicular data, enabling more accurate detection of anomalies. With this note, Althubiti [69] proposed a trust-aware authentication scheme protocol for Wireless Sensor Networks (WSNs) using DBNs to select threshold trust values dynamically. A critical analysis of unsupervised deep learning in the context of vehicular authentication is shown in Table 3.

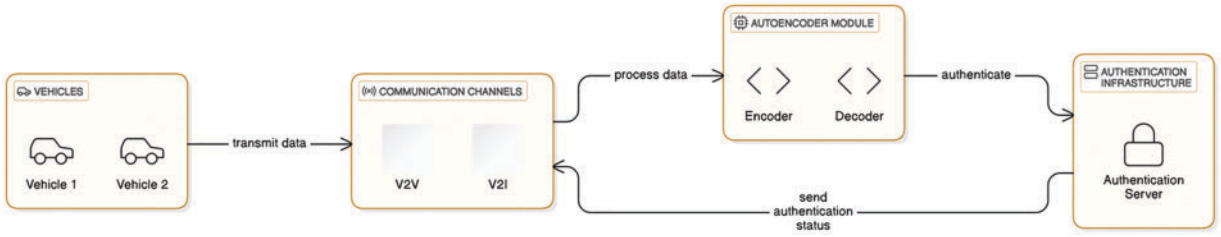

Figure 7: AE in Vehicular communication

Table 3: Critical analysis of unsupervised deep learning in vehicular authentication

Model	Strengths	Weaknesses	Limitations
SOM	- Unsupervised clustering of high-dimensional data. - Good for anomaly detection (e.g., detecting intrusions). - Visual interpretability (topolog ical maps).	- Not inherently supervised; requires hybrid approaches for classification. - Struggles with dynamic, sequential data. - Scalability issues with large datasets.	- Limited in direct authentication tasks. - Best suited for intrusion detection rather than user/device authentica tion. - Poor at handling real-time sensor streams.
GAN	- Can generate synthetic training data (e.g., fake RF signals for adversarial robustness). - Useful for augmenting rare attack samples in authentication datasets. - Can enhance privacy via synthetic data generation.	- Training instability (mode collapse). - High computational cost. - Difficult to deploy in real-time systems	- Not directly used for authentication; more useful for data augmentation or adversarial defense. - Risk of generating misleading data if not properly constrained.
AE	- Effective for anomaly detection (e.g., detecting spoofing attacks). - Dimensionality reduction helps in feature extraction. - Can work with unlabeled data (unsupervised pre-training).	- May reconstruct anomalies if not properly regularized. - Requires fine-tuning for supervised tasks. - Struggles with sequential dependencies.	- Best for behavioral anomaly detection (e.g., unusual driving patterns). - Not ideal for real-time authentica tion decisions without hybrid models.
RBM	- Unsupervised feature learning. - Can be stacked for deep archi tectures (e.g., DBN).	- Slow training (contrastive divergence). - Poor scalability to high-dimensional data.	- Rarely used standalone in authentication. - Mostly a pre-training tool for deep er networks.

(Continued)

Table 3 (continued)

Model	Strengths	Weaknesses	Limitations
	- Useful for collaborative filtering (e.g., multi-user authentication).	- Limited interpretability	- Not optimized for real-time vehicular systems.
DBN	- Combunsupervised pre-training + supervised fine-tuning.	- Computationally expensive.	- Useful for multi-modal authentication (e.g., combining RF, GPS, and biometrics).
	- Good for hierarchical feature extraction.	- Requires careful hyperpa rameter tuning.	- Too heavy for edge deployment in vehicles.
	- Robust to noisy inputs (e.g., sensor noise).	- Outperformed by modern deep learning models.	- Lacks real-time efficiency.

3.3 Deep Reinforcement Learning (DRL)

DRL, a novel and adaptive approach to enhancing security and decision-making in ITS. DRL combines the representational power of deep neural networks with the decision-making capabilities of reinforcement learning, enabling systems to learn optimal policies through interaction with their environment. In vehicular authentication, DRL can be employed to dynamically adapt authentication mechanisms based on real-time data, such as vehicle behavior, communication patterns, or environmental conditions. For example, a DRL agent can learn to detect and respond to evolving cyber threats, such as spoofing or intrusion attempts, by continuously optimizing its actions to maximize security while minimizing false positives.

Furthermore, DRL can be categorized as model-based and model-free deep reinforcement learning. Model-based DRL relies on learning an explicit model of the environment, which simulates state transitions and rewards, enabling the agent to plan and optimize actions efficiently. In vehicular authentication, this approach can be used to predict potential cyber threats, such as spoofing or intrusion attempts, by modeling the behavior of malicious actors and proactively adapting authentication protocols [70]. With this note, the Markov Decision Process (MDP), a model-based DRL, serves as a fundamental framework in modeling decision-making problems under uncertainty, making it particularly relevant in the context of deep learning-based vehicular authentication. On the other hand, in intelligent transportation systems, vehicular authentication must dynamically adapt to evolving network conditions, adversarial threats, and varying authentication costs [71]. By formulating the authentication process as an MDP, the system can optimize security decisions based on states representing vehicle credentials, trust scores, and environmental factors [72]. Alternatively, Deep Transfer Learning (DTL) plays a crucial role in enhancing the efficiency and adaptability of deep learning-based vehicular authentication by leveraging knowledge learned from related domains to improve authentication performance in dynamic vehicular environments. DTL enables the reuse of pre-trained models, allowing authentication systems to transfer learned features and patterns from previously seen vehicular contexts to new but related authentication tasks [73]. This approach not only reduces training time and data dependency but also improves the model's generalization ability across different vehicular scenarios. Given the high mobility and real-time constraints of vehicular networks, authentication mechanisms must adapt to continuously changing conditions while ensuring security and minimal latency [74]. Dynamic Programming facilitates optimal policy selection by breaking down the authentication process into subproblems, solving them recursively, and leveraging stored solutions to avoid

redundant computations [75]. Dynamic Programming relies on defining a problem recursively [76]. If $f(n)$ represents the optimal solution for a problem of size n, it can often be expressed in terms of smaller subproblems as per (2).

$$\mathrm{f}\,(\mathrm{n}) = \underset{a\in \mathrm{A}}{min}\,\{g\,(n,a) + f\,(T\,(n,a))\} \tag{2}$$

where $V(s)$ is the value of being in a state s, $R(s,a)$ is the immediate reward of taking action a, $P(s' \mid s,a)$ is the probability of transitioning to a state s', γ is a discount factor $(0 \le \gamma \le 1)$.

On the other hand, Value iteration leverages Bellman equations to iteratively update authentication value functions iteratively, converging toward an optimal security strategy [30]. In contrast, policy iteration alternates between policy evaluation and improvement to enhance authentication decisions [77]. The Bellman equation serves as the foundation for these methods, providing a recursive framework to evaluate authentication state transitions based on security risks, trust scores, and latency constraints [78]. By integrating these approaches with deep reinforcement learning, vehicular authentication systems can dynamically adapt to evolving cyber threats and optimize authentication policies, ensuring both security and efficiency in intelligent transportation networks.

On the other hand, model-free DRL directly learns optimal policies or value functions without explicitly modeling the environment, making it highly flexible and suitable for dynamic and complex vehicular networks. For instance, a model-free DRL agent can learn to detect anomalies in real-time communication patterns or driving behaviors by interacting with the environment and refining its decision-making process through trial and error. On the same note, Deep Q-learning (DQL), a model-free DRL, emerged as a powerful technique for vehicular authentication. DQL combines the strengths of Q-learning, a model-free reinforcement learning algorithm, with deep neural networks to approximate the Q-value function, which estimates the expected utility of actions in a given state [79]. In vehicular authentication, DQL can be employed to develop adaptive and intelligent systems capable of detecting and responding to cyber threats. Roy et al. [80] proposed a secure healthcare model utilizing DQL and DNN. On the other hand, Monte Carlo Control (MCC) plays a significant role in optimizing deep learning-based vehicular authentication by enabling model-free reinforcement learning in dynamic vehicular networks [81]. Given the unpredictability of vehicular environments, where authentication requests, network conditions, and security threats continuously evolve, MCC provides an effective approach to learning optimal authentication policies through experience. Unlike dynamic programming methods that require complete knowledge of the environment, MCC estimates value functions based on sampled authentication interactions, allowing the system to improve authentication strategies over time [82]. Alternatively, the Actor-criticism method combines the advantages of both policy-based and value-based approaches, where the actor learns an optimal authentication policy by interacting with the environment [83]. At the same time, the critic evaluates the policy using value functions. This dual-network structure accelerates learning and improves stability, allowing the authentication system to quickly adapt to changing vehicular behaviors, network conditions, and adversarial threats [83]. In the other context, Policy Gradient (PG) approaches parameterize the authentication policy and adjust it iteratively using gradients of expected rewards [84]. This allows the authentication mechanism to handle complex, high-dimensional vehicular environments where traditional rule-based or heuristic methods fail. On the same note, Jiu et al. [85] proposed an authentication scheme for an unknown network using a deep deterministic policy gradient.

In contrast, DRL can facilitate the development of adaptive authentication protocols that adjust to the dynamic nature of vehicular networks, ensuring robust performance in diverse and unpredictable scenarios. By leveraging its ability to learn from experience and improve over time, deep reinforcement learning provides a powerful framework for enhancing the security, resilience, and efficiency of vehicular

authentication systems, contributing to the safety and reliability of connected and autonomous vehicle ecosystems. The critical analysis of deep reinforcement learning in the context of vehicular authentication is shown in Table 4.

