Utilising blockchain technology and federated learning on the internet of vehicles for the preservation of security and privacy: systematic review

Wisam Makki Alwash*

Department of Computer Engineering,
Faculty of Electrical and Electronics Engineering,
Yildiz Technical University,
Istanbul, Turkey
Email: wisam.alwash@std.yildiz.edu.tr
Email: wissam.alwash@gmail.com
*Corresponding author

Muhammed Ali Aydin

Department of Computer Engineering,
Faculty of Engineering,
Istanbul University-Cerrahpasa,
Istanbul, Turkey
Email: aydinali@iuc.edu.tr

Hasan Hüseyin Balik

Department of Computer Engineering,
Faculty of Engineering,
Istanbul Aydin University,
Istanbul, Turkey
Email: balik@aydin.edu.tr

Abstract: In the field of the IoV, connected vehicles utilise network connections to improve transportation efficiency and safety. This will give rise to a range of vulnerabilities, specifically advanced cyber-attacks. These breaches will interrupt the normal functioning of vehicles and pose a significant hazard to the safety of passengers. This paper explores and reviews systematically the dual application of blockchain technology and FL as a fortified defence mechanism within the IoV ecosystem. This article presents illustrations of the risks present within the IoV domain and evaluates the efficacy of existing blockchain and FL methodologies, outlined in several papers, in addressing these potential challenges, particularly in the field of security and privacy. The paper provides an analysis of the advantages, limitations, and factors associated with these technologies in the context of maintaining the security and privacy of the IoV.

Keywords: internet of vehicles; IoV; cyber-attacks; security; privacy; blockchain; federated learning; FL.

Reference to this paper should be made as follows: Alwash, W.M., Aydin, M.A. and Balik, H.H. (xxxx) 'Utilising blockchain technology and federated learning on the internet of vehicles for the preservation of security and privacy: systematic review', *Int. J. Web and Grid Services*, Vol. X, No. Y, pp.xxx–xxx.

Biographical notes: Wisam Makki Alwash completed his MSc (2003) and BSc (2000) degrees in Computer Science at Al-Nahrain University/College of Science/Department of Computer Science, Baghdad-Iraq. He is a lecturer at the University of Babylon. He is currently a PhD student at the Department of Computer Engineering/Yildiz Technical University. His research encompasses Cyber Security, Software, IoT, Computer Networks, and Communications.

Muhammed Ali Aydin completed his undergraduate degree in Computer Engineering at Istanbul University's Faculty of Engineering in 2001. He earned his Master's and PhD degrees in Computer Engineering from Istanbul Technical University and Istanbul University, respectively. He is currently an Associate Professor at the Department of Computer Engineering, at Istanbul University-Cerrahpasa. His research encompasses cyber security, software, IoT, computer networks, and communications.

Hasan Hüseyin Balik is currently with the Faculty of Engineering, Department of Computer Engineering, Istanbul Aydın University, Florya Campus, Küçükçekmece, İstanbul, Turkey, in the fields of computer networks, computer organisation and architecture, operating systems, sensors and sensor networks, biomedical networks, bio-informatics, distance learning, computer system design and management, forensics, computer and network security, electromagnetic fields and waves, and enterprise resource planning implementation and management.

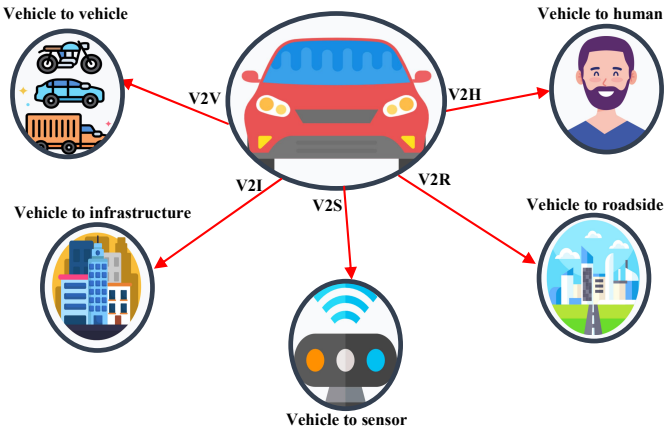
1 Introduction

The effectiveness and security of transportation networks are crucial for companies that depend on the prompt delivery of products and services in today's continuously changing environment. Yet, the expense of modernising and maintaining transportation infrastructure as well as specific vehicles can be a major impediment. By 2035, there will be 2 billion vehicles on the planet, according to the latest review. Advanced technologies like cloud computing, integrated processing units, and IoT-based systems are being created and enhanced to address this issue and increase the efficiency and dependability of modern vehicles (Abiodun et al., 2021).

Vehicular ad hoc networks (VANETs) offer a fundamental framework for connecting to and corresponding with moving objects within a designated or limited range. They are unable to fully analyse or maintain global real-time data, though. The internet of vehicles (IoV), in contrast, combines intelligence and connectivity to link vehicles, people, networks, vehicle traffic, and routes in order to create dependable and efficient services. A global network can be developed to assess all real-time data by connecting vehicles and other cyber-physical elements, including sensors, the internet, and satellites. This will result in a world where transportation is safer, more dependable, and more efficient. VANETs consist of only vehicles connected in an ad-hoc manner exchanging data with each other, while IoV spans a bigger network involving entities such as humans, things,

and other heterogeneous networks (Lone et al., 2021). Figure 1 illustrates various categories of links for communication within the IoV network.

Figure 1 Types of IoV network communications connections (see online version for colours)



Since the introduction of smart vehicles with integrated sensors and electronic control units (ECUs), the IoV has been developing technology. These devices contribute to the long-awaited objective of autonomous transportation (Garg et al., 2022). Wireless communication has additionally opened the way for quicker data transfer, increased reliability, decreased latency, and accessibility. Various protocols and applications are used in the IoV to employ these wireless communication enhancements (Duan et al., 2020). IoV is, broadly speaking; the combination of VANET and the internet of things (IoT). Currently, connected vehicles utilise IoT to establish connections to networks and gain access to real-time traffic data, routing, and other driving aids (Dureja and Sangwan, 2021).

While IoV provides numerous benefits, it is also extremely vulnerable to attack. IoV leverages numerous networking technologies that enable the connection between various units within the vehicle in addition to communication between various road entities (for instance, other vehicles and wayside infrastructure) to facilitate intelligent knowledge sharing. Nevertheless, network connectivity carries inherent risks, particularly given that the IoV network contains numerous IoT sensors and processors. In addition, continuous interaction among road entities along the network makes IoV a vulnerable target for intruders (Sun et al., 2022). IoV security is a significant concern because erroneous information that affects the vehicles' decision-making could result in human casualties. Attackers may use the flaws in networking communication to carry out malicious actions like seizing control of the vehicle, disseminating false information over the network, and other attacks that jeopardise the confidentiality, integrity, and availability of the vehicle system as well as the legitimacy of users. Furthermore, autonomous driving generates vast quantities of data that may be used to feed artificial intelligence (AI) applications and data mining. Due to the sensitivity of data communicated between users, the privacy of users' data may be at risk (Alladi et al., 2021).

Due to the aforementioned IoV security risks, it is extremely important to set up security measures involving authentication, integrity of data, confidence, encryption at all

levels, as well as access control. Without these security measures, IoV would be vulnerable to cyberattacks and tampering, which could lead to catastrophic events, breaches of information, alongside the loss of important data (Garg et al., 2020).

To create a productive and effective intelligent transport system (ITS), it is necessary to implement a learning system that not only provides pedestrian safety and other traffic-related services but also has the capacity to identify any type of inconsistency or disruption and take corrective action. Conventional methods for addressing security issues only guarantee safety during obvious attacks. However, the types and instances of these attacks have changed dramatically in recent years. As their signatures are constantly changing, polymorphic virus-based attacks are challenging to identify and predict. In recent years, the conventional machine learning (ML) strategy for detecting any type of security threat in IoV systems has garnered a great deal of attention from researchers (Billah et al,. 2022).

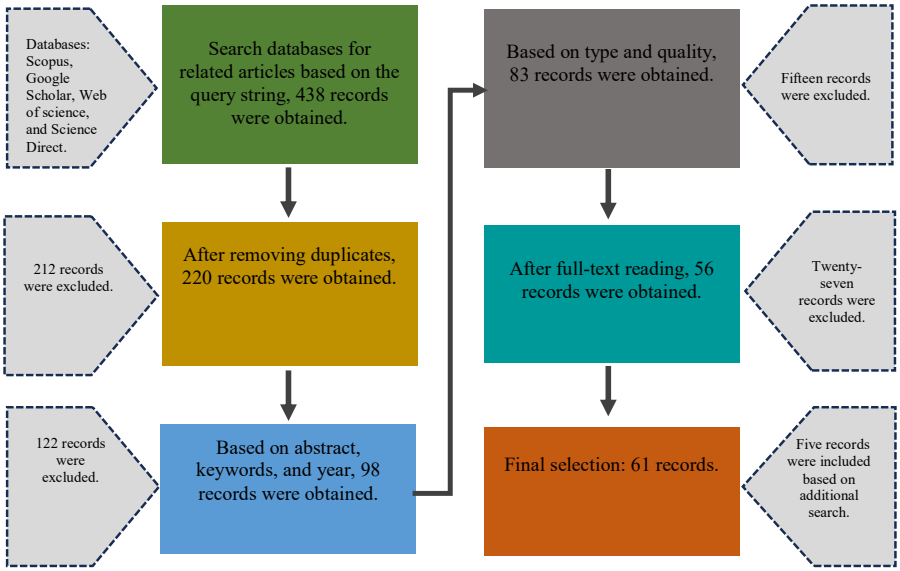
In order to address privacy and security issues IoV may make use of the developing technologies of blockchain and federated learning (FL). The blockchain serves as a digital record-keeping ledger (Aslam et al., 2021; Gadekallu et al., 2022). It has tamper-resistant and tamper-evident properties (Mills et al., 2022; Yu et al., 2021; Yaga et al., 2019) and operates in a decentralised, distributed manner. Google Inc. developed the FL concept to address privacy preservation and communication latency issues that arose from combining data from multiple nodes and storing it centrally (Yarradoddi and Gadekallu, 2022; Parimala et al., 2021). ML techniques produce superior results when additional information is allocated for the training of the model; however, handling such an enormous amount of data during training takes longer. As stated by Agrawal et al. (2021), less-data training requires a shorter duration and produces a less accurate score. A combination of FL and encryption for secrecy ensures practical and feasible solutions that can be integrated into the vehicular network, while blockchain might offer vehicle integrity and trustworthiness (Yu et al., 2021). Inspired by these considerations, this paper aims to present an in-depth review of blockchain and FL integration in vehicular networks.

This article's objective is to enumerate potential threats and investigate ways to enhance IoV security and privacy using blockchain technology and FL. There will be a discussion of different kinds of attacks and protection measures affiliated with the IoV. This article provides a systematic review conducted on the emerging paradigm that combines blockchain with FL within the IoV environment. This systematic review illustrates the integration of blockchain and FL inside the IoV framework, resulting in a convergence of these two technologies. In order to provide a comprehensive overview of the relevant literature, we conducted a systematic review of existing studies that primarily examine aspects such as design, performance optimisation efforts, incentive mechanism design, security, and privacy considerations within the framework domain. The timeframe for this analysis spans from 2018 to 2023 containing reviews regarding blockchain and IoV articles, reviews regarding FL and IoV articles, and reviews literature regarding integrating blockchain and FL with IoV articles. Based on the existing literature, this study's contributions aim to:

- Conduct an examination of the potential hazards and vulnerabilities that pose threats to the IoV network.
- Present a conceptual introduction to blockchain technology and FL.

- The discussion provides an overview of the fundamental principles and key components of blockchain technology and FL, highlighting their significance in the field of technology and their potential applications in other domains.
- Illustrate a systematic literature review (SLR) on the utilisation of blockchain technology in the IoV environment.
- Illustrate a SLR on the utilisation of FL inside the IoV environment.
- Conduct a SLR on the potential benefits of integrating blockchain and FL in the context of the IoV, specifically focusing on the implications for security and privacy.
- Discuss the effects of system unpredictability, vehicle heterogeneity, and statistical disparity on the performance of blockchain-enabled FL frameworks in the IoV context. Outline key research difficulties and potential directions for future investigation.

Figure 2 The literature selection method involves the use of a SLR (see online version for colours)



The steps comprising the SLR are illustrated in Figure 2. In order to conduct a database search, the operator and keywords associated with the necessary literature were incorporated into query strings via AND. The following are the queries used for searching:

'IoV AND Blockchain, internet of vehicles AND blockchain, IoV AND federated learning, internet of vehicles AND federated learning, IoV AND FL, internet of vehicles AND FL, IoV AND blockchain AND federated learning, internet of vehicles AND blockchain AND federated learning, IoV AND blockchain AND FL, internet of vehicles AND blockchain AND FL'.

Using the chosen SLR method, a database search yielded a total of 438 articles, of which only 61 research publications were deemed suitable for the review. Tables 1, 2, 3, and 4, and also Figures 3, 4, 5, and 6 displays the analysis of the research paper's publisher, type of research article, year of publication, and topic of the article, respectively.

Table 1 Number of articles from each publisher

Publisher	*Number of articles*
Springer Link	2
IEEE Xplore	34
MDPI	6
ScienceDirect	8
Sage Journals	1
arXiv	3
Hindawi	1
Wiley	3
Tech Science Press	1
ACM Digital Library	2

Figure 3 Analysis of selected research articles according to the publishers (see online version for colours)

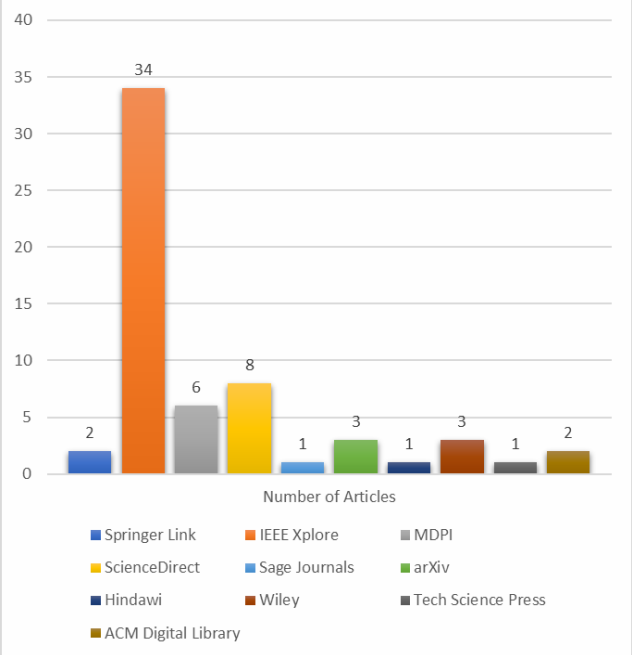


Table 2 Number of articles from each type

Type of research article	*Number of articles*
Journal	44
Conference	17

Figure 4 Analysis of selected research articles according to article types (see online version for colours)

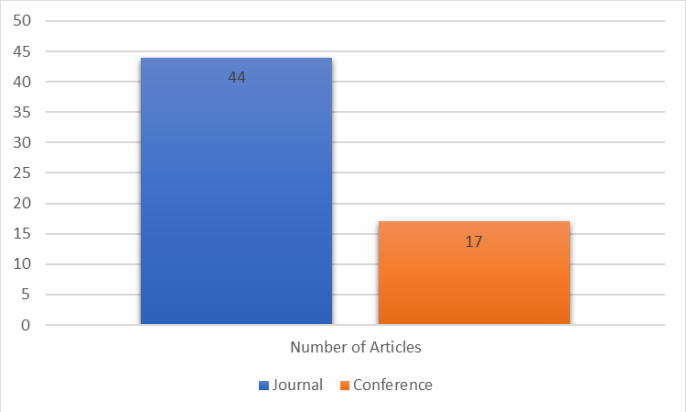


Table 3 Number of articles from each year

Year	*Number of articles*
2018	2
2019	7
2020	6
2021	8
2022	20
2023	18

Table 4 Number of articles from each topic

Topic of article	*Number of articles*
IoV with blockchain focusing on security	18
IoV with blockchain focusing on privacy	3
IoV with blockchain focusing on security and privacy	5
IoV with FL focusing on security	6
IoV with FL focusing on privacy	3
IoV with FL focusing on security and privacy	7
IoV with blockchain and FL focusing on security	7
IoV with blockchain and FL focusing on privacy	5
IoV with blockchain and FL focusing on security and privacy	7

Figure 5 Analysis of selected research articles according to article year (see online version for colours)

