Overview of Vehicle Edge Computing and Its Security

Shaodong Han, Maojie Wang, and Guihong Chen(✉)

Guangdong Polytechnic Normal University, Guangzhou 510635, China
chenguihong@gpnu.edu.cn

Abstract. The Internet of Vehicles (IoV) is a part of the Internet of Things (IoT). With the continuous development of the Internet of Things technology, the Internet of Vehicles technology has also made great progress. However, as more and more vehicles are connected to the Internet of Vehicles, the calculation and transmission of data in the Internet of Vehicles becomes more and more difficult, and at the same time, it is inevitable to face the pressure of data security and privacy protection. In order to solve the above problems, academia and industry have adopted many methods, combining mobile edge computing technology with the Internet of Vehicles to establish a vehicle edge computing network to solve the problems of data computing and transmission. Introducing blockchain technology and federated learning technology into vehicle edge computing. Therefore, the network addresses the issues of data security and privacy protection. Based on these, this paper summarizes the research results of many scholars in related fields, in order to provide reference and reference for subsequent related research.

Keywords: Vehicle edge computing · Reinforcement learning · Federated learning

1 Introduction

With the rapid growth of the automotive industry, particularly in the field of new energy vehicles, and the advancement of the internet industry with artificial intelligence at its forefront, the market has witnessed the emergence of intelligent connected vehicles, giving rise to a thriving industry. These vehicles are equipped with a range of sensors such as LiDAR, ultrasonic sensors, and cameras, significantly enhancing their perception of the surrounding environment. Additionally, intelligent connected vehicles possess robust communication capabilities, facilitating communication between vehicles, pedestrians, infrastructure,

The work is supported in part by Key Research Projects of Universities in Guangdong Province under Grant 2022ZDZX1011, Guangdong Provincial Natural Science Fund Project under Grant 2023A1515011084 and Doctoral Program Construction Unit Research Capability Enhancement Project at Guangdong Polytechnic Normal University under Grant 22GPNUZDJS27.

J. Cai et al. (Eds.): SPNCE 2023, LNICST 525, pp. 105–121, 2025.
https://doi.org/10.1007/978-3-031-73699-5_8

and servers [50]. Together, these interconnected networks form the Internet of Vehicles (IoV) system, providing convenient transportation solutions. This system has given rise to numerous applications, including in-vehicle entertainment, navigation and positioning, and autonomous driving, resulting in a substantial amount of data generation. Consequently, vehicles must not only process this data in real-time but also transmit and exchange it with the surrounding environment to deliver high-quality applications [39].

However, vehicles encounter several challenges in dealing with and transmitting large volumes of data [29] [20]. Firstly, the onboard computer systems' computational capacity is insufficient to support real-time processing of substantial data. Secondly, the high mobility of vehicles poses significant obstacles to communication with surrounding infrastructure. Lastly, the data transmission process during communication between vehicles and the surrounding infrastructure is inherently vulnerable to security threats, including attacks and data breaches. Addressing these challenges has prompted scholars to propose various solutions.

To address the issue of inadequate computing capabilities in vehicles, researchers have proposed integrating Mobile Edge Computing (MEC) with the Internet of Vehicles (IoV), resulting in a new computing paradigm called Vehicle Edge Computing (VEC) [4]. The VEC architecture, depicted in Fig 1, involves offloading computation tasks from vehicles to edge servers for processing. The computation results are then returned to the vehicles, combined with local computation results, and used to obtain the final outcome. This approach effectively alleviates the computational burden on vehicles, significantly enhancing the efficiency of IoV applications and improving the overall driving experience for users [22,25,34].

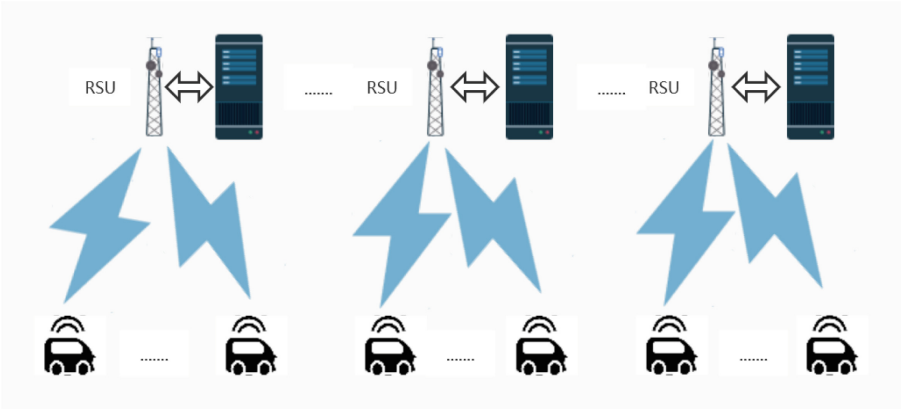

Fig. 1. Vehicle edge computing architecture

However, the introduction of vehicle edge computing necessitates careful consideration of the impact of vehicle mobility on communication latency, energy consumption, and communication quality within the IoV. Furthermore, the computation latency and energy consumption of both vehicles and servers during task processing must be taken into account. Only by comprehensively addressing these issues can an efficient system architecture be established, and suitable algorithms be formulated. In practical applications, it is crucial to adopt well-designed computation offloading schemes to minimize communication latency, energy consumption, as well as computation latency and energy consumption. To achieve an optimal computation offloading scheme, researchers have proposed various optimization methods, including those based on Reinforcement Learning (RL) [2].