Table 4: Critical analysis of deep reinforcement learning in vehicular authentication

Model	Strengths	Weaknesses	Limitations
MDP	- Framework for sequential decision-making. - Models state transitions and rewards effectively.	- Assumes Markov property (memoryless), which may not hold in dynamic environments. - Requires known transition probabilities.	- Limited in direct authentication; better for adaptive security policies (e.g., dynamic key updates).
DTL	- Leverages pre-trained models for faster convergence. - Reduces data requirements for new tasks.	- Risk of negative transfer if source/tasks are mismatched. - Requires fine-tuning.	- Useful for cross-domain authentication (e.g., adapting face recognition from general to vehicular settings).
DP	- Optimal for known, finite MDPs. - Guaranteed convergence.	- Computationally expensive (curse of dimensionality). - Requires full model knowledge	- Impractical for real-time vehicular systems due to high latency.
Value Iteration	- Finds optimal policy iteratively. - Works well for discrete states.	- Slow convergence for large state spaces. - Not suitable for continuous spaces.	- Not scalable for high-dimensional vehicular sensor data.
Policy Iteration	- Faster convergence than value iteration in some cases. - Alternates between policy evaluation and improvement.	- Still suffers from high computational cost. - Requires full model knowledge knowledge.	- Limited use in authentication due to real-time constraints.
Bellman Equations	- Foundation for RL algorithms. - Provides recursive decomposition of value functions.	- Theoretical; requires approximation in practice.	- Used indirectly in Deep Q-Learning & Actor-Critic methods.

(Continued)

Table 4 (continued)

Model	Strengths	Weaknesses	Limitations
DQN	- Handles high-dimensional state spaces (e.g., raw sensor data). - Off-policy learning (replay buffer).	- Instability due to moving targets. - Overestimates Q-values.	- Can optimize adaptive authentication thresholds but lacks explicit policy representation.
Monte Carlo Control	- No model needed; learns from episodes. - Good for episodic tasks.	- High variance in estimates. - Requires complete episodes.	- Unsuitable for continuous authentication due to episodic nature.
Actor-Critic	- Combines value-based and policy-based methods. - Lower variance than pure policy gradients.	- Complex to tune (two networks). - Risk of instability.	- Potential for real-time adaptive authentication (e.g., adjusting trust scores dynamically).
Policy Gradients	- Directly optimizes policy for stochastic environments. - Works well in continuous action spaces.	- High variance in gradient estimates. - Sample inefficient.	- Useful for behavioral biometrics but requires extensive training.

3.4 Hybrid Learning

Hybrid learning, which integrates multiple learning paradigms, plays a vital role in enhancing deep learning-based vehicular authentication by improving adaptability, efficiency, and security in dynamic vehicular networks. Given the challenges of high mobility, evolving cyber threats, and latency constraints, a hybrid learning approach combines supervised, unsupervised, and reinforcement learning techniques to optimize authentication strategies. Supervised learning helps recognize known authentication patterns, while unsupervised learning detects anomalies and potential threats in real time. Subsequently, reinforcement learning enables adaptive decision-making by continuously refining authentication policies based on environmental interactions. By leveraging hybrid learning, vehicular authentication systems can achieve robust, context-aware security, minimizing authentication delays and improving resistance against adversarial attacks, making them well-suited for intelligent transportation systems. Hybrid learning, such as deep ensemble learning and Adaptive Deep Neural Networks (ADNN), play a crucial role in securing vehicular communications by providing authentication facilities. Recently, Pan et al. [86] proposed a vehicle license plate detection and recognition model using hybrid DL algorithms. The model is further extended to combine the CNN-based You Only Look Once (YOLO) algorithm and Convolutional Recurrent Neural Network (CRNN) for license-plate character recognition. On the other hand, SSD-MobileNet is a popular deep learning architecture for real-time object detection, combining the efficiency of the MobileNet convolutional neural network with the Single Shot MultiBox Detector (SSD) algorithm, allowing for fast and

accurate identification of multiple objects within an image, making it ideal for applications where low latency and high throughput are crucial, like mobile devices and surveillance systems [87].

On the other hand, Deep ensemble learning [32] has gained significant attention as a robust methodology for addressing the challenges of vehicular authentication in dynamic and security-sensitive environments. By aggregating the predictions of multiple deep learning models, this approach mitigates the limitations of single-model systems, which are often prone to overfitting, sensitivity to noisy data, and inadequate generalization in heterogeneous vehicular networks. The ensemble framework typically incorporates diverse architectures, such as CNNs for spatial feature extraction, RNNs for capturing temporal dependencies, and transformers for handling sequential data to enhance authentication accuracy and resilience collectively. Additionally, deep ensemble learning provides uncertainty estimates, enabling risk-aware decision-making in real-time authentication scenarios, which is critical for mitigating sophisticated threats like spoofing and replay attacks.

In deep ensemble learning [88], authentication can be framed as a binary classification problem, where the goal is to predict whether an input x belongs to the legitimate class ($y = 1$) or the malicious class $y = 0$. Let $f1, f2, f3, \ldots, fm$ be M deep learning models, each trained to predict the probability of legitimacy as per (3).

$$P_i(y = 1 \mid x) = f_i(x), \tag{3}$$

where $P_i(y = 1 \mid x)$ is the probability of x being legitimate, as predicted by the model f_i.

In the same context, Song et al. [89] proposed two-layer security on the authentication layer and ensemble learning-based monitoring layer.

Recent research related to authentication in vehicular communication has been successful in using face detection by DCNN, which has proven to be a significant result. However, Du et al. [90] outperformed DCNN-based user authentication by incorporating the PelFace model in parallel deep ensemble learning. On the other hand, ADNN has the power to adapt the new features by adjusting the parameters based on new data. A standard DNN with L layers is represented as (4).

$$h^{(l)} = \sigma\left(W^{(l)}h^{(l-1)} + b^{(l)}\right) \tag{4}$$

where $h^{(l)}$ is the activation at layer l, $W^{(l)}$ is the weight matrix, $b^{(l)}$ is the bias vector, and $\sigma(\cdot)$ is the activation function. However, instead of using all layers, an ADNN selects only a subset S of layers to compute based on an adaptive gating function $G(x)$ as per (5).

$$S = \{l|G\left(h^{(l)}\right) > \tau \tag{5}$$

where, $G\left(h^{(l)}\right)$ determines layer importance, τ is a threshold controlling adaptivity.

Instead of fixed weights, ADNNs update weights based on the input dynamically as per (6).

$$W^{(l)}(x) = f\left(W^{(l)}, x\right) \tag{6}$$

where $f(\cdot)$ is an adaptive function such as an attention mechanism or meta-learning.

Recently, Jia et al. [91] used ADNN to perform node authenticity and analyzed the trust score to minimize the attack in the VANET system. This approach not only enhances security but also ensures adaptability to the dynamic and evolving nature of vehicular networks, making it a promising direction for future research and deployment. On the other hand, Zhang et al. [92] proposed a user identification method by extracting the user's gait information using a convolution kernel and applying ANN to authenticate.

On the other hand, merging two or three DL models together to create individual safeguards is potentially beneficial for VANET authentication, especially for offering enhanced adaptability, robustness, and accuracy by combining the strengths of multiple learning paradigms. For instance, Inzillo et al. [93] combined CNNs for spatial feature extraction with LSTM networks for temporal pattern recognition in vehicle movement data. Alternatively, Chougule et al. [94] proposed CNN-LSTM to bolster the in-vehicle network security. In the first stage of the proposed model, LSTM is used to detect weather a communication is an attack or not and in the second stage the category of the attaches are judged by using CNN. On the other hand, Khan et al. [95] proposed a hybrid intrusion detection system combining CNN, LSTM networks, and DBN with feature selection techniques such as Random Projection (RP) and Principal Component Analysis (PCA). This framework achieved a detection accuracy of 99.4% for DoS and DDoS attacks, surpassing traditional machine learning models. Recently, Minu et al. [96] proposed an authentication framework for vehicular network using hybrid approaches. ADBN is used to enhance the reliability of the network messages and Hybrid Attribute-Based Advanced Encryption Standard (HABAES) encryption techniques used for secure communication. In another research, Eman et al. [97] combined deep-learning-based mask detection, landmark and oval face detection for key features, and Robust Principal Component Analysis (RPCA) to separate occluded and non-occluded image parts. Particle Swarm Optimization (PSO) is used to optimize k-nearest neighbors (KNN) features and the number of 'k' for improved performance. Experimental results show the proposed method achieves a 97% recognition rate, significantly outperforming existing methods in accuracy and robustness to occlusion.

In a nutshell, deep learning has revolutionized vehicular authentication by providing adaptive, efficient, and highly secure mechanisms for identity verification in intelligent transportation systems. Unlike traditional authentication methods, deep learning enables real-time decision-making, anomaly detection, and dynamic adaptation to evolving cyber threats. Techniques such as deep reinforcement learning, transfer learning, and hybrid learning enhance authentication resilience by leveraging past experiences and optimizing authentication strategies under varying network conditions [22]. A comprehensive analysis of deep learning is shown in Table 5.

Table 5: Analysis of deep learning in vehicular authentication

Related research	DL method	Strength	Weakness
Zhang and Li [46]	MLP	Utilized MLP neural network in an authentication scheme for VANET.	Used on Open Shortest Path First (OSPF) protocol, which further needs to be compared with other protocols, such as the Enhanced Interior Gateway Routing Protocol (EIGRP).
Park [41]	ANN	Used deep learning for road safety clubbed with authentication to reach 99.8% F-score in CAN traffic.	The experiment was conducted in a controlled area network with limited attack models.