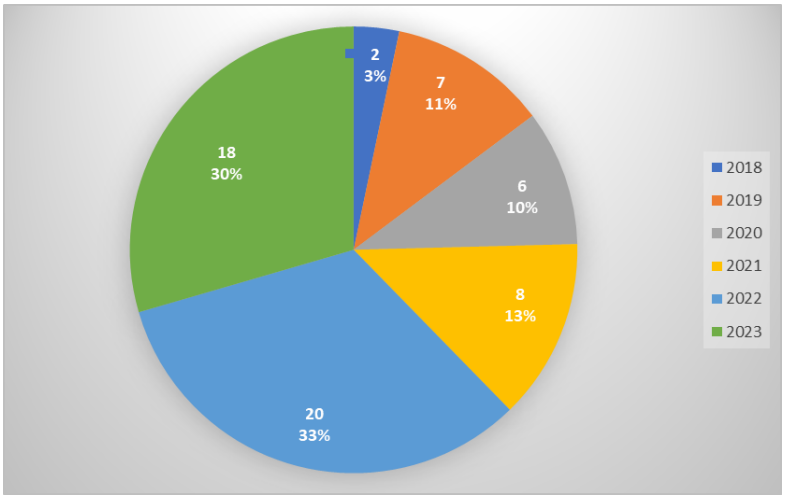
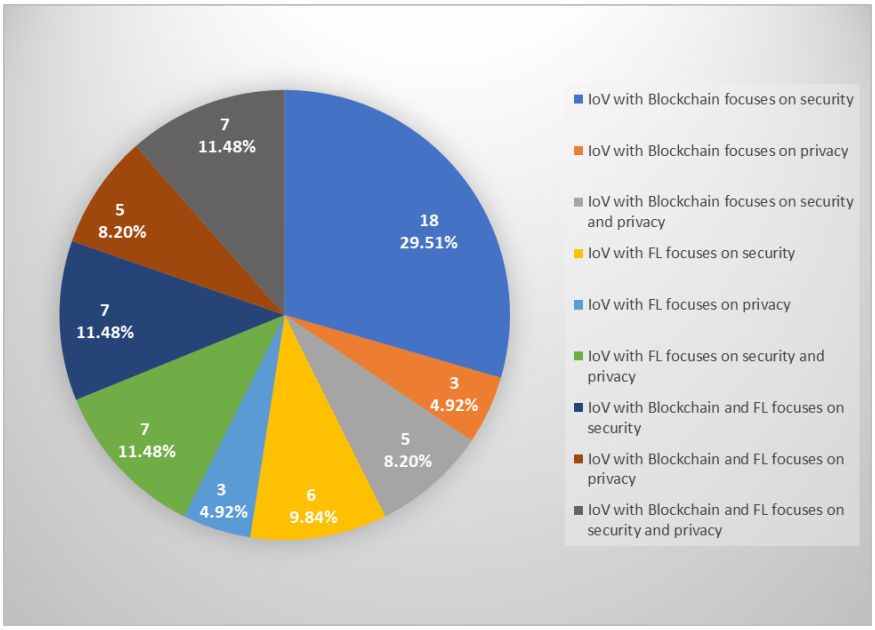


Figure 6 Analysis of selected research articles according to article topic (see online version for colours)



The rest of this article is organised as follows: in Section 2, we introduce the threats to the IoV networks, then in Section 3, we introduce the background and fundamentals of blockchain technology and review the IoV utilising blockchain articles. After that, in Section 4, we introduce the background and fundamentals of FL and review the IoV

utilising FL articles. Subsequently, in Section 5, we present the convergence of blockchain and FL in IoV and analyse the articles regarding IoV utilising blockchain and FL. In Section 6, we discuss the effects of system unpredictability, vehicle heterogeneity, and statistical disparity on the performance of blockchain-enabled FL frameworks in the IoV context. Outline key research difficulties and potential directions for future investigation. Finally, we conclude our review in Section 7.

2 Threats to the IoV networks

The benefits of connected vehicles and the features that they provide have been covered previously, but it's vital to remember that network connectivity has risks as well. With its numerous sensors, data management processors, and open communication interfaces, including vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I), the IoV network can be a tempting target for cybercriminals. It is of the utmost importance to ensure that IoV is secure since anything that interferes with the vehicles' ability to make decisions as a result of incorrect information might have devastating effects. Vehicles also collect user information such as geolocation and other information, and any privacy violation can undermine consumers' faith in the system and harm manufacturers' reputations (Taslimasa et al., 2023). IoV security flaws can jeopardise the networks and vehicle's confidentiality, integrity, availability, and validity. Inter-vehicle attacks (which target communication between vehicles and other vehicles or road infrastructure) and intra-vehicle attacks (which target communication between ECUs and sensors inside a vehicle) are the two basic categories into which these threats can be divided. It is important to note that different security attacks, whether passive or aggressive, insider or outsider can be conducted against IoV. All of these attacks have one thing in common: they all pose a major threat to user security, data integrity, and ultimately, the safety of the drivers and passengers of the vehicle. The literature has identified a number of security assaults and threats in vehicle networks, and a number of the more prevalent ones are highlighted as follows (Sharma and Kaushik, 2019; Al-Jarrah et al., 2019; Nanda et al., 2019; Karim et al., 2022; Ghosal and Conti, 2020; Talpur and Gurusamy, 2021; Balakrishnan et al., 2019; Abbas et al., 2021; Adhikary et al., 2020; Sahraoui et al., 2022; Zhang et al., 2023b; Al-Shareeda et al., 2020; Naveen et al., 2020; Almalki and Song, 2020): GPS deception/spoofing/modification attack, message holding/selfish attack, masquerading/impersonation attack, eavesdropping/stealth attack, routing attack, denial of service (DoS) and distributed denial of service (DDoS) attack, channel interference attack, phishing attack, malware attack, rogue updates attack, man-in-the-middle (MITM) attack, replay attack, Sybil attack, and message tampering/data falsifying attack.

The attacks outlined above illustrate common security flaws that can undermine the confidentiality, integrity, and authentication of the IoV architecture, posing a risk to the overall availability of the entire IoV system. Table 5 presents a comprehensive overview of various attacks, together with accompanying illustrative examples for each approach. A comparison of these attack categories on IoV is shown, along with a discussion of various security attacks, their effects, and the security targets for each category.

Table 5 Overview of various IoV attacks

Attack objective	*Attack method*	*Attack type*	*Attack category*	*Example*
Authentication Integrity	GPS spoofing attack	Active	Intra vehicle	The attacker seeks to deactivate the electronic control unit (ECU) or introduce additional fabricated messages.
Confidentiality Availability	Selfish attack	Active	Inter vehicle	As the quantity of selfish nodes escalates, the availability of information to the infrastructure becomes compromised.
Authentication	Masquerading attack	Active	Inter vehicle	Deceive the server within a charging facility queue by incorporating fictitious nodes.
Confidentiality	Eavesdropping attack	Passive	Inter/intra vehicle	In certain instances, individuals with malicious intent may disguise themselves as authentic road service units (RSUs) in order to unlawfully get private vehicle information. Through the act of eavesdropping on the bus, an adversary has the potential to illegally acquire private driver data, such as data obtained from a connected mobile phone or data acquired by the vehicle.
Authentication Availability	Routing attack	Passive/active	Inter vehicle	The prevention of the broadcast of legitimate packets, the replaying of malicious packets, or the intentional attraction of traffic to interfere with cooperative driving assistance.
Availability	DoS/DDoS attack	Active	Inter/intra vehicle	The prevention of car services from functioning properly and the inability to access information related to road conditions or payment services.
Availability	Channel interference attack	Active	Inter vehicle	Consider vehicle A trying to notify vehicle B of a road obstacle. Channel interference attacks can delay or prevent vehicle a messages from reaching vehicle B. Thus, vehicle B might not have had sufficient opportunity to respond to the impediment, causing an accident.
Authentication	Phishing attack	Passive/active	Inter vehicle	A deceptive access point (AP) masquerades as an authorised AP, inducing unsuspecting individuals to disclose confidential data, such as banking information or other authentication credentials.

Table 5 Overview of various IoV attacks (continued)

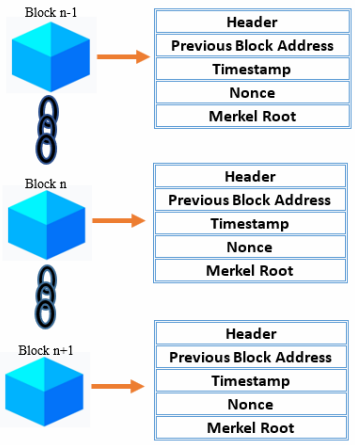
Attack objective	*Attack method*	*Attack type*	*Attack category*	*Example*
Availability Authentication Integrity Confidentiality	Malware attack	Active	Inter/intra vehicle	The navigation system in the vehicle could be compromised by malware, leading to erroneous route guidance.
Availability Authentication Integrity Confidentiality	Rogue updates attack	Active	Inter/intra vehicle	Deploying harmful updates that originate from non-authentic manufacturers to applications.
Confidentiality	MITM attack	Passive/active	Inter vehicle	The data acquired from the global positioning system (GPS) is subject to manipulation.
Authentication	Replay attack	Active	Inter vehicle	Intercepting and subsequently reproducing data packets in order to prevent the disclosure of a vehicle's identification to law enforcement agencies in the case of a vehicular collision.
Authentication Integrity Availability Authentication	Sybil attack	Active	Inter vehicle	An attacker has the capability to generate numerous fake vehicle identities, which can be employed to disseminate inaccurate traffic-related data to other vehicles. This will lead to erroneous decision-making in other vehicles, leading them to choose longer routes in order to avoid nonexistent traffic jams.
Integrity	Message tampering attack	Active	Inter/intra vehicle	Deliberately transmit inaccurate data regarding battery condition, speed, or weather to the server with the intention of compromising the integrity of the energy map or similar directing systems. Engaging in the manipulation of gas levels and speedometer readings.

3 Blockchain technology

Blockchain technology commonly referred to as BC, offers a decentralised storage system for information that encompasses attributes such as transparency and security. It can be thought of as a technological innovation that enables various entities engaged in communication to execute diverse transactions without the need for intermediaries. The verification and certification of these transactions are conducted by specialised nodes. In a blockchain system, the fundamental unit of data is referred to as a block, which is produced through cryptographic processes. The blockchain is responsible for storing and maintaining a comprehensive record of all verified and legitimate transaction data. The credibility of this information is assessed by the members of the network. The conventional composition of a block encompasses two primary components: the block header and the body. The block header contains various metadata elements, like as the previous hash and timestamp, among others. On the other hand, the block body is responsible for storing transaction data. Figure 7 illustrates a representative instance of a fundamental blockchain, characterised by an unbroken succession of interconnected blocks. Nevertheless, BC employs distinct ways to regulate network access. BC can be broken down into three different types based on the underlying mechanisms (Billah et al., 2022):

- Public domain: the public can observe the consensus process. Anyone can view the chain as well as send or receive transactions.
- Private domain: the use of stringent access control measures restricts participation at particular nodes.
- Consortium domain: the system can be seen as partially decentralised, as certain nodes with authoritative capabilities are able to engage in the blockchain network.

Figure 7 Illustration of a simple blockchain's internal structure (see online version for colours)



The majority of scenarios on the IoV include real-time and mobile operations, resulting in the generation and exchange of substantial volumes of data. For instance, it seems improbable that numerous traditional centralised security methods would be appropriate

for such situations. Hence, blockchain technology has the potential to offer a multitude of new solutions for a wide range of security scenarios. In contrast, the incorporation of blockchain technology into the IoV yields benefits like heightened security, privacy, and trust, along with improved system performance and automation. In conclusion, the integration of blockchain technology with the IoVs is necessary in order to facilitate adaptability and effectively manage substantial volumes of data (Chen et al., 2020).

3.1 Review of IoV utilising blockchain

In the IoV network, vehicles communicate through intermediates, making them more vulnerable to rogue vehicles sending incorrect data. Thus, identifying vehicles and service providers is crucial to solving this issue. Personal vehicle information is revealed during authentication. (Sharma and Chakraborty, 2018) created the BLOCKAPP protocol, which uses blockchain technology to address the difficulties listed. This system reduces verifications and speeds up transactions by providing pseudo-IDs to automobiles.

Mendiboure et al. (2018) used SDN and blockchain technology to mitigate IoV security problems. The simulation scenario and conclusions were not described, and theoretical answers were questioned.

The expansion of the IoV has revealed a number of difficulties with regard to data processing, storage, privacy, and security. To tackle these concerns, Jiang et al. (2019) employed blockchain technology in their deployment of the IoV. The researchers conducted a simulation of the network's communication performance using MATLAB and observed that in the presence of traffic congestion, there is a notable increase in the number of retransmissions. This escalation in retransmissions may potentially necessitate a transition to a cellular network. Nevertheless, the research fails to include the potential influence of vehicular congestion or the dependability of cellular infrastructure.

In their research, Wang et al. (2019) investigated the application of a blockchain-based authentication method in the context of IoV networks. The findings of the simulation demonstrate that this particular methodology is capable of effectively managing the exchange of information, ensuring authentication, and implementing encryption measures, all while maintaining a high level of security against potential hostile attacks. Nevertheless, a notable occurrence of packet loss was detected in the vehicle registration and key delivery procedures.

The task of ensuring the security of the IoV network gets increasingly complex as the network expands in size and exhibits greater dynamism. In order to tackle this matter, Rahman et al. (2019) put out a secure architecture grounded in blockchain technology. The framework facilitates the flow of knowledge among vehicles while simultaneously upholding privacy and security measures. The research employed distributed smartphone applications and On-Board Diagnostics II (OBD-II) to collect data and store it within the blockchain. The findings indicated that the framework exhibited robustness in managing a substantial volume of concurrent traffic. However, it was noticed that some connection issues resulted in packet losses.

The soft security enhancement solution put forth by Kang et al. (2019) consists of two parts: a reputation voting mechanism for choosing miners and a contract theory for verifying blocks by standby miners. The simulation results demonstrated that the suggested approach exhibits superior performance compared to conventional reputation

schemes in identifying potential malevolent miners and enhancing the security of shared information.

In the research they performed, Hu et al. (2019) employed a Byzantine consensus algorithm that relied on a time sequence and gossip protocol (BCA-TG) in conjunction with blockchain technology. The objective was to augment the security of communication, consensus, and node authentication within an IoV network. The findings from the simulation indicate that achieving consensus is possible when the proportion of Byzantine nodes is below 50% of the overall number of nodes inside the network. However, additional experimentation is required in practical systems that involve a greater number of nodes and dynamic IoV scenarios.

Cheng et al. (2019) proposed a blockchain-based semi-centralised alternative. This method controls the timing of traffic signals to ensure smooth traffic flow while keeping personal information and collective knowledge secure. However, this paradigm necessitates a decrease in the computational costs associated with interaction and encryption.

Rathee et al. (2019) presented a blockchain-based infrastructure aimed at safeguarding smart sensors against hostile intrusions. The researchers proposed a blockchain architecture specifically designed to tackle security concerns in the context of smart sensors utilised in connected vehicles. These sensors are vulnerable to compromise by skilled intruders. The results were compared to known methods and then confirmed through better simulations, which showed that 79% of the security problems were solved successfully. However, it failed to encompass a comprehensive examination of additional potential security vulnerabilities inherent in the broader interconnected and autonomous vehicle system.

Narbayeva et al. (2020) used blockchain technology to improve IoV cybersecurity. The researchers used blockchain technology to create a robust system that uses surrounding vehicle signals to provide vehicle information. They also monitored vehicle motion using Exonum. However, users must handle private keys carefully for this strategy to work. By building a fast framework for detecting fake news, the researchers aimed to protect vehicle information transfer. This platform uses edge computing and blockchain to identify fake news and stop its propagation. The simulation shows that the proposed architecture can provide accurate traffic data within one minute of commencement and four minutes after the incident. The study did not explore load balancing; hence the framework's efficiency has not been tested in real life.

Due to the variety of security needs, vehicle-to-vehicle communication presents many security risks. Blockchain technology could secure information exchange. Malicious attacks on top layers and applications remain possible. Raja et al. (2020) implemented an AI-enabled blockchain system in the IoV to minimise blockchain security concerns. Traditional blockchain smart contracts were compared to the proposed solution. The research showed that smart contract vulnerabilities cost the system a lot. Additionally, technological advances could threaten the entire network. However, AI-driven intelligent contracts can self-learn and improve security. The research found that AI-powered intelligent contracts maintained blockchain fundamentals better than smart contracts.

In a research study conducted by Xiao et al. (2020), the objective was to tackle the challenge of secure information transmission among vehicles. The researchers developed a fast false news recognition framework that leverages edge computing and blockchain technology to effectively detect and prevent the dissemination of fabricated news, ensuring the integrity of exchanged information. The simulation findings indicate that the

suggested framework has the capability to offer precise information regarding ongoing traffic occurrences within one minute of their initiation and four minutes following the occurrence of the incident. Yet, the research does not examine the real-world scalability or viability of the framework with many vehicles and traffic incidents. The framework's blockchain technology security and privacy problems are not addressed in the article.

The study conducted by Theodouli et al. (2020) primarily addressed the issue of ensuring the security of firmware updates for smart sensors. This is crucial since any erroneous update has the potential to generate inaccurate data inside the network. The present study introduces a novel system that utilises blockchain technology to effectively manage identity and trust within the IoV network. The primary objective of this system is to enhance the security of the update process. However, establishing such a framework in a real-world IoV ecosystem may be difficult and require further study.

The integration of AI with blockchain was undertaken by Singh et al. (2021). Still, the integrity of the system could potentially be jeopardised by malevolent or unauthorised nodes within the network. AI utilising ML algorithms to make predictions, offers a viable approach for addressing the issue of rogue nodes. The suggested system has the capability to promptly identify malicious peers; nevertheless, there is a lack of empirical evidence from real-world testing to assess its efficacy.

In order to optimise network performance, Rathee et al. (2021) proposed the insertion of a blockchain framework into the cognitive radio network (CRN)-based IoV. This approach enables vehicles to effectively monitor all network operations and identify untrusted devices through the utilisation of the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) procedure. Based on the analysis of simulation data, it has been seen that the use of this strategy leads to a significant enhancement in attack detection, with an improvement rate of 70%. Nevertheless, the study failed to address the authentication difficulties associated with the TOPSIS method. Additionally, the evaluation of elements aimed at enhancing the spectrum sensing procedure and data transmission between vehicles was limited in scope.

In an academic investigation conducted by Kim (2021), the objective was to mitigate the risk of network disruption caused by malicious attacks. This was achieved by developing a secure connected vehicle network through the utilisation of a blockchain governance game (BGC). The robustness of the BGC model in safeguarding systems against malicious attacks has been mathematically demonstrated. Nevertheless, the report did not include any references to simulation experiments.