Addressing the data security challenges in vehicle edge computing, the integration of blockchain technology and Federated Learning (FL) techniques with VEC has garnered significant attention [23]. Blockchain technology, known for its security features such as anonymity and tamper-proof properties of on-chain data, naturally enhances the security of vehicle edge computing [9]. Federated Learning, on the other hand, is an emerging machine learning approach that enables multiple users to collaboratively train a shared model. Participants maintain their data privacy by transmitting only the computed model parameters without sharing their local data [17]. This characteristic aligns with the data security requirements of vehicle edge computing, making it feasible to combine federated learning with VEC to establish a secure IoV system.

At present, research in relevant fields has reached a high level of maturity, with various advanced achievements continually emerging. Our objective is to provide a targeted summary of existing research outcomes to assist researchers in understanding the current state of research in these areas. This paper presents a comprehensive overview of edge computing offloading solutions in vehicular networks based on reinforcement learning. Additionally, we focus on summarizing research solutions that employ blockchain and federated learning for safeguarding the privacy and security of shared vehicular data. This will enable researchers in these domains to quickly grasp the current status and accomplishments of related research, thereby gaining inspiration for advancing their own research and proposing more advanced solutions.

The specific content of this paper is as follows: Sect. 2 will introduce an optimization scheme for vehicle edge computing offloading based on reinforcement learning methods. Section 3 will present a data security solution by integrating vehicle edge computing with blockchain technology. The data security solution combining federated learning and vehicle edge computing will be detailed in Sect. 4. Section 5 will highlight some future research directions for vehicle edge computing. Finally, Sect. 6 will provide a summary of the entire paper.

2 Reinforcement Learning-Based Offloading Optimization

In the vehicle edge computing network, the dynamic nature of vehicles in a mobile state during computation offloading tasks significantly impacts the network's topology. This dynamicity introduces variations in communication latency and signal-to-noise ratio, which, in turn, influence the formulation of optimal offloading strategies. Moreover, many tasks have strict time constraints, requiring offloaded computations to be completed within specified deadlines. This entails ensuring that the sum of local computation time on vehicles and the edge server's computation time is less than the task's response time. Furthermore, energy constraints must be considered due to the limited energy resources available in vehicles. Therefore, it is essential to account for energy consumption during communication and computation tasks on vehicles [19].

To obtain an optimal offloading solution, multiple factors need to be considered, including channel bandwidth, signal-to-noise ratio, communication latency, energy consumption, computation latency, energy consumption, as well as vehicle mobility. An optimal solution should minimize communication latency and energy consumption, along with computation latency and energy consumption. Consequently, finding the optimal offloading solution becomes a multi-objective optimization decision problem. In this regard, reinforcement learning methods prove to be one of the most effective approaches for tackling this challenge.

Reinforcement learning, depicted in Fig 2, is a method that enables an intelligent agent to engage in continuous interactions with the environment, gathering experiences and learning the optimal solution to a sequential decision-making

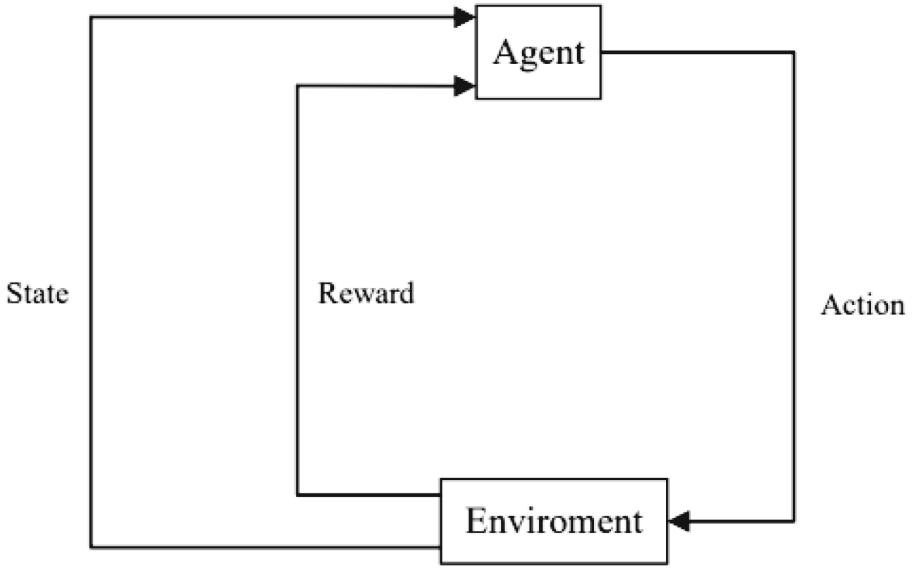

Fig. 2. Interactive process of reinforcement learning

Table 1. The publication years and main contributions of reinforcement learning based papers

Paper	Year of publication	Main contributions
paper[45]	2020	Proposing a multi-vehicle user optimization algorithm that integrates deep reinforcement learning with convex optimization.
paper[25]	2019	Developing a task offloading algorithm for vehicular networking tasks solely using the DQN algorithm.
paper[31]	2023	Proposing a multi-step reinforcement learning-based vehicle edge computation offloading scheme.
paper[22]	2019	Abstracting vehicle edge computing offloading and resource allocation as a semi-Markov process and employed both deep reinforcement learning and Q-Learning algorithms to obtain the optimal offloading strategy.
paper[28]	2018	Proposing a knowledge-driven (KD) offloading decision algorithm.
paper[35]	2021	Proposing a highly reliable vehiclar edge computing offloading decision network.
paper[37]	2021	Designing a multi-access vehicular edge computing network utilizing MEC technology.
paper[26]	2020	Proposing a joint optimization scheme for computation and caching in future 5G vehicular networks.
paper[44]	2021	Employing digital twin technology to build a virtual model mirroring real vehicle networks, and using a distributed multi-agent reinforcement learning algorithm to obtain the optimal offloading decisions.
paper[40]	2020	Proposing a deep reinforcement learning-based digital twin service offloading algorithm.