(Continued)

Table 5 (continued)

Related research	DL method	Strength	Weakness
Islam et al. [47]	ANN	Used detection and recognition to achieve 98.45% accuracy.	Multi-stage deep learning architecture needs to be investigated. Alternatively, only one vehicle can be visible in the field of the experiment due to the controlled barrier structure.
Kaur and Kakkar [34]	DMN	Creates a secure authentication using DMN outperformed other related works on memory usage, recall, precision, and computation time.	Important security parameters such as bandwidth and latencies are not considered.
Xun et al. [48]	CNN	The proposed driving fingerprint scheme is able to authenticate the driver without affecting the driver's driving.	The experimental domain is restricted to two cars, the Luxgen U5 SUV and the Buick Regal.
Borra et al. [40]	ML-CNN, DHCA	Used ML-CNN and DHCA to extract high-level and low-level features.	The proposed system should explore more diverse biometric characteristics, such as irises, faces, and voices, for more accurate results.
Qiu et al. [49]	DCGAN	The proposed model reduces noise interference during training and enhances the recognition and detection rate.	The experiment is based on the NIST dataset [98], which is not suitable for highly dynamic networks, such as VANET.
Umar et al. [50]	LSTM	Outperformed existing PLA schemes based on update strategies, attribute tracking, feature identification, and selection.	The experiment is done using a synthetic dataset on simulation; however, real-world tests are not considered.
Shen et al. [52]	LSTM	Proposed a lightweight authentication without complex calculation along with simple group key generation and verification process.	The proposed model highly trusts the RSU; however, the RSU is more exposed to equipment in VANET.
Pan et al. [86]	Hybrid	Achieved higher mean average precision even in constrained scenarios.	The proposed model only works on English script and alphanumeric characters. On the other hand, a real scenario needs to be experimented with to confirm the viability of the proposed model.

(Continued)

Table 5 (continued)

Related research	DL method	Strength	Weakness
Roy et al. [87]	SSD-MobileNet	A precision of 98% was achieved on the Malaysian number plate.	The model is restricted to monolingual characters.
Song et al. [89]	Ensemble	Two-way security was used, using the authentication layer and monitoring layer, to maintain approximately 96% accuracy.	The assumption of this research is a bit unrealistic such as fully trusted TA and partially trusted fog.
Du et al. [90]	DCNN	Used parallel ensemble learning (PelFace) to authenticate the user's face and reached 99.53% accuracy on the LFW dataset.	Used a limited number of loss functions implementation and restricted hyperparameters.
Jia et al. [91]	ADNN	The ADNN-based authentication reduces the possibility of privacy violation.	Optimal fog resource allocation has not been performed properly.
Zhang et al. [92]	Convolution Kernel and ANN	Used users' gait information extracted by convolution kernel and utilized ANN to authenticate.	Signal Noise Ratio (SNR) is not considered to check the system's robustness.
Pulligilla and Vanmathi [99]	RideNN	Provides great reliability during an exchange of messages.	Used BotIoT dataset [100]. A model creation based on a single dataset may crash. The model should be validated using multiple datasets.

4 Challenges, Open Issues and Future Directions

The integration of deep learning into vehicular authentication has opened new avenues for enhancing security, efficiency, and user experience in connected and autonomous vehicles. However, despite its transformative potential, the deployment of deep learning in this domain is fraught with significant challenges and open issues that must be addressed to ensure its successful implementation. These challenges span technical, ethical, and practical dimensions, ranging from adversarial vulnerabilities and real-time processing constraints to data privacy concerns and scalability limitations. Furthermore, as the automotive landscape continues to evolve, new opportunities and directions for research are emerging, driven by advancements in technology and the growing complexity of vehicular networks. This section provides a comprehensive exploration of the key challenges and open issues associated with deep learning-based vehicular authentication while also outlining promising future directions that can guide researchers and practitioners in overcoming these hurdles.

4.1 Challenges and Open Issues in the Vehicular Authentication

Deep learning has emerged as a transformative technology in various domains, including vehicular authentication. Its ability to learn complex patterns from large datasets makes it a promising solution for

enhancing the security and efficiency of vehicular systems. However, the deployment of deep learning in vehicular authentication is not without significant challenges and open issues. This section delves into the key challenges and unresolved problems that must be addressed to ensure the reliable and secure implementation of deep learning-based authentication systems in vehicles.

4.1.1 Data Privacy and Security Concerns

Vehicular authentication systems often process sensitive data, such as driver biometrics, vehicle identification numbers, and location information [101]. Ensuring the privacy and security of this data is critical, as any breach could lead to severe consequences, including identity theft and unauthorized access to vehicles. On the other hand, deep learning models are susceptible to adversarial attacks, where malicious actors introduce subtle perturbations to input data to deceive the model. In vehicular authentication, such attacks could allow unauthorized users to gain access to vehicles or systems, posing significant security risks. Alternatively, ensuring the integrity of data used for training and inference is essential. Compromised or tampered data could lead to flawed models that fail to authenticate legitimate users or grant access to unauthorized entities [102]. For instance, while pseudonyms protect driver identity, they complicate traceability for liability, such as an accident. Achieving GDPR-compliant anonymity without enabling misbehavior is an open problem.

4.1.2 Real-Time Processing and Computational Constraints

Vehicular systems operate in real-time environments where delays in authentication can lead to safety risks or user inconvenience [103]. Deep learning models, particularly those with high complexity, may struggle to meet the stringent latency requirements of real-time applications. Many vehicles, especially older models, have limited computational resources such as processing power and memory. Running deep learning models on such hardware can be challenging, necessitating the development of lightweight and efficient models. On the other hand, edge computing can help to reduce latency by processing data locally; deploying deep learning models on edge devices in vehicles requires careful optimization to balance performance and resource usage [104]. On the other hand, deploying deep learning models on vehicular edge devices is limited by memory, processing power, and energy availability. This necessitates efficient model compression and optimization techniques without compromising accuracy, posing a key challenge for practical, real-time deep learning-based authentication [105].

4.1.3 Robustness and Reliability in Dynamic Environments

Vehicles operate in diverse and dynamic environments, including varying weather conditions [106], lighting, and road scenarios. Deep learning models must be robust to these variations to ensure reliable authentication under all conditions. Moreover, sensor data used for authentication, such as cameras, microphones [107], or biometric sensors [108], can be noisy or incomplete. Models must be designed to handle such uncertainties without compromising accuracy. Therefore, DL models must be resilient to adversarial attacks and sensor noise that can corrupt input data, potentially leading to misauthentication and struggles in real-time decision-making. On the other hand, deep learning models often struggle to generalize to scenarios not encountered during training. In vehicular authentication, this could lead to failures when faced with new types of vehicles, users, or environmental conditions [109]. Moreover, ensuring consistent performance across varying environmental conditions is critical, as model degradation in these dynamic settings could compromise the continuous and trustworthy authentication of vehicles and their communications.

4.1.4 Scalability and Interoperability

Scaling [110] deep learning-based authentication systems across millions of vehicles requires efficient model deployment [111], updates, and management. Ensuring consistency and reliability at scale is a significant challenge. Furthermore, many existing vehicular systems rely on traditional authentication methods. Integrating deep learning solutions with these legacy systems can be complex and may require significant modifications to existing infrastructure. On the other hand, interoperability requires DL models and authentication protocols to seamlessly integrate and communicate across heterogeneous vehicular networks, different vehicle manufacturers, and various regulatory frameworks, which can be addressed by adhering to standards like those from IEEE [112]. The lack of standardized frameworks and protocols for deep learning in vehicular authentication hinders interoperability and complicates integration efforts [113].

4.1.5 Explainability and Transparency

Deep learning models are often considered "black boxes" due to their complexity and lack of interpretability [114]. In critical applications like vehicular authentication, understanding how decisions are made is essential for building trust and ensuring accountability. On the other hand, many industries, including automotive, are subject to strict regulations regarding transparency and explainability [115]. Meeting these requirements with deep learning models remains a challenge. Moreover, the lack of transparency in deep learning models makes it difficult to diagnose and fix issues when authentication failures occur [23].

4.1.6 Data Quality and Availability

Deep learning models require large amounts of labeled data for training [116]. Collecting and annotating high-quality datasets for vehicular authentication can be time-consuming and expensive. Moreover, imbalanced datasets, where certain classes, such as rare attack patterns, are underrepresented, can lead to biased models that perform poorly on minority classes [117]. Furthermore, while synthetic data can be used to augment training datasets, it may not fully capture the complexity and variability of real-world scenarios, leading to suboptimal model performance [118].

4.1.7 Ethical and Legal Considerations

Deep learning models can inadvertently learn biases present in training data, leading to unfair treatment of certain users or groups. Ensuring fairness in vehicular authentication is crucial to avoid discrimination [119]. On the other hand, determining liability in cases where deep learning-based authentication fails or is compromised is a complex legal issue. Clear guidelines and frameworks are needed to address accountability. Moreover, users must be informed about how their data is used for authentication and must consent to its use. Building trust in deep learning-based systems is essential for widespread adoption [106].

4.1.8 Continuous Learning and Adaptation

Cybersecurity threats are constantly evolving, requiring deep learning models to adapt to new types of attacks. Continuous learning and model updates are necessary to maintain robust authentication [120]. Alternatively, changes in the underlying data distribution over time, such as new vehicle models or user behavior, can degrade model performance. Techniques for detecting and adapting to concept drift are needed. Furthermore, implementing lifelong learning mechanisms that allow models to improve over time without forgetting previously learned knowledge is a significant challenge [121].