Gao et al. (2021) introduced a vehicle density-based parameter selection process for multichannel blockchain. However, the plan primarily improves the blockchain technology in the IoV area. This is done by dynamically adapting block size to vehicle density. Comprehensive simulations show improved performance over baselines. It fails to address potential concerns or downsides during multi-channel blockchain installation. Additional research and empirical experiments are needed to identify any restrictions or practical obstacles when using this strategy in real-world IoV situations. The proposed scheme may require additional processing resources and infrastructure to support blockchain channels. Scalability issues or system administration complexity may result.

Due to exponential vehicle expansion, spectrum resources are overused. Li et al. (2022) proposed multiuser k-anonymity location protection to address this issue. A system with anonymous zones and spectrum sharing among key users protects users' location privacy. The process requires a K-anonymity strategy, which may increase

computing burden and complexity. A dual mandate requires demanding and collaborative users to deposit, which limits user behaviour. This could limit the number of players and the technique's acceptance. Since it ignores flaws or targeted attacks that could compromise blockchain security and secrecy, the approach is ineffective.

Devi et al. (2022) created a blockchain-based vehicle network trustworthiness architecture. This framework addresses vehicle communication and information exchange security issues relating to trust, data integrity, and privacy. The study introduces the modified-two-stage auction algorithm (M-ITA) to assess candidate trust, data quality, and privacy. This strategy helps find dependable miners and maximises their benefits. A DPSO-based block selection method was introduced by the authors. This approach selects miners to validate blocks and alter their locations. However, the article does not examine the architecture's scalability to manage a large number of vehicles and transactions. The findings may be less applicable because the paper's numerical technique may not account for real-world vehicle networks' complexity and diversity.

Wu et al. (2022) developed a blockchain-based IoV vehicle identification verification technique. The main goal of this approach is secure information sharing and efficient use of idle resources. The proposed solution reduces network vehicle harm and task processing delays. This method overcomes the issues with current Io systems, such as slow certification and inefficient resource use. The article fails to discuss how the proposed technique may affect the IoV system's performance. Comparing the proposed technique to existing certification systems would reveal its efficacy. Blockchain technology's security risks on the IoV system are not addressed in the paper. To make the framework resilient and effective, it's crucial to consider and assess potential attack possibilities and remedies. Validating the given solution with further vehicle trials or simulations could improve its validity.

Qureshi et al. (2022) proposed a blockchain-based IoV concept. This method ensures secure, anonymous conditional privacy and authentication. The paper discusses the challenges of dynamic and developing arrangements, node mobility, and security issues in IoV networks. The built solution uses Hyperledger Fabric to provide a blockchain architecture for vehicle information sharing that ensures confidentiality, traceability, and unlinkability. It also proposes reputation-based voting to secure leader selection. Compared to modern approaches, the proposed strategy performs better. However, Hyperledger Fabric's reputation-based voting approach for leader selection must be thoroughly assessed for reliability and security. Further research is needed to determine the scheme's ability to handle real-world events and adapt to dynamic network conditions. The proposed plan's privacy and traceability compromise must be carefully examined to ensure that both are handled.

A lightweight secure framework for blockchain integration in the IoV was published by Gupta et al. (2022). This framework ensures secure IoV communication and strong authentication. The concept of branched blockchain helps low-powered devices implement blockchain's security benefits. This paper proposes an architecture to manage blockchain technology on low-processing devices at the physical layer of the IoV. The features include load balancing, scalability, accessibility, and decentralisation. Blockchain technology promises cost-effective, secure, and anonymous services, drawing interest. It has advanced the IoV. The authors noted that blockchain is vulnerable to physical capture and planned to expand the model to include such instances. This expansion improves IoV physical device security.

Table 6 Literature on IoV with blockchain focusing on security

Authors	*Consensus algorithm*	*Other used algorithms*	*Data*	*Simulation technique*	*Results*	*Limitations*
Mendiboure et al. (2018)	PoET	N/A	N/A	N/A	The study does not quantify the architecture's performance or efficiency.	The paper does not examine system vulnerabilities or attacks. SD-IoV blockchain scalability and performance are not included in the study. Blockchain technology's scalability and performance are not studied. The system's effectiveness and efficiency are not tested.
Jiang et al. (2019)	N/A	Lag timestamp range	N/A	MATLAB	When traffic is larger, the number and probability of retransmissions increase.	Underperformance and scalability. Trials and studies are needed to determine the system's practicality, efficiency, and feasibility.
Wang et al. (2019)	Rayleigh	Password-accumulator PKI	N/A	Veins simulation platform	Authentication efficiency is 29.5% higher and peak efficiency 37.4% higher. Maintaining authentication efficiency with a 34 ms time cost when blockchain length approaches 7×10^4 orders of magnitude.	Substantial packet loss in vehicle registration and key distribution may limit system efficiency and reliability.
Rahman et al. (2019)	N/A	PKI	D2.	Hardware	Tests with 266 TPS averaged 2.9 seconds. Losing packets happens. It handled many traffic streams. It processed 5,000 transactions/s.	The framework needs to improve efficiency and enhance consensus algorithms.
Kang et al. (2019)	Enhanced DPoS	ECDSA, PKI, and infeasible sub-sequence replacing algorithms.	Real-world dataset of San Francisco Yellow Cab.	N/A	Real-world data shows security and efficiency.	The proposed system may need further deployments to understand its limitations and restrictions.
Hu et al. (2019)	BCA-TG	Hash function, and digital signature algorithms.	N/A	An experimental system that runs on five servers.	Byzantine gossip protocol improved node identification and failure tolerance. Updates, consensus-making, and communication on a blockchain-based IoV system with five RCNs and multiple VCNs worked. For Byzantine nodes, consensus-making rounds updated UI components.	The paper does not compare the proposed algorithm to other IoV authentication methods or algorithms.

Table 6 Literature on IoV with blockchain focusing on security (continued)

Authors	*Consensus algorithm*	*Other used algorithms*	*Data*	*Simulation technique*	*Results*	*Limitations*
Rathee et al. (2019)	N/A	N//A	N/A	The NS2 simulator mimics the CAV blockchain framework.	Fake user requests, smart device compromise, probabilistic authentication, and rating adjustments were tested. Framework fixes 79% of security issues.	Gaps in scalability and security analysis in the networked and autonomous vehicle system.
Narbayeva et al. (2020)	N/A	ECDSA.	N/A	Exonum platform	Advances blockchain technology in transport networks, logistics, and the vehicle sector.	The study ignored load balancing, and the framework's efficacy is untested in real-life situations.
Raja et al. (2020)	N/A	Naive Bayes, KNN, decision tree	Bayesian networks	N/A	Occasionally AI-implemented intelligent contracts outperform smart contracts. AI-powered blockchain accelerates energy efficiency and transaction verification.	The research does not fully analyse IoV vehicle communication security and privacy issues. The article does not address AI-powered blockchain protocol scalability issues in large-scale IoV.
Xiao et al. (2020)	PoA	N/A	Dempster-Shafer evidence theory is exploited to collect evidence on the trustworthiness of data.	Veins, Hyperledger Fabric, and Netica	With its technologies and SDRSUs, the QcFND framework can detect IoV fake news and improve system performance.	The QcFND framework's scalability and viability with many vehicles and traffic situations are not tested. The article ignores QcFND's blockchain security and privacy issues.
Theodouli et al. (2020)	PBFT	Indy	Car registration documents and formalities provided by the European Union.	N/A	The report does not quantify the framework's performance or efficacy.	IoV ecosystem efficiency does not consider software update processing time or blockchain computational resources. Not covered: blockchain network attacks and identity credential breaches. Research ignores IoV ecosystem framework resources and maintenance.
Rathee et al. (2021)	N/A	TOPSIS	Dataset of San Francisco yellow cabs.	MATLAB	The suggested approach increases attack detection and true report creation by 70% over baseline.	Real-world testing and validation are needed to evaluate the model.
Kim (2021)	VRF	BGG	N/A	N/A	Analysing decision-making factors predicts safety measures and the appropriate reserved node and backup node acceptance probability to secure connected vehicles. The BGG enhanced IoV security in a decentralised network.	No simulation testing or model evaluation using software or hardware was mentioned in the article.

Table 6 Literature on IoV with blockchain focusing on security (continued)

Authors	*Consensus algorithm*	*Other used algorithms*	*Data*	*Simulation technique*	*Results*	*Limitations*
Wu et al. (2022)	PBFT	Hybrid identity code verification method and time window-based algorithm.	N/A	N/A	Blockchain-based vehicle certification increases data security, decreases hostile behavior, and optimises IoV resource utilisation.	The proposed technique's impact on IoV system performance is understated. Assessing several attack scenarios and solutions is essential for system resilience and effectiveness. Vehicle testing or simulations could verify the solution.
Gupta et al. (2022)	PDP	VehReg, check successor, and SHA-256.	N/A	WoTCity. Java, Node.js, and Python	This system outperforms others in computing and transmission costs. The paper evaluates security and energy use using cryptographic methods and wireless communication.	For the suggested architecture, attack scenarios, and security flaws are not examined. Framework performance and scalability are not tested. The framework's impact on IoV design and infrastructure is ignored. Framework IoV mechanism and protocol compatibility issues are neglected.
Biswas et al. (2023)	Distributed consensus algorithm	N/A	N/A	N/A	The suggested blockchain-enabled communication infrastructure may solve IoV security and trust issues.	Research and development are needed to make the blockchain-based communication architecture practical and compatible with IoV systems. Optimising blockchain infrastructure and consensus methods improves smart contract performance.
Ayed et al. (2023)	Local mining consensus	Cluster head selection, and incentive algorithm for cooperative nodes.	N/A	Python, NS-3 under Ubuntu-18.04.5, SUMO, and Ganache	Low-cluster clustering responded better to attacks and lowered message propagation as hostile nodes increased, but trust value average declined.	Energy-intensive clustering improves IoV network security and QoS. The study leaves out IoV implementation and deployment issues.
Tu et al. (2023)	VBSBC	Vehicle migration between zones algorithm	N/A	N/A	VBSBC outperformed state-of-the-art approaches in authentication delay, key processing time, attack detection rate, throughput, and packet loss rate in simulations.	Computer-powered attackers can modify or exclude blockchain transactions. Faster mobility may impair wireless link verification, migration, and stability. Only SYN/UDP/TCP and authentication DoS were simulated. Practical applications must consider attacker defenses.

Table 7 Literature on IoV with blockchain focusing on privacy

Authors	*Consensus algorithm*	*Other used algorithms*	*Data*	*Simulation technique*	*Results*	*Limitations*
Cheng et el. (2019)	Cooperation consensus algorithm among recorder	Elliptic curve, setup phase in real, setup phase for each user, drafting phase, reply phase, and decision phase algorithms.	N/A	Java Runtime Environment 1.8.	An attribute-based blockchain solves signalised junctions in IoV SCTSC mode. CP-ABE and blockchain protect messages and users' identities while openly verifying accountability. Pre-drafting reduces local operating costs.	The research ignores model constraints, implementation costs, and resources. Lack of security and attacker discussion. The model works only with light traffic.
Li et al. (2022)	N/A	IMLPP.	N/A	N/A	Results show that the suggested strategy may protect primary users' locations and promote IoV spectrum sharing.	Players and technique adoption may be limited by deposits. The procedure fails because it ignores blockchain security and confidentiality vulnerabilities or targeted attacks.
Zhang et al. (2023)	DPoS	Paillier homomorphic encryption algorithm	N/A	N/A	Experimental results indicate that the suggested technique protects user location privacy and outperforms other alternatives.	Encryption and decryption may require a lot of computational power, affecting system performance. Investigating computational burden reduction and efficiency strategies can improve the recommended strategy.

Table 8 Literature on IoV with blockchain focusing on security and privacy

Authors	*Consensus algorithm*	*Other used algorithms*	*Data*	*Simulation technique*	*Results*	*Limitations*
Sharma and Chakraborty (2018)	N/A	ECDH.	N/A	Ethereum and solidity language on the remix platform.	The study does not quantify the architecture's performance or efficiency.	Long transaction time.
Singh et al. (2021)	N/A	N/A	N/A	N/A	The report does not quantify the framework's performance or efficacy.	Energy, latency, throughput, and scalability may restrict IoV AI and blockchain. Big data and transaction processing may slow IoV latency. Because of many nodes, high IoV hours may hinder AI-blockchain integration.
Gao et al. (2021)	N/A	Channel Selection Algorithm.	Fabric database set to level DB.	Hyperledger Fabric 1.4 and caliper	Choosing the best blockchain channel based on vehicle density and application throughput and latency optimised the scheme's performance.	Lack of description of suggested scheme's security weaknesses. Certain vehicles and transactions are not scalable. Untested network congestion, communication delays, and scheme performance. Skip IoV infrastructure upgrades and compatibility. No consideration is given to multi-channel blockchain adoption and maintenance.
Devi et al. (2022)	Subjective logic models	DPSO and M-ITA	N/A	MATLAB	Simulations show the proposed method efficiently identifies trusted and malicious IoVs, ensuring network security.	The paper does not test the architecture's scalability for most vehicles and transactions. Its numerical method may not account for real-world vehicle networks' complex and diverse features, limiting its applicability.
Qureshi et al. (2022)	Crash fault tolerance	BESA.	Fabric CouchDB and level DB	Hyperledger Fabric and MATLAB	The suggested system outperforms state-of-the-art solutions in IoV security and privacy.	The paper did not assess Hyperledger Fabric's reputation-based leader selection method's security and reliability. Studying the scheme's adaptability to dynamic network conditions and real-world scenarios is necessary.

The communication system proposed by Biswas et al. (2023) uses blockchain technology to improve IoV application security and reliability. The writers emphasise blockchain's decentralisation and security in their suggestions. The framework includes an identity management system that authenticates and authorises users and devices, ensuring safe communication routes between IoV system components. The framework's efficiency was assessed using real-world IoV scenarios. These situations showed the framework's capacity to enable safe and dependable IoV connectivity. Further research and development are needed to optimise the blockchain-based communication infrastructure for practical application and compatibility with present and future IoV systems. Smart contracts can be optimised by optimising blockchain infrastructure and using more efficient consensus mechanisms.

An extensive investigation of IoV ecosystem security issues was undertaken by Ayed et al. (2023). They developed a blockchain-based trust management architecture to secure IoV systems in response to these issues. The previous study introduced centralised trust-based methods. This research study adds a decentralised trust process and clustering mechanism to this technique. Scalability and energy consumption restrictions are addressed by this extension. The proposed framework considers trust value, safety distance, and energy components to ensure security and service quality. The concept improves detection accuracy, communication costs, and runtime features, suggesting that blockchain clusters improve IoV reliability. Energy can be added to the clustering process to improve security and QoS in the IoV network.

Tu et al. (2023) developed vehicle-based secure blockchain consensus (VBSBC) to address IoV issues. It secures vehicle communication via blockchain and a consensus algorithm. As suggested, the VBSBC strategy outperforms existing methods in authentication delay, key time for processing, attack detection rate, productivity, and packet loss rate. As stated, the VBSBC algorithm assumes that the controllers, roadside units (RSUs), can utilise and process energy as they like. Conversely, vehicles have energy and processing power limits. Resource distribution and efficiency may be difficult. The paper concedes that many constraints remain, but it does not elaborate.

Zhang et al. (2023a) proposed blockchain-based secure online car-hailing. The suggested solution uses blockchain and Paillier homomorphic encryption to protect passengers' and drivers' location anonymity. The technology encrypts passenger and driver location data using lattice-based encryption. Additionally, it uses the Paillier homomorphic encryption technique for ciphertext location verification. The online car-hailing industry uses blockchain technology to secure transactions. The experimental results show that the suggested technique protects user location privacy and outperforms other strategies. It is important to realise that the proposed approach may need significant computational resources for encryption and decryption, affecting system performance. Further research can focus on reducing the computing burden and improving efficiency to improve the proposed scheme's efficacy.

Based on the literature cited, it is evident that the primary challenges faced in the implementation of blockchain technology for IoV networks revolve around issues of security and privacy, as well as constraints related to computing power and the availability of resources. According to El Mazouzi et al. (2023), the utilisation of blockchain technology in isolation is considered inadequate for effectively resolving concerns related to privacy and security. The integration of blockchain with AI has demonstrated the potential to augment the security of the system. However, the process of integration continues to encounter obstacles, including constraints on resources and

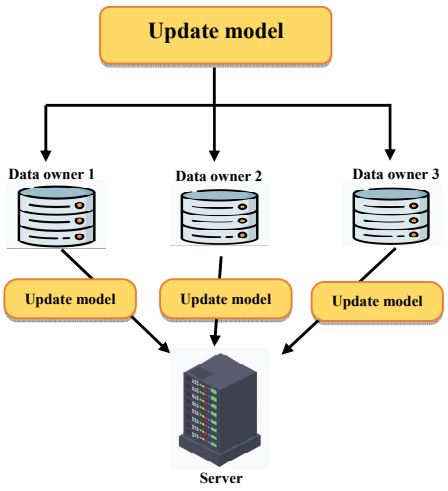
failures in infrastructure. Hence, it is recommended that forthcoming studies focus on the integration of AI technology and blockchain in order to enhance the levels of privacy and security within IoV networks. In addressing the challenge of resource constraints, the utilisation of edge computing and distributed clustering has emerged as viable strategies for resource management and consumption reduction. Future studies should also address the ability to expand the network, particularly in light of the increasing number of linked vehicles and dynamic IoV scenarios. The subsequent tables will provide representations of several characteristics found in the literature regarding blockchain technology in the IoV domain. Table 6 will present a review of the articles focusing on the field of security. Table 7 will provide an overview of the literature specifically addressing the topic of privacy. Lastly, Table 8 will present a synthesis of the research that explores the intersection of security and privacy.