problem [6]. The determination of vehicle edge computing offloading solutions follows a similar sequential decision-making process. Treating the vehicle as an intelligent agent, it interacts with the environment comprising channel bandwidth, communication latency and energy consumption, computation latency and energy consumption, and signal-to-noise ratio, in order to obtain an optimal offloading solution. To achieve this objective, various non-deep reinforcement learning methods and deep reinforcement learning (DRL) methods can be employed, with DRL methods being widely favored for their superior performance [12,15,32,43]. Besides, in the remainder of this section, we present some of the related papers in detail. The publication years and main contributions of these literatures are shown in Table 1.

Zhang et al. proposed a multi-vehicle user optimization algorithm that integrates deep reinforcement learning with convex optimization [45]. This algorithm utilizes the Deep Q Network (DQN) to make offloading decisions, and then applies the Lagrange multiplier method to allocate the edge server's computing capacity among multiple users, thereby achieving an optimal offloading alloca-

tion scheme. Simulation results demonstrate that this approach reduces system latency to only 56% compared to traditional methods. Additionally, deep reinforcement learning methods can also be used independently, delivering satisfactory performance. For example, Ning et al. developed a task offloading algorithm for vehicular networking tasks solely using the DQN algorithm. Performance analysis and experimental results confirm the efficiency and effectiveness of this approach [25]. Han et al. proposed a multi-step reinforcement learning-based vehicle edge computation offloading scheme. They create a two layer VEC architecture, and use an improved algorithm multi-step DQN (MSDQN) to obtain the optimal decision. Simulation results demonstrate that MSDQN-based algorithm can reduce the offloading latency and energy consumption [31].

Liu et al. abstracted vehicle edge computing offloading and resource allocation as a semi-Markov process and employed both deep reinforcement learning and Q-Learning algorithms to obtain the optimal offloading strategy [22]. Experimental results demonstrated that utilizing these algorithms yielded the best offloading strategies, surpassing the efficiency of local computing on vehicles for executing vehicular networking computing tasks. To account for vehicle mobility during the edge computing offloading process, Qi et al. proposed a knowledge-driven (KD) offloading decision algorithm [28]. This algorithm comprehensively considers three major factors: resource requirements, access networks, and vehicle mobility. It utilizes the A3C algorithm for online offloading optimization decision-making. The algorithm incorporates the vehicle's mobility while traveling and accessing different edge computing nodes, leading to varying task computation times. This model is directly applied to the training and learning process of optimal offloading decisions. Simulation experiments demonstrate that the algorithm delivers faster offloading decisions and exhibits strong applicability.

As the number of vehicles in the vehicular network increases, the network's complexity rises, resulting in longer offloading transmission times, higher energy consumption, decreased Quality of Service (QoS), and reduced network reliability. To tackle this challenge, a highly reliable vehicular edge computing offloading decision network has been proposed [35]. This network integrates vehicle edge computing with Software Defined Networking (SDN) to offer a reliable approach for network control and resource management. It encompasses computation, communication, and privacy protection models, and introduces a joint strategy for offloading and resource allocation. The Q-Learning algorithm is employed to explore optimal decisions.

With the continuous advancement of communication technologies, such as 5G, new-generation communication technologies have been applied to vehicular networking. In response, scholars have proposed vehicular edge computing offloading schemes based on 5G networks. Notably, Multi-access Edge Computing (MEC) technology plays a vital role in 5G networks. Wu et al. designed a multi-access vehicular edge computing network utilizing MEC technology [37]. Their approach takes into account multiple tasks concurrency, system computing resource distribution, and network communication bandwidth. They propose

a joint optimization algorithm for computation offloading and task migration based on the DQN algorithm. This algorithm effectively reduces task processing latency and device energy consumption compared to traditional methods. It optimizes computation offloading and resource allocation approaches, thereby enhancing system resource utilization.

Ning et al. proposed a joint optimization scheme for computation and caching in future 5G vehicular networks [26]. This scheme takes into account the revenue of Mobile Network Operators (MNOs) and users' usage experience. They designed a joint optimization algorithm based on the Deep Deterministic Policy Gradient (DDPG) algorithm to maximize the profit of MNOs. To address the challenges encountered by vehicular edge computing in real-world environments, some researchers have introduced digital twin technology to create innovative vehicular edge computing networks. Zhang et al. employed digital twin technology to build a virtual model mirroring real vehicle networks, effectively illustrating the connectivity relationships among vehicles. With this model in place, a distributed multi-agent reinforcement learning algorithm is utilized to determine the optimal offloading decisions, minimizing offloading costs. Experimental results demonstrate the superiority of this method over traditional offloading algorithms [44].

To enhance the effectiveness of vehicular edge computing empowered by digital twins, regular updates to the digital twin network of vehicles are crucial for providing improved computing services. However, relying solely on the vehicles' computing capabilities is insufficient to support a wide range of digital twin services. To address this, Xu et al. proposed a deep reinforcement learning-based digital twin service offloading algorithm [40]. This algorithm employs the DQN algorithm to determine the optimal offloading strategy that meets the Quality of Service (QoS) requirements of various digital twin services. Experimental results highlight the effectiveness and applicability of this algorithm in diverse environments.