4.1.9 Integration with Multi-Factor Authentication

Vehicular authentication often relies on multiple factors, such as biometrics, behavioral patterns, and cryptographic keys. Integrating deep learning with multi-factor authentication systems while maintaining security and usability is challenging [122]. Moreover, striking the right balance between robust security and user convenience is essential. Overly complex authentication processes may deter users, while overly simplistic ones may compromise security [91].

The application of deep learning in vehicular authentication holds immense potential but is accompanied by significant challenges and open issues. Addressing these challenges requires interdisciplinary efforts involving advancements in deep learning algorithms, cybersecurity, hardware optimization, and regulatory frameworks. Future research should focus on developing robust, scalable, and transparent deep learning models that can operate reliably in the dynamic and resource-constrained environments of vehicular systems. By overcoming these challenges, deep learning can play a pivotal role in enhancing the security and efficiency of next-generation vehicular authentication systems.

4.2 Future Directions of Deep Learning in Vehicular Authentication

As the automotive industry continues to evolve toward connected and autonomous vehicles, the role of deep learning in vehicular authentication is expected to grow significantly. While current research has demonstrated the potential of deep learning for enhancing security and user experience, several future directions can further advance the field. These directions aim to address existing challenges, leverage emerging technologies, and explore novel applications of deep learning in vehicular authentication. This section outlines key areas of focus for future research and development.

4.2.1 Development of Robust and Adversarial-Resilient Models

Future research should focus on developing deep learning models that are resilient to adversarial attacks [123]. Techniques such as adversarial training, where models are trained on both clean and adversarial examples, can improve robustness. On the other hand, incorporating defensive mechanisms, such as gradient masking, randomization, and input transformations, can help mitigate the impact of adversarial attacks. Moreover, developing explainable methods for detecting and defending against adversarial attacks will enhance transparency and trust in deep learning-based authentication systems [124].

4.2.2 Lightweight Models

Techniques such as pruning, quantization, and knowledge distillation can be used to create lightweight [125] deep-learning models that are suitable for deployment on resource-constrained vehicular systems [34]. On the other hand, dynamic batch-based group key management using deep learning in vehicular authentication can be further analyzed [52]. Furthermore, leveraging edge computing to run deep learning models locally on vehicles can reduce latency and improve efficiency.

4.2.3 Federated Learning for Privacy-Preserving Authentication

Federated learning allows models to be trained across multiple vehicles without sharing raw data, preserving user privacy [126]. Future research should explore federated learning frameworks tailored for vehicular authentication. Alternatively, techniques for secure aggregation of model updates in federated learning can prevent data leakage and ensure the confidentiality of user information [35]. Moreover, federated learning can enable personalized authentication models that adapt to individual user behavior while maintaining privacy [127].

4.2.4 Multi-Modal and Context-Aware Authentication

Combining data from multiple sensors, such as cameras, microphones, and biometric sensors, can enhance the accuracy and reliability of authentication systems. Future research should explore deep learning architectures that effectively fuse multimodal data. Recently, Shen et al. [128] proposed a continuous authentication based on multiple modalities such as user pattern, usage context, and motion pattern. However, the multiclass classifier can be used to improve the authentication accuracy. In addition, developing context-aware models that consider situational factors such as location, time, and driving behavior can improve authentication accuracy and user experience. Besides, leveraging behavioral biometrics, such as driving patterns, voice recognition, and gesture analysis, can provide additional layers of security [120]. Bulat and Ogiela [129] utilized personal characteristics and knowledge as context to prepare a digital signature to authenticate users.

4.2.5 Continuous Learning and Adaptation

Implementing lifelong learning mechanisms that allow models to adapt to new data and scenarios without forgetting previously learned knowledge is crucial for maintaining robust authentication over time [90]. Additionally, developing online learning algorithms that update models in real time as new data becomes available can improve adaptability and responsiveness to evolving threats [130]. Furthermore, integrating anomaly detection techniques into authentication systems can help identify and respond to unusual patterns or potential security breaches [99].

4.2.6 Explainable and Transparent Models

Research should focus on developing explainable deep learning models that provide insights into their decision-making processes [131]. Techniques such as attention mechanisms, saliency maps, and rule-based explanations can enhance transparency. Moreover, creating user-friendly interfaces that explain authentication decisions to users can build trust and improve acceptance of deep learning-based systems. Ensing that deep learning models comply with regulatory requirements for transparency and accountability is essential for their adoption in the automotive industry [132].

4.2.7 Integration with Blockchain and Decentralized Systems

Integrating deep learning with blockchain technology can enhance the security and transparency of vehicular authentication systems [133]. Blockchain can be used to store and verify authentication records securely. On the other hand, developing decentralized identity management systems that leverage deep learning for user verification can reduce reliance on centralized authorities and improve security. Additionally, using smart contracts to automate authentication processes and enforce security policies can enhance efficiency and reliability. Gautam et al. [134] mentioned that post-quantum cryptography and lattice-based cryptography, coupled with blockchain in digital twin-based vehicular authentication, can have more potential to secure vehicular communication. In the other work, Razmjouei et al. [135] proposed a mutual authentication based on smart contract blockchain on a Man-In-The-Middle (MITM) attack scenario. This research can be extended to wide network attack scenarios.

4.2.8 Emphasis on Other Security Domains

The integration of essential references from the broader security domain is essential, which has been overlooked in recent research. While focusing on deep learning applications in vehicular authentication, the current discussion lacks a robust foundation drawn from established security principles, frameworks,

and foundational research [136]. A more comprehensive incorporation of seminal and contemporary works in cybersecurity, authentication protocols, and threat modeling would significantly enhance the model's credibility, provide a richer context for its proposed solutions, and demonstrate a deeper understanding of the security landscape within which vehicular communication operates. This would allow for a more nuanced analysis of the vulnerabilities deep learning aims to address and the security implications of the suggested techniques, such as zero-trust [137].

4.2.9 Cross-Domain Collaboration and Standardization

Collaboration between researchers in deep learning, cybersecurity, automotive engineering, and human-computer interaction can drive innovation and address complex challenges in vehicular authentication [138]. Additionally, establishing industry-wide standards for deep learning-based authentication systems can promote interoperability and facilitate large-scale deployment. Moreover, developing standardized benchmarks and evaluation metrics for vehicular authentication systems can enable fair comparison and drive progress in the field [139].

4.2.10 Ethical and Inclusive Design

Future research should focus on developing techniques to identify and mitigate biases in deep learning models, ensuring fair and inclusive authentication for all users Liu et al. [140]. Designing authentication systems with a focus on user experience and accessibility can improve adoption and satisfaction. Additionally, addressing ethical concerns, such as data privacy, consent, and accountability, is essential for building trust in deep learning-based authentication systems [141].

4.2.11 Exploration of Emerging Technologies

Exploring the potential of quantum machine learning for vehicular authentication can unlock new possibilities for secure and efficient authentication [142]. Leveraging neuromorphic computing architectures, which mimic the human brain, can enable more efficient and adaptive deep learning models for authentication. In addition, the rollout of 5G and future communication technologies can enable faster and more reliable data transmission, enhancing the performance of deep learning-based authentication systems.

The future of deep learning in vehicular authentication is promising, with numerous opportunities for innovation and improvement. By addressing current challenges (see Table 6) and exploring emerging technologies, researchers can develop robust, secure, and user-friendly authentication systems that meet the demands of next-generation vehicles. Interdisciplinary collaboration, standardization, and a focus on ethical design will be key to realizing the full potential of deep learning in this domain. As the automotive industry continues to evolve, deep learning will play a pivotal role in shaping the future of vehicular authentication, ensuring both security and convenience for users.

Table 6: Future direction of the vehicular authentication research

Related research	Year	Technology	Future direction
Prateek et al. [142]	2021	Quantum computing	Privacy preservation and data security using quantum key authentication and key agreement mechanism.
Shen et al. [52]	2022	Neural network	Dynamic batch-based group authentication

(Continued)

Table 6 (continued)

Related research	Year	Technology	Future direction
Bulat and Ogiela [129]	2022	Context-based	User behavior and knowledge are used to create a context-based digital signature for authenticity, and this can be improved with other features.
Liu et al. [130]	2023	Online learning	A redactable signature scheme with a designated verifier and AI-based security can enhance the traceability of the redactor.
Du et al. [90]	2024	Continuous learning	A range of loss parameters can be experimented.
dos Santos et al. [123]	2024	Fog computing	The work can be extended to different environments with limited resources.
Shen et al. [128]	2024	Multi-modal	Continuous authentication was proposed using multiple modalities. However, the multiclass classifier can improve the authentication accuracy.
Gautam et al. [134]	2024	Blockchain	Quantum cryptography, lattice-based cryptography along with blockchain in digital twin-based vehicular authentication.
Razmjouei et al. [135]	2024	Blockchain	The research is based on an MITM attack scenario and can be extended in upgraded other attack models and can be improved in further attack models.
Ying et al. [143]	2024	Transmitter based	Covert channels can be further investigated with modified messages and different attack models.
Zhang and Wei [126]	2025	Federal learning	Collaborative authentication in high dynamic topology.