4 Federated learning

The accuracy and effectiveness of trained ML models in the field of ML are reliant upon the training data and computational resources of the central server. In the typical ML approach, data that is stored centrally is used for training as well as testing in order to develop models that are efficient and comprehensive. Centralised ML algorithms have several obstacles in relation to user data, encompassing time constraints, computational resources, privacy concerns, and security issues. In order to address the aforementioned issues through a technical approach, the concept of FL has evolved in the last few years. The strategy of FL involves the utilisation of statistical model training on data centres or remote devices, with the aim of ensuring that user data remains localised (Li et al., 2020; Kang et al. (2020).

FL has been seen as a viable approach to addressing the challenges associated with centralised data in critical networks. As illustrated in Figure 8, the fundamental architecture of FL is the utilisation of local data by users to train individual models. These local models are subsequently employed to update the global model residing in the base station. The global model, which has been collected from many sources, is subsequently distributed to the local models for additional training. The aforementioned procedures are iteratively executed until the global model reaches convergence. This distributed ML architecture protects user privacy while retaining the efficacy of AI-based computation in end-device applications like autonomous vehicles. The ML and deep learning model undergoes global training and subsequently propagates the latest parameters to end units through a centralised server, consequently initiating the FL process. Using the aid of this proficient model, all terminal devices engage in training their individual ML and deep learning models on their respective local datasets. After the local ML model has undergone training, clients transmit the parameters to a centralised server for the purpose of global training. In order to meet the requirements and achieve accuracy in the context of centralised servers, the process is iterated numerous times until completion is achieved. There exist multiple applications, including e-commerce, the IoV, and e-healthcare, where FL can be implemented efficiently (Yang et al., 2019; Tseng et al., 2020).

Figure 8 The architecture of FL in a general manner (see online version for colours)



4.1 Review of IoV utilising FL

Using the federated bidirectional connection broad learning system, Yuan et al. (2021) improved IoV data transfer efficiency and effectiveness. The suggested method trains vehicular node datasets using BiBLS. The FedBLS algorithm aggregates the parameters it acquires. This work also introduces a new clustering FedBLS technique to improve model aggregation by efficiently allocating data tasks among clusters. Simulations reveal that FeBBLS improves IoV data-sharing efficacy and forecast precision. The FeBBLS system also protects data privacy during sharing. There is no testing or comparison of the suggested technique's usefulness or performance. The research does not address scalability issues that may occur when deploying the proposed system with several car nodes or clusters. The paper does not assess the scheme's security or privacy risks.

Using federated ML, Uprety et al. (2021) proposed an IoV privacy-protecting misbehaviour detection mechanism. This study uses the vehicle basic safety message (BSM) dataset to construct a ML model to analyse data fabrication threats in VANETs. A federated methodology was presented in which vehicles in the VANET for the IoV receive an initial model to train locally using their data. This methodology allows the creation of a collaborative intelligent model that can accurately categorise position falsification assaults in VANETs without providing data to other parties. This study compares the success rate of federated and centrally trained attack detection models. Locally produced BSM data from individual vehicles is used to train the model on position fabrication assaults. The vehicle's position is crucial for broadcasting messages in a self-managed IoV network, according to this study. The project uses a publicly available labelled dataset for experimentation. This dataset lacks a real non-IID property and a non-balanced data distribution, which are needed for FL. The paper ignores the possibility of chosen local training nodes disconnecting during a round, causing training errors. Each attack type is tagged in the study dataset. Real-world BSM data is usually unmarked. Local data labeling in a pre-processing unit is outside the scope of this

investigation. The visibility of communicated weights to attackers' compromises FL's privacy.

Using software-defined networking (SDN), Hbaieb et al. (2022) developed a new IoV intrusion detection system (IDS). FL and trust metrics improve network security. To streamline model training, the IDS model uses FL, Trust, and SDN. This paper addresses the security and privacy issues in the IoV, a complex data transmission network with many nodes. IoV cyberattack detection and data security are the goals of the proposed solution. To verify approach efficiency, simulation experiments are done. Trust metrics used to assess IoV node reliability are not examined in the study. It also lacks the simulation configuration and metrics needed to evaluate the FL-based IDS. The researchers have not compared the recommended solution to existing IDS approaches for detection accuracy or processing efficiency.

Ding et al. (2022) adopted FL to coordinate IoV environments. This technique changes agent Q network parameters and sends the aggregated model to IoV vehicles. The local model can be upgraded. The authors use FL to increase IoV vehicle coordination and collaboration. This method allows decentralised training while protecting data. The proposed strategy helps cars learn by sharing experiences, improving their IoV decision-making. The suggested FL methodology can be tested in practical IoV situations, considering network latency, communication reliability, and scalability. A study should evaluate how different aggregation strategies affect the FL strategy's ability to coordinate IoV systems. This may involve examining different ways to collect gradients or models from multiple cars. Future studies may focus on FL privacy-preserving solutions. Data privacy in IoV settings may be improved by using advanced encryption or differential privacy measures. The authors also advise adding other ML algorithms to FL to improve IoV vehicle decision-making. We can investigate hybrid methods that combine reinforcement learning with other learning techniques.

Gated recurrent unit (GRU)-based federated continual learning (GFCL) was introduced by Talpur and Gurusamy (2022). Detecting Sybil-based data poisoning attacks in IoV networks is the goal of this approach. The framework was created to address time-sensitive, dynamic, and mobile tasks in IoV applications. The GFCL framework is lightweight and scalable since it does not require a training dataset with attack samples. The GRU model predicts future data sequences and performs distributed analysis to discover and stop illegal vehicle behaviour. The suggested approach is tested using actual vehicle movement traces and found to be effective across various performance metrics. The proposed framework learns and detects IoV intrusions in real-time, unlike prior methods. This defence against data poisoning is more flexible and responsive. The research does not examine the computing and communication overhead of the GFCL architecture, which are important in practice.

Using ConvLSTM, Yang et al. (2022) identified network intrusions in internet-connected in-vehicle networks (IVNs). ConvLSTM model training uses FL and client selection to take advantage of network message ID regularity. In the FL framework, intelligent connected vehicles (ICVs) are local clients while mobile edge computing (MEC) servers, coupled to base stations (BSs), are servers. A new method, proximal policy optimisation (PPO)-based federated client selection (FCS), improves model accuracy and system overhead. Simulations in IoV environments using IVN datasets have shown that the ConvLSTM model may reduce model size and convergence time without reducing detection accuracy. The authors suggest studying the IoV using a

multi-agent system framework. This technique tries to fully reflect the intricate links between multiple ICVs and their environment. This approach may help us understand the many facets of the IoV ecosystem. The ConvLSTM-based model requires a lot of processing effort to train and deploy and current methods may not scale to larger networks.

Ni et al. (2022) proposed the Lagrange coded FL (L-CoFL) model to improve system security and FL computation precision during low-quality trained data, wireless channel errors, and malicious vehicles. The L-CoFL model adds computational redundancy to vehicle data in the FL-enabled IoV system, improving system noise security. The L-CoFL system's scalability and adaptability can be studied in multiple IoV settings and network conditions. This research should consider vehicle count, data heterogeneity, and network dynamics. Future research can study integrating additional privacy-preserving approaches or security features with the L-CoFL model to improve vehicle privacy in FL-enabled IoV systems.

Yu et al. (2022) proposed employing federated long short-term memory (LSTM) neural networks to detect attacks on networks in ICVs. The regularity of the IVN ID sequence is used to predict the message ID using an LSTM neural network architecture. The article also described a client-server FL architecture for secure and efficient LSTM model training on IoV networks. ICVs are used for local model training, while base stations are equipped with MEC servers to aggregate global model parameters. The paper's lack of a comparative analysis makes it difficult to assess the suggested intrusion detection method's performance and efficiency. IoV systems use FL architecture, which this study will improve. Client selection criteria will consider the non-IID extent of the local dataset, local computer capacity, and wireless communication link quality.

To improve road safety, Chhabra et al. (2023) employed FL to assess driver behaviour in IoV systems. FL helps build driver behaviour classification models without exchanging raw data, maintaining privacy, and reducing data transfer. This work proposes utilising CNN-LSTM and CNN-Bi-LSTM deep learning architectures with real-time driving behaviour data from smartphone sensors or vehicle electronics. The model's performance is measured by accuracy, AUC, loss, precision, and recall. Different parts of the proposed model are analysed using IID and non-IID datasets. Compared to non-distributed deep learning implementations, FL architectures perform similarly on IID and non-IID datasets. This work aims to create a robust intelligent transportation system (ITS) using FL to reduce data privacy and communication costs. Future studies must examine the potential challenges of FL in driver behaviour analytics.

FL emphasises privacy in collaborative ML. Several clients collaborate to establish a worldwide model. They do this by training their own models with their own data and sending the modifications to a central server. Local model updates to the server can leak information, making it vulnerable to privacy attacks. Secure aggregation methods may help mitigate such attacks, although they may not provide security processes against specific assaults. Karakoç et al. (2023) proposed a secure FL privacy method. This system hides client identities through multi-hop communication. The researchers also suggested ways to strengthen the solution against malicious packet drop behaviours. The research has yet to evaluate the proposed approach's practicality. The analysis does not consider how the proposed approach may affect the efficacy and computing burden of FL. The research fails to address potential challenges when implementing the multi-hop communication approach to hide customers' identities.

The IoV-specific heterogeneous FL approach FedVPS was introduced by Hangdong et al. (2023). This system overcomes local data's non-IID features and model volatility. Terminals, edge devices, and the cloud form the IoV distributed architecture. Additionally, it uses prototype-based aggregation to efficiently use local datasets. FedVPS protects privacy via Secure Multi-Party Computation. This technique ensures that FL terminals calculate accurately while protecting local datasets by preventing valuable information from being disclosed. The paper emphasises FedVPS's role in terminal privacy and communication efficiency, enabling accurate and effective distributed ML in the IoV. This benefit is shown in the BIT-Vehicle dataset examination. The research also indicates that FedVPS can handle model variability and lower message transmission parameters by a lot. Additionally, it achieves multiparty secure computing. More research is needed to determine if the FedVPS plan can be used in a wider IoV scenario, considering communication issues and model prediction accuracy as terminals increase.

Based on differentially private FL (DPFL) and the framework for IDS, Xu et al. (2023) developed DPFL-F2IDS for secure intrusion detection in inter-vehicle networks. The proposed architecture uses dynamic packet filtering and fuzzy-based intrusion detection to protect networked and automated vehicles from cyberattacks. Its main goal is to quickly identify and stop dangerous actions. The paper also evaluates DPFL-F2IDS under different vehicle amounts, optimisation methods, and noise levels. The analysis finds noise multipliers that protect privacy and model quality. The research establishes a strong intrusion detection mechanism for inter-vehicle networks and evaluates its usability and privacy preservation. The study does not compare the DPFL-F2IDS architecture to other IDSs or methods, limiting its efficacy assessment. The research does not address the effects of hostile attacks or attempts to bypass DPFL-F2IDS' privacy-preserving features.

Wang and Yan (2023) developed the FL-TP algorithm using the FL framework and an LSTM network to identify cyberattacks and accurately predict vehicle routes under intensive cyberattacks. The authors suggested using model-robust estimation (MrE) to determine model aggregation weights, improving FL for global model aggregation. Multiple trials on the IoV system evaluated the FL-TP algorithm's trajectory prediction and attack detection capabilities. VeReMi was used for these tests. Further research will prioritise large-scale realistic simulations to test the suggested algorithm's effectiveness, according to the paper. The publicly available VeReMi dataset trains and tests the FL-TP algorithm. The dataset's constraints and biases may limit the algorithm's generalisability.

Tham et al. (2023) developed three FL techniques, FedAvg, FedAvg-Adam, and FedProx, to acquire deep learning models decentralisedly for vehicle network anomaly detection. Sequential data irregularities are the focus of this investigation. FL uses LSTM and CNN-LSTM deep learning networks to detect anomalies. These approaches are evaluated using the VeReMi Extension misbehaviour dataset, which includes independent, non-independent, and identically distributed (IID and non-IID) cases. This examination shows their capacity to learn correct vehicular network anomaly detection models. The researchers advised studying how independent, non-independent, and identically distributed (IID and non-IID) data distributions affect FL's ability to detect vehicular network anomalies and misbehaviour. Assessing the recommended FL systems in real-world vehicular networks is crucial. This evaluation should include communication latency, network connectivity, and scalability.

Table 9 Literature on IoV with FL focusing on security

Authors	*FL algorithm*	*Other used algorithms*	*Data*	*Simulation technique*	*Results*	*Limitations*
Hbaieb et al. (2022)	Random forest, 1-D CNN, and 1-D RNN	N/A	N/A	Python, SUMO, and Mininet-WiFi.	Simulations show that the proposed IDS can enhance IoV security using CNN.	The IoV IDS's scalability is not discussed. Real-world testing may improve the method. IDS communication overhead, which could affect network performance and resource usage, is not addressed in the study.
Talpur and Gurusamy (2022)	GRU-based RNN	HMSE and window-based learning method.	CRAW-DAD, CRAWDAD dataset Roma, and Tdrive	MATLAB	Vehicle movement traces demonstrate the GFCL anomaly detection method's efficacy. A framework performance analysis shows good accuracy, detection rate, FPR, and FNR.	The paper does not discuss the framework's computing, communication, or scalability. Network conditions and data distribution not mentioned may impair GFCL framework performance. Architecture does not extend beyond Sybil-based data poisoning.
Yang et al. (2022)	ConvLSTM	PPO.	CAN messages	Numerical experiments	ConvLSTM-based IDS reduces model size and convergence time while maintaining 95% accurate detection. Convergence rate, model consistency, and system overhead are better with PPO-based FCS.	Training and deploying the ConvLSTM-based model need a lot of computing effort, and current methods may not scale to larger networks.
Yu et al. (2022)	LSTM	N/A	CAN messages	N/A	Achieved a detection accuracy beyond 90% for spoofing, replay, drop, and DoS attacks in intelligent connected vehicles (ICVs).	Larger ICV systems with more clients and more sophisticated attacks have not tested this strategy. Although not addressed in the research, delays and packet loss may impair the offered method's performance.
Safavat and Rawat (2023)	FB-FL-BAA-LSML	MLP, RNN, CNN, DES, RSA, ECC, IPP-ROT, HAVAL, MD5, SHA-2, and DFHAVAL	CICIDS2017	MATLAB	The proposed strategy outperformed previous methods in tests. The FB-FL-BAA-LSMLP classification identifies attacked data. Hashing authenticated RSU vehicles and prevented data collisions and delays. ECC and IPP-ROT protected cloud vehicle registration data and assaults.	The paper ignores vehicle, network, and communication latency and scalability. Security-computational overhead-resource limits trade-offs are ignored. Traffic and environmental factors are neglected while assessing technique performance.
Zhou et al. (2023)	LR and CNN	FedAVG, RoHFL, Romoa, Krum, Trim-mean, Bulyan, RoMA, and ReSU.	MNIST, Fashion-MNIST, and CIFAR-10	Mathematical experiments	The global model with robust aggregation criteria reveals that RoHFL outperforms alternative Byzantine-resistant FL methods. ROHFL surpasses resilient FL systems in accuracy despite attacks.	Only untargeted poisoning attacks are discussed. Neither the hierarchical FL process's computation overhead nor communication costs are discussed in the RoHFL framework's scalability or efficiency.

Table 10 Literature on IoV with FL focusing on privacy

Authors	*FL algorithm*	*Other used algorithms*	*Data*	*Simulation technique*	*Results*	*Limitations*
Yuan et al (2021)	BiBLS	FedBLS, BLS, FINCH, and TF-FedBLS	MNIST.	PyTorch, VEINS, and OpenStreetMap	The FeBBLS system increases model aggregation and IoV data exchange reliability and efficiency.	Scalability, computational complexity, and real-world implementation issues of the proposed approach are unresolved.
Ding et al. (2022)	FRL-PES	PES and FRL-Dueling	N/A	Numerical experiments	Experiments show that the proposed strategy surpasses fundamental methods in success rate and convergence stability. The system shares information while maintaining connected vehicle privacy.	Model assumptions, scalability to larger IoV settings, and generalisability may be paper weaknesses.
Chhabra et al. (2023)	CNN-LSTM, and CNN-Bi-LSTM	N/A	Smartphone sensor data collection.	Android application, and Python	FL design produced equal parametric results on IID and non-IID datasets, unlike current deep learning implementations on non-distributed datasets. With FL, the IoV network enhances driver behavior classification accuracy without compromising data privacy.	The hardware modeling and implementation of the suggested approach were not included. No data aggregation or dissemination is emphasised.

Table 11 Literature on IoV with FL focusing on security and privacy

Authors	*FL algorithm*	*Other used algorithms*	*Data*	*Simulation technique*	*Results*	*Limitations*
Uprety et al. (2021)	ANN	Federated averaging algorithm	BSM, VeReMi, and ML-friendly VeReMi	Tensorflow framework	The paper shows that FL outperforms centralised training in threat detection, communication overhead, and scalability.	Databases lack non-IID features and balanced distribution. Wireless weight communication resource restrictions might cause training errors. Local training nodes may disconnect mid-round. A public dataset labeled for each attack category was tested. In reality, BSM data are unlabeled.
Ni et al. (2022)	L-CoFL	LCC	Urban vehicular traffic in the city of Sao Paulo.	MATLAB	Improves FL calculations for low-quality trained data and wireless channel problems with the model. Secures IoV systems from hostile vehicles. L-CoFL predicts IoV traffic slowness better in many scenarios.	This research should consider vehicle count, data heterogeneity, and network dynamics.
Karakoç et al. (2023)	FedAVG and CNN	Partially blind signatures	CIFAR-10, CIFAR-100, and Fashion MNIST	Python	With client count, all datasets are trained faster. Protocol parameters overhead was negligible compared to computation time. Inter-hop communication delayed low-speed networks.	FL's poisoning and backdoor threats are ignored. No additional FL privacy or security vulnerabilities are covered in the study. The trials only cover a basic laptop with hardware and software setups. Multihop may delay networks.
Hangdong et al. (2023)	FedVPS	SMPC and multi-key semi-homomorphic encryption.	BIT-Vehicle	Pytorch 1.13, and hardware	The findings show that FedVPS improves IoV communication efficiency, privacy, and prediction accuracy.	FedVPS's sophisticated IoV scalability and performance are not mentioned. FedVPS network and communication delays are ignored in the study. The analysis ignores FedVPS privacy-model accuracy tradeoffs. FedVPS is not compared to IoV FL systems.