In this section, we have enumerated various edge computing data offloading solutions for vehicular networks based on reinforcement learning methods, all of which serve to enhance the efficiency of edge computing in vehicular networks. However, vehicular edge computing involves transmitting data in a completely open environment when establishing communication connections, making it highly susceptible to various network attacks that can compromise the security of data transmission and potentially lead to data privacy breaches. To address this issue and ensure the confidentiality, integrity, and availability of vehicular network data, blockchain technology and federated learning techniques can be employed.

3 Security Offload Optimization Combined with Blockchain

Ensuring data privacy and security is crucial for the widespread adoption of vehicular edge computing and vehicular networking, which is not addressed in

the previous section. However, leveraging blockchain technology can serve as a valuable tool to safeguard the privacy and security of vehicle edge computing data [13].

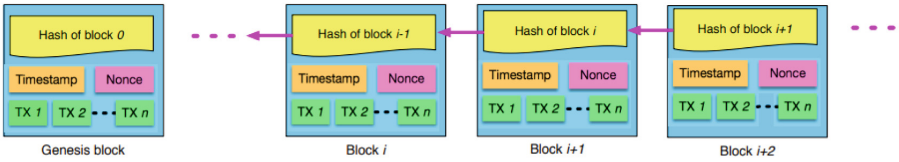

Fig. 3. A typical blockchain structure [49]

In 2008, Satoshi Nakamoto published the paper "Bitcoin: A Peer-to-Peer Electronic Cash System," introducing the concept of blockchain [24]. The structure of a typical blockchain is illustrated in Fig 3. Blockchain can be described as an encrypted distributed digital ledger, characterized by decentralization, immutability, traceability, and the participation of multiple parties. It establishes trust among untrusted nodes through consensus mechanisms like Proof-of-Work (PoW) and Proof-of-Stake (PoS), enabling data sharing and peer-to-peer transmission. These properties have led to the widespread adoption of blockchain in environments where data protection is crucial. Vehicular edge computing, as a use case requiring data security and privacy, can leverage blockchain technology for data protection. Scholars have conducted research on this topic and proposed methods to address related issues [1,5,14,36]. Some literatures are listed in detail below, and their publication years and main contributions are shown in the Table 2.

Zhang et al. presented a blockchain-based three-tier security architecture for vehicular edge computing [46]. This architecture consists of the perception layer, edge computing layer, and service layer. The perception layer ensures secure data transmission through the use of blockchain. The edge computing layer provides computing resources and edge cloud services for the perception layer, while the service layer combines traditional cloud storage with blockchain to ensure data security. Zhang et al. introduced a consortium blockchain-based scheme called Data Security Sharing and Storage for Connected Vehicles (DSSCB) [47]. This scheme establishes a decentralized, secure, and reliable database using a consortium blockchain. It employs digital signature technology to ensure the reliability and integrity of transmitted data. Smart contracts are utilized to set conditions for participating nodes during data transmission and storage, and tokens are allocated to vehicles contributing data. Experimental results demonstrate that this method significantly enhances data security compared to traditional approaches. Considering the vulnerability of shared vehicular data to attacks, Singh et al. proposed a blockchain-based trusted data sharing environment [33]. This environment utilizes a blockchain backbone to ensure accuracy and reliability during the transmission of vehicular data.

Table 2. The publication years and main contributions of blockchain based papers

Paper	Year of publication	Main contributions
paper[46]	2018	Presenting a blockchain-based three-tier security architecture for vehicular edge computing.
paper[47]	2019	Introducing a consortium blockchain-based scheme called Data Security Sharing and Storage for Connected Vehicles.
paper[33]	2017	Proposing a blockchain-based trusted data sharing environment.
paper[3]	2020	Proposing a blockchain-driven distributed secure content forwarding and storage framework.
paper[30]	2021	Developing a blockchain system using the PBFT consensus machanism for offloading and migration of vehicular edge computing services.
paper[18]	2018	Proposing a secure blockchain system based on the Proof of Work (POW) consensus mechanism for vehicular cloud computing and edge computing.
paper[10]	2018	Proposing a secure data storage and sharing scheme in a vehicular edge computing network using a consortium blockchain and smart contracts.
paper[8]	2020	Utilizing the computational resources of parked vehicles for vehicular edge computing and introduce blockchain technology to address security issues in practical applications.

The combination of vehicular edge computing and blockchain ensures data security during offloading tasks, leveraging reinforcement learning, particularly deep reinforcement learning, to obtain optimal offloading strategies. Once the optimal strategy is determined, data transmission takes place using blockchain technology to preserve data privacy and security.

Building upon this concept, Dai et al. proposed a blockchain-driven distributed secure content forwarding and storage framework. This framework utilizes a deep reinforcement learning algorithm based on DDPG to obtain the optimal allocation scheme. It employs an encrypted blockchain for content storage and forwarding, with a custom consensus mechanism called Proof of Utility (PoU) designed specifically for their scheme. The PoU mechanism achieves consensus on blocks based on the different utilities possessed by nodes executing offloading tasks [3]. In addition to custom consensus mechanisms, traditional consensus mechanisms can also be employed. Ren et al. developed a blockchain system using the PBFT consensus mechanism for offloading and migration of vehicular edge computing services. SDN technology is utilized to partition and manage the vehicular edge computing network, and a deep reinforcement learning algorithm based on A3C is incorporated to obtain an optimal offloading strategy for secure and efficient task offloading and migration [30]. Liu et al. proposed a secure blockchain system based on the Proof of Work (PoW) consensus mechanism for vehicular cloud computing and edge computing. Inspired by blockchain-based virtual currencies, their system introduces data coins and energy coins obtained based on data contribution frequency and energy contribution, respectively, to implement PoW and acquire tokens. Experimental results

support the secure realization of vehicular cloud computing and edge computing, demonstrating the effectiveness of their approach [18].