5 Conclusion

The integration of deep learning into vehicular authentication marks a significant leap forward in securing connected and autonomous vehicles, offering innovative solutions to complex challenges such as real-time processing, adversarial resilience, and adaptability to dynamic environments. However, none of the surveys on vehicular communication discuss these issues in their studies, as far as we know. This paper has thoroughly explored the transformative potential of DL in advancing vehicular authentication systems, while also dissecting the intricate challenges that must be overcome for widespread, secure, and reliable deployment. We have demonstrated that DL offers unparalleled capabilities in anomaly detection, behavioral biometrics, and cryptographic key management, promising significantly enhanced security over traditional methods. However, critical issues surrounding real-time computational constraints, ensuring robustness against adversarial attacks and dynamic environmental conditions, and achieving seamless scalability and interoperability across heterogeneous vehicular ecosystems remain open avenues for intensive research.

Future research must develop lightweight, energy-efficient models, leverage emerging technologies like federated learning and blockchain, and foster interdisciplinary collaboration to create robust, scalable, and user-friendly authentication systems. As the automotive industry evolves, deep learning will play a pivotal role in shaping secure and seamless vehicular communication, provided that ongoing efforts prioritize innovation, standardization, and ethical design. By addressing these challenges, we can unlock the full potential of deep learning, ensuring a safer and more efficient future for vehicular networks.

Acknowledgement: The authors of this manuscript would like to thank all the anonymous reviewers for improving the quality and readability of this document.

Funding Statement: This research is funded and supported by the UCSI University Research Excellence & Innovation Grant (REIG), REIG-ICSDI-2024/044.

Author Contributions: The author contribution is stated as follows: Tarak Nandy: Conceptualization, Literature Review, Writing—Original Draft; Sananda Bhattacharyya: Literature Review, Writing—Original Draft, Visualization. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: This survey was conducted based on publicly available, published scholarly research articles. This study does not generate any data.

Ethics Approval: This study did not involve human participants, animal subjects, or sensitive data collection requiring ethical approval.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. NHTSA. Early estimate of motor vehicle traffic fatalities for the first half (January–June) of 2023 [Internet]. Washington, DC, USA: U.S. Department of Transportation; 2023 [cited 2025 Jun 19]. Available from: https://crashstats.nhtsa.dot.gov/Api/Public/Publication/813514.
2. Placek M. Connected cars worldwide—statistics & facts Statista [Internet]. Hamburg, Germany: Statista; 2023 [cited 2025 Jun 19]. Available from: https://www.statista.com/topics/1918/connected-cars.
3. Security U. Upstream's 2025 global automotive and smart mobility cybersecurity report. [Internet]; 2024 [cited 2025 Jun 18]. Available from: https://upstream.auto/reports/global-automotive-cybersecurity-report.
4. Gong T, Zhu L, Yu FR, Tang T. Edge intelligence in intelligent transportation systems: a survey. IEEE Trans Intell Transp Syst. 2023;24(9):8919–44. doi:10.1109/tits.2023.3275741.
5. Noor RM, Rasyidi NBG, Nandy T, Kolandaisamy R. Campus shuttle bus route optimization using machine learning predictive analysis: a case study. Sustainability. 2021;13(1):225. doi:10.3390/su13010225.
6. Creß C, Bing Z, Knoll AC. Intelligent transportation systems using roadside infrastructure: a literature survey. IEEE Trans Intell Transp Syst. 2023;25(7):6309–27. doi:10.1109/tits.2023.3343434.
7. Nandy T, Idris MYIB, Noor RM, Ahmedy I, Bhattacharyya S. A multiple-criteria decision analysis clustering and cluster head selection algorithm in vehicular network. In: Proceedings of the 2020 IEEE 8th R10 Humanitarian Technology Conference (R10-HTC); 2020 Dec 1–3; Kuching, Malaysia.
8. Kenney JB. Dedicated short-range communications (DSRC) standards in the United States. Proc IEEE. 2011;99(7):1162–82. doi:10.1109/jproc.2011.2132790.
9. Google. Google Trends [Internet]; 2025 [cited 2025 Jun 20]. Available from: https://trends.google.com.
10. Ali I, Hassan A, Li F. Authentication and privacy schemes for vehicular ad hoc networks (VANETs): a survey. Veh Commun. 2019;16:45–61. doi:10.1016/j.vehcom.2019.02.002.
11. Farooq SM, Hussain SMS, Ustun TS. A survey of authentication techniques in vehicular ad-hoc networks. IEEE Intell Transp Syst Mag. 2020;13(2):39–52. doi:10.1109/mits.2020.2985024.

12. Abbas S, Talib MA, Ahmed A, Khan F, Ahmad S, Kim D-H. Blockchain-based authentication in internet of vehicles: a survey. Sensors. 2021;21(23):7927. doi:10.3390/s21237927.
13. Al-Shareeda MA, Anbar M, Hasbullah IH, Manickam S. Survey of authentication and privacy schemes in vehicular ad hoc networks. IEEE Sens J. 2021;21(2):2422–33. doi:10.1109/jsen.2020.3021731.
14. Azam F, Yadav SK, Priyadarshi N, Padmanaban S, Bansal RC. A comprehensive review of authentication schemes in vehicular ad-hoc network. IEEE Access. 2021;9:31309–21. doi:10.1109/access.2021.3060046.
15. Muhammad K, Ullah A, Lloret J, Ser JD, Albuquerque VHCD. Deep Learning for safe autonomous driving: current challenges and future directions. IEEE Trans Intell Transp Syst. 2021;22(7):4316–36. doi:10.1109/tits.2020.3032227.
16. Jenefa J, Mary Anita EA. Secure Authentication schemes for vehicular Adhoc networks: a survey. Wirel Pers Commun. 2022;123(1):31–68. doi:10.1007/s11277-021-09118-3.
17. Dong S, Su H, Xia Y, Zhu F, Hu X, Wang B. A comprehensive survey on authentication and attack detection schemes that threaten it in vehicular ad-hoc networks. IEEE Trans Intell Transp Syst. 2023;24(12):13573–602. doi:10.1109/tits.2023.3297527.
18. Sripathi Venkata Naga SK, Yesuraj R, Munuswamy S, Arputharaj K. A comprehensive survey on certificate-less authentication schemes for vehicular ad hoc networks in intelligent transportation systems. Sensors. 2023;23(5):2682. doi:10.3390/s23052682.
19. Sutradhar K, Pillai BG, Amin R, Narayan DL. A survey on privacy-preserving authentication protocols for secure vehicular communication. Comput Commun. 2024;219:1–18. doi:10.1016/j.comcom.2024.02.024.
20. Shawky MA, Shah ST, Abdrabou M, Usman M, Abbasi QH, Flynn D, et al. How secure are our roads? An in-depth review of authentication in vehicular communications. Veh Commun. 2024;47:100784. doi:10.1016/j.vehcom.2024.100784.
21. Soujanya BK, Azam F. Ensuring security and privacy in VANET: a comprehensive survey of authentication approaches. J Comput Netw Commun. 2024;2024(1):1818079. doi:10.1155/2024/1818079.
22. Aljehane NO. A study to investigate the role and challenges associated with the use of deep learning in autonomous vehicles. World Electr Veh J. 2024;15(11):518. doi:10.3390/wevj15110518.
23. Zhang J, Wang J, Zang H, Ma N, Skitmore M, Qu Z, et al. The application of machine learning and deep learning in intelligent transportation: a scientometric analysis and qualitative review of research trends. Sustainability. 2024;16(14):5879. doi:10.3390/su16145879.
24. Yang T, Sun R, Rathore RS, Baig I. Enhancing cybersecurity and privacy protection for cloud computing-assisted vehicular network of autonomous electric vehicles: applications of machine learning. World Electr Veh J. 2025;16(1):14. doi:10.3390/wevj16010014.
25. Pali I, Amin R, Abdussami M. Autonomous vehicle security: current survey and future research challenges. Secur Priv. 2024;7(3):e367. doi:10.1002/spy2.367.
26. Taslimasa H, Dadkhah S, Neto ECP, Xiong P, Ray S, Ghorbani AA. Security issues in Internet of Vehicles (IoV): a comprehensive survey. Internet Things. 2023;22:100809. doi:10.1016/j.iot.2023.100809.
27. Pöllny O, Held A, Kargl F. Survey of air, sea, and road vehicles research for motion control security. IEEE Trans Intell Transp Syst. 2023;24(7):6748–63. doi:10.1109/tits.2023.3264453.
28. Zaboli A, Hong J, Kwon J, Moore J. A survey on cyber-physical security of autonomous vehicles using a context awareness method. IEEE Access. 2023;11:136706–25. doi:10.1109/access.2023.3338156.
29. Sun X, Yu FR, Zhang P. A survey on cyber-security of Connected and Autonomous Vehicles (CAVs). IEEE Trans Intell Transp Syst. 2022;23(7):6240–59. doi:10.1109/tits.2021.3085297.
30. Lai J, Xiong JL. Robust value iteration for optimal control of discrete-time linear systems. Automatica. 2025;174:112121. doi:10.1016/j.automatica.2025.112121.
31. Nandy T, Kolandaisamy R, Noor RM, Bhattacharyya S. An adaptive vehicle location prediction using machine learning: a case study of campus shuttle bus. IEEE Access. 2025;13:78290–302. doi:10.1109/access.2025.3562785.
32. Dang Y, Benzaïd C, Yang B, Taleb T, Shen Y. Deep-ensemble-learning-based GPS spoofing detection for cellular-connected UAVs. IEEE Internet Things J. 2022;9(24):25068–85. doi:10.1109/jiot.2022.3195320.
33. Shang F, Deng X. A data sharing scheme based on blockchain for privacy protection certification of Internet of Vehicles. Veh Commun. 2025;51:100864. doi:10.1016/j.vehcom.2024.100864.