Table 11 Literature on IoV with FL focusing on security and privacy (continued)

Authors	*FL algorithm*	*Other used algorithms*	*Data*	*Simulation technique*	*Results*	*Limitations*
Xu et al. (2023)	MLP(FL), MLP(CL), LSTM, CNN-LSTM, AdaBoost, and XGBoost	Adabound optimiser, categorical cross-entropy.	VeReMi Extension, ConstPos_0709, DoS_0709, and GridSybil_0709.	Veins	Compared to conventional methods, the Adabound optimiser and FedAvg algorithm yield superior returns mimicking centralised learning.	This study does not examine scalability and data management for several vehicles. The study does not examine noise multipliers' effects on DPFL performance or ideal range. Hostile attacks and DPFL-F2IDS framework privacy bypasses are not studied.
Wang and Yan (2023)	LSTM	MrE, and Fed-Avg.	VeReMi.	Python and veins	Under maximum cyberattack penetration situations, FL-TP outperforms benchmark approaches in cyberattack detection by 6.99% and trajectory prediction by 54.86%.	In real-world IoV systems, FL-TP implementation faces computational, communication, and scaling issues. The paper ignores the FL framework and LSTM network drawbacks in FL-TP cyberattack detection and prediction. FL-TP's applicability outside VeReMi was not considered.
Tham et al. (2023)	LSTM and CNNLSTM	FedAvg-SGD, FedAvg-Adam, and FedProx.	VeReMi Extension	Luxembourg SUMO traffic (LuST)	FL learned reliable vehicular anomaly detection models in different data distributions and network architectures. FL models on a global cloud server and local nodes at the network edge accurately detected vehicular network anomalies.	FL vehicular anomaly detection methods' strengths and limitations are not discussed. The research ignores FL techniques' scalability and efficiency in big vehicle networks.

Safavat and Rawat (2023) proposed secure FL methods using interpolated public key and private key-ROTation (IPP-ROT)-based elliptic curve cryptography (ECC) and Fed Buff FB-FL-BAA-LSMLP for vehicular cyber-physical system intrusion detection. The methodology includes vehicle registration, hashing authentication, and data classification to identify hacked data. A subsequent study could examine how connection latency and communication delays affect the recommended strategy, particularly in real-world circumstances with several vehicles and data streams. This would help explain the method's practicality and efficacy.

According to Zhou et al. (2023), RoHFL for the IoV is a resilient hierarchical FL system. This framework supports contemporary IoV hierarchies. When two-layer FL connects automobiles to the cloud across wide-area networks, excessive latency occurs. The RoHFL framework addresses this issue. CBSs and RSUs assist in aggregate model changes in the proposed system. The cloud server aggregates last. Simulations are used to evaluate RoHFL, not empirical investigations or real-world implementations. Targeted poisoning attacks, which are harder to carry out but can have serious consequences, are not considered in the research. The research does not consider how adversarial assaults may affect RoHFL architectural efficiency and integrity. The proposed architecture assumes CBSs and RSUs offer intermediate aggregation. These assumptions may not be feasible in all IoV systems.

Based on the aforementioned comprehensive review, it is proposed that FL be employed as a means to ensure privacy safeguards for the data at the local level. Nevertheless, in a situation where there are untrustworthy clients and servers, the traditional FL approach may encounter potential privacy vulnerabilities. Hence, the issue of achieving a more reliable FL framework by mitigating all potential hazards necessitates additional consideration. The security concern holds significant importance for an FL system since it directly impacts the system's effectiveness by ensuring its resilience against potential attacks. The central model aggregation and communication processes with the clients increase the vulnerability of FL to external attacks. According to Hu et al. (2023), there remain certain challenges associated with the implementation of FL in the context of the IoV:

- The FL design uses a single centralised server for all client model parameters. A malicious attack or centralised server failure would crash FL.
- Malicious attackers can intercept model parameters communicated across unreliable channels in FL, which requires multi-party communication. Malicious attackers who access model parameters can infer client information.
- Model convergence takes time with FL iterative learning. Thus, parameter transfer is delayed, reducing data-sharing efficiency.
- If some unqualified client data is used in model training, it may reduce model accuracy and reliability.

One potential strategy for mitigating the impact of cyberattacks is the integration of the blockchain idea with FL. The integration of blockchain technology with decentralised FL has the potential to further improve the security of FL by improving privacy preservation and ensuring the integrity of data through tamper resistance mechanisms. The following tables will give depictions of various attributes documented in the academic literature regarding FL in the IoV domain. Table 9 will provide an overview of the scholarly works related to the field of security. Table 10 will present a summary of the scholarly works

that explicitly pertain to the subject matter of privacy. Finally, Table 11 will provide an overview of the scholarly investigations that examine the convergence of security and privacy.

5 The convergence of blockchain and FL in IoV

While it is true that FL provides a robust framework for ensuring security in the learning process, its effectiveness mostly relies on a central aggregator. In addition, the implementation of a viable business model is necessary to enhance the propagation of mobile devices and mitigate the risks associated with adversarial attacks. Driven by the promising potential of FL in constructing an IoV and the need to mitigate the possibility of attacks in FL, blockchain technology is being employed in conjunction with FL to provide a decentralised solution. This solution aims to regulate promotions, ensure security, and safeguard privacy in a trustworthy manner (Billah et al., 2022). Blockchain and FL represent two emerging solutions that have the potential to be utilised in the context of the IoV in order to address issues related to privacy and security, as well as mitigate challenges associated with communications expenses and latency issues (Javed et al., 2022).

5.1 Review of IoV utilising blockchain and FL

Lu et al. (2020) focused on the IoV and data use to improve driving and provide high-quality services. The researchers propose a mobility-based edge content caching method for vehicle networks. DRL and MEC inspired this technique. The authors solve the radio channel assignment problem to create a dynamic wireless network with D2D communication. This is done using partially overlapping channels and game theory. The article also highlights edge intelligence for vehicular network resource sharing. The research does not evaluate the best edge content caching system's practicality in real-world situations, limiting its understanding. Edge intelligence and resource sharing in car networks may have security and privacy issues that the study does not examine. Future studies must investigate these issues to improve the dependability and credibility of offered solutions.

Decentralised FL (DFL) for connected autonomous vehicles was proposed by Pokhrel and Choi (2020) to improve communication and overcome the limitations of global federated learning (GFL) models. DFL uses blockchain technology to secure and decentralise communication amongst connected and autonomous vehicles (CAVs), eliminating the need for a central server. The model accounts for communication delays and the number of link-layer frames needed to transmit data in the cellular channel, better representing real-world conditions. This study employed simulations to show that the DFL technique improves CAVs performance, promoting collaboration and knowledge acquisition. This research focuses on the DFL framework and methods rather than specific datasets or real-world data sources. The report recommends more research to accurately determine rigorous convexity without approximation. Integrating other consensus algorithms like Byzantine fault tolerance and proof-of-stake into the proposed technique may require sophisticated computations and preambles, according to the report. Future study can examine these issues. The research also presents a method for

determining the ideal L that minimises proof-of-work latency based on the projected system delay. Since the research focuses on a decentralised FL technique for networked autonomous automobiles, actual trials and evaluations may be needed to prove its efficacy and practicality in CAV scenarios.

To ensure autonomous driving safety, Liu et al. (2021) proposed a trust-based consensus system that uses FL and blockchain to securely share model between vehicles. A two-stage IDS using FL across edge vehicles and roadside infrastructure, such as base stations and RSUs, was developed by the researchers. This study develops a trust-based incentive scheme with a trust evaluation algorithm to improve FL model training accuracy. The IDS uses many mobile agents to perform ML on network edge nodes. Mobile gateways enable aggregation. The paper admits that edge nodes face privacy leakage issues while exchanging sub-models with the gateway. The research also considers using a centralised certification authority to secure network communication, including SSL and message signing. This study focuses on system architecture, algorithms, and mechanisms rather than training or assessment datasets. Method assumes 100% honest edge devices with training resources. However, malicious edge devices or insufficient resources can influence training model accuracy. Network and communication latency's impact on system performance is overlooked. The proposed approach is tested on one dataset.

A hierarchical blockchain topology was suggested by Chai et al. (2021) to facilitate IoV information exchange. They also introduced proof-of-knowledge (PoK), a lightweight consensus method. This study presented a hierarchical FL method with an intermediary layer to aggregate lower-level data and investigates data linkages. This study views knowledge sharing as a market-based process where people trade to share knowledge. The paper gives a theoretical framework for trading as a multi-leader and multi-player game. The simulation shows that the hierarchical approach improves sharing efficiency and learning quality. Blockchain technology also mitigates specific malicious attacks. The paper also describes the PoK protocol's transaction mechanism and security features and evaluates its performance. The hierarchical blockchain structure's scalability in large vehicle networks is not fully examined in the research. Hierarchical FL algorithm performance and convergence rate constraints are not fully analysed in the research. The suggested blockchain-enabled system's security procedures and weaknesses against various attacks are not thoroughly assessed in the research.

ITS and widespread connectivity have made security and privacy difficult. Moulahi et al. (2022) suggested a blockchain-based, privacy-protecting FL system for ITS cyber threat detection. Vehicle-level classification algorithms identify cyber hazards in VANET with ITS. The VeReMi dataset is used to test the prototype's efficacy in this study. Vehicle-specific categorisation algorithms are performed on five subsets of the dataset. Precision and accuracy dropped 7.1% on average. Note that F1-score and recall remained similar. The experiment used the VeReMi dataset, however, it did not analyse its attacks and faults. Though notable, the research does not examine the causes of the 7.1% decline in precision and accuracy. The research does not compare the suggested strategy to existing or alternative privacy-preserving cyber-threat identification methods in ITS. This omission inhibits a complete evaluation of the proposed framework's strengths and flaws.

By offloading learning to distributed vehicle edge nodes, (Abdel-Basset et al., 2022) proposed a federated deep learning-based intrusion detection technique (FED-IDS) to improve smart transportation system attack detection. The FED-IDS system uses a context-aware transformer network to describe vehicle traffic flows spatially and

temporally. This helps the system classify attacks. Blockchain-based federated training lets edge nodes engage in training safely and reliably without centralised authority. Experimental results on two publicly available datasets, car-hacking and TON_IoT, show that FED-IDS protect ITS networks from cyberattacks. FED-IDS outperform other methods, demonstrating its potential to improve network security. The paper also explores how vehicular edge intelligence (VEI) might improve IDSs. Devoted short-range communication (DSRC) and blockchain improve data transfer connectivity, reliability, and trustworthiness. The number and variety of the datasets, the scalability of the suggested architecture, and how it compares to recent approaches are not clearly addressed in the experimental review.

The blockchain-based FL system presented by Lv et al. (2022) detects malicious activities in VANETs while protecting sensitive data. Federation learning and blockchain technology optimise model training and secure model sharing in the suggested technique. This method improves traffic data interactions and driving safety. The Gaussian method and differential privacy are used in this study to protect the blockchain model's privacy. The suggested method is effective because it can discover common data fabrication attacks quickly and accurately. The research fails to address the scalability of the proposed strategy, notably the number of vehicles and edge devices involved in cooperative training. The research does not examine how network latency and communication delays may affect misbehaviour detection system efficacy and efficiency.

Ghimire and Rawat (2022) suggested using blockchain technology to provide FL in the IoV for safe, private, and verifiable ITS services. The suggested solution addresses FL issues on the IoV. Resource management, integration, precision, system diversity, statistical diversity, and mobility are obstacles. Light nodes in the blockchain network mediate between users and full nodes. These light nodes send users' transactions to the full node and store block headers without synchronising with the blockchain. This paper explains RSUs' importance in IoV. RSUs have different processing and storage capacities and are assigned different functions based on their resources. The blockchain-enabled FL incentive mechanism is not explained in the study. Future studies could investigate ways to incentivise cars for their genuine efforts and contributions. In the proposed IoV architecture, where the server sets the difficulty level, finding the best block creation threshold is tough. Using more nodes for parameter aggregation could lower the proposed system's performance; future studies could focus on IoV design and deployment.

Using FL and blockchain technology, (Alotaibi and Alazzawi, 2022) designed PPIoV to secure vehicle privacy in IoV and fog computing. FL trains ML models on vehicles and fog nodes decentralisedly. This method reduces network usage and improves prediction accuracy. Credible vehicles can improve the global model and precision by being assessed by the framework during FL training. The peer-to-peer IoV (PPIoV) framework uses blockchain to build trust between communication nodes. This implementation ensures secure and transparent global learning model refreshment transactions. The efficiency and performance of the blockchain in PPIoV is compared to non-blockchain transactions. This comparison shows how blockchain technology maintains IoV-Fog confidence. The conclusions may be limited by the lack of a real-world examination of the suggested framework in the research. To address the scalability and computational cost of the proposed PPIoV architecture, the dynamic and resource-limited IoV ecosystem should be studied. Since network latency and

communication delays might affect real-time analysis and decisions in an IoV-Fog context, studying how they affect the PPIoV framework would be valuable.

A privacy-preserving IoT-enabled smart vehicular network solution by Singh et al. (2022) addresses centralisation, secrecy, information authentication, communication bandwidth, and privacy issues. To protect privacy and enable smart car data authentication, the intermediate layer uses blockchain and FL. This study explores vehicle trust confidence offset values and weights for local base station verification. The proposed method offers interactive solutions to improve traffic efficiency, driving safety, autonomous driving, and smart city infrastructure information exchange. Performance evaluation is done with simulation of urban mobility (SUMO) simulators and GUI-assisted traffic simulation. The study used 60,000 colour images from the CIFAR-10 dataset, divided into ten groups. The IVTP framework manages vehicular network trust and secrecy. The percentage of active nodes is compared to the suggested approach and past studies. This paper analyses the technological flow of the proposed approach for IoT-enabled smart vehicle networks in smart city infrastructure. There is no discussion of the approach's limitations for managing big IoT-enabled smart car networks. The research does not address blockchain and FL implementation challenges in intelligent vehicle networks. The suggested approach's scalability and resource needs are inadequately assessed.

Islam et al. (2022) suggest using blockchain technology to better IoV anomaly detection. The scheme aims to fix internal IoV system defects. These errors could cause accidents and raise privacy concerns, hampering anomaly detection data transfer. FL and blockchain technology are used to build a decentralised car data model and secure it in the blockchain. Testing the suggested system with real datasets and hardware proves its practicality. The study also suggests adding a reputation system and increasing experimental trial size. In the proposed system, vehicles train local models, MEC in the base station mines and trains models in real-time, and the cloud mines and stores models. The Scania trucks dataset is used to test the method. The dataset has 60,000 samples divided 75:25 between training and testing sets. The tests used a multi-layer perceptron (MLP) neural network model with 170 features. The dataset experiments demonstrate the methodology's practicality and efficacy. The paper does not examine blockchain technology's limits or vulnerabilities in the suggested system. Blockchain activities raise energy and computing challenges. The research does not analyse privacy restrictions in FL and data sharing in the IoV network.

In their study, Ayaz et al. (2022) presented a new vehicular network message dissemination method. Their blockchain-FL method lets automobiles compete to become relay nodes. A proof-of-federated-learning (PoFL) consensus technique in the blockchain smart contract does this. This paper uses a Stackelberg game to evaluate the economic framework for rewarding FL and message distribution vehicles. A hierarchical blockchain-based FL system for decentralised V2I message propagation is presented in this paper. It addresses latency and scalability issues with cloud-centric approaches. The proposed system is evaluated theoretically and practically by comparing consensus time delay, message delivery rate, and privacy protection to other blockchain methods. The study also examines asymptotic complexity and shows that PoFL is the most scalable vehicular network consensus algorithm. The research dataset and source are not disclosed in the paper. The study focuses on proposing and analysing the solution rather than examining the approach's limits. The paper does not directly address the disadvantages of the proposed strategy, leaving its restrictions unaddressed. No real-world data or

extended simulations are used in the research to evaluate the proposed solution. Cross-layer data from the physical and MAC layers may improve message distribution and relay selection in the future.

Wang et al. (2022) presented IoV BPFL for private FL. This method leverages extended Multi-Krum for ciphertext-level distributed verification and filtering. The authors use additive homomorphic encryption to encrypt model changes, increasing privacy. This work introduces a blockchain-based reputation-based reward system. The strategy encourages users with high-quality data to participate in FL and be honest. The proposed system uses a semi-decentralised consortium blockchain structure with FL and master (MA) nodes. FL nodes have read-access privileges and need authorisation to join the blockchain. However, MA nodes manage consensus and have write access. Every proposition in FL is the first transaction in a channel, and nodes can choose which channel to join. Practical Byzantine fault tolerance (PBFT) is used for consensus. For privacy, the suggested method uses upgraded Multi-Krum technology for distributed ciphertext verification and filtering and additive homomorphic encryption. The blockchain uses reputation-based incentives to encourage high-quality data producers. This project uses RSU data to build knowledge models for road barrier analysis and car misbehaviour detection. Simulation-only performance evaluation of the proposed method excludes real-world implementation and experimentation. The research does not address the challenges of implementing and accepting the suggested solution in real-world IoV scenarios. This study will focus on vehicle dynamics-related communication issues. It addresses the issue of stragglers in asynchronous FL.