Incorporating smart contracts into vehicular edge computing systems is an essential aspect of leveraging the full potential of blockchain technology. Smart contracts are event-driven, stateful code and algorithm contracts [48]. The following section introduces a vehicular edge computing system that incorporates smart contracts. Kang et al. proposed a secure data storage and sharing scheme in a vehicular edge computing network using a consortium blockchain and smart contracts [10]. This scheme utilizes a consortium blockchain to establish a distributed system for secure management of vehicular data. Smart contracts are employed to achieve secure and efficient data storage and sharing. The Three-weight Subjective Logic (TWSL) model is adopted to select more reliable data sources and enhance data trustworthiness. Huang et al. utilize the computational resources of parked vehicles for vehicular edge computing and introduce blockchain technology to address security issues in practical applications [8]. They establish a distributed vehicular edge computing network using blockchain technology. This network utilizes smart contracts to automate upload tasks, return results, and verify the tasks and results. To obtain the optimal contract, this approach employs a reinforcement learning algorithm based on the Stackelberg game. Security analysis and experimental results demonstrate that the algorithm provides high security and efficiency guarantees.

4 Offload Optimization Scheme Combined with Federated Learning

Federated learning is a distributed machine learning approach introduced by Google in 2016 to address the issue of updating models on Android mobile devices locally. It has gained widespread adoption in the field of artificial intelligence research and effectively tackles the problem of "data silos." Data silos refer to the isolation of data owned by different entities due to privacy and confidentiality concerns, resulting in a lack of data sharing [11]. In the context of federated learning, participating users retain their data locally, eliminating the need to upload it to cloud or edge servers during training. Only the locally trained model parameters are uploaded, forming a shared aggregated model when combined with the parameters from other users [42]. These uploaded model parameters are continuously updated to achieve the training objective, breaking down data silos. Additionally, federated learning can be utilized in scenarios that require privacy protection, such as vehicular edge computing, to preserve privacy. By combining vehicular edge computing with federated learning, it becomes possible to establish a robust and privacy-preserving framework for secure vehicular edge computing. This approach allows for the retention of data locally on vehicles, ensuring privacy, while enabling collaborative model training. The general architecture of a vehicle edge federated learning system is illustrated in Fig 4. Many scholars have adopted methods based on federated learning to protect data privacy for vehicle edge computing such as [7,16,21]. Some literatures are

Table 3. The publication years and main contributions of federated learning based papers

Paper	Year of publication	Main contributions
paper[23]	2020	Proposing a blockchain-driven asynchronous federated learing scheme for secure data sharing in the vehicular Internet of Things.
paper[27]	2021	Proposing a differential privacy-based federated learning scheme for resilient vehicular networks.
paper[51]	2021	Employing federated learning in 6G-based vehicular network to achieve the aggregation of heterogeneous models.
paper[38]	2021	Proposing a vehicle selection and resource optimization scheme to select vehicles participate federated learning.
paper[41]	2020	Proposing a selective model aggregaation algorithm that focuses on a commonly employed task in vehicular networks which is image classification.

listed in detail below, and their publication years and main contributions are shown in the Table 3.

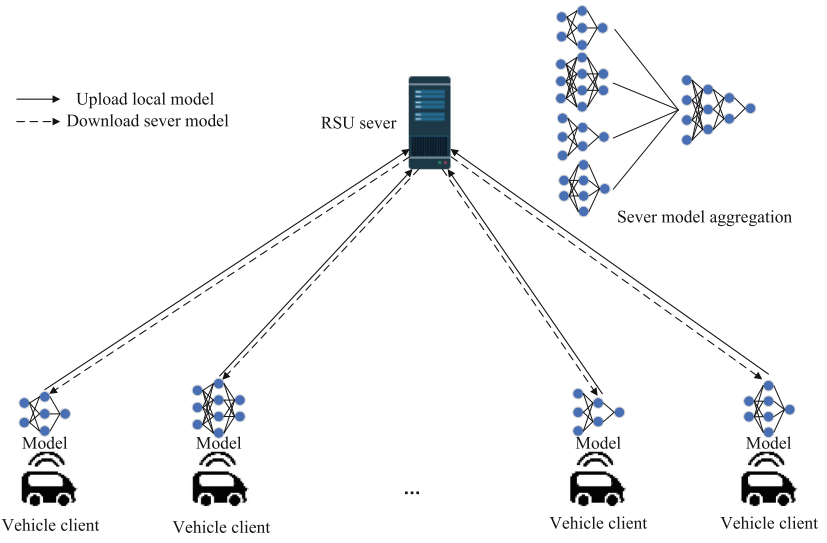

Fig. 4. General architecture of vehicle edge federated learning system

Lu et al. proposed a blockchain-driven asynchronous federated learning scheme for secure data sharing in the vehicular Internet of Things [23]. This scheme utilizes a blockchain system, consisting of a confidential privacy blockchain and a local Directed Acyclic Graph (DAG), to enhance the security and reliability of model parameters. The scheme employs a reinforcement learning algorithm based on the actor-critic network to select efficient nodes for estab-

lishing an asynchronous federated learning model. Experimental results demonstrate that the scheme achieves high learning accuracy and convergence speed. In addition to integrating with blockchain systems, federated learning algorithms can be combined with other privacy protection methods, such as differential privacy, to further enhance security and privacy. Olowononi et al. proposed a differential privacy-based federated learning scheme for resilient vehicular networks [27]. This scheme combines federated learning and differential privacy to enhance the resilience and attack resistance of vehicular networks. Experimental results show that the scheme improves the resilience, i.e., the ability to withstand attacks, of vehicular networks.