34. Kaur G, Kakkar D. A secure lightweight authentication model with interference aware routing and attack detection approach in VANET. Clust Comput. 2025;28(2):21. doi:10.1007/s10586-024-04772-1.
35. Xu SW, Liu RS. A conditional privacy-preserving identity-authentication scheme for federated learning in the Internet of Vehicles. Entropy. 2024;26(7):23. doi:10.3390/e26070590.
36. Colombathanthri A, Jomaa W, Chinniah YA. Human-centered cyber-physical systems in manufacturing industry: a systematic search and review. Int J Adv Manuf Technol. 2025;136(5–6):2107–41. doi:10.1007/s00170-024-14959-w.
37. Nandy T, Idris MYIB, Noor RM, Ahmedy I, Bhattacharyya S. An enhanced two-factor authentication protocol for V2V communication in VANETs. In: Proceedings of the the 3rd International Conference on Information Science and Systems; 2020 Mar 19–22; Cambridge, UK.
38. Zhang XH, Liu P, Lu BH, Wang Y, Chen XH, Zhang YX, et al. MTSFBet: a hand-gesture-recognition-based identity authentication approach for passive keyless entry against relay attack. IEEE Trans Mob Comput. 2024;23(2):1902–13. doi:10.1109/tmc.2023.3243772.
39. Li YT, Liu L, Deng SJ, Qin HF, El-Yacoubi MA, Zhou G. Memory-augmented autoencoder based continuous authentication on smartphones with conditional transformer gans. IEEE Trans Mob Comput. 2024;23(5):4467–82. doi:10.1109/tmc.2023.3290834.
40. Borra SR, Premalatha B, Divya G, Srinivasarao B, Eshwar D, Reddy VBS, et al. Deep hashing with multilayer CNN-based biometric authentication for identifying individuals in transportation security. J Transp Secur. 2024;17(1):4. doi:10.1007/s12198-024-00272-w.
41. Park H. Edge based lightweight authentication architecture using deep learning for vehicular networks. J Internet Technol. 2022;23(1):193–200.
42. Nandy T, Md Noor R, Kolandaisamy R, Idris MYI, Bhattacharyya S. A review of security attacks and intrusion detection in the vehicular networks. J King Saud Univ—Comput Inf Sci. 2024;36(2):101945. doi:10.1016/j.jksuci.2024.101945.
43. Ju Y, Gao ZP, Wang HY, Liu L, Pei QQ, Dong MX, et al. Energy-efficient cooperative secure communications in mmwave vehicular networks using deep recurrent reinforcement learning. IEEE Trans Intell Transp Syst. 2024;25(10):14460–75. doi:10.1109/tits.2024.3394130.
44. Almehdhar M, Albaseer A, Khan MA, Abdallah M, Menouar H, Al-Kuwari S, et al. Deep learning in the fast lane: a survey on advanced intrusion detection systems for intelligent vehicle networks. IEEE Open J Veh Technol. 2024;5:869–906. doi:10.1109/ojvt.2024.3422253.
45. Nandy T, Idris MYI, Noor RM, Das AK, Li X, Ghani NA, et al. An enhanced lightweight and secured authentication protocol for vehicular ad-hoc network. Comput Commun. 2021;177:57–76. doi:10.1016/j.comcom.2021.06.013.
46. Zhang H, Li M. Towards an intelligent and automatic irrigation system based on internet of things with authentication feature in VANET. J Inf Secur Appl. 2025;88:103927. doi:10.1016/j.jisa.2024.103927.
47. Islam KT, Raj RG, Shamsul Islam SM, Wijewickrema S, Hossain MS, Razmovski T, et al. A vision-based machine learning method for barrier access control using vehicle license plate authentication. Sensors. 2020;20(12):3578. doi:10.3390/s20123578.
48. Xun Y, Liu J, Kato N, Fang Y, Zhang Y. Automobile driver fingerprinting: a new machine learning based authentication scheme. IEEE Trans Ind Inform. 2020;16(2):1417–26. doi:10.1109/tii.2019.2946626.
49. Qiu X, Yu J, Jiang W, Sun X. Intelligent security authentication for connected and autonomous vehicles: attacks and defenses. Electronics. 2024;13(8):1577. doi:10.3390/electronics13081577.
50. Umar M, Wang J, Ahmad HK, Zhao S, Li F, Wang S, et al. Multiple attributes based physical layer authentication through propagation scenario identification in the internet of vehicles. Veh Commun. 2024;45:100708. doi:10.1016/j.vehcom.2023.100708.
51. Liu SY, You ST, Zeng CJ, Yin H, Lin ZZ, Dong YQ, et al. Data source authentication of synchrophasor measurement devices based on 1D-CNN and GRU. Electr Power Syst Res. 2021;196:4. doi:10.1016/j.epsr.2021.107207.
52. Shen X, Huang C, Pu W, Wang D. A lightweight authentication with dynamic batch-based group key management using LSTM in VANET. Secur Commun Netw. 2022;2022:9779670. doi:10.1155/2022/9779670.

53. Ding KM, Chen SP, Zeng Y, Wang YY, Yan XY. Transformer-based subject-sensitive hashing for integrity authentication of high-resolution remote sensing (HRRS) images. Appl Sci. 2023;13(3):21. doi:10.3390/app13031815.
54. Winston JJ, Turker GF, Kose U, Hemanth DJ. Novel optimization based hybrid self-organizing map classifiers for iris image recognition. Int J Comput Intell Syst. 2020;13(1):1048–58.
55. Qin JM, Xun YJ, Deng ZY, Liu JJ. GPIDS: GAN assisted contextual pattern-aware intrusion detection system for IVN. IEEE Trans Veh Technol. 2024;73(9):12682–93. doi:10.1109/tvt.2024.3383449.
56. Narayanan KL, Naresh R. Privacy-preserving dual interactive wasserstein generative adversarial network for cloud-based road condition monitoring in VANETs. Appl Soft Comput. 2024;154:111367. doi:10.1016/j.asoc.2024.111367.
57. Fei CY, Zhang XM, Wang DY, Hu HM, Huang R, Wang ZJ. EPRNG: effective pseudo-random number generator on the internet of vehicles using deep convolution generative adversarial network. Information. 2025;16(1):21. doi:10.3390/info16010021.
58. Hemavathi, Akhila S, Zubeda S, Shashidhara R. DS2AN: deep stacked sparse autoencoder for secure and fast authentication in HetNets. Secur Priv. 2022;5(3):e208. doi:10.1002/spy2.208.
59. Saponara S, Elhanashi A, Gagliardi A. Reconstruct fingerprint images using deep learning and sparse autoencoder algorithms. In: Proceedings of the Conference on Real-Time Image Processing and Deep Learning; 2021 Apr 12–16; Online.
60. Chen YR, He HY, Liu SJ, Zhang YY, Li Y, Xing B, et al. Physical layer authentication for industrial control based on convolutional denoising autoencoder. IEEE Internet Things J. 2024;11(9):15633–41. doi:10.1109/jiot.2023.3347603.
61. Azri A, Haddi A, Allali H. IUAutoTimeSVD++: a hybrid temporal recommender system integrating item and user features using a contractive autoencoder. Information. 2024;15(4):204. doi:10.3390/info15040204.
62. Meng R, Xu XD, Wang BZ, Sun H, Xia SD, Han SJ, et al. Physical-layer authentication based on hierarchical variational autoencoder for industrial internet of things. IEEE Internet Things J. 2023;10(3):2528–44. doi:10.1109/jiot.2022.3213593.
63. Qiu YL, Peng XY, Huang XR, Chai Z, Li MY, Hu WS, et al. Variational autoencoder-assisted unsupervised hardware fingerprint authentication in a fiber network. Opt Lett. 2024;49(8):2029–32. doi:10.1364/ol.518952.
64. Li YT, Ouyang CK, Huang HY. AEGANAuth: autoencoder gan-based continuous authentication with conditional variational autoencoder generative adversarial network. IEEE Internet Things J. 2024;11(16):27635–50. doi:10.1109/jiot.2024.3399549.
65. Wang CL, Zhang YX, Ma YR, Chen P, Xiang Y. CNN-based continuous authentication for digital therapeutics using variational autoencoder. J Supercomput. 2025;81(1):5. doi:10.1007/s11227-024-06490-2.
66. Manimurugan S, Karthikeyan P, Narmatha C, Aborokbah MM, Paul A, Ganesan S, et al. A hybrid Bi-LSTM and RBM approach for advanced underwater object detection. PLoS One. 2024;19(11):e0313708. doi:10.1371/journal.pone.0313708.
67. Sakthi B, Sundar D. An efficient attention-based hybridized deep learning network with deep RBM features for customer behavior prediction in digital marketing. Kybernetes. 2024;4:35. doi:10.1108/K-03-2024-0837.
68. Rani S, Raj PVP, Khedr AM. SDESA: secure cloud computing with gradient deep belief network and congruential advanced encryption. J Supercomput. 2024;80(15):23147–76. doi:10.1007/s11227-024-06322-3.
69. Althubiti SA. A Trust aware authentication scheme for wireless sensor networks optimized by salp swarm optimization and deep belief networks. Math Probl Eng. 2022;2022(1):7842287. doi:10.1155/2022/7842287.
70. Yahuza M, Idris MYI, Wahab AWA, Nandy T, Ahmedy IB, Ramli R. An edge assisted secure lightweight authentication technique for safe communication on the internet of drones network. IEEE Access. 2021;9:31420–40. doi:10.1109/access.2021.3060420.
71. Samriya JK, Kumar M, Gill SS. Secured data offloading using reinforcement learning and Markov decision process in mobile edge computing. Int J Netw Manage. 2023;33(5):e2243. doi:10.1002/nem.2243.
72. Shinde SS, Tarchi D. A Markov decision process solution for energy-saving network selection and computation offloading in vehicular networks. IEEE Trans Veh Technol. 2023;72(9):12031–46. doi:10.1109/tvt.2023.3264504.
73. Shi F, Wang SF, Cai ZX, Peng Y, Liu YC, Wang Y, et al. Few-shot specific emitter identification via neural architecture search and deep transfer learning. In: Proceedings of the IEEE 99th Vehicular Technology Conference (VTC-Spring); 2024 Jun 24–27; Singapore.