Jiang et al. (2023) developed a blockchain-FL data-sharing platform. This concept addresses IoV data sharing security and privacy issues. FL facilitates data sharing while protecting data privacy and availability. This paper introduces an adaptive differential privacy technique to improve data privacy-availability equilibrium in the data-sharing context. Integrating the verification system into the consensus process helps identify and remove low-quality models, reducing data poisoning risk. Experimental results show that the proposed data-sharing paradigm increases data availability, privacy, and security. This study extends the generative regression neural network (GRNN) paradigm to recover client data simply from shared gradients without further input. This work introduces an adaptive differential privacy method that integrates reputation value and data information entropy to increase data-sharing privacy. The DBFT consensus approach is commonly used in local model update verification to prevent data poisoning and maintain model quality. Without a single point of attack, security and privacy may be compromised, which the essay does not address. We do not explore how malicious assaults during parameter transmission could affect the proposed data-sharing system. The research does not address data poisoning attempts by bad actors, and the notion that all participants behave well may not be true. The differential privacy approach to data sharing may compromise the global model's accuracy by ignoring noise errors.

A CGAN-based collaborative intrusion detection solution with distributed FL enabled by blockchain was proposed by He et al. (2023) to address insufficient data, privacy, training on tiny samples, and unequal data distribution. The recommended intrusion detection approach uses conditional generative adversarial network (CGAN). This framework generates synthetic samples and distinguishes between real and synthetic data using a generator and discriminator. FL, a distributed training method, lets unmanned aerial vehicles (UAVs) train models and acquire model updates without disclosing raw

data or neighbouring UAV data. The suggested strategy's accuracy, precision, recall, and other evaluation criteria are not examined. The research ignores the computational and communication challenges of applying the suggested methodology in real-world settings. The suggested strategy may not perform well for independent and identically distributed (IID and non-IID) data sets. This study did not investigate this because it is something that needs to be done later.

Li et al. (2023) proposed VTFL, a blockchain-based FL platform, to address vehicle topology security issues. The method ensures secure model aggregation and reduces the influence of rogue cars on global model correctness. This paper abstracts the FL local model, which is handled as a transaction, and proposes a blockchain consensus technique for low delay and limited vehicle computation resources. The VTFL framework secures vehicular FL processing and tracks and identifies threats. To test the system, malicious nodes were used in several extensive studies. In FL, the FedAvg algorithm is a popular aggregator. The central server assigns aggregation coefficients to participants based on their training sample count. The article also discusses Bulyan aggregation, which uses the Euclidean distance metric to compare local models from training nodes. To prevent damaging attacks, hazardous models are excluded from aggregation. The trim mean aggregate technique horizontally compares each gradient in the local model and removes deviating gradient values to ensure proper gradient deviation. The median aggregation method reduces error rate if the objective function is strongly convex. The research fails to examine the computational and resource requirements of the proposed VTFL framework, which are critical for actual deployment. The framework's training efficiency and convergence speed are not thoroughly assessed in the research. Security and privacy issues related to blockchain-based approach are not addressed in the study.

For safe data transfers in connected vehicles, Rajan et al. (2023) created a blockchain-based MLFEM-enabled IDS (BEF-IDS). FL generates multi-layered extreme learning machines, which are offloaded to dispersed vehicular edge devices like RSU and linked automobiles to reduce resource utilisation without compromising security in the proposed IDS. Blockchain was used to record and exchange training models, assuring network security in the proposed IDS. The authors used real-time datasets to evaluate the algorithm under several assault scenarios and found high results. The study employs methods that incorporate model customisation, scalability, traffic scenario generation, adaptability, and event recording to generate testing data. Approximately 4,000,000 data elements were gathered from the projected environment. The report does not address privacy or data protection issues in the proposed system, which uses real-time data sets and blockchain technology to share training models. The paper does not explore the suggested system's computational or resource needs, which may be crucial in real implementations.

An adaptive blockchain-enabled FL framework for ITS was proposed by Lin et al. (2023). This framework addresses preset parameters and high communication costs in conventional frameworks. The suggested approach uses blockchain sharding to improve. Sharding distributes a dataset across many databases for storage on multiple stations. The system includes a streamline-based shard transmission mechanism and an adaptive sharding mechanism that uses deep reinforcement learning (DRL) to automatically choose parameters. This method offers flexible, efficient, trustworthy, and scalable information communications among intelligent vehicles. In their future research, the authors plan to study intelligent dynamic collaboration among vehicles throughout chains.

Table 12 Literature on IoV with blockchain and FL focusing on security

Authors	*FL algorithm*	*Consensus algorithm*	*Other used algorithms*	*Data*	*Simulation technique*	*Results*	*Limitations*
Abdel-Basset et al. (2022)	N/A	dBFT	Federated training of FED-IDS model on the edge, and local training of FED-IDS model at the edge, and ECDSA.	Car-hacking, and TON_IoT	Dell workstation, PySyft, and Scipy.	The study found the suggested architecture works well as a distributed IDS in heterogeneous ITSs.	FED-IDS supervised training generalises heterogeneous vehicle data labeling slowly. Collaborative detection is affected by training data imbalance. Distributed, imprecise, and computationally expensive blockchain consensus mechanisms.
Islam et al. (2022)	MLP	POA	RSA.	Scania trucks	Python, Jetson TX2 board, and Ethereum.	The research demonstrates that FL and blockchain technology reduce IoV road accidents and address privacy concerns better than conventional schemes. Performance analysis proves the strategy works.	The study does not address blockchain's energy and computing constraints in the proposed system. FL privacy and IoV data exchange are not examined in this study.
Ayaz et al. (2022)	Isolation forest	PoFL	Stackelberg game, PoQF, PoS, and MSE.	N/A	OMNeT++, Python, C++, and SUMO.	This study provides validation for equilibrium points and uncovers the potential of blockchain-based federated learning in the context of vehicle applications.	Dataset and source of analysis are unknown. The study promotes the answer over the approach's limits. The approach's drawbacks and limitations are not addressed. This study lacks real-world data and extended simulations to evaluate the approach.
He et al. (2023)	LSTM	POA	Two-player min-max game, DP Gaussian noise, SVM, RF, DT, and RNN.	CIC-IDS2017	N/A	The study shows the technique can solve CIC-IDS2017's unequal data types and increase model training accuracy. Better classifications are in all categories. CGAN model collaborative training is private and secure using blockchain-empowered distributed FL.	The approach may limit computing and bandwidth in large IoV networks. The quality and accuracy of training data can vary between IoV devices and scenarios, impacting algorithm performance. The approach may need real-world optimisation and confirmation.

Table 12 Literature on IoV with blockchain and FL focusing on security (continued)

Authors	*FL algorithm*	*Consensus algorithm*	*Other used algorithms*	*Data*	*Simulation technique*	*Results*	*Limitations*
Li et al. (2023)	CNN.	PoMSFL	Merkel root and SHA256	MNIST, and Fashion-MNIST.	Python and flask framework.	Enhancing global model convergence in malicious scenarios. Strategy eliminates global model accuracy poisoning attacks. Safe model aggregation, HRT, and vehicular FL processing. FL using blockchain minimises central server-induced training instability and uses distributed capabilities.	Scalability and performance of the framework are not assessed in the research. The paper ignores FL process security. The article does not mention the blockchain-based framework's transportation overhead and processing needs.
Rajan et al. (2023)	Multi-layer ELM	Distributed consensus	SVM, BC, LR, DT, ELM, CNN, BFF, KNN, and RF.	Generated dataset	Python, TensorFlow Federated Version 2.1.0, MiniNet emulator, CSS script, OMNET++, INET, SUMO, VEINS, TraCL, and AIM.	The suggested IDS offers robust security measures while also minimising transmission expenses.	Big data sets, real-time processing, and cellular connectivity issues may hinder model training and conclusions. Sharing blockchain and real-time training models violates privacy. Implementation-related computational and resource needs are not covered.
Lin et al. (2023)	CNN	RAFT, HOTSTUFF, PBFT, and VRF	DQN and DAG	MNIST, KMNIST, Fashion-MNIST, and CIFAR-10.	PyTorch, Gym framework, and GO	The experimental results show that the framework is adaptable, reduces communication overhead, and outperforms baseline techniques.	Two-layer frameworks' reliance on vehicle blockchain settings reduces blockchain performance and dependability. Fixed shards may slow blockchain-enabled FL frameworks.

Table 13 Literature on IoV with blockchain and FL focusing on privacy

Authors	*FL algorithm*	*Consensus algorithm*	*Other used algorithms*	*Data*	*Simulation technique*	*Results*	*Limitations*
Pokhrel and Choi (2020)	N/A	POW	Newton's method, oVML algorithm, and miner algorithm	N/A	Numerical and simulation experiments with 3GPP LTE Cat. M1 specification.	The research analyses BFL network communication dynamics and block arrival rate using wireless channels as bottlenecks. No actual results are provided in the work on decentralised FL for linked autonomous vehicles.	No shared model training dataset was specified in the study. BFL miners may not be practicable in practice. BFL's consensus system may raise computation and communication costs. Decentralised FL security, privacy, and integrity are ignored.
Chai et al. (2021)	MLP and CNN	PoK	Hierarchical weighted updating federated learning, Stackelberg game, ADMM, CVS, CB, conventional FL, and AU-layered FL.	MNIST and CIFAR10.	N/A	The strategy improves IoV learning and sharing. Simulations demonstrated the strategy can protect against some malicious attacks. HWU-layered FL enhances learning and loss function.	In massive vehicle networks, hierarchical blockchain scalability is not studied. Performance and convergence rate restrictions of the hierarchical FL method are largely unanalysed. The blockchain-enabled system's security and attack weaknesses are not assessed in the research.
Alotaibi and Alazzawi (2022)	CNN	PoS, and BFT	Gossip protocol, and VRF.	MNIST	N/A	In experiments, the method improves global model accuracy. FL and Blockchain integration protect vehicle privacy and improves global model accuracy for IoV and fog computing. Blockchain secures fog node, cloud, and vehicle model updates.	Research may be limited by a lack of realistic testing. Dynamic and resource limited IoV environments can address PPIoV architectural scalability and computational cost. In IoV-Fog, network and communication delays might slow real-time analysis and decisions.
Singh et al. (2022)	N/A	PoA and advanced PoS	Cryptographic computational puzzle.	CIFAR-10	SUMO and GUI traffic simulator.	Smart vehicular networks, IoT, and IoV in smart city infrastructure may increase traffic efficiency, safety, autonomous driving, and information exchange.	The method's drawbacks for administering large IoT-enabled smart vehicle networks are not discussed. Intelligent vehicle network blockchain and FL implementation issues are not addressed in the research. Assessing the approach's scalability and resource needs is inadequate.
Smahi et al. (2023)	SVM	Improved PoV	LDP, CP zkSNARKS-based verification, Laplacian noise, random shuffling, KeyGen algorithm, ECC, hash function, MIN	MNIST and BelgiumTS.	VMware, ZoKrates, Ethereum, Python, TensorFlow, and TensorFlow-federated.	BV-ICVs can limit data poisoning concerns, preserve privacy, and improve FL accuracy in vehicle-to-everything (V2X) situations, according to security analysis and research results.	Federated SVM-only BV-ICVs cannot support all ML algorithms. Systems lacking trustworthy authorities may benefit from decentralised consensus. False-proof attacks can happen despite zkSNARKs reliability. Exercises that raise zkSNARKs' computational cost may influence BV-ICVs.

Table 14 Literature on IoV with blockchain and FL focusing on security and privacy

Authors	*FL algorithm*	*Consensus algorithm*	*Other used algorithms*	*Data*	*Simulation technique*	*Results*	*Limitations*
Lu et al. (2020)	CNN	Dpos and Pow	PermiDAG, DAG, MSE, MAE, DRL based on actor-critic (AC), MCMC, MDP, TGD, and DDPG.	Uber pickups in New York City, and MNIST.	Matplotlib basemap toolkit	System improves FL data security, training efficiency, and accuracy. Method handles diverse computing capacity, dynamic communication, and vehicle network security and privacy.	The optimal edge content caching system's performance is unknown. Security and privacy effects of edge intelligence and resource sharing in vehicle networks are not examined.
Liu et al. (2021)	MLP and CNN	POW and POA	Edge model averaging and masking, and global model averaging and aggregation.	KDDCup99	Python, Pytorch, Go language, and Syft.	The study shows the proposed approach cooperatively protects vehicle privacy while reducing communication and calculating expenses.	The strategy assumes 100% honest edge devices with training. Insufficient resources or malicious edge devices can influence training model accuracy. Communication and network latency affect system performance but are disregarded.
Moulahi et al. (2022)	SVM, RF, NB, and KNN	N/A	N/A	VeReMi	Python, Solidity, Truffle 5.0.5, and Ganache v 5.4.	With privacy-preserving FL and blockchain-based security, the ITS cyber-threat detection prototype performed well. Blockchain technology provides vehicle privacy, data aggregation security, and gas savings.	No mention is made of the approach's scalability and performance in a larger ITS environment. Network and communication latency may impair FL in real-time cyber-threat identification.
Lv et al. (2022)	MLP, RNN, and CNN	Enhanced DPoA	RDP, SGD, Gaussian mechanism, ECDSA	VeReMi	VEINS and Pytorch	Experimental results show the proposed method is accurate and efficient. Gaussian and differential privacy ensure blockchain model privacy.	This approach's implementation and scalability are ignored in the paper. Researchers do not compare the proposed misbehavior detection system. Neither congestion nor communication delays are mentioned as potential performance issues for the proposed approach.

Table 14 Literature on IoV with blockchain and FL focusing on security and privacy (continued)

Authors	*FL algorithm*	*Consensus algorithm*	*Other used algorithms*	*Data*	*Simulation technique*	*Results*	*Limitations*
Ghimire and Rawat (2022)	N/A	N/A	N/A	N/A	N/A	Pruning removes non-critical parameters for efficient learning task storage, calculation, and distribution in each job's ledger. The blockchain network is only accessible to required participants, reducing FL server and communication errors and attack surface.	The study ignores FL's main IoV concerns. The paper misses incentives, datasets, training, and consensus. The recommended technique may be inefficient due to many parameter aggregating nodes; a better solution is needed. The paper is numerically insufficient.
Wang et al. (2022)	CNN	PBFT.	Multi-Krum, Paillier algorithm, ECDSA, Merkle tree, and SHA-256.	Mnist, BelgiumTS, and Emnist.	Python, TensorFlow, TensorFlow-federated, Hyperledger Fabric, and Go.	The method uses additive homomorphic encryption to secure model changes. Blockchain's reputation-based reward structure encourages honest data participants to join FL.	This method's simulation-only performance evaluation ignores real-world implementation and experimentation. Implementing and accepting the proposed solution in real-world IoV circumstances is not addressed in the paper.
Jiang et al. (2023)	CNN	DBFT	Gaussian function, differential privacy, sensitivity of the function, Laplace mechanism, SGD, and SHA-256.	SVHN	Python and Pytroch	The study found that the blockchain-FL data-sharing approach balances data availability and privacy while improving IoV security.	FL's single point of attack's security risk is ignored. FL parameter transfer is neutral. Data poisoning by malicious parties may weaken the data-sharing model's presumed responsibility. Data privacy changes ignore global model noise, lowering model accuracy.

A blockchain-enabled and privacy-preserving FL framework for ICVs in V2X environments, BV-ICVs, was introduced by Smahi et al. (2023) to address FL system security issues and prevent unreliable model updates from compromising the global model. The BV-ICVs architecture uses smart contracts and permissioned blockchain consensus to verify zero-knowledge succinct non-interactive argument of knowledge (zkSNARKs). This architecture increases FL privacy, accuracy, model update reliability, and data poisoning mitigation. The researchers replace the central server with dependable consensus nodes that manage local model updates from participating ICVs. Decentralisation improves FL system security and efficiency. The BV-ICVs framework is evaluated for computing and communication efficiency, model correctness, and verification overhead. The framework's performance is evaluated by measuring the verification protocol's multipart computation complexity. The BV-ICVs system only supports federated SVM, limiting its ability to support other ML methods. However, the authors concede that the method was purposely designed to be highly versatile, allowing it to be applied to other ML protocols. A trustworthy party must construct the consortium blockchain system for FL verification to operate the system. Research on decentralised consensus methods may be valuable. A genuinely decentralised system without a trustworthy authority may be best. Despite their strong integrity guarantees, zkSNARKs are vulnerable to invalid or fake proof assaults. These attacks are rare, but they can occur if the trusted setup method is compromised or if the prover uses a circuit that differs from the verifier's expected circuit. As training data grows, zkSNARKs' computational costs may rise, affecting system efficiency. Scalability may be improved by investigating zero-knowledge proof methods like Bulletproofs that have minimal computational overhead. Enhancing zkSNARK implementations and using hardware acceleration can improve system performance.

The subsequent tables will provide illustrations of several characteristics that have been recorded in scholarly literature concerning the integration of blockchain with FL in the IoV field. Table 12 presents a summary of the academic literature pertaining to the discipline of security. Table 13 will provide an overview of the academic literature that specifically addresses the topic of privacy. Table 14 presents a summary of the scholarly inquiries that have explored the intersection of security and privacy.

