Computers and Electrical Engineering 120 (2024) 109812

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

The role of mobile edge computing in advancing federated learning algorithms and techniques: A systematic review of applications, challenges, and future directions

Amir Masoud Rahmani [a], Shtwai Alsubai [b], Abed Alanazi [b], Abdullah Alqahtani [b], Monji Mohamed Zaidi [c,d], Mehdi Hosseinzadeh [e,f,g,*]

[a] Future Technology Research Center, National Yunlin University of Science and Technology, Yunlin, Taiwan
[b] Department of Computer Science, College of Computer Engineering and Sciences in Al-Kharj, Prince Sattam bin Abdulaziz University, P.O. Box 151, Al-Kharj 11942, Saudi Arabia
[c] Department of Electrical Engineering, College of Engineering, King Khalid University, Abha, 61421, Saudi Arabia
[d] Center for Engineering and Technology Innovations, King Khalid University, Abha 61421, Saudi Arabia
[e] School of Computer Science, Duy Tan University, Da Nang, Vietnam
[f] Center of Excellence in Genomics and Precision Dentistry, Department of Physiology, Faculty of Dentistry, Chulalongkorn University, Bangkok 10330, Thailand
[g] Jadara University Research Center, Jadara University, Irbid, Jordan

ARTICLE INFO

Keywords:
Mobile Edge Computing
Federated Learning
Privacy-Preserving Algorithms
Resource Allocation
Data Offloading

ABSTRACT

Mobile Edge Computing (MEC) and Federated Learning (FL) have recently attracted considerable interest for their potential applications across diverse domains. MEC is an architecture for distributed computing that utilizes computational capabilities near the network edge, enabling quicker data processing and minimizing latency. In contrast, FL is a method in the field of Machine learning (ML) that allows for the simultaneous involvement of multiple participants to collectively train models without revealing their raw data, effectively tackling concerns related to security and privacy. This systematic review explores the core principles, architectures, and applications of FL within MEC and vice versa, providing a comprehensive analysis of these technologies. The study emphasizes FL and MEC's unique characteristics, advantages, and drawbacks, highlighting their attributes and limitations. The study explores the complex architectures of both technologies, showcasing the cutting-edge methods and tools employed for their implementation. Aside from examining the foundational principles, the review explores the depths of the internal mechanisms of FL and MEC, offering a valuable in-depth of their architecture understanding and the fundamental principles and processes that facilitate their operation. At last, the concluding remarks and future research directions are provided.

1. Introduction

The rapid proliferation of the Internet of Things (IoT), as well as interconnected devices, has led to a substantial increase in data

* Corresponding author.
E-mail addresses: rahmania@yuntech.edu.tw (A.M. Rahmani), sa.alsubai@psau.edu.sa (S. Alsubai), ad.alanazi@psau.edu.sa (A. Alanazi), aq.alqahtani@psau.edu.sa (A. Alqahtani), amzaydi@kku.edu.sa (M.M. Zaidi), mehdihosseinzadeh@duytan.edu.vn (M. Hosseinzadeh).

https://doi.org/10.1016/j.compeleceng.2024.109812
Received 7 April 2024; Received in revised form 25 September 2024; Accepted 20 October 2024

generation, presenting new challenges in processing and data management [1,2]. The data generated by these devices frequently need more organization, completeness, and cohesiveness, posing difficulties in extracting valuable insights [3]. Furthermore, gathering sensitive and personal data has generated considerable concerns in terms of security and privacy concerns [4]. Although cloud computing has been extensively utilized for managing considerable amounts of data, the suitability of IoT devices can be improved because of the enormous amount of data that has been generated and the demand for the processing which is real-time [5,6]. The typical method of cloud computing involves sending all data produced by IoT devices to a central server for processing [7,8]. Nevertheless, this approach poses two notable challenges. Primarily, it requires a considerable amount of the available network capacity for data transmission, leading to increased expenses and decreased processing speeds [9]. Moreover, the data transmission to a managed server raises concerns in terms of security and privacy concerns since the network is transferring confidential data [10].

MEC is one of the solutions to these issues. By conducting data processing and computations at the network edge near the data source, MEC presents a distributed computing model as an alternative to allocating it to a managed data center. As a result, MEC enables local data processing and minimize network latency [11]. By bringing computing resources closer to the edge of the network, MEC enables real-time data processing and analysis, improving the performance of mobile applications and reducing the amount of data that needs to be transmitted over the network [12]. This can help to reduce network congestion and improve overall network efficiency, enabling operators to deliver high-quality services to their customers. MECs find applications in diverse industries, showcasing their versatility across various use cases [13]. For instance, MECs can enhance factory operations in the manufacturing sector by detecting and monitoring machine performance malfunctions and forecasting maintenance requirements [14,15]. In healthcare, MEC can track and analyze medical imagery and patient vital signs and deliver immediate feedback to healthcare practitioners [16]. In the transportation sector, MEC can be utilized to optimize traffic flow, mitigate accidents, and enhance vehicle safety [17].

FL is a methodology in ML that enables multiple devices to collaborate and learn together without sharing raw data [18,19]. For the first time, Google Company introduced FL in 2016 to enable users to update their models while keeping their data private. FL is also important for IoT devices and MEC users because sensitive data be transmitted over wireless networks [20,21]. By allowing devices to obtain knowledge from the data of other devices without the need for data transmission to a managed central server, FL ensures the preservation of security and privacy [22].

Considering the potential capabilities of the MEC in distributed computing, recently MECs have been widely used for implementing FL. By providing real-time data processing and analysis, MECs enable the development of new types of applications and services that are based on FL [23]. Nevertheless, realizing these objectives presents considerable difficulties, including ensuring the security and privacy of user data and managing the intricacies of distributed computing architectures [21]. To address these challenges, researchers and industry experts explore new approaches and introduce solutions for conducting FL using MEC. Fig. 1 depicts the cohesive architecture of FL integrated with MEC. This illustration emphasizes the role of localized data processing and model training directly at the network edge, which are crucial for enhancing data privacy and minimizing communication delays. By executing data processing tasks closer to the data source, this integration significantly improves response times and operational efficiency. Such architectural synergy is advantageous in edge computing environments where speed and privacy are paramount.

To the best of our knowledge, there are significant gaps in the literature regarding the recent studies [24-28], such as the comprehensive evaluation of privacy-preserving techniques in FL systems, the integration between different FL and MEC architectures, and the real-world scalability of these technologies across diverse networks and devices. Additionally, there is a lack of in-depth

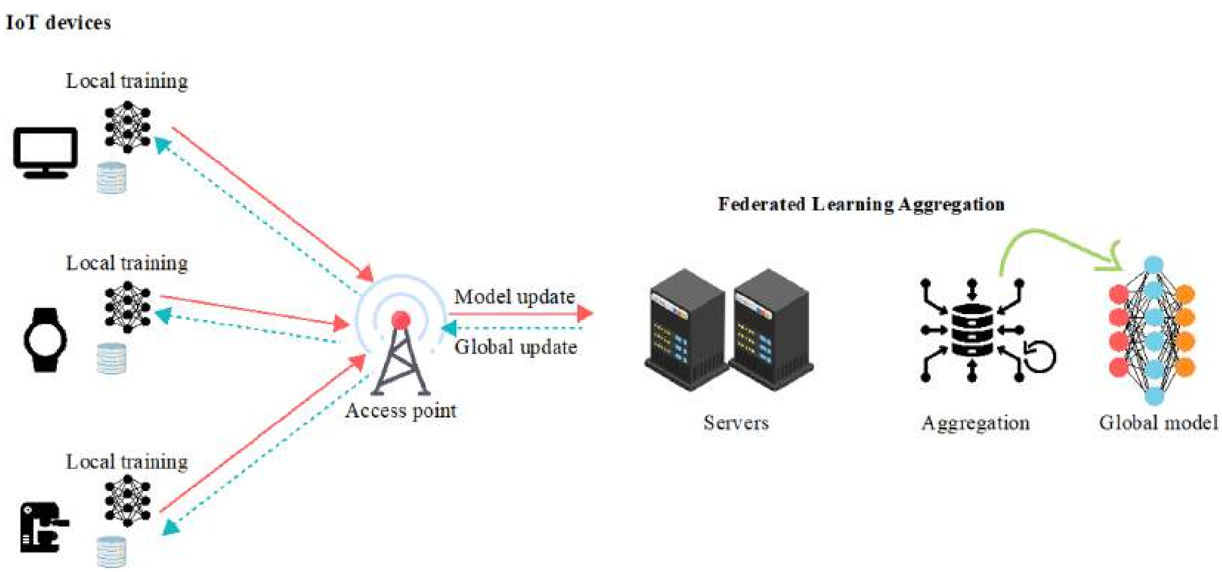

Fig. 1. Architecture combining FL and MEC to enhance privacy.

analysis on the impact of edge device variability on overall system performance and the development of adaptive algorithms that can dynamically adjust to changing network conditions and data distributions. Our research addresses these gaps by exploring optimized resource allocation methods to enhance computational efficiency across diverse IoT environments, examining the impact of various data offloading strategies on device performance and energy efficiency, and evaluating how scheduling and load balancing improve FL system efficacy and reliability. We also assess different architectural configurations for optimal performance, scalability, and security, analyze the effects of simulation tools on model validation and reproducibility, and propose the need for new benchmark datasets and evaluation metrics to assess FL frameworks accurately. These explorations aim to advance FL and MEC integration, filling crucial research voids and supporting the development of robust, efficient, distributed computing environments.