74. Sakr AS, Plawiak P, Tadeusiewicz R, Hammad M. Cancelable ECG biometric based on combination of deep transfer learning with DNA and amino acid approaches for human authentication. Inf Sci. 2022;585:127–43. doi:10.1016/j.ins.2021.11.066.
75. Chen JJ, Zhu JQ, Zhuo YL, Ye HF, Wang ZS, Liu HX. An improved dynamic programming algorithm for security-constrained unit commitment under spatial-temporal decomposition framework. Int J Electr Power Energy Syst. 2024;155:109652. doi:10.1016/j.ijepes.2023.109652.
76. Zhu JQ, Zeng K, Chen JJ, Zhao WM, Liu WH, Zhu WK. Transfer-based approximate dynamic programming for rolling security-constrained unit commitment with uncertainties. Prot Control Mod Power Syst. 2024;9(5):42–53. doi:10.23919/pcmp.2023.000140.
77. Dong BT, Huang LY, Ma XW, Chen HT, Zhang WD. Visionary policy iteration for continuous control. IEEE Trans Syst Man Cybern-Syst. 2025;55(4):2707–20. doi:10.1109/tsmc.2025.3525473.
78. Chen GY. Deep neural network approximations for the stable manifolds of the Hamilton-Jacobi-Bellman equations. IEEE Trans Autom Control. 2024;69(10):7239–46. doi:10.1109/tac.2024.3396107.
79. Wang XJ, Xu YL, Wang HY, Kang MZ, Hua J, Wang FY. Region-farm crop planning through double deep q-learning toward sustainable agriculture. IEEE Trans Comput Soc Syst. 2024;11(6):7608–17. doi:10.1109/tcss.2024.3441543.
80. Roy PP, Teju V, Kandula SR, Sowmya KV, Stan AI, Stan OP. Secure healthcare model using multi-step deep q learning network in internet of things. Electronics. 2024;13(3):669. doi:10.3390/electronics13030669.
81. Chakour I, Mhammedi S, Daoui C, Baslam M. Unlocking QoS potential: integrating IoT services and Monte Carlo control for heterogeneous IoT device management in gateways. Comput Netw. 2024;238:110134. doi:10.1016/j.comnet.2023.110134.
82. Nocco C, Brunetti A, Lins SAB. Monte Carlo simulations of ED-XRF Spectra as an authentication tool for nuragic bronzes. Heritage. 2021;4(3):1912–9. doi:10.3390/heritage4030108.
83. Wu GW, Chen XH, Shen YZ, Xu ZQ, Zhang H, Shen SG, et al. Combining Lyapunov optimization with actor-critic networks for privacy-aware IIoT computation offloading. IEEE Internet Things J. 2024;11(10):17437–52. doi:10.1109/jiot.2024.3357110.
84. Ribeiro DA, Melgarejo DC, Saadi M, Rosa RL, Rodríguez DZ. A novel deep deterministic policy gradient model applied to intelligent transportation system security problems in 5G and 6G network scenarios. Phys Commun. 2023;56:101938. doi:10.1016/j.phycom.2022.101938.
85. Jiu D, Wang YC, Liu MQ, Cheng JL. Deep deterministic policy gradient-based physical layer authentication scheme under unknown attacking environment. IEEE Wirel Commun Lett. 2024;13(11):3247–51. doi:10.1109/lwc.2024.3464858.
86. Pan X, Li S, Li R, Sun N. A hybrid deep learning algorithm for the license plate detection and recognition in vehicle-to-vehicle communications. IEEE Trans Intell Transp Syst. 2022;23(12):23447–58. doi:10.1109/tits.2022.3213018.
87. Roy K, Ahmad M, Ghani NA, Uddin J, Shin J. An automated precise authentication of vehicles for enhancing the visual security protocols. Information. 2023;14(8):466. doi:10.3390/info14080466.
88. Mohammed A, Kora R. A comprehensive review on ensemble deep learning: opportunities and challenges. J King Saud Univ—Comput Inf Sci. 2023;35(2):757–74. doi:10.1016/j.jksuci.2023.01.014.
89. Song L, Sun G, Yu H, Du X, Guizani M. FBIA: a fog-based identity authentication scheme for privacy preservation in Internet of vehicles. IEEE Trans Veh Technol. 2020;69(5):5403–15. doi:10.1109/tvt.2020.2977829.
90. Du HP, Nguyen AD, Nguyen DT, Nguyen HN, Nguyen DHP. A novel deep ensemble learning to enhance user authentication in autonomous vehicles. IEEE Trans Autom Sci Eng. 2024;21(3):2362–73. doi:10.1109/tase.2023.3270764.
91. Jia J, Kumarasamy SS, Pokkuluri KS, Kumar KS, Priyanka TP, Wang F. A robust authentication and trust detection with privacy preservation of data for fog computing in VANET using adaptive deep neural network. IEEE Access. 2024;12:161227–46. doi:10.1109/access.2024.3486811.
92. Zhang J, Wang Z, Yan Q. Intelligent user identity authentication in vehicle security system based on wireless signals. Complex Intell Syst. 2022;8(2):1243–57. doi:10.1007/s40747-021-00593-6.

93. Inzillo V, Garompolo D, Giglio C. Enhancing smart city connectivity: a multi-metric CNN-LSTM beamforming based approach to optimize dynamic source routing in 6G networks for MANETs and VANETs. Smart Cities. 2024;7(5):3022–54. doi:10.3390/smartcities7050118.
94. Chougule A, Kulkarni I, Alladi T, Chamola V, Yu FR. HybridSecNet: in-vehicle security on controller area networks through a hybrid two-step LSTM-CNN model. IEEE Trans Veh Technol. 2024;73(10):14580–91. doi:10.1109/tvt.2024.3413849.
95. Khan FM, Rahman T, Zeb A, Haider ZA, Khan IU, Bilal H, et al. Vehicular network security through optimized deep learning model with feature selection techniques. IECE Trans Sens Commun Control. 2024;1(2):136–53. doi:10.62762/tscc.2024.626147.
96. Minu MS, Rani PJI, Sonthi VK, Shankar G, Mohan E, Rajesh A. An innovative privacy preservation and security framework with fog nodes in enabled vanet system using hybrid encryption techniques. Peer-to-Peer Netw Appl. 2024;17(4):2065–89. doi:10.1007/s12083-024-01672-4.
97. Eman M, Mahmoud TM, Ibrahim MM, Abd El-Hafeez T. Innovative hybrid approach for masked face recognition using pretrained mask detection and segmentation, robust PCA, and KNN classifier. Sensors. 2023;23(15):6727. doi:10.3390/s23156727.
98. Candell R, Remley C. Radio frequency measurements for selected manufacturing and industrial environments [Dataset]. Gaithersburg, MD, USA: National Institute of Standards and Technology; 2016.
99. Pulligilla MK, Vanmathi C. An authentication approach in SDN-VANET architecture with Rider-Sea Lion optimized neural network for intrusion detection. Internet Things. 2023;22:100723. doi:10.1016/j.iot.2023.100723.
100. Kalinin MO, Krundyshev VM, Rezedinova EY, Reshetov DV. Hierarchical software-defined security management for large-scale dynamic Networks. Autom Control Comput Sci. 2018;52(8):906–11. doi:10.3103/s014641161808014x.
101. Nandy T, Idris MYIB, Noor RM, Bhattacharyya S, Ghani NBA. Collaborative data anonymization for privacy-preserving vehicular Ad-hoc Network. In: Proceedings of the 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT); 2020 Dec 20–21; Manama, Bahrain.
102. Nandy T, Bin Idris MYI, Noor RM, Kiah MLM, Lun LS, Juma'at NBA, et al. Review on security of internet of things authentication mechanism. IEEE Access. 2019;7:151054–89. doi:10.1109/access.2019.2947723.
103. Yuan JS, Li B, Mei XM, Zhou YF. Real-time tracking and authentication protocol for anonymous operating vehicles in vehicle-infrastructure collaborative systems. IEEE Access. 2024;12:16218–32. doi:10.1109/access.2024.3357490.
104. Xu JW, Wang LL, Wen M, Long Y, Chen KF. DPB-MA: low-latency message authentication scheme based on distributed verification and priority in vehicular Ad Hoc network. IEEE Trans Veh Technol. 2023;72(4):5152–66. doi:10.1109/tvt.2022.3225204.
105. Ku G, Choi C, Yang C, Jeong J, Kim P, Park S, et al. Electrocardiogram-based driver authentication using autocorrelation and convolutional neural network techniques. Electronics. 2024;13(24):4974. doi:10.3390/electronics13244974.
106. Mishra L, Kaabouch N. Impact of weather factors on unmanned aerial vehicles' wireless communications. Future Internet. 2025;17(1):27. doi:10.3390/fi17010027.
107. Zhang M, Lu L, Wu YH, Yan Z, Sun JQ, Lin F, et al. DroneAudioID: a lightweight acoustic fingerprint-based drone authentication system for secure drone delivery. IEEE Trans Inf Forensic Secur. 2025;20:1447–61. doi:10.1109/tifs.2025.3527814.
108. Wang LL, Xu JW, Qin BD, Wen M, Chen KF. An efficient fuzzy certificateless signature-based authentication scheme using anonymous biometric identities for vanets. IEEE Trans Dependable Secur Comput. 2025;22(1):292–307. doi:10.1109/tdsc.2024.3392470.
109. Wen LH, Hu LY, Zhou W, Ren G, Zhang N. Soft actor-critic deep reinforcement learning for train timetable collaborative optimization of large-scale urban rail transit network under dynamic demand. IEEE Trans Intell Transp Syst. 2025;26(5):7021–35. doi:10.1109/tits.2025.3525538.
110. Qiu CQ, Tang H, Xu XX, Peng Y, Liu X, Ji J, et al. Lightweight real-time vehicle collision warning based on deep learning multi-scale feature fusion. J Automob Eng. 2024;13:09544070241297552. doi:10.1177/09544070241297552.
111. Li BC, Li CG. Optimization of video surveillance system deployment based on space syntax and deep reinforcement learning. Electronics. 2025;14(1):38. doi:10.3390/electronics14010038.