Federated learning, as an emerging technology, finds applications not only in traditional vehicular edge computing environments but also in vehicular edge computing networks based on future wireless communication environments, such as 6G networks. Zhou et al. employed federated learning in 6G-based vehicular networks to achieve the aggregation of heterogeneous models [51]. They designed a novel two-layer federated learning architecture specifically tailored for 6G vehicular networks. This architecture aims to improve learning accuracy while preserving privacy. The authors also developed a multi-layer model selection and aggregation method, effectively utilizing both local and global contextual information to enhance data utilization. Consequently, the learning time for intelligent object detection in vehicular networks is reduced, leading to improved system efficiency.

Federated learning algorithms for vehicular networks face challenges such as energy consumption and time constraints, as vehicles need to utilize their own energy for training, model uploading, and aggregation. Additionally, the varying data quality among vehicles impacts model training and aggregation in federated learning. To tackle these challenges, Xiao et al. proposed a vehicle selection and resource optimization scheme [38]. The scheme takes into account the position and speed of vehicles and formulates a minimum-maximum optimization problem that jointly optimizes computing capacity, transmission power, and local model accuracy, with the goal of minimizing the cost of federated learning. The scheme begins by employing a greedy algorithm to dynamically select vehicles with the highest data quality to participate in federated learning. Subsequently, it decomposes the joint optimization problem into resource allocation and local model accuracy sub-problems. The Lagrange dual problem and gradient projection iterations are used to approximate the optimal values. For solving the local model accuracy problem, a heuristic search algorithm is employed. Simulation results demonstrate that the proposed scheme outperforms other algorithms in terms of balancing learning time and energy consumption, highlighting its effectiveness in addressing the challenges of federated learning in vehicular networks.

To improve the quality of federated learning models, selecting high-quality models for aggregation after local training is a viable approach. Ye et al. proposed a selective model aggregation algorithm that focuses on image classification, a commonly employed task in vehicular networks [41]. The algorithm starts by selecting the "optimal" models for uploading, considering both local image qual-

ity and computing capacity. Given the information asymmetry between vehicles and the server, where local data is not uploaded, the algorithm formulates the problem as a two-dimensional contract theory problem. This problem is sequentially solved through relaxation and simplification, employing a greedy algorithm. To evaluate image quality, the algorithm establishes a geometric model that assesses the motion blur level of images, enabling implicit prediction of image quality based on the vehicle's instantaneous speed. Finally, the algorithm constructs a model aggregation scheme based on the FedAvg federated learning algorithm. The proposed algorithm is tested on standard datasets, including MNIST and BelgiumTSC. The results demonstrate that the model aggregation algorithm achieves higher performance, showcasing its effectiveness in improving the quality of federated learning models.

5 Future Research Directions

With the widespread adoption of new communication technologies, such as 5G, vehicular edge computing and its security remain active areas of research. In the domains of task offloading and resource allocation, alongside traditional reinforcement learning algorithms, improved algorithms like multi-agent reinforcement learning can be utilized. These algorithms involve multiple agents distributed throughout the network, facilitating better integration with blockchain and federated learning technologies for distributed offloading decisions. While reinforcement learning algorithms ensure the efficiency of computation offloading and resource allocation, offloading methods based on reinforcement learning often suffer from high computational complexity, requiring substantial training time to attain an optimal solution. Thus, a crucial research direction for the future is the design of low-complexity offloading algorithms that meet efficiency requirements.

To address the issue of extended response times in existing blockchain systems, it is crucial to focus on advancing blockchain systems that offer shorter response times, aligning with the task requirements of vehicular edge computing. This advancement would enhance system efficiency while ensuring data security. In the context of blockchain, data security is commonly achieved through a public key encryption system, which involves the establishment of Public Key Infrastructure (PKI) and certificate authorities (CAs). However, this encryption method can introduce computational delays in vehicular edge computing. To reduce data transmission latency, one approach is to position the certificate authorities or registration authorities closer to the vehicles. This enables short-term registrations and improves the efficiency of offloaded computations. Additionally, leveraging smart contracts for certificate registration and issuance can enhance the resilience of the blockchain system against attacks. Therefore, there is significant research potential in designing a secure vehicular edge computing architecture that combines PKI and smart contracts, optimizing system security and efficiency.

In the context of vehicular edge computing, the strong heterogeneity of computational resources and data poses challenges for federated learning algorithms.

To address this, it is important to select federated learning algorithms that excel in handling heterogeneous data as privacy-preserving solutions. This choice enhances overall system efficiency and applicability to meet the requirements of vehicular edge computing data.

Currently, certain federated learning algorithms adopt equal aggregation of model parameters from each client during model aggregation, leading to unnecessary computational and communication overhead that can reduce accuracy and model quality. To mitigate this issue, client-centric model aggregation algorithms can be employed. These algorithms assess the utility of each client based on metrics like data quality and model parameter quality. During aggregation, corresponding model aggregation coefficients are assigned based on the varying utility values of clients. This approach significantly improves the efficiency and accuracy of the algorithm when dealing with heterogeneous data. Therefore, in the integration of federated learning algorithms and vehicular edge computing, it is essential to flexibly design various algorithms that cater to different requirements based on practical application scenarios.

In conclusion, as vehicular networks continue to gain popularity, research in the fields of data security and privacy protection remains highly relevant. These areas play a critical role in ensuring the stability and reliability of vehicular network applications in the long term. This paper presents potential future research directions in vehicle edge computing offloading, data security, and privacy protection. The aim is to offer insights and serve as a reference for future scholars conducting research in these domains.