6 Challenges and opportunities

With the goal of improving the security and privacy of IoV systems, this research delivers a comprehensive examination of blockchain technology in collaboration with FL frameworks. The investigation incorporates a comprehensive review of numerous research publications on this particular topic. While several studies predominantly present theoretical frameworks, others also include empirical findings through simulation results. Nevertheless, it is crucial to acknowledge that the suggested blockchain-based FL frameworks for IoV systems are currently in their initial phases of advancement. In order to fully realise the promise of merging these technologies inside the IoV domain, a number of significant research obstacles, prospective solutions, and avenues for additional exploration have been highlighted. The dominant body of research suggests that an increased quantity of participating vehicles correlates with the improved efficiency of the ultimate FL model. Hence, a significant obstacle exists in the endeavour to increase the number of vehicles engaging in the blockchain-enabled FL model of IoV

systems. One plausible approach to addressing this difficulty involves formulating an appropriate incentive system for user devices. The preservation of the integrity of the edge devices or terminal devices is crucial in facilitating the transmission of each transaction from user devices to the blockchain network. Moreover, several research endeavours exclusively put forth theoretical frameworks without doing empirical tests or simulations, hence posing challenges in assessing the efficacy of these propositions. In contrast, the majority of tests carried out in this field rely on simulated data. Hence, the utilisation of authentic datasets would augment the reliability and reception of the provided methodologies. The presence of branching events presents a notable obstacle in practical situations. In the event that a vehicle has network delays that are beyond its control and is unable to obtain the latest block, it may generate an independent branch chain. Nevertheless, the simultaneous existence of numerous chains is not a viable proposition, as blocks originating from alternative chains will eventually be disregarded. As a result, these instances of forking might lead to a decline in overall system performance. Several academics have utilised consensus algorithms from blockchain technology in an attempt to address poison attacks. However, it is important to note that these algorithms possess inherent security vulnerabilities. One example of potential blockchain forking events is when rogue miners aim to exploit the system by maximising their computational capability. Numerous studies have undertaken the development and execution of novel consensus algorithms with the objective of mitigating power usage. Nevertheless, the issue of security has not been adequately resolved. Because of this, it is important to create safe consensus algorithms for public blockchains in order for FL frameworks that use blockchain technology to be used in IoV networks. On the other hand, private blockchains and consortium technologies can provide additional safety features for IoV networks. While advancements have been made in enhancing the security of blockchain-enabled FL frameworks, the preservation of privacy continues to be a subject of apprehension. In order to effectively tackle this issue, it is imperative to incorporate supplementary methods that prioritise privacy, such as the integration of differential privacy techniques. Differential privacy protects sensitive information from attackers who might steal the learned model in order to derive private information. That's why it's important for IoV platforms to adopt additional privacy-protecting measures. Incentive methods can benefit from the use of a variety of metrics driven by data quality. Customers may be eligible for bonuses if they contribute datasets that are more diverse or display unusual trends. To gauge the efficacy of their recommended methodology, the vast majority of research investigations have relied on traditional performance-measuring approaches. However, it is advised to consider a broader range of evaluations, including metrics such as accuracy percentage, latency, desired time, lifetime reduction, energy consumption, expenses, network coverage, transmission success percentage, packet delivery ratio, throughput, total delay, and other relevant factors. It is crucial to look at the research of various FL methods, including ensemble learning approaches, across numerous datasets. Poisoning attacks, backdoor attacks, sign-flipping attacks, same-value attacks, and reverse engineering techniques are only some of the assaults that are not routinely used to rigorously assess a model's robustness. The real-world ramifications of combining blockchain technology with FL approaches are, thus, still poorly understood. Many of the problems that plague FL approaches may be solved with the help of blockchain technology. However, to guarantee the best performance of blockchain-enabled FL mechanisms for IoV networks, it is vital to address worries about

vehicle heterogeneity, system variability, and statistical disparity. Blockchain-enabled FL frameworks in real-world IoV systems must have their operational expenses and transaction throughput measured and analysed. Message propagation and relay selection have both been tackled by earlier methods, but the dataset could benefit from adding cross-layer information from the physical levels.

7 Conclusions

The IoV is a paradigm that leverages inter-and intra-vehicle network technologies to improve the driving experience and boost safety. However, these technologies also introduce potential vulnerabilities that can be exploited by malicious adversaries, threatening the security, privacy, accessibility, and authenticity of legitimate users. This study provides a comprehensive overview of the IoV and its various attack surfaces. It also categorises different security attacks based on their techniques, impacts, and objectives. Furthermore, it reviews the existing literature on the security and privacy of the IoV system and classifies the proposed solutions according to their use of blockchain technology, FL, or both. It also identifies the essential criteria for implementing effective security measures in the IoV environment and compares the advantages and disadvantages of different approaches. Blockchain technology and FL are two promising techniques that can enhance the security and privacy of the IoV system. However, there is a lack of reviews that summarise the state-of-the-art research and highlight the future directions in this domain. Therefore, this study also analyses the challenges, solutions, and opportunities for further development in this area. Finally, it discusses the open issues and research gaps that need to be addressed. The aim of this review is to assist researchers in advancing and accelerating their research efforts in this field.

References

Abbas, S., Talib, M.A., Ahmed, A., Khan, F., Ahmad, S. and Kim, D-H. (2021) 'Blockchain-based authentication in internet of vehicles: a survey', *Sensors*, Vol. 21, No. 23, p.7927, https://doi.org/10.3390/s21237927.

Abdel-Basset, M., Moustafa, N., Hawash, H., Razzak, I., Sallam, K.M. and Elkomy, O.M. (2022) 'Federated intrusion detection in blockchain-based smart transportation systems', *IEEE Transactions on Intelligent Transportation Systems*, Vol. 23, No. 3, pp.2523–2537, https://doi.org/10.1109/TITS.2021.3119968.

Abiodun, O.I., Abiodun, E.O., Alawida, M., Alkhawaldeh, R.S. and Arshad, H. (2021) 'A review on the security of the internet of things: challenges and solutions', *Wireless Personal Communications*, Vol. 119, pp.2603–2637, https://doi.org/10.1007/s11277-021-08348-9.

Adhikary, K., Bhushan, S., Kumar, S. and Dutta, K. (2020) 'Hybrid algorithm to detect DDoS attacks in VANETs', *Wireless Personal Communications*, Vol. 114, pp.3613–3634, https://doi.org/10.1007/s11277-020-07549-y.

Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Bhattacharya, S., Maddikunta, P.K.R. and Gadekallu, T.R. (2021) *Federated Learning for Intrusion Detection System: Concepts, Challenges and Future Directions*, arXiv, 2106.09527, https://doi.org/10.48550/arXiv.2106.09527.

Al-Jarrah, O.Y., Maple, C., Dianati, M., Oxtoby, D. and Mouzakitis, A. (2019) 'Intrusion detection systems for intra-vehicle networks: a review', *IEEE Access*, Vol. 7, pp.21266–21289, https://doi.org/10.1109/ACCESS.2019.2894183.

Alladi, T., Kohli, V., Chamola, V., Yu, F.R. and Guizani, M. (2021) 'Artificial intelligence (AI)-empowered intrusion detection architecture for the internet of vehicles', *IEEE Wireless Communications*, Vol. 28, No. 3, pp.144–149, https://doi.org/10.1109/MWC.001.2000428.

Almalki, S.A. and Song, J. (2020) 'A review on data falsification-based attacks in cooperative intelligent transportation systems', *International Journal of Computer Science and Security (IJCSS),* Vol. 14, No. 2, pp.22–37 [online] https://www.cscjournals.org/library /manuscriptinfo.php?mc=IJCSS-1548#MCAI (accessed 16 January 2024) .

Alotaibi, J. and Alazzawi, L. (2022) 'PPIoV: a privacy preserving-based framework for IoV-fog environment using federated learning and blockchain', *2022 IEEE World AI IoT Congress (AIIoT)*, Seattle, WA, USA, pp.597–603, https://doi.org/10.1109/AIIoT54504.2022.9817205.

Al-Shareeda, M.A., Anbar, M., Hasbullah, I.H., Manickam, S., Abdullah, N. and Hamdi, M.M. (2020) 'Review of prevention schemes for replay attack in vehicular ad hoc networks (VANETs)', *2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP)*, Shanghai, China, pp.394–398, https://doi.org/10.1109/ ICICSP50920.2020.9232047.

Aslam, B., Javed, A.R., Chakraborty, C., Nebhen, J., Raqib, S. and Rizwan, M. (2021) 'Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic', *Personal and Ubiquitous Computing*, https://doi.org/10.1007/s00779-021-01596-3.

Ayaz, F., Sheng, Z., Tian, D. and Guan, Y.L. (2022) 'A blockchain based federated learning for message dissemination in vehicular networks', *IEEE Transactions on Vehicular Technology*, Vol. 71, No. 2, pp.1927–1940, https://doi.org/10.1109/TVT.2021.3132226.

Ayed, S., Hbaieb, A. and Chaari, L. (2023) 'Blockchain and trust-based clustering scheme for the IoV', *Ad Hoc Networks*, Vol. 142, p.103093, https://doi.org/10.1016/j.adhoc.2023.103093.

Balakrishnan, S., Wang, P., Bhuyan, A. and Sun, Z. (2019) 'Modeling and analysis of eavesdropping attack in 802.11ad mmWave wireless networks', *IEEE Access*, Vol. 7, pp.70355–70370, https://doi.org/10.1109/ACCESS.2019.2919674.

Billah, M., Mehedi, S.T., Anwar, A., Rahman, Z. and Islam, R. (2022) *A Systematic Literature Review on Blockchain Enabled Federated Learning Framework for Internet of Vehicles*, arXiv, cs.CR, 2203.05192, https://doi.org/10.48550/arXiv.2203.05192.

Biswas, M., Das, D., Banerjee, S., Mukherjee, A., AL-Numay, W., Biswas, U. and Zhang, Y. (2023) 'Blockchain-enabled communication framework for secure and trustworthy internet of vehicles', *Sustainability*, Vol. 15, No. 12, p.9399, https://doi.org/10.3390/su15129399.

Chai, H., Leng, S., Chen, Y. and Zhang, K. (2021) 'A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles', *IEEE Transactions on Intelligent Transportation Systems*, Vol. 22, No. 7, pp.3975–3986, https://doi.org/10.1109/ TITS.2020.3002712.

Chen, S., Zhu, X., Zhang, H., Zhao, C., Yang, G. and Wang, K. (2020) 'Efficient privacy preserving data collection and computation offloading for fog-assisted IoT', *IEEE Transactions on Sustainable Computing*, Vol. 5, No. 4, pp.526–540, https://doi.org/10.1109/ TSUSC.2020.2968589.

Cheng, L., Liu, J., Xu, G., Zhang, Z., Wang, H., Dai, H-N., Wu, Y. and Wang, W. (2019) 'SCTSC: a semicentralized traffic signal control mode with attribute-based blockchain in IoVs', *IEEE Transactions on Computational Social Systems*, Vol. 6, No. 6, pp.1373–1385, https://doi.org/ 10.1109/TCSS.2019.2904633.

Chhabra, R., Singh, S. and Khullar, V. (2023) 'Privacy enabled driver behavior analysis in heterogeneous IoV using federated learning', *Engineering Applications of Artificial Intelligence*, Vol. 120, p.105881, https://doi.org/10.1016/j.engappai.2023.105881.

Devi, A., Rathee, G. and Saini, H. (2022) 'Secure blockchain-internet of vehicles (B-IoV) mechanism using DPSO and M-ITA algorithms', *Journal of Information Security and Applications*, Vol. 64, p.103094, https://doi.org/10.1016/j.jisa.2021.103094.

Ding, T., Liu, L., Zhu, Y., Cui, L. and Yan, Z. (2022) 'IoV environment exploring coordination: a federated learning approach', *Digital Communications and Networks*, https://doi.org/10.1016/j.dcan.2022.07.006.

Duan, W., Gu, J., Wen, M., Zhang, G., Ji, Y. and Mumtaz, S. (2020) 'Emerging technologies for 5G-IoV networks: applications, trends and opportunities', *IEEE Network*, Vol. 34, No. 5, pp.283–289, https://doi.org/10.1109/MNET.001.1900659.

Dureja, A. and Sangwan, S. (2021) 'A review: efficient transportation – future aspects of IoV', in *Evolving Technologies for Computing, Communication and Smart World. Lecture Notes in Electrical Engineering*, Vol. 694, Springer, Singapore, https://doi.org/10.1007/978-981-15-7804-5_8.

El Mazouzi, H., Khannous, A., Amechnoue, K. and Rghioui, A. (2023) 'Security challenges facing blockchain based-IoV network: a systematic review', *International Journal of Advanced Computer Science and Applications*, Vol. 14, No. 5, https://dx.doi.org/10.14569/IJACSA.2023.0140526.

Gadekallu, T.R., Pham, Q-V., Nguyen, D.C., Maddikunta, P.K.R., Deepa, N., Prabadevi, B., Pathirana, P.N., Zhao, J. and Hwang, W-J. (2022) 'Blockchain for edge of things: applications, opportunities, and challenges', *IEEE Internet Things Journal*, Vol. 9, No. 2, pp.964–988, https://doi.org/10.1109/JIOT.2021.3119639.

Gao, L., Wu, C., Yoshinaga, T., Chen, X. and Ji, Y. (2021) 'Multi-channel blockchain scheme for internet of vehicles', *IEEE Open Journal of the Computer Society*, Vol. 2, pp.192–203, https://doi.org/10.1109/OJCS.2021.3070714.

Garg, A., Chauhan, A. and Shambharkar, P.G. (2022) 'Security threats & attacks in IoV environment: open research issues and challenges', in *2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT)*, Kannur, India, pp.803–810, https://doi.org/10.1109/ICICICT54557.2022.9917816.

Garg, T., Kagalwalla, N., Churi, P., Pawar, A. and Deshmukh, S. (2020) 'A survey on security and privacy issues in IoV', *International Journal of Electrical and Computer Engineering*, Vol. 10, No. 5, pp.5409–5419, http://doi.org/10.11591/ijece.v10i5.pp5409-5419.

Ghimire, B. and Rawat, D.B. (2022) 'Secure, privacy preserving, and verifiable federating learning using blockchain for internet of vehicles', *IEEE Consumer Electronics Magazine*, Vol. 11, No. 6, pp.67–74, https://doi.org/10.1109/MCE.2021.3097705.

Ghosal, A. and Conti, M. (2020) 'Security issues and challenges in V2X: a survey', *Computer Networks*, Vol. 169, p.107093, https://doi.org/10.1016/j.comnet.2019.107093.

Gupta, M., Patel, R.B., Jain, S., Garg, H. and Sharma, B. (2022) 'Lightweight branched blockchain security framework for internet of vehicles', *Transactions on Emerging Telecommunications Technologies*, https://doi.org/10.1002/ett.4520.

Hangdong, K., Bo, M., Darong, H. and Zhaoyang, D. (2023) 'FedVPS: Federated learning for privacy and security of Internet of Vehicles on non-IID data', *2023 IEEE 12th Data Driven Control and Learning Systems Conference (DDCLS)*, Xiangtan, China, pp.178–183, https://doi.org/10.1109/DDCLS58216.2023.10166791.

Hbaieb, A., Ayed, S. and Chaari, L. (2022) 'Federated learning based IDS approach for the IoV', in *Proceedings of the 17th International Conference on Availability, Reliability and Security, Association for Computing Machinery*, New York, NY, USA, Article 123, pp.1–6, https://doi.org/10.1145/3538969.3544422.

He, X., Chen, Q., Tang, L., Wang, W. and Liu, T. (2023) 'CGAN-based collaborative intrusion detection for UAV networks: a blockchain-empowered distributed federated learning approach', *IEEE Internet of Things Journal*, Vol. 10, No. 1, pp.120–132, https://doi.org/10.1109/JIOT.2022.3200121.

Hu, W., Hu, Y., Yao, W. and Li, H. (2019) 'A blockchain-based Byzantine consensus algorithm for information authentication of the internet of vehicles', *IEEE Access*, Vol. 7, pp.139703–139711, https://doi.org/10.1109/ACCESS.2019.2941507.

Hu, X., Li, R., Wang, L., Ning, Y. and Ota, K. (2023) 'A data sharing scheme based on federated learning in IoV', *IEEE Transactions on Vehicular Technology*, Vol. 72, No. 9, pp.11644–11656, https://doi.org/10.1109/TVT.2023.3266100.

Islam, A., Morol, M.K. and Shin, S.Y. (2022) 'A federated learning-based blockchain-assisted anomaly detection scheme to prevent road accidents in internet of vehicles', *ICCA '22: Proceedings of the 2nd International Conference on Computing Advancements*, Association for Computing Machinery, New York, NY, USA, pp.516–521, https://doi.org/10.1145/3542954.3543028.

Javed, A.R., Hassan, M.A., Shahzad, F., Ahmed, W., Singh, S., Baker, T. and Gadekallu, T.R. (2022) 'Integration of blockchain technology and federated learning in vehicular (IoT) networks: a comprehensive survey', *Sensors*, Vol. 22, No. 12, p.4394, https://doi.org/10.3390/s22124394.

Jiang, T., Fang, H. and Wang, H. (2019) 'Blockchain-based internet of vehicles: distributed network architecture and performance analysis', *IEEE Internet of Things Journal*, Vol. 6, No. 3, pp.4640–4649, https://doi.org/10.1109/JIOT.2018.2874398.

Jiang, W., Chen, M. and Tao, J. (2023) 'Federated learning with blockchain for privacy-preserving data sharing in internet of vehicles', *China Communications*, Vol. 20, No. 3, pp.69–85, https://doi.org/10.23919/JCC.2023.03.006.

Kang, J., Xiong, Z., Niyato, D., Ye, D., Kim, D.I. and Zhao, J. (2019) 'Toward secure blockchain-enabled internet of vehicles: optimizing consensus management using reputation and contract theory', *IEEE Transactions on Vehicular Technology*, Vol. 68, No. 3, pp.2906–2920, https://doi.org/10.1109/TVT.2019.2894944.