112. IEEE 1609.2-2022 IEEE standard for wireless access in vehicular environments—security services for application and management messages. New, York, NY, USA: IEEE; 2023.
113. Bocharov V, Besancon R, de Chalendar G, Ferret O, Semmar N. From LIMA to DeepLIMA: following a new path of interoperability. Lang Resour Eval. 2024;58(4):1463–80. doi:10.1007/s10579-024-09773-5.
114. Guth F, Ménard B, Rochette G, Mallat S. A rainbow in deep network black boxes. J Mach Learn Res. 2024;25(350):1–59.
115. Efe EM, Böcekçi VG. Deep learning-driven regulation of vehicle speed limits in response to weather conditions. Trait Du Signal. 2023;40(6):2321–36. doi:10.18280/ts.400601.
116. Ta QT, Mac VH, Huh J, Yim HJ, Lee G. Automatic detection of subsurface defects in concrete structures using state-of-the-art deep learning-based object detectors on the infrared dataset. Eng Struct. 2025;329:119829. doi:10.1016/j.engstruct.2025.119829.
117. Ramesh SH, Basava A, Perumal SP. BENN: balanced ensemble neural network for handling class imbalance in big data. Expert Syst. 2025;42(2):e13754. doi:10.1111/exsy.13754.
118. Zhou KL, Zhang ZY, Lu XH. Non-intrusive load monitoring based on an efficient deep learning model with local feature extraction. IEEE Trans Ind Inform. 2024;20(7):9497–507. doi:10.1109/tii.2024.3383521.
119. Sicari S, Cevallos MJF, Rizzardi A, Coen-porisini A. Open-ethical AI: advancements in open-source human-centric neural language models. Acm Comput Surv. 2025;57(4):1–47. doi:10.1145/3703454.
120. Ryu R, Yeom S, Herbert D, Dermoudy J. A comprehensive survey of context-aware continuous implicit authentication in online learning environments. IEEE Access. 2023;11:24561–73. doi:10.1109/access.2023.3253484.
121. Zhao JY, Nan JR, Wang JB, Ling HP, Lian YB, Burke A, et al. Battery diagnosis: a lifelong learning framework for electric vehicles. In: Proceedings of the IEEE Vehicle Power and Propulsion Conference (VPPC); 2022 Nov 1–4; Merced, CA, USA.
122. Shanmugavalli V, Kannan AR. Optimizing dynamic keystroke pattern recognition with hybrid deep learning technique and multiple soft biometric factors. Int J Comput Commun Control. 2024;19(2):816–26. doi:10.15837/ijccc.2024.2.6097.
123. dos Santos FC, Duarte-Figueiredo F, De Grande RE, dos Santos AL. Enhancing a fog-oriented IoT authentication and encryption platform through deep learning-based attack detection. Internet Things. 2024;27:16. doi:10.1016/j.iot.2024.101310.
124. Kumar R, Javeed D, Aljuhani A, Jolfaei A, Kumar P, Islam A. Blockchain-based authentication and explainable ai for securing consumer IoT applications. IEEE Trans Consum Electron. 2024;70(1):1145–54. doi:10.1109/tce.2023.3320157.
125. Nandy T, Idris MYI, Noor RM, Wahab AWA, Bhattacharyya S, Kolandaisamy R, et al. A secure, privacy-preserving, and lightweight authentication scheme for VANETs. IEEE Sens J. 2021;21(18):20998–1011. doi:10.1109/jsen.2021.3097172.
126. Zhang JH, Wei J. On the security of privacy-enhanced authentication protocol for federated learning in VANETs. IEEE Trans Inf Forensic Secur. 2024;19:9433–5. doi:10.1109/tifs.2024.3445730.
127. Yuan XH, Liu JQ, Wang B, Wang W, Wang B, Li T, et al. FedComm: a privacy-enhanced and efficient authentication protocol for federated learning in vehicular Ad-Hoc networks. IEEE Trans Inf Forensic Secur. 2024;19:777–92. doi:10.1109/tifs.2023.3324747.
128. Shen ZH, Li S, Zhao X, Zou JH. MMAuth: a continuous authentication framework on smartphones using multiple modalities. IEEE Trans Inf Forensic Secur. 2022;17:1450–65. doi:10.1109/tifs.2022.3160361.
129. Bulat R, Ogiela MR. Personalized context-aware authentication protocols in IoT. Appl Sci. 2023;13(7):11.
130. Liu JH, Yang J, Huang XY, Xu L, Xiang Y. Privacy enhanced authentication for online learning healthcare systems. IEEE Trans Serv Comput. 2024;17(4):1670–81. doi:10.1109/tsc.2023.3348497.
131. Raouf HA, Fouda MM, Ibrahem MI. Revolutionizing user authentication exploiting explainable AI and CTGAN-based keystroke dynamics. IEEE Open J Comput Soc. 2025;6:97–108. doi:10.1109/ojcs.2024.3513895.
132. Ahmed A, Yang PL, Mirza AF, Khan T, Rizwan M, Hawbani A, et al. SipDeep: swallowing-based transparent authentication via bone-conducted in-ear acoustics. IEEE Trans Mob Comput. 2024;23(12):14171–85. doi:10.1109/tmc.2024.3450919.

133. Khan R, Mehmood A, Maple C, Curran K, Song HH. Performance analysis of blockchain-enabled security and privacy algorithms in connected and autonomous vehicles: a comprehensive review. IEEE Trans Intell Transp Syst. 2024;25(6):4773–84. doi:10.1109/tits.2023.3341358.
134. Gautam D, Thakur G, Kumar P, Das AK, Park Y. Blockchain assisted intra-twin and inter-twin scheme for vehicular digital twin system. IEEE Trans Intell Transp Syst. 2024;25(10):15002–15. doi:10.1109/tits.2024.3394438.
135. Razmjouei P, Kavousi-Fard A, Dabbaghjamanesh M, Jin T, Su W. Ultra-lightweight mutual authentication in the vehicle based on smart contract blockchain: case of MITM attack. IEEE Sens J. 2021;21(14):15839–48. doi:10.1109/jsen.2020.3022536.
136. Roy PK, Kumar P, Bhattacharya A. ZeroVCS: an efficient authentication protocol without trusted authority for zero-trust vehicular communication systems. Future Gener Comput Syst. 2025;163:107520. doi:10.1016/j.future.2024.107520.
137. Annabi M, Zeroual A, Messai N. Towards zero trust security in connected vehicles: a comprehensive survey. Comput Secur. 2024;145:104018. doi:10.1016/j.cose.2024.104018.
138. Zeng MW, Cui J, Zhang QY, Zhong H, He DB. Efficient revocable cross-domain anonymous authentication scheme for IIoT. IEEE Trans Inf Forensic Secur. 2025;20:996–1010. doi:10.1109/tifs.2024.3523198.
139. Chittoriya S, Shivdeep, Jha KK, Das DM, Sharma R. A low-overhead puf based hardware security technique to prevent scan chain attacks for industry-standard DFT architecture. In: Proceedings of the IEEE 65th International Midwest Symposium on Circuits and Systems (MWSCAS); 2022 Aug 7–10; Fukuoka, Japan.
140. Liu HJ, Jiang SR, Qi XX, Qu Y, Li H, Li TT, et al. Detect software vulnerabilities with weight biases via graph neural networks. Expert Syst Appl. 2024;238:121764. doi:10.1016/j.eswa.2023.121764.
141. Feng B, Xu HT, Huang G, Liu ZP, Guo CX, Chen Z. Byzantine-resilient economical operation strategy based on federated deep reinforcement learning for multiple electric vehicle charging stations considering data Privacy. J Mod Power Syst Clean Energy. 2024;12(6):1957–67. doi:10.1109/psgec62376.2024.10720999.
142. Prateek K, Maity S, Saxena N. QSKA: a quantum secured privacy-preserving mutual authentication scheme for energy internet-based vehicle-to-grid communication. IEEE Trans Netw Serv Manage. 2024;21(6):6810–26. doi:10.1109/tnsm.2024.3445972.
143. Ying XH, Bernieri G, Conti M, Bushnell L, Poovendran R. Covert channel-based transmitter authentication in controller area networks. IEEE Trans Dependable Secur Comput. 2022;19(4):2665–79. doi:10.1109/tdsc.2021.3068213.