6 Conclusion

This paper focuses on the challenges of offloading decision-making in vehicle edge computing, as well as data security and privacy protection. It begins by summarizing the design of optimal offloading decision-making and resource allocation algorithms using reinforcement learning, with a particular emphasis on deep reinforcement learning. Additionally, it highlights the data security and privacy challenges encountered in edge computing offloading. To mitigate these challenges, the paper provides an overview of data security and privacy protection approaches utilizing blockchain and federated learning methods. Through a review of relevant literature, it presents the current research landscape in this field, identifies existing issues, and outlines future research directions. Overall, the paper offers valuable insights for subsequent studies in this area.

References

1. Cui, L., et al.: A blockchain-based containerized edge computing platform for the internet of vehicles. IEEE Internet Things J. **8**(4), 2395–2408 (2020)
2. Dai, Y., Xu, D., Maharjan, S., Qiao, G., Zhang, Y.: Artificial intelligence empowered edge computing and caching for internet of vehicles. IEEE Wirel. Commun. **26**(3), 12–18 (2019)

3. Dai, Y., Xu, D., Zhang, K., Maharjan, S., Zhang, Y.: Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks. IEEE Trans. Veh. Technol. **69**(4), 4312–4324 (2020)
4. Feng, J., Liu, Z., Wu, C., Ji, Y.: Mobile edge computing for the internet of vehicles: offloading framework and job scheduling. IEEE Veh. Technol. Mag. **14**(1), 28–36 (2018)
5. Firdaus, M., Rahmadika, S., Rhee, K.H.: Decentralized trusted data sharing management on internet of vehicle edge computing (IoVEC) networks using consortium blockchain. Sensors **21**(7), 2410 (2021)
6. François-Lavet, V., Henderson, P., Islam, R., Bellemare, M.G., Pineau, J., et al.: An introduction to deep reinforcement learning. Found. Trends® Mach. Learn. **11**(3-4), 219–354 (2018)
7. Huang, X., Li, P., Yu, R., Wu, Y., Xie, K., Xie, S.: FedParking: a federated learning based parking space estimation with parked vehicle assisted edge computing. IEEE Trans. Veh. Technol. **70**(9), 9355–9368 (2021)
8. Huang, X., Ye, D., Yu, R., Shu, L.: Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design. IEEE/CAA J. Automatica Sinica **7**(2), 426–441 (2020)
9. Jiang, T., Fang, H., Wang, H.: Blockchain-based internet of vehicles: distributed network architecture and performance analysis. IEEE Internet Things J. **6**(3), 4640–4649 (2018)
10. Kang, J., et al.: Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet Things J. **6**(3), 4660–4670 (2018)
11. Kim, J., Ha, H., Chun, B.G., Yoon, S., Cha, S.K.: Collaborative analytics for data silos. In: 2016 IEEE 32nd International Conference on Data Engineering (ICDE), pp. 743–754. IEEE (2016)
12. Kong, X., et al.: Deep reinforcement learning-based energy-efficient edge computing for internet of vehicles. IEEE Trans. Industr. Inf. **18**(9), 6308–6316 (2022)
13. Kumar, S., Velliangiri, S., Karthikeyan, P., Kumari, S., Kumar, S., Khan, M.K.: A survey on the blockchain techniques for the internet of vehicles security. Trans. Emerg. Telecommun. Technol. **35**(4), e4317 (2021)
14. Lang, P., Tian, D., Duan, X., Zhou, J., Sheng, Z., Leung, V.C.: Cooperative computation offloading in blockchain-based vehicular edge computing networks. IEEE Trans. Intell. Veh. **7**(3), 783–798 (2022)
15. Lee, S.S., Lee, S.: Resource allocation for vehicular fog computing using reinforcement learning combined with heuristic information. IEEE Internet Things J. **7**(10), 10450–10464 (2020)
16. Li, C., Zhang, Y., Luo, Y.: A federated learning-based edge caching approach for mobile edge computing-enabled intelligent connected vehicles. IEEE Trans. Intell. Transp. Syst. **24**(3), 3360–3369 (2022)
17. Li, T., Sahu, A.K., Talwalkar, A., Smith, V.: Federated learning: challenges, methods, and future directions. IEEE Signal Process. Mag. **37**(3), 50–60 (2020)
18. Liu, H., Zhang, Y., Yang, T.: Blockchain-enabled security in electric vehicles cloud and edge computing. IEEE Network **32**(3), 78–83 (2018)
19. Liu, L., Chen, C., Pei, Q., Maharjan, S., Zhang, Y.: Vehicular edge computing and networking: a survey. Mob. Netw. Appl. **26**, 1145–1168 (2021)
20. Liu, S., Liu, L., Tang, J., Yu, B., Wang, Y., Shi, W.: Edge computing for autonomous driving: opportunities and challenges. Proc. IEEE **107**(8), 1697–1716 (2019)