Kang, J., Xiong, Z., Niyato, D., Zou, Y., Zhang, Y. and Guizani, M. (2020) 'Reliable federated learning for mobile networks', *IEEE Wireless Communications*, Vol. 27, No. 2, pp.72–80, https://doi.org/10.1109/MWC.001.1900119.

Karakoç, F., Karaçay, L., De Cnudde, P.Ç., Gülen, U., Fuladi, R. and Soykan, E.U. (2023) 'A security-friendly privacy-preserving solution for federated learning', *Computer Communications*, Vol. 207, pp.27–35, https://doi.org/10.1016/j.comcom.2023.05.004.

Karim, S.M., Habbal, A., Chaudhry, S.A. and Irshad, A. (2022) 'Architecture, protocols, and security in IoV: taxonomy, analysis, challenges, and solutions', *Security and Communication Networks*, Article ID 1131479, https://doi.org/10.1155/2022/1131479.

Kim, S-K. (2021) 'Enhanced IoV security network by using blockchain governance game', *Mathematics*, Vol. 9, No. 2, p.109, https://doi.org/10.3390/math9020109.

Li, A., Chang, X., Ma, J., Sun, S. and Yu, Y. (2023) 'VTFL: a blockchain based vehicular trustworthy federated learning framework', *2023 IEEE 6th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, Chongqing, China, pp.1002–1006, https://doi.org/10.1109/ITNEC56291.2023.10082698.

Li, H., Li, J., Zhao, H., He, S. and Hu, T. (2022) 'Blockchain-based incentive mechanism for spectrum sharing in IoV', *Wireless Communications and Mobile Computing*, Article ID 6807257, https://doi.org/10.1155/2022/6807257.

Li, T., Sahu, A.K., Talwalkar, A. and Smith, V. (2020) 'Federated learning: challenges, methods, and future directions', *IEEE Signal Processing Magazine*, Vol. 37, No. 3, pp.50–60, https://doi.org/10.1109/MSP.2020.2975749.

Lin, Y., Gao, Z., Du, H., Kang, J., Niyato, D., Wang, Q., Ruan, J. and Wan, S. (2023) 'DRL-based adaptive sharding for blockchain-based federated learning', *IEEE Transactions on Communications*, https://doi.org/10.1109/TCOMM.2023.3288591.

Liu, H., Zhang, S., Zhang, P., Zhou, X., Shao, X., Pu, G. and Zhang, Y. (2021) 'Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing', *IEEE Transactions on Vehicular Technology*, Vol. 70, No. 6, pp.6073–6084, https://doi.org/10.1109/TVT.2021.3076780.

Lone, F.R., Dhanore, Verma, H.K. and Sharma, K.P. (2021) 'Evolution of VANETS to IoV: applications and challenges', *Tehnički glasnik*, Vol. 15, No. 1, pp.143–149, https://doi.org/10.31803/tg-20210205104516.

Lu, Y., Huang, X., Zhang, K., Maharjan, S. and Zhang, Y. (2020) 'Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles', *IEEE Transactions on Vehicular Technology*, Vol. 69, No. 4, pp.4298–4311, https://doi.org/10.1109/TVT.2020.2973651.

Lv, P., Xie, L., Xu, J., Wu, X. and Li, T. (2022) 'Misbehavior detection in vehicular ad hoc networks based on privacy-preserving federated learning and blockchain', *IEEE Transactions on Network and Service Management*, Vol. 19, No. 4, pp.3936–3948, https://doi.org/10.1109/TNSM.2022.3220779.

Mendiboure, L., Chalouf, M.A. and Krief, F. (2018) 'Towards a blockchain-based SD-IoV for applications authentication and trust management', in *International Conference on Internet of Vehicles, Technologies and Services Towards Smart City*, Vol. 11253, Springer, Cham, pp.265–277, https://doi.org/10.1007/978-3-030-05081-8_19.

Mills, J., Hu, J. and Min, G. (2022) 'Multi-task federated learning for personalised deep neural networks in edge computing', *IEEE Transactions on Parallel and Distributed Systems*, Vol. 33, No. 3, pp.630–641, https://doi.org/10.1109/TPDS.2021.3098467.

Moulahi, T., Jabbar, R., Alabdulatif, A., Abbas, S., El Khediri, S., Zidi, S. and Rizwan, M. (2022) 'Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security', *Expert Systems*, Vol. 40, No. 5, p.e13103, Wiley, https://doi.org/10.1111/exsy.13103.

Nanda, A., Puthal, D., Rodrigues, J.J.P.C. and Kozlov, S.A. (2019) 'Internet of autonomous vehicles communications security: overview, issues, and directions', *IEEE Wireless Communications*, Vol. 26, No. 4, pp.60–65, https://doi.org/10.1109/MWC.2019.1800503.

Narbayeva, S., Bakibayev, T., Abeshev, K., Makarova, I., Shubenkova, K. and Pashkevich, A. (2020) 'Blockchain technology on the way of autonomous vehicles development', *Transportation Research Procedia*, Vol. 44, pp.168–175, https://doi.org/10.1016/j.trpro.2020.02.024.

Naveen, R., Chaitanya, N.S.V., Srinivas, N.M. and Vineeth, N. (2020) 'Implementation of a methodology for detection and prevention of security attacks in vehicular adhoc networks', *2020 IEEE International Conference for Innovation in Technology (INOCON)*, Bangalore, India, pp.1–6, https://doi.org/10.1109/INOCON50539.2020.9298365.

Ni, W., Zhu, S., Karim, M.M., Aloqaily, M., Kang, Z. and Maple, C. (2022) 'Lagrange coded federated learning (L-CoFL) model for Internet of vehicles', *2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS)*, Bologna, Italy, pp.864–872, https://doi.org/10.1109/ICDCS54860.2022.00088.

Parimala, M. Priya, R.M.S., Pham, Q-V., Dev, K., Maddikunta, P.K.R., Gadekallu, T.R. and Huynh-The, T. (2021) *Fusion of Federated Learning and Industrial Internet of Things: A Survey*, arXiv, 2101.00798, https://doi.org/10.48550/arXiv.2101.00798.

Pokhrel, S.R. and Choi, J. (2020) 'A decentralized federated learning approach for connected autonomous vehicles', *2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, Seoul, Korea (South), pp.1–6, https://doi.org/10.1109/WCNCW48565.2020.9124733.

Qureshi, K.N., Shahzad, L., Abdelmaboud, A., Eisa, T.A.E., Alamri, B., Javed, I.T., Al-Dhaqm, A. and Crespi, N. (2022) 'A blockchain-based efficient, secure and anonymous conditional privacy-preserving and authentication scheme for the internet of vehicles', *Applied Sciences*, Vol. 12, No. 1, p.476, https://doi.org/10.3390/app12010476.

Rahman, M.A., Rashid, M.M., Barnes, S.J. and Abdullah, S.M. (2019) 'A blockchain-based secure internet of vehicles management framework', *2019 UK/China Emerging Technologies (UCET)*, Glasgow, UK, pp.1–4, https://doi.org/10.1109/UCET.2019.8881874.

Raja, G., Manaswini, Y., Vivekanandan, G.D., Sampath, H., Dev, K. and Bashir, A.K. (2020) 'AI-powered blockchain – a decentralized secure multiparty computation protocol for IoV', *IEEE INFOCOM 2020 – IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Toronto, ON, Canada, pp.865–870, https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162866.

Rajan, D., Eswaran, P., Srivastava, G., Ramana, K. and Iwendi, C. (2023) 'Blockchain-based multi-layered federated extreme learning networks in connected vehicles', *Expert Systems*, Vol. 40, No. 6, p.e13222, Wiley, https://doi.org/10.1111/exsy.13222.

Rathee, G., Ahmad, F., Kurugollu, F., Azad, M.A., Iqbal, R. and Imran, M. (2021) 'CRT-BIoV: a cognitive radio technique for blockchain-enabled internet of vehicles', *IEEE Transactions on Intelligent Transportation Systems*, Vol. 22, No. 7, pp.4005–4015, https://doi.org/10.1109/TITS.2020.3004718.

Rathee, G., Sharma, A., Iqbal, R., Aloqaily, M., Jaglan, N. and Kumar, R. (2019) 'A blockchain framework for securing connected and autonomous vehicles', *Sensors*, Vol. 19, No. 14, p.3165, https://doi.org/10.3390/s19143165.

Safavat, S. and Rawat, D.B. (2023) 'Asynchronous federated learning for intrusion detection in vehicular cyber-physical systems', *IEEE INFOCOM 2023 – IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Hoboken, NJ, USA, pp.1–6, https://doi.org/10.1109/INFOCOMWKSHPS57453.2023.10225917.

Sahraoui, Y., Kerrache, C.A., Korichi, A., Vegni, A.M. and Amadeo, M. (2022) 'LearnPhi: a real-time learning model for early prediction of phishing attacks in IoV', *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, pp.252–255, https://doi.org/10.1109/CCNC49033.2022.9700545.

Sharma, R. and Chakraborty, S. (2018) 'BlockAPP: using blockchain for authentication and privacy preservation in IoV', *2018 IEEE Globecom Workshops (GC Wkshps)*, Abu Dhabi, United Arab Emirates, pp.1–6, https://doi.org/10.1109/GLOCOMW.2018.8644389.

Sharma, S. and Kaushik, B. (2019) 'A survey on internet of vehicles: applications, security issues & solutions', *Vehicular Communications*, Vol. 20, p.100182, https://doi.org/10.1016/j.vehcom.2019.100182.

Singh, P.K., Nandi, S., Nandi, S.K., Ghosh, U. and Rawat, D.B. (2021) *Blockchain Meets AI for Resilient and Intelligent Internet of Vehicles*, arXiv preprint arXiv:2112.14078. https://doi.org/10.48550/arXiv.2112.14078.

Singh, S.K., Park, L. and Park, J.H. (2022) 'Blockchain-based federated approach for privacy-preserved IoT-enabled smart vehicular networks', *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, Republic of Korea, pp.1995–1999, https://doi.org/10.1109/ICTC55196.2022.9952835.

Smahi, A., Li, H., Yang, Y., Yang, X., Lu, P., Zhong, Y. and Liu, C. (2023) 'BV-ICVs: a privacy-preserving and verifiable federated learning framework for V2X environments using blockchain and zkSNARKs', *Journal of King Saud University – Computer and Information Sciences*, Vol. 35, No. 6, p.101542, https://doi.org/10.1016/j.jksuci.2023.03.020.

Sun, X., Yu, F.R. and Zhang, P. (2022) 'A survey on cyber-security of connected and autonomous vehicles (CAVs)', *IEEE Transactions on Intelligent Transportation Systems*, Vol. 23, No. 7, pp.6240–6259, https://doi.org/10.1109/TITS.2021.3085297.

Talpur, A. and Gurusamy, M. (2021) 'Adversarial attacks against deep reinforcement learning framework in internet of vehicles', *2021 IEEE Globecom Workshops (GC Wkshps)*, Madrid, Spain, pp.1–6, https://doi.org/10.1109/GCWkshps52748.2021.9681966.

Talpur, A. and Gurusamy, M. (2022) *GFCL: A GRU-based Federated Continual Learning Framework against Data Poisoning Attacks in IoV*, arXiv, cs.LG, 2204.11010, https://doi.org/10.48550/arXiv.2204.11010.

Taslimasa, H., Dadkhah, S., Pinto Neto, E.C., Xiong, P., Ray, S. and Ghorbani, A.A. (2023) 'Security issues in internet of vehicles (IoV): a comprehensive survey', *Internet of Things*, Vol. 22, p.100809, https://doi.org/10.1016/j.iot.2023.100809.

Tham, C-K., Yang, L., Khanna, A. and Gera, B. (2023) 'Federated learning for anomaly detection in vehicular networks', *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, Florence, Italy, pp.1–6, https://doi.org/10.1109/VTC2023-Spring57618.2023.10199870.

Theodouli, A., Moschou, K., Votis, K., Tzovaras, D., Lauinger, J. and Steinhorst, S. (2020) 'Towards a blockchain-based identity and trust management framework for the IoV ecosystem', *2020 Global Internet of Things Summit (GIoTS)*, Dublin, Ireland, pp.1–6, https://doi.org/10.1109/GIOTS49054.2020.9119623.

Tseng, L., Wong, L., Otoum, S., Aloqaily, M. and Ben Othman, J. (2020) 'Blockchain for managing heterogeneous internet of things: a perspective architecture', *IEEE Network*, Vol. 34, No. 1, pp.16–23, https://doi.org/10.1109/MNET.001.1900103.

Tu, S., Yu, H., Badshah, A., Waqas, M., Halim, Z. and Ahmad, I. (2023) 'Secure internet of vehicles (IoV) with decentralized consensus blockchain mechanism', *IEEE Transactions on Vehicular Technology*, Vol. 72, No. 9, pp.11227–11236, https://doi.org/10.1109/TVT.2023.3268135.

Uprety, A., Rawat, D.B. and Li, J. (2021) 'Privacy preserving misbehavior detection in IoV using federated machine learning', *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, pp.1–6, https://doi.org/10.1109/CCNC49032.2021.9369513.

Wang, N., Yang, W., Wang, X., Wu, L., Guan, Z., Du, X. and Guizani, M. (2022) 'A blockchain based privacy-preserving federated learning scheme for internet of vehicles', *Digital Communications and Networks*, https://doi.org/10.1016/j.dcan.2022.05.020.

Wang, X., Zeng, P., Patterson, N., Jiang, F. and Doss, R. (2019) 'An improved authentication scheme for internet of vehicles based on blockchain technology', *IEEE Access*, Vol. 7, pp.45061–45072, https://doi.org/10.1109/ACCESS.2019.2909004.

Wang, Z. and Yan, T. (2023) *Federated Learning-based Vehicle Trajectory Prediction against Cyberattacks*, arXiv, cs.CR, 2306.08566, https://doi.org/10.48550/arXiv.2306.08566.

Wu, J., Jin, Z., Li, G., Xu, Z., Fan, C. and Zheng, Y. (2022) 'Design of vehicle certification schemes in IoV based on blockchain', *World Wide Web*, Vol. 25, pp.2241–2263, https://doi.org/10.1007/s11280-022-01078-3.

Xiao, Y., Liu, Y. and Li, T. (2020) 'Edge computing and blockchain for quick fake news detection in IoV', *Sensors*, Vol. 20, No. 16, p.4360, https://doi.org/10.3390/s20164360.

Xu, Q., Zhang, L., Ou, D. and Yu, W. (2023) 'Secure intrusion detection by differentially private federated learning for inter-vehicle networks', *Transportation Research Record*, Vol. 2677, No. 9, pp.421–437, https://doi.org/10.1177/03611981231159118.

Yaga, D., Mell, P., Roby, N. and Scarfone, K. (2019) *Blockchain Technology Overview*, arXiv, National Institute of Standards and Technology, https://doi.org/10.6028/nist.ir.8202.

Yang, J., Hu, J. and Yu, T. (2022) 'Federated AI-enabled in-vehicle network intrusion detection for internet of vehicles', *Electronics*, Vol. 11, No. 22, p.3658, https://doi.org/10.3390/electronics11223658.

Yang, Q., Liu, Y., Chen, T. and Tong, Y. (2019) 'Federated machine learning: concept and applications', *Association for Computing Machinery, Transactions on Intelligent Systems and Technology*, Article No. 12., Vol. 10, No. 2, https://doi.org/10.1145/3298981.

Yarradoddi, S. and Gadekallu, T.R. (2022) 'Federated learning role in big data, jot services and applications security, privacy and trust in Jot: a survey', in *Trust, Security and Privacy for Big Data*, 1st ed., p.28, CRC Press, Boca Raton, FL, USA [online] https://www.taylorfrancis.com/chapters/edit/10.1201/9781003194538-2/federated-learning-role-big-data-iot-services-applications-security-privacy-trust-iot-survey-supriya-yarradoddi-thippa-reddy-gadekallu (accessed 12 January 2024).

Yu, T., Hua, G., Wang, H., Yang, J. and Hu, J. (2022) 'Federated-LSTM based network intrusion detection method for intelligent connected vehicles', *ICC 2022 – IEEE International Conference on Communications*, Seoul, Republic of Korea, pp.4324–4329, https://doi.org/10.1109/ICC45855.2022.9838655.

Yu, Z., Hu, J., Min, G., Zhao, Z., Miao, W. and Hossain, M.S. (2021) 'Mobility-aware proactive edge caching for connected vehicles using federated learning', *IEEE Transactions on Intelligent Transportation Systems*, Vol. 22, No. 8, pp.5341–5351, https://doi.org/10.1109/TITS.2020.3017474.

Yuan, X., Chen, J., Zhang, N., Fang, X. and Liu, D. (2021) 'A federated bidirectional connection broad learning scheme for secure data sharing in internet of vehicles', *China Communications*, Vol. 18, No. 7, pp.117–133, https://doi.org/10.23919/JCC.2021.07.010.

Zhang, J., Xin, Y., Wang, Y., Lei, X. and Yang, Y. (2023a) 'Secure blockchain-enabled internet of vehicles scheme with privacy protection', *Computers, Materials & Continua*, Vol. 75, No. 3, pp.6185–6199, https://doi.org/10.32604/cmc.2023.038029.

Zhang, M., Zhou, J., Cong, P., Zhang, G., Zhuo, C. and Hu, S. (2023b) 'LIAS: a lightweight incentive authentication scheme for forensic services in IoV', *IEEE Transactions on Automation Science and Engineering*, Vol. 20, No. 2, pp.805–820, https://doi.org/10.1109/TASE.2022.3165174.

Zhou, H., Zheng, Y., Huang, H., Shu, J. and Jia, X. (2023) 'Toward robust hierarchical federated learning in internet of vehicles', *IEEE Transactions on Intelligent Transportation Systems*, Vol. 24, No. 5, pp.5600–5614, https://doi.org/10.1109/TITS.2023.3243003.