1.1. Scope of the study

This paper reviews and classifies the MEC-based FL schemes proposed in the recent literature. We aim to provide a comprehensive overview of these two emerging technologies' potential benefits and challenges, thereby informing future research in this dynamic field. We adhere to a specific methodology to ensure the systematic and transparent selection and analysis of the research articles. The paper meticulously classifies the studied MEC-based FL schemes based on their utilized algorithms, architecture, and the services they provide. A detailed comparison of their capabilities is also presented, focusing on the employed algorithms, datasets, evaluation factors, simulation tools, environments, and the contexts in which they are operational.

1.2. Motivation of the study

The motivation behind this study originates from the growing significance of FL in enhancing the capabilities of distributed computing through MEC environments. This combination is increasingly acknowledged as a transformative method that can revolutionize various fields by facilitating the creation of intelligent systems. Moreover, the paper highlights the key findings and main contributions of recent studies in the field, providing a background that is particularly beneficial for novice researchers in Federated Learning. By elucidating the promising nature of FL on MEC, this study aims to spur further research and development, addressing the open issues and challenges that remain. The conclusion summarizes the main contributions and outlines the potential directions for future work in enhancing and expanding the capabilities of MEC-based FL schemes. The main contributions of this research are as follows:

- This research thoroughly examines FL operational methods within MEC environments, highlighting the current state of the art and identifying critical areas for improvement.
- It introduces recent schemes for optimizing FL in MEC settings, focusing on enhancing performance and reliability, which are crucial for deploying FL in real-world scenarios.
- The study introduces frameworks for FL approaches in MEC environments and vice versa, incorporating a wide range of parameters and metrics to assess performance and efficiency comprehensively.
- It offers valuable insights into the architecture of FL-based schemes, providing a detailed analysis of how different architectures and environments influence the effectiveness of FL-MEC implementations.
- This research reviews simulation frameworks, platforms, and tools used in existing FL studies within the MEC environment. It also examines the datasets employed to evaluate FL schemes, contributing to a better understanding of FL's practical applications.
- The study identifies current research gaps and outlines future directions for FL in MEC and vice versa, including potential areas for improvement, novel applications, and emerging challenges, laying the groundwork for future advancements in the field.

The rest of this article is organized as follows: Section 2 outlines the review methodology employed in this study. Section 3 provides an essential background on FL and MEC, which is crucial for a deeper understanding of these technologies. Section 4 introduces a taxonomy of the proposed FL schemes within MEC environments, offering an in-depth examination of these approaches. Section 5 delves into a discussion and comparison of the critical attributes of the FL schemes designed for MEC settings, and Section 6 highlights future research directions and unresolved challenges. The article concludes with Section 7, summarizing the main findings.

2. Research methodology

This section outlines the research methodology employed to conduct this study. At first, a specific procedure is employed to categorize and choose articles, which involves the following steps:

- We establish the research questions that this review article will answer.
- Based on these research questions and the study topic, we identify the relevant keywords.
- Using these keywords, the necessary search strings are constructed and searched in the proper scientific databases.
- The identified papers undergo screening, where inclusion and exclusion criteria are applied to determine the final selection.

2.1. Research questions

This study addresses critical questions related to the optimization of FL in MEC environments, focusing on enhancing performance, reliability, and architectural design. The questions we intend to explore include:

- How can resource allocation methods be optimized in FL systems within MEC to enhance computational efficiency and learning outcomes across diverse IoT environments?
- What are the effects of different data offloading strategies on IoT devices' performance and energy efficiency within FL and MEC frameworks?
- How do scheduling and load balancing contribute to the overall efficacy and reliability of FL deployments in MEC environments?
- What architectural configurations between 2-tier and 3-tier models offer the best performance, scalability, and security balance for FL implementations in MEC?
- How do the different simulation tools and environments impact the validation and reproducibility of FL models in MEC settings?
- What new benchmark datasets and evaluation metrics are required to more accurately assess the performance and robustness of FL frameworks in IoT and MEC applications?

2.2. Review process

To indicate the necessity of conducting this study, the related review articles on MEC-based FL schemes are searched:

- Edge Computing Federated Learning Survey
- Edge Computing Federated Learning Review
- Edge Computing Federated Learning Overview
- Mobile Edge Computing Federated Learning Survey
- Mobile Edge Computing Federated Learning Review
- Mobile Edge Computing Federated Learning Overview
- MEC Federated Learning Survey
- MEC Federated Learning Review
- MEC Federated Learning Overview

Table 1
Overview of related review articles on FL in MEC networks.

Ref	Publisher	Year	Study area	Limitations	The main purpose of the survey
[29]	IEEE	2021	Blockchain-enabled FL in MEC Networks.	This article does not cover many important articles that have been published.	This survey explores opportunities and challenges, this survey integrates FL and blockchain in MEC, aiming to enhance privacy, security, and decentralization while addressing communication costs, resource allocation, and incentive mechanisms.
[24]	MDPI	2021	FL implementation and challenges in Edge Computing.	This survey only reviews the articles published earlier than 2021.	Provide a study on implementing FL in EC environments, addressing challenges, solutions, and applications.
[25]	MDPI	2022	FL for EC with Limited Computational Resources.	Poor categorization of subjects and inadequate robust papers.	Surveying the methods of FL for EC, focusing on limited computational resources, addressing challenges, exploring application possibilities, and highlighting privacy and security concerns in the context of edge devices.
[30]	IEEE	2020	FL in Mobile Edge Networks is used to optimize mobile edge networks.	An inadequate number of newly presented papers.	To comprehensively survey and explore the use of FL in Mobile Edge Networks, addressing challenges such as communication costs, resource allocation, privacy, and security, and discussing applications and future research directions for FL in mobile edge network optimization.
[31]	IEEE	2022	Blockchain-enabled FL for UAV Edge Computing Networks.	The present investigation has not covered many of the key articles that have been published.	This survey explores the use of blockchain-enabled FL in UAV edge computing networks, focusing on issues and solutions related to privacy, trust, and performance improvement in intelligent UAV applications.
[32]	Elsevier	2023	Asynchronous FL with directed acyclic graph-based blockchain in edge computing.	Inadequate directions for future investigation and the unavailability of a systematic format to select the papers.	This survey explores the integration of Asynchronous FL and directed acyclic graph-based blockchain in edge computing. It discusses terminologies, system models, design factors, solutions, and future directions and evaluates its potential compared to blockchain-FL.

Some articles were found using these search terms. Table 1 compares surveys by publication year and study focus and identifies key limitations. It offers a detailed reference for understanding the research evolution in this field and highlights existing gaps our study addresses.

Also, for searching the new proposal in the MEC-based federated learning context, the following search terms are used:

- Edge Computing Federated Learning
- Mobile Edge Computing Federated Learning
- MEC Federated learning

Our review paper explores the integration of FL within MEC systems, addressing significant gaps in the existing literature. While previous studies have utilized AI to enhance MEC operations, they often lack a comprehensive discussion on the specific types of AI—such as ML, deep learning, and reinforcement learning—and their suitability for different MEC scenarios. Our research questions probe how AI-driven resource allocation, data offloading, and load balancing can optimize performance and energy efficiency across diverse IoT environments. We also scrutinize the effectiveness of different architectural configurations and simulation tools in improving FL implementation. This review highlights the novelty and recent contributions of AI in FL, including advancements in algorithms that ensure better data handling and decision-making accuracy. We address the limitations of current methodologies, such as the convergence and stability of AI models, and provide a thorough impact assessment and cost-benefit analysis. Our discussion extends to the fairness of the AI-driven decisions and the transparency of the methods used, filling a critical gap by providing a detailed categorization of AI strategies and evaluating their practical implications within FL and MEC frameworks. This approach clarifies AI's potential in enhancing MEC and underscores the need for robust, fair, and efficient AI solutions in managing complex network environments.

Fig. 2 showcases the various scientific databases utilized to compile relevant literature on MEC and FL. This figure highlights the extensive range of sources from well-known academic journals and conference proceedings hosted on platforms such as IEEE Xplore, ACM Digital Library, and ScienceDirect to ensure a thorough review. Initially, this search yielded a total of 1379 research articles, which were subsequently refined and filtered to include only relevant articles to our study. Our literature review primarily focused on the topics of FL, MEC, and edge computing, which served as our primary search terms. After eliminating duplicate records, 482 articles were excluded from further analysis. Subsequently, we assessed the remaining articles based on their titles and abstracts, determining that 620 publications did not meet the eligibility criteria set for our review. We considered all original research articles and conference papers, provided they were written in English. Among the remaining articles, 196 were eliminated due to their failure to meet our eligibility requirements, and 23 were rejected for other reasons. Consequently, following a meticulous application of our inclusion and exclusion criteria, we identified 58 articles for in-depth analysis. Fig. 3 outlines the systematic process from the initial retrieval of articles to their final selection. It demonstrates the comprehensive screening and evaluation methodologies employed to maintain the integrity and relevance of the literature included in our study. Table 2 details the specific inclusion and exclusion criteria to select the most relevant and high-quality articles for our systematic review. The articles were screened based on their source, title, and text. After

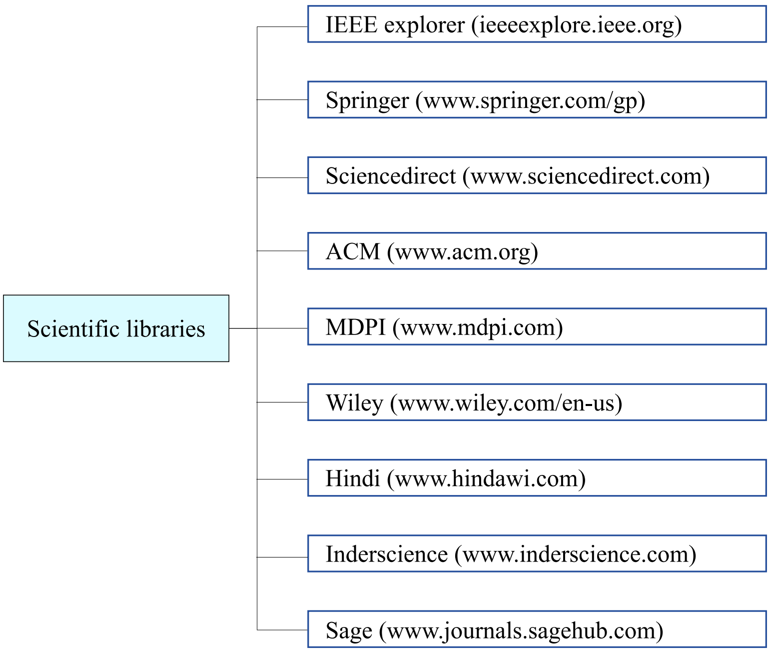

Fig. 2. Scientific libraries were utilized in the literature search.

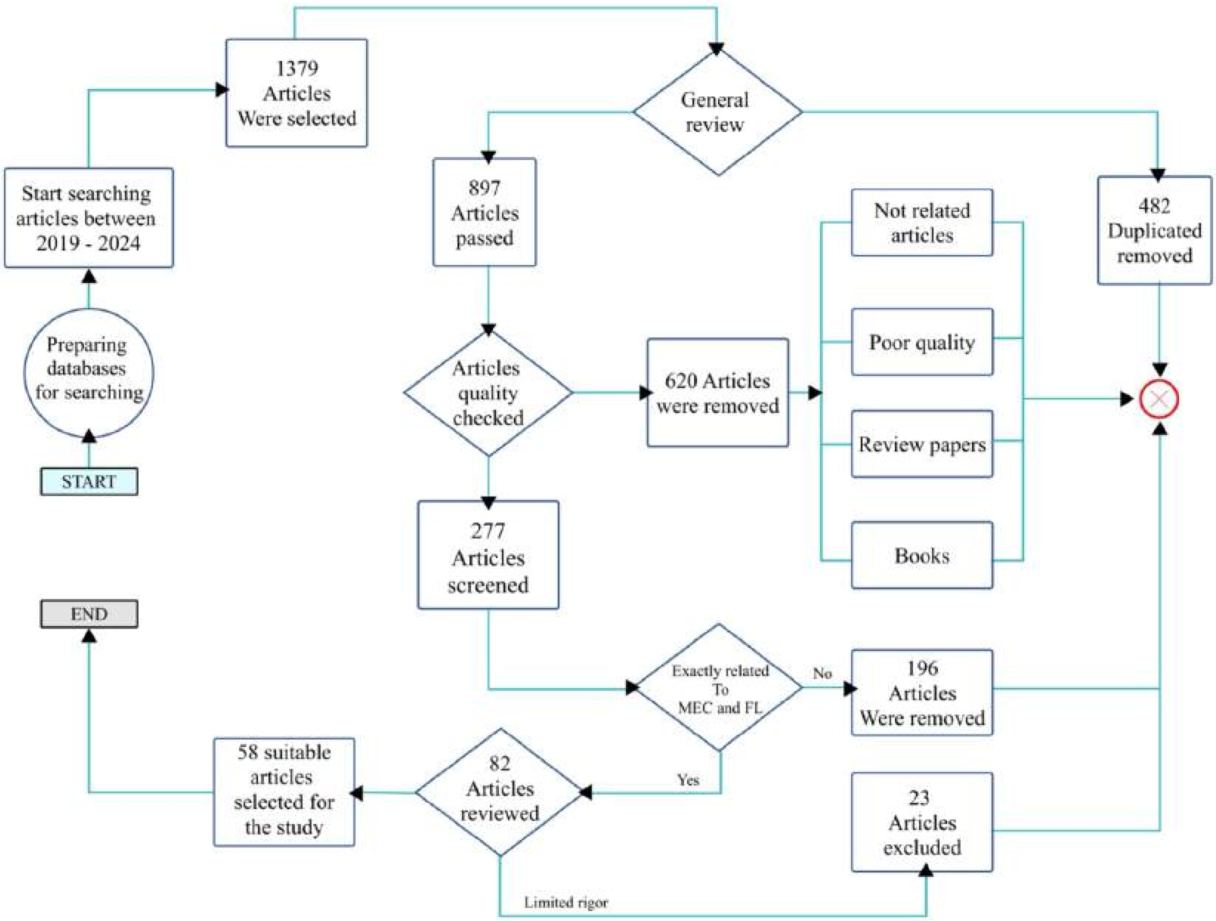

Fig. 3. The systematic review process.

Table 2
Criteria for including and excluding studies in this systematic review.

Inclusion criteria	Peer-reviewed and original research articles, as well as conference proceedings. Articles published between 2019 and 2023. Articles are written in English. Articles that discuss MEC and FL. Articles from the fields of computer science, engineering, and mathematics.
Exclusion criteria	Non-peer-reviewed articles. Articles not written in English. Poor quality articles. Case studies. Books and book chapters. Review papers that do not contain original research. Articles that do not discuss MEC and FL.

that, a scrutinizing selection process is conducted to pinpoint valid conference and journal papers. As shown in Fig. 4, this literature review focused on 2019 through 2024. Fig. 5 depicts the number of MEC-based FL schemes provided by each publisher.

3. Research background

This section provides essential background knowledge about the MEC and FL.

3.1. MEC

IoT and a range of interconnected devices facilitated by MEC have become essential components of our daily existence, allowing

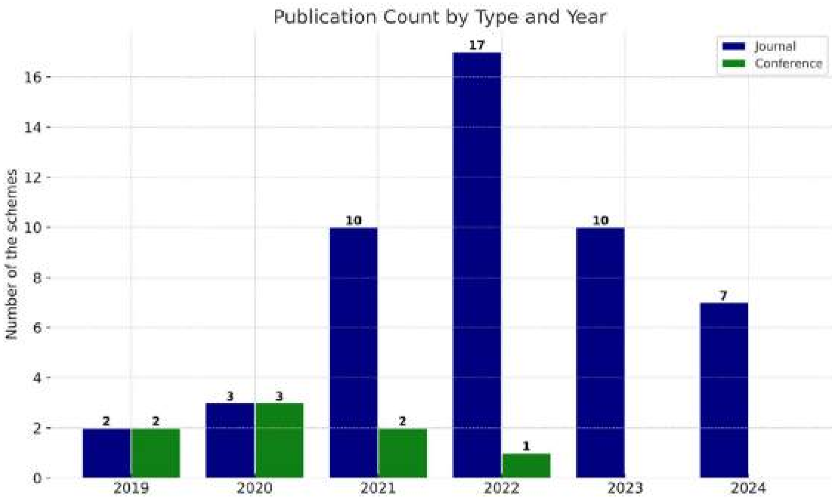

Fig. 4. Trends in the development of MEC-based FL schemes from 2019 to 2024.

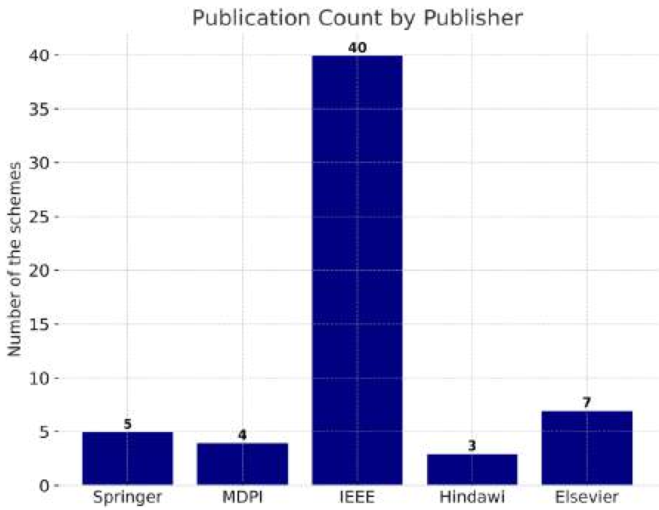

Fig. 5. Distribution of MEC-based FL schemes published by different scientific publishers.

continuous connectivity and access to information and services regardless of location or time [33]. However, MEC also poses several challenges, which can limit its usability and effectiveness in certain contexts [33]. This section will discuss some of the main challenges associated with MEC and explore possible solutions.

One of the primary challenges of MEC is limited bandwidth. Mobile devices typically have slower and less reliable network connections than desktop computers, which can limit their ability to access and transfer data quickly [34]. This can lead to slower loading times for websites and applications and can make it difficult to stream media or engage in real-time communication [35]. Furthermore, as more and more people rely on mobile devices for work and communication, network congestion can become a major issue, further limiting bandwidth availability [36].

Various approaches have been proposed to address this challenge, including the use of compression algorithms, caching, and content delivery networks. Compression algorithms can reduce the size of data being transmitted, thereby reducing the amount of bandwidth required [37]. Caching involves storing frequently accessed data on local devices or servers, allowing them to be accessed more quickly without requiring a network connection [38]. Content delivery networks involve distributing content across multiple servers, reducing the distance that data needs to travel, and improving the speed and reliability of access [39]. Another challenge is energy consumption. Mobile devices are typically powered by batteries, which have limited capacity and can quickly drain when devices are used heavily [40]. This can limit the usability of mobile devices, especially in contexts where charging is not readily available. Furthermore, the energy consumption of mobile devices can also have environmental impacts, as more energy is required to charge batteries and power devices [35].

Various approaches have been proposed to address this challenge, including power-saving modes, energy-efficient hardware and software, and wireless charging. Power-saving modes involve reducing the energy consumption of devices by turning off certain features or reducing their usage, such as by reducing screen brightness or disabling background applications [41]. Energy-efficient hardware and software involve using components and algorithms that are designed to minimize energy consumption, such as low-power processors or power management software [42]. Wireless charging involves using electromagnetic fields to transfer energy wirelessly, eliminating the need for physical connections and enabling charging on the go.

MEC also poses significant security challenges. Mobile devices are often used to access sensitive information, such as personal data and financial transactions, and are therefore vulnerable to a variety of security threats, including malware, phishing attacks, and device theft [43]. Furthermore, as mobile devices are used in various contexts, such as public Wi-Fi networks and shared workspaces, they are also vulnerable to interception and eavesdropping. Various security measures have been proposed to address these challenges, including encryption, biometric authentication, and remote device management. Encryption involves encoding data to prevent unauthorized access [44], while biometric authentication involves using physiological or behavioral characteristics, such as fingerprints or facial recognition, to verify the identity of users [33,45]. Remote device management involves using software to monitor and control devices from a central location, enabling administrators to enforce security policies and remotely wipe data in case of theft or loss [46]. Fig. 6 summarizes the major challenges associated with implementing MEC and highlights critical areas that require strategic attention.

In addition to addressing these operational challenges, a deeper examination of MEC architecture reveals its capacity for handling complex data operations at the edge tier. This involves complex data routing protocols, dynamic resource allocation mechanisms, and security features customized to edge operations. For instance, MEC can implement distributed ledger technologies to ensure transparent and secure data transactions between edge devices and central servers, enhancing trust and integrity within the network.

3.2. Federated ML

ML is a subfield of Artificial Intelligence (AI) that involves developing algorithms and models that can automatically learn and make predictions or decisions based on input data [47]. ML has become increasingly important in recent years, as it has enabled the development of intelligent systems in a variety of domains, including computer vision, natural language processing, and autonomous driving [48]. This method aims to enable computers to learn from data without being directly programmed. This is achieved by using algorithms that can identify patterns in data and use these patterns to make predictions or decisions [47]. Training an ML model requires providing it with a substantial dataset of examples, followed by adjusting its parameters to enhance its ability to accurately forecast results for new, previously unobserved data [49].

FL is a recent development in the field of ML that aims to enable the training of models on decentralized data without requiring data to be centralized in a single location. This is achieved by allowing multiple devices or nodes to collaboratively train an ML model while keeping their data private and secure [50]. The concept of FL is particularly relevant in the context of IoT, where there are large numbers of connected devices that generate vast amounts of data [51]. By enabling these devices to collaborate on training ML models, FL can enable the development of intelligent IoT systems that can make predictions and decisions in real-time [52,53]. FL offers several

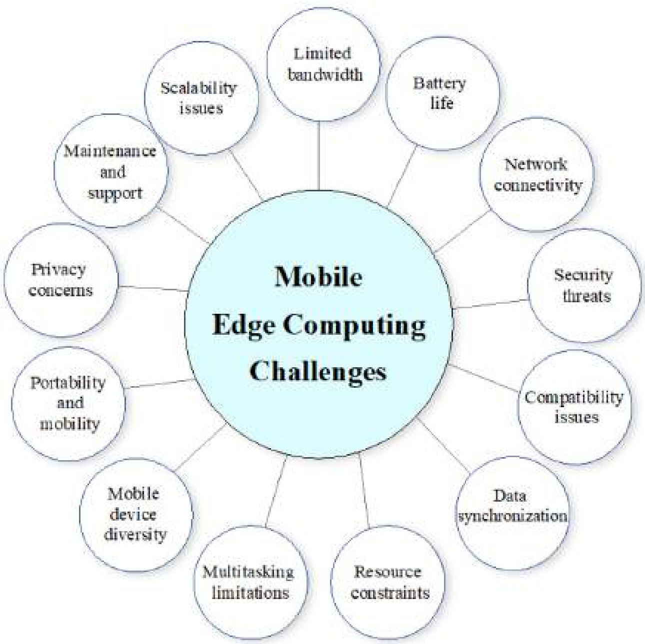

Fig. 6. Overview of key challenges in MEC.

advantages that address key concerns in the field of ML, particularly about data privacy, data security, decentralized learning, reduced data transmission, increased data diversity, collaborative learning, edge intelligence, personalization, resource efficiency, and model fairness [50].

Data privacy is a critical advantage of FL. Privacy-preserving algorithms, such as secure aggregation and differential privacy, allow participating devices to contribute their local data for model training without revealing sensitive information. Federated encryption methods enhance privacy by encrypting data during transmission and storage, ensuring only authorized entities can access the data. Data security is another important aspect of FL. Keeping data decentralized on local devices minimizes the risk of data breaches or unauthorized access. Secure model aggregation techniques enable the aggregation of model updates from multiple devices while preserving the confidentiality and integrity of the data. Decentralized learning in FL reduces communication costs by performing local model updates on participating devices. This eliminates the need to transmit large amounts of raw data to a central server, resulting in more efficient use of network resources. Distributed model training enables the training of models across multiple devices, leveraging the computational power of edge devices and creating a more scalable and collaborative learning environment. FL reduces data transmission by only transmitting model updates instead of raw data. Local model updates are sent to the central server, where they are aggregated to create a global model. This selective data-sharing approach minimizes bandwidth requirements and reduces the latency of transmitting large datasets. FL leverages the increased data diversity available across multiple devices. Diverse data sources contribute to a more comprehensive representation of the underlying population, leading to improved generalization and robustness of the global model. Collaborative learning is a fundamental principle of FL. Cross-device knowledge transfer allows devices to learn from each other's experiences, benefiting from the network's collective intelligence. Joint model training enables devices to collaboratively optimize the global model collaboratively, resulting in higher performance and accuracy. Model fairness is an essential consideration in FL. FL enables fairness-aware learning, where biases in the training data can be detected and corrected. By incorporating fairness metrics and bias detection techniques, FL facilitates the development of more equitable and unbiased models [54-59].

However, FL also poses several challenges. These challenges include communication overhead, heterogeneity of devices, non-IID data, data bias, model aggregation complexity, unbalanced data distribution, limited model expressivity, lack of transparency, model poisoning attacks, and legal and regulatory challenges. One of the primary disadvantages of FL is the communication overhead it introduces. With FL, devices must communicate with a central server or among themselves to exchange model updates and other information. This increased network traffic can lead to longer training times and higher resource utilization, particularly in scenarios with many participating devices. The diversity of devices in FL poses challenges. Different devices may have varying computational capabilities, storage capacities, and network connectivity. This heterogeneity can lead to model compatibility issues, where models trained on one device may not directly apply to others. Unequal computing resources among devices can also result in imbalanced contributions to the global model, impacting its overall performance. Non-IID (Independent and Identically Distributed) data is another challenge in FL. Due to the decentralized nature of FL, the data available on different devices may have different distributions. This mismatch in data distribution can lower model performance because the global model must generalize across these different data distributions. Ensuring representative data sampling and appropriate data preprocessing techniques are important to mitigate this disadvantage. Moreover, data bias is a concern in FL, particularly when devices have limited datasets or the data collection process introduces biases. Limited dataset sizes may not capture the full diversity of the underlying population, potentially leading to biased models. Additionally, biased dataset collection, such as unequal user participation or demographic biases, can further exacerbate biases in the resulting models. The complexity of model aggregation is a significant challenge in FL. Aggregating model updates from multiple devices while maintaining model accuracy and convergence can be computationally intensive. The communication and computational overhead required for model aggregation can limit the scalability and efficiency of FL systems. Unbalanced data distribution among devices can affect the overall performance of FL models. If some devices contribute significantly more or more diverse data than others, the resulting global model may be biased toward those devices. Strategies like weighted aggregation or data augmentation techniques can address this challenge and improve model accuracy. FL may have limitations in terms of model expressivity. Due to the need for efficient communication and resource utilization, the choice of model architectures in FL systems may be constrained. This limited model expressivity can impact the model's ability to capture complex relationships and may result in reduced performance compared to centralized models with more flexible architectures. The lack of transparency is another disadvantage of FL. The distributed nature of FL makes it challenging to interpret and debug models. Understanding the decision-making process of the global model and identifying potential issues or biases becomes more complex when the model training is distributed across multiple devices. FL is also vulnerable to model poisoning attacks, where malicious devices inject manipulated data to undermine the integrity or performance of the global model. Detecting and addressing these attacks requires robust security measures, including data validation and model verification techniques. Lastly, FL introduces legal and regulatory challenges. Data privacy and ownership become significant concerns as sensitive data remains on user devices rather than centrally stored. Compliance with regulations, such as data protection laws or industry-specific regulations, must be ensured when implementing FL systems. In the context of FL, different network topologies can be used to establish communication and coordination among the participating devices or nodes [60-66].

3.3. Potential benefits of MEC and FL

The integration of MEC and FL brings about numerous benefits, enhancing various aspects of data processing, network efficiency, application performance, privacy and security, energy consumption, scalability, distributed processing, and more. By leveraging the combined strengths of MEC and FL, organizations can unlock significant advantages for their operations and user experiences [67-70]. The integration of MEC and FL offers numerous benefits. It enables real-time data processing at the edge, leading to improved operational efficiency and agility. The combination reduces latency, resulting in faster response times and an enhanced user experience. Network efficiency is enhanced by localized processing and distributed model training, reducing congestion and optimizing resource allocation. Data transmission is minimized, saving costs and enhancing privacy. Edge computing enhances application performance and accelerates model inference. Privacy and security are enhanced by keeping sensitive data closer to the source and employing privacy-preserving algorithms. Energy consumption is reduced through localized processing and distributed computation. Scalability is achieved through flexible infrastructure and distributed learning. Distributed processing enables parallel processing and faster analysis. Local data storage improves access speed and facilitates offline operations. Edge caching reduces network congestion and enhances application performance. Context-aware computing personalizes services based on contextual information. Proximity-based services deliver location-based and localized services. The integration improves the user experience, allows dynamic resource allocation, and enhances operational efficiency.

Edge intelligence is a significant advantage of FL. By performing real-time decision-making on edge devices, FL enables faster inference and response times. On-device processing reduces the reliance on cloud resources and ensures that critical decisions can be made locally, even in disconnected environments. Personalization is enhanced through FL. User-specific model adaptation enables devices to personalize the global model based on individual preferences and data. This allows for customized services and tailored user experiences while maintaining privacy and data security. FL promotes resource efficiency by offloading computation to edge devices. Edge computing offloading reduces the load on the central server and leverages the capabilities of resource-constrained devices, optimizing resource usage and improving overall system efficiency. Fig. 7 depicts the advantages of utilizing FL within MEC systems, emphasizing improvements in data privacy and network efficiency. This integration significantly enhances real-time data processing capabilities while safeguarding user data against potential breaches.

Moreover, technically, FL within MEC environments capitalizes on the localized computational power by distributing model

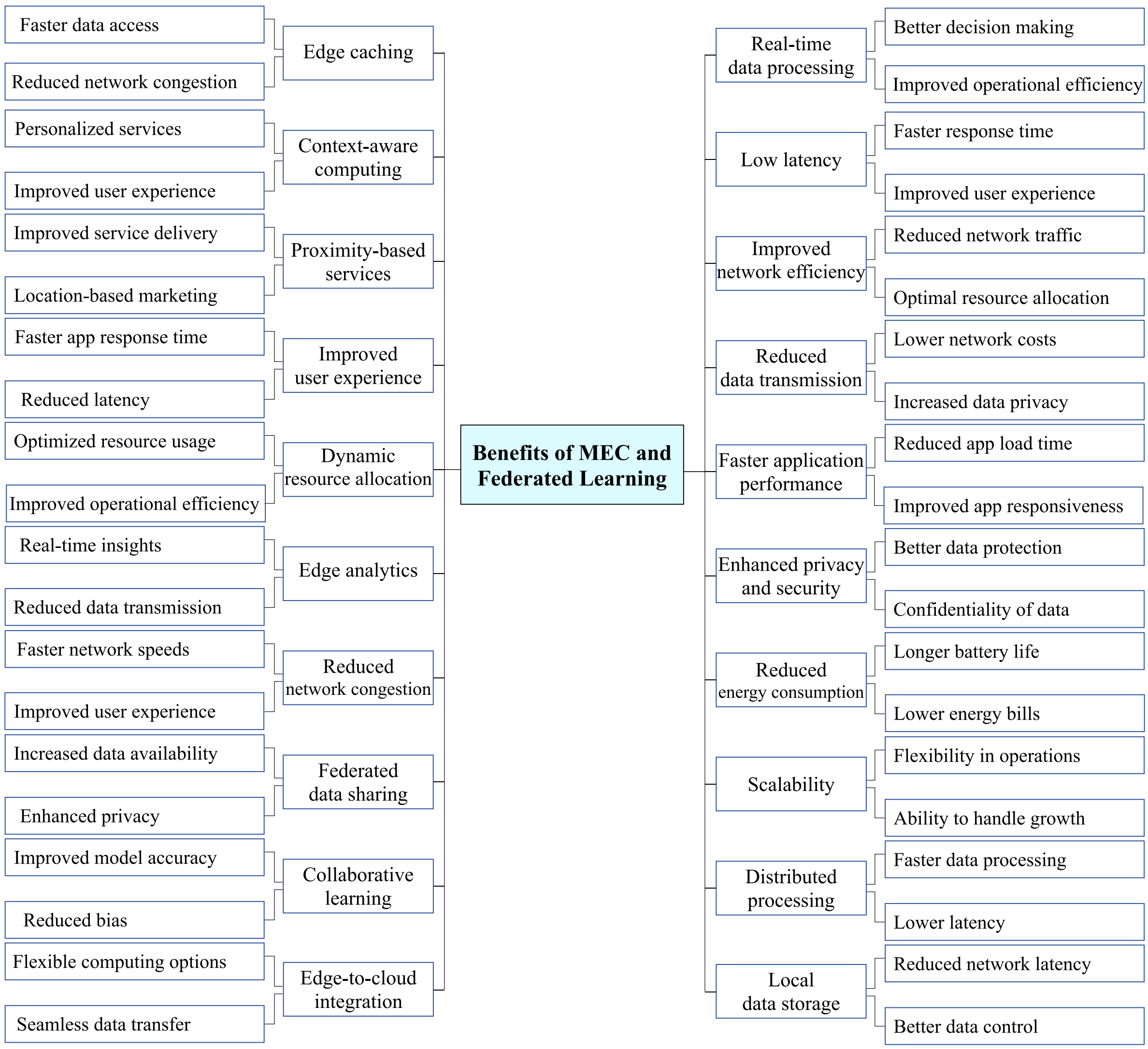

Fig. 7. Potential benefits of using FL with MEC.

training tasks across multiple edge nodes. This decentralized approach allows each node to process data locally, which significantly reduces the need to transmit large volumes of data over the network, thereby preserving bandwidth and enhancing privacy. However, the efficiency of FL in such setups heavily relies on the ability to maintain consistency and timeliness in model updates across all participating nodes.

To manage this, robust synchronization protocols are essential. These protocols ensure that updates from disparate nodes are aggregated in a coherent manner to update the global model. Techniques like clock synchronization and event-triggered updates can be utilized to maintain uniformity in the training process across all nodes. Additionally, advanced techniques such as edge-based model aggregation and gradient compression are crucial. Edge-based model aggregation allows intermediate model updates to be processed locally at edge servers before being combined into the global model, which reduces the load on the network and accelerates the training process.

Gradient compression further optimizes this setup by reducing the size of the model updates that need to be communicated between nodes and the central aggregator. This conserves bandwidth and speeds up the model's convergence by enabling more frequent updates under limited network capacity. Implementing these techniques in MEC environments enhances FL's scalability and responsiveness, making it more practical for real-time applications such as autonomous driving and IoT systems, where decision-making speed is critical. This strategic integration of FL and MEC leverages the strengths of both technologies to address the challenges of data security, network efficiency, and computational scalability.

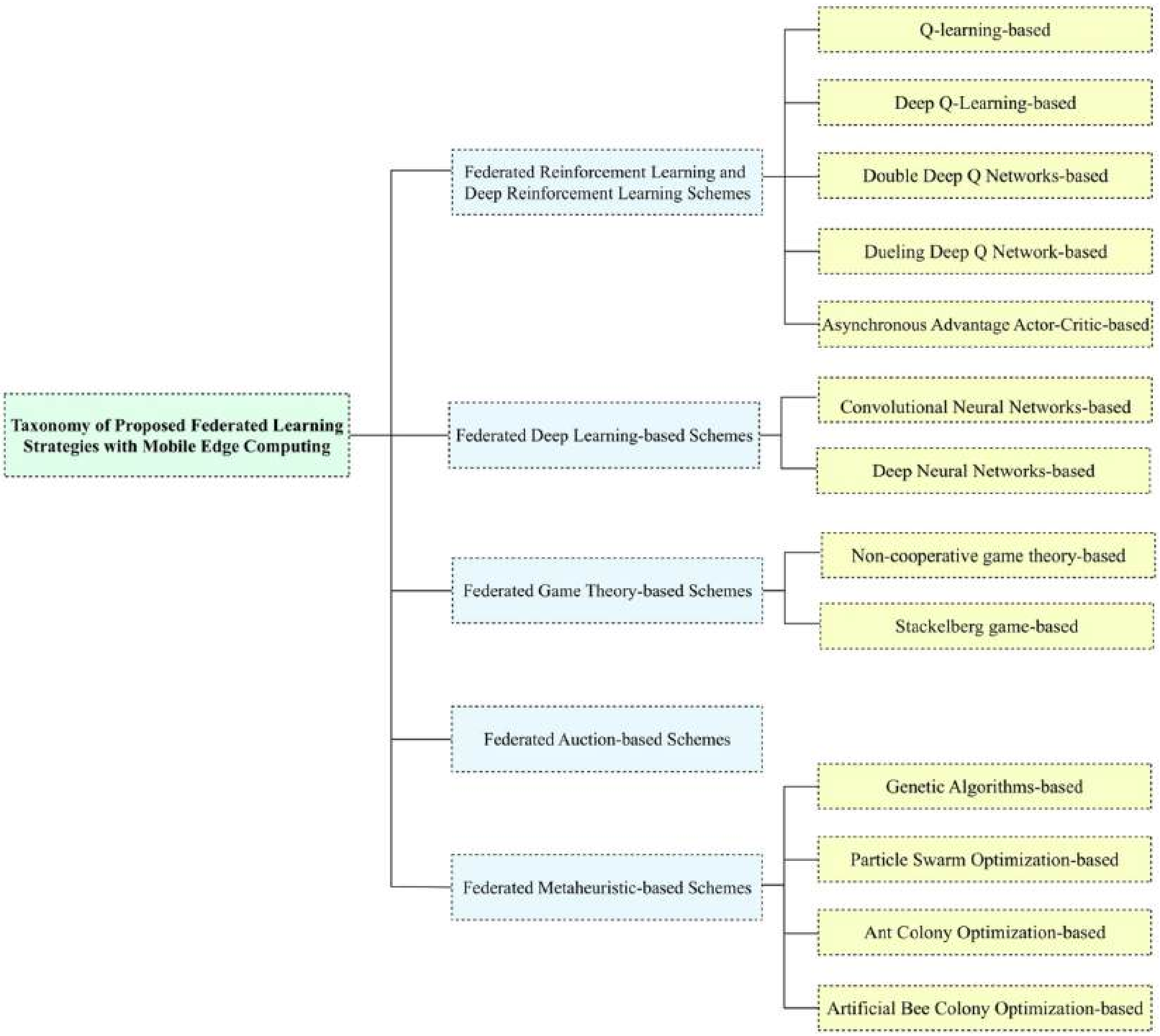

Fig. 8. Taxonomy of FL Strategies with MEC.

4. The proposed MEC-based FL schemes

This section explores the structure and detailed examination of various FL strategies devised for distinct MEC settings. Numerous FL frameworks, referenced as [71-98], have been customized for MEC environments, aiming either to enhance MEC capabilities or to optimize FL within MEC-specific multi-tiered infrastructures. The discourse centers on the architectural design of these proposed systems, highlighting that they predominantly adopt either a dual-tier setup, encompassing IoT devices paired with MEC resources, or a tri-tier framework that integrates an IoT layer, a MEC layer, and a cloud computing layer. The tri-tier architecture, in particular, facilitates model training directly on MEC devices, eliminating the need to transfer sensitive data across networks to centralized cloud data stores. Additionally, the key innovations of each FL-centric method are outlined, alongside a critical appraisal of their defining characteristics. In this context, certain schemes leverage FL to bolster the functionality of MEC environments, while others employ MEC to enhance the efficiency and effectiveness of FL processes. Fig. 8 classifies variousFL strategies integrated with MEC, grouping them by underlying approaches like reinforcement learning, deep learning, game theory, auctions, and metaheuristics, highlighting specific methods and algorithms used within each category.

4.1. Federated RL and DRL-based schemes

In a series of studies exploring the integration of FL and RL within MEC environments, researchers have proposed various schemes to optimize system performance, energy efficiency, and decision-making processes. To begin with, Jing et al. [99], introduced a combined optimization approach using a Q-learning-based algorithm to improve the ratio of delay and energy efficiency in FL and satellite communications, achieving a reduction in resource requirements with lower computational complexity. However, this study not consider unpredictable satellite behavior and lacks real-world testing across different environments. In other sutyd, Huang et al. [100], focused on a worker-first model distribution issue within the MEC context, employing DDQN and DQL algorithms within a DRL framework to provide nearly optimal solutions for energy expenditure, training duration, and communication overheads, demonstrating optimized performance compared to baseline methods. Nevertheless, this study not cover different network conditions or different types of tasks, which could affect the results. In their research, Shin et al. [101], proposed a federated DQN strategy to enhance energy efficiency through load balancing in UAV MEC servers, optimizing migration processes and facilitating the creation of an efficient global model, although the study did not consider the directional movement of vehicles which could impact data transmission. However, this study did not account for vehicle directionality, which could affect data transmission and model accuracy. The H-MAAC framework, developed by Zhu et al. [102], is a mixed-policy-based multi-modal DRL framework for age-sensitive MEC systems. It incorporates an edge-FL mode to optimize bandwidth allocation, data scheduling, and trajectory planning, outperforming baseline methods in average system age and training process stability. Further research [103-105], highlighted the synergistic effects of FL and RL in MEC systems, with FL facilitating collaborative learning among devices to improve performance and maintain user data privacy, while RL enables optimal decision-making through interaction with the environment. Yang et al. [106], introduced a framework for RIS-aided NOMA MEC optimizing computing resources, offloading decisions, and phase shifter design using an FRL approach, with the RWS system within the FRL framework incorporating task offloading history for worker selection, showing superior performance in image classification tasks using the MNIST and IRIS datasets, though the performance of RWS depends on offloading history, potentially leading to biased worker selection. However, this study's performance relies on past offloading, which might cause biased choices in worker selection. In their publication, Sun et al. [107], utilized a Multi-agent Reinforcement Learning (MARL) technique, enhancing FL integration by allowing edge nodes to adaptively modify training strategies according to network changes, significantly boosting resource utilization and learning accuracy. This approach was complemented by meta-learning for rapid adaptation to new environments, although potential delays in complex networks could pose challenges. This study greatly improves resource use and learning accuracy by letting edge nodes adjust training as network changes. Complementing this, Nie et al. [108], focused on energy efficiency in MEC systems incorporating UAVs by introducing a power-saving design optimized through a semi-distributed MAFRL algorithm. This algorithm effectively managed power control, user association, and resource allocation, demonstrating considerable improvements in operational efficiency and latency reduction, albeit with concerns regarding UAV stability and computational resource demands. Nonetheless, this study had limitations like possible UAV instability and high demands for computational resources. Security and fairness within FL were addressed by Huang et al. [109], who proposed a system based on node selection according to reputation to mitigate attacks and ensure equitable participation. The use of VRF-based steganography and a meritocracy-based aggregation strategy aimed to protect against poisoning attacks and ensure model integrity, showcasing enhanced security and effectiveness. Nevertheless, this study not reflected real-world complexities, and model's scalability and efficiency in diverse environments not tested. Further enhancing security, Feng et al. [110], introduced a dual-blockchain system comprising the Global and Local Model Update Chains (GMUC and LMUC) to secure FL operations over mobile edge networks. This structure ensured the integrity of model updates and facilitated rapid learning, but it also introduced computational overheads that could impact efficiency in resource-constrained environments. Moreover, the proposed method greatly enhances FL security and integrity, speeds up learning, and effectively secures model updates in MEC networks. Zhang et al. [111], addressed the challenge of low latency in multimedia services with the advancement of 5 G technology by utilizing MEC to offload intensive tasks to edge servers, thereby reducing latency and computational load on devices. They proposed FDRL-DDQN for efficient multimedia task offloading and resource allocation, integrating distributed DRL with FL for model training and parameter aggregation. This approach, specially designed to handle non-IID data issues, demonstrated significant cost reductions in simulations compared to traditional methods, showcasing its effectiveness in optimizing latency and energy consumption for multimedia tasks. In another study, Liu et al. [112], integrated FL and DRL with multi-agent collaboration in the FDRT method to reduce latency in computational offloading tasks. Employing DDQN and

Dueling D3QN agents for decision-making, this approach significantly enhanced training efficiency and minimized communication overhead, though its scalability might be limited in larger network settings. However, this paper struggles with scalability in bigger networks, affecting its overall effectiveness. Consul et al. [113], addressed complexities in the IoMT for improved QoS in 6 G healthcare. They proposed a FRL based Time Optimization (TO) Approach to optimize frame aggregation in Wireless Body Area Networks (WBAN) and MEC, reducing latency and energy consumption. Their approach categorizes service-related information, automatically adjusts aggregation duration, and optimizes task offloading. Simulation results demonstrated significant improvements in throughput, energy efficiency, and reduced latency compared to traditional methods.

In other published paper [114], Consul et al. introduced a generalized FRL approach tailored for complex scenarios in UAV-assisted MEC. By employing meta-learning and a normalized characteristic matrix, their method effectively divides a network into manageable units, enabling efficient computation offloading and resource allocation strategies. Their research, which integrates RL models from various devices into a cohesive framework, demonstrates significant improvements in system performance over numerous operations. Nevertheless, this study may have limitations. For example, the methods used might not work well in all real-world settings. Also, the study mainly focuses on UAV-assisted scenarios, which might not apply to other contexts. Further, the performance metrics were limited, focusing mainly on reward variance and average rewards. Guo et al. [115] developed an FL-based management system for MEC-supported IIoT, which significantly enhanced network performance. They achieved this by optimizing tasks at computational access points and employing a DRL algorithm to adjust key parameters, thereby reducing system costs. This approach to dynamic adaptation and efficiency mirrors Zhang et al. [116], who introduced an adaptive client selection method for MEC. They utilized a DDQN-based algorithm to minimize energy consumption and training delays, thus improving resource usage and addressing scalability and model divergence challenges. Building on these concepts, Shahidinejad et al. [117] proposed a context-sensitive offloading strategy within a multi-user MEC environment. They combined FL and DRL through the FLUCO algorithm for optimized offloading, which significantly outperformed traditional methods in energy efficiency, cost, and latency. These studies collectively highlight the benefits of context-aware and distributed algorithms in enhancing network performance, demonstrating the power of collaboration in advancing the field (Fig. 9).

Similarly, Li et al. [116], focused on dynamic task offloading in MEC using a DDQN and FL-based algorithm, which not only reduced computational costs but also improved Quality of Service (QoS) by addressing challenges like catastrophic forgetting and ensuring data privacy, showing the effectiveness of integrating FL with DRL for offloading optimization. However, the scalability with larger networks could pose challenges, and further tests are needed to confirm these results in different settings. In the vehicular context, Li et al. [117], explored participant selection and resource allocation in vehicular FL, employing F-DRL to minimize training delays while maintaining energy efficiency, highlighting the importance of joint optimization in vehicular networks for FL efficiency and performance. This study not include diverse environments or different vehicle types, which could affect the applicability of the findings in real-world scenarios. Also, it mainly focuses on theoretical aspects, lacking practical tests. Moreover, Zang et al. [118], introduced the FDOR algorithm, leveraging F-DRL for task offloading and resource allocation in a dynamic IoT environment, enhancing performance through wireless-powered communication technology and addressing the challenges of non-IID data with an adaptive learning rate approach, showcasing superior performance in integration speed, execution delay, and overall system stability. This study effectively enhances IoT performance using FDOR algorithm with F-DRL, improving integration speed, reducing execution delays, and boosting system stability through adaptive learning approaches. In [119], Li et al. proposed a layered, cluster-based MEC network designed specifically for virtual reality panoramic video services, and devised a data perception-guided clustered-edge transmission model. They formulated the combined optimization problem of caching and bitrate adjustment as an MDP and proposed the FDRL-CBA algorithm as a solution. The simulated outcomes indicated that FDRL-CBA surpassed existing DRL-based techniques regarding cache hit ratio and quality of experience. It could also facilitate cooperation between MEC edge nodes and offer ample computational and caching resources for virtual reality panoramic video services. The study provides a significant technical

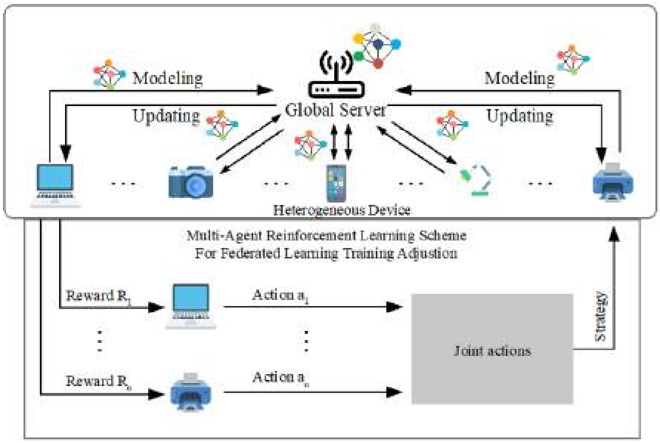

Fig. 9. Framework for FL in the heterogeneous scenario presented in study [107].

contribution by enhancing virtual reality service quality through advanced caching and bitrate optimization. It improves resource efficiency and cooperation among MEC nodes, boosting user experience effectively. The research shows a strong combination of FL and DRL to improve MEC in different areas, like IIoT and vehicular networks. These new methods help with moving tasks dynamically, making the best use of resources, and picking the right clients, which significantly helps work more efficiently, cut down delays, and keep data private. By mixing FL with DRL, the systems can adapt and be aware of their surroundings, which is critical in handling the complex nature of MEC settings. However, a big problem in these studies is how they might not work well when scaled up to more extensive or complex networks. Also, using advanced algorithms like DRL can lead to high computational demands and require a lot of data handling, which can be a problem for edge devices that do not have many resources. This shows a difficult balance between getting better optimization and using it practically in real situations. Table 3 compares schemes like LSTM, RL, Actor-Critic Learning, Q-Learning, DRL, and DQN based on evaluation parameters such as accuracy, loss, delay, privacy, and more. Each scheme's properties are evaluated across various metrics to ensure comprehensive analysis.

4.2. Federated deep learning-based schemes

In this subsection, we review studies on federated deep learning-based schemes. Deep learning is a type of ML using layered neural networks to analyze various data types. It differs from RL, which learns through trial and error using rewards, and DRL, which combines deep learning with RL to process complex input data for decision-making. To start with, Li et al. [122], introduced AdptVFedConv, an innovative image classification algorithm customized for vertical FL, where participants work with distinct image fragments. Unlike traditional FL approaches that share model parameters, AdptVFedConv facilitates sharing hidden feature representations, enhancing local feature extraction and the backend classifier model's training with these features. Despite its lower precision than conventional models, AdptVFedConv's effectiveness was validated through extensive experiments. However, its performance might be compromised by the variability in the positioning and sizes of image fragments, highlighting the challenges of applying vertical FL in real-world scenarios with inconsistent data. However, this study has limitations due to varied sizes and positions of image parts used in AdptVFedConv. This could affect how well the algorithm works in real situations.

Building on the theme of optimization within FL frameworks, Xu et al. [123], focused on reducing costs in MEC networks by developing an optimization framework for FL, including algorithms for both single and dynamic FL requests. Their approach, tested through simulations and real-world datasets, demonstrated significant cost savings and improved performance, particularly in a hierarchical FL training structure named HierFedML. Yet, the algorithm's efficacy could be limited by highly dynamic user behaviors and complex model requirements, underscoring the need for adaptive solutions in fluctuating network conditions. Fig. 10 illustrates the hierarchical structure of FL as applied within MEC frameworks. This structure optimizes computational resources by distributing tasks across multiple layers, improving processing scalability and performance. Nonetheless, the study might face limitations from not applying FL and MEC frameworks universally. For instance, the algorithm may not work well if user behaviors change quickly or the models get too complex. This could mean the need for more flexible solutions in networks that often change.

Similarly, Zheng et al. [124], explored unsupervised, privacy-preserving popularity prediction within MEC-enabled IIoT environments, proposing the URFL algorithm within a framework that utilizes global and local popularity concepts modeled through a Markov chain. This approach, enhanced by a FedLWA parameter aggregation method, significantly improved prediction accuracy without relying on manual labeling or compromising data privacy. The success of URFL, however, depends on the quality of unsupervised learning, which may fluctuate in complex industrial settings. Zhang et al. [125], proposed the FedMEC framework, an approach designed to address the dual challenges of computational burden on mobile Edge Devices (EDs) and privacy concerns inherent in FL protocols. By dividing the DNN into two parts, FedMEC successfully transfers intensive computational tasks to edge servers, considerably reducing the processing burden on EDs. Incorporating differential privacy, through the injection of Laplacian noise, further enhances user data confidentiality. Despite its notable achievements in model precision and privacy assurance, the efficacy of FedMEC is heavily dependent on fine-tuning the differential privacy parameters, posing a challenge for optimal configuration. Zhong et al. [126] introduced a LightWeight Federated Graph Learning (LW-FGL) framework to enhance FGL in UAV-assisted MEC systems. They addressed the challenge of UAVs' limited resources by developing an adaptive information bottleneck principle and tiny Graph Neural Networks. This approach filters irrelevant information and reduces computational complexity, leading to faster inference speeds and higher classification accuracy, as experiments on real-world datasets demonstrate. However, this paper did not cover different environments or other data types. Also, the approach may not work well with fewer UAVs or limited data access. Building on model efficiency, Wu et al. [126], proposed the HybridFL protocol, which employs a two-tiered model aggregation strategy within MEC systems. The protocol introduces regional slack factors to mitigate the impact of stragglers and device dropouts, enhancing the robustness of the FL process. The experimental results underscored the protocol's ability to accelerate global model convergence and reduce energy consumption on EDs, marking a significant step forward in optimizing FL training efficiency.

Lin et al. [127], introduced Fed-PEMC, a federated deep learning algorithm enhancing privacy and efficiency in MEC by combining local differential privacy with model compression. Utilizing DRL for compression and customized label sampling for training, Fed-PEMC minimizes privacy risks from inference attacks and reduces communication overhead. The algorithm, proven to adhere to differential privacy standards, outperforms traditional methods in maintaining accuracy and optimizing communication, showing significant improvements on benchmark datasets. However, the proposed scheme face challenges as it relies on ideal network conditions for performance and assumes uniform data distribution across devices. In other study, Hammedi et al. [128], explored the domain of collaborative systems by developing a collision avoidance system for inland ships, with a focus on data security and privacy. Utilizing deep FL and blockchain technology, the system ensures secure and efficient ship positioning predictions at the MEC level, enabling real-time collision detection. While the system boasts high communication efficiency and data privacy, the challenges of

Table 3
Properties of the LSTM, RL, Actor-Critic Learning, Q learning, DRL and DQN schemes. See references [99-102,106-110,112,115-121].

Ref	Operation methods				Security			Application				Cloud		Approach			Datasets			Simulator			Evaluation Parameters						
	Offloading	Scheduling	Load balancing	Resource allocation	Blockchain	Intrusion detection	Secure aggregation	Other	IoV	IoT	UAV	Without Cloud	With Cloud	Centralized	Distributed Edge Server	Distributed Edge Device	Benchmark	Real-world	Synthetic	NA	Python	MATLAB	Reward	Energy	Cost	Privacy	Delay	Loss	Accuracy
[106]	✓						✓			✓		✓				✓	✓			✓						✓	✓		✓
[107]		✓					✓	✓					✓		✓		