21. Liu, S., Yu, J., Deng, X., Wan, S.: FedCPF: an efficient-communication federated learning approach for vehicular edge computing in 6G communication networks. IEEE Trans. Intell. Transp. Syst. **23**(2), 1616–1629 (2021)
22. Liu, Y., Yu, H., Xie, S., Zhang, Y.: Deep reinforcement learning for offloading and resource allocation in vehicle edge computing and networks. IEEE Trans. Veh. Technol. **68**(11), 11158–11168 (2019)
23. Lu, Y., Huang, X., Zhang, K., Maharjan, S., Zhang, Y.: Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Trans. Veh. Technol. **69**(4), 4298–4311 (2020)
24. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Decentralized business review (2008)
25. Ning, Z., Dong, P., Wang, X., Rodrigues, J.J., Xia, F.: Deep reinforcement learning for vehicular edge computing: an intelligent offloading system. ACM Trans. Intell. Syst. Technol. (TIST) **10**(6), 1–24 (2019)
26. Ning, Z., et al.: Joint computing and caching in 5G-envisioned internet of vehicles: a deep reinforcement learning-based traffic control system. IEEE Trans. Intell. Transp. Syst. **22**(8), 5201–5212 (2020)
27. Olowononi, F.O., Rawat, D.B., Liu, C.: Federated learning with differential privacy for resilient vehicular cyber physical systems. In: 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), pp. 1–5. IEEE (2021)
28. Qi, Q., Ma, Z.: Vehicular edge computing via deep reinforcement learning. arXiv preprint arXiv:1901.04290 (2018)
29. Raza, S., Wang, S., Ahmed, M., Anwar, M.R., et al.: A survey on vehicular edge computing: architecture, applications, technical issues, and future directions. Wirel. Commun. Mob. Comput. **2019**(1), 3159762 (2019)
30. Ren, Y., Chen, X., Guo, S., Guo, S., Xiong, A.: Blockchain-based VEC network trust management: a DRL algorithm for vehicular service offloading and migration. IEEE Trans. Veh. Technol. **70**(8), 8148–8160 (2021)
31. Shaodong, H., Yingqun, C., Guihong, C., Yin, J., Wang, H., Cao, J.: Multi-step reinforcement learning-based offloading for vehicle edge computing. In: 2023 15th International Conference on Advanced Computational Intelligence (ICACI), pp. 1–8. IEEE (2023)
32. Shi, J., Du, J., Wang, J., Wang, J., Yuan, J.: Priority-aware task offloading in vehicular fog computing based on deep reinforcement learning. IEEE Trans. Veh. Technol. **69**(12), 16067–16081 (2020)
33. Singh, M., Kim, S.: Blockchain based intelligent vehicle data sharing framework. arXiv preprint arXiv:1708.09721 (2017)
34. Sun, Y., et al.: Adaptive learning-based task offloading for vehicular edge computing systems. IEEE Trans. Veh. Technol. **68**(4), 3061–3074 (2019)
35. Wang, K., Wang, X., Liu, X.: A high reliable computing offloading strategy using deep reinforcement learning for IoVs in edge computing. J. grid comput. **19**, 1–15 (2021)
36. Wang, S., Ye, D., Huang, X., Yu, R., Wang, Y., Zhang, Y.: Consortium blockchain for secure resource sharing in vehicular edge computing: a contract-based approach. IEEE Trans. Netw. Sci. Eng. **8**(2), 1189–1201 (2020)
37. Wu, Z., Yan, D.: Deep reinforcement learning-based computation offloading for 5G vehicle-aware multi-access edge computing network. China Commun. **18**(11), 26–41 (2021)
38. Xiao, H., Zhao, J., Pei, Q., Feng, J., Liu, L., Shi, W.: Vehicle selection and resource optimization for federated learning in vehicular edge computing. IEEE Trans. Intell. Transp. Syst. **23**(8), 11073–11087 (2021)

39. Xu, W., et al.: Internet of vehicles in big data era. IEEE/CAA J. Automatica Sinica **5**(1), 19–35 (2017)
40. Xu, X., et al.: Service offloading with deep q-network for digital twinning-empowered internet of vehicles in edge computing. IEEE Trans. Industr. Inf. **18**(2), 1414–1423 (2020)
41. Ye, D., Yu, R., Pan, M., Han, Z.: Federated learning in vehicular edge computing: a selective model aggregation approach. IEEE Access **8**, 23920–23935 (2020)
42. Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., Gao, Y.: A survey on federated learning. Knowl.-Based Syst. **216**, 106775 (2021)
43. Zhang, D., Cao, L., Zhu, H., Zhang, T., Du, J., Jiang, K.: Task offloading method of edge computing in internet of vehicles based on deep reinforcement learning. Clust. Comput. **25**(2), 1175–1187 (2022). https://doi.org/10.1007/s10586-021-03532-9
44. Zhang, K., Cao, J., Zhang, Y.: Adaptive digital twin and multiagent deep reinforcement learning for vehicular edge computing and networks. IEEE Trans. Industr. Inf. **18**(2), 1405–1413 (2021)
45. Zhang, L., Zhou, W., Xia, J., Gao, C., Zhu, F., Fan, C., Ou, J.: DQN-based mobile edge computing for smart internet of vehicle. EURASIP J. Adv. Signal Process. **2022**(1), 1–16 (2022)
46. Zhang, X., Li, R., Cui, B.: A security architecture of vanet based on blockchain and mobile edge computing. In: 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), pp. 258–259. IEEE (2018)
47. Zhang, X., Chen, X.: Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network. Ieee Access **7**, 58241–58254 (2019)
48. Zheng, Z., et al.: An overview on smart contracts: challenges, advances and platforms. Futur. Gener. Comput. Syst. **105**, 475–491 (2020)
49. Zheng, Z., Xie, S., Dai, H.N., Chen, X., Wang, H.: Blockchain challenges and opportunities: a survey. Int. J. Web Grid Serv. **14**(4), 352–375 (2018)
50. Zhou, H., Xu, W., Chen, J., Wang, W.: Evolutionary V2X technologies toward the internet of vehicles: challenges and opportunities. Proc. IEEE **108**(2), 308–323 (2020)
51. Zhou, X., Liang, W., She, J., Yan, Z., Kevin, I., Wang, K.: Two-layer federated learning with heterogeneous model aggregation for 6g supported internet of vehicles. IEEE Trans. Veh. Technol. **70**(6), 5308–5317 (2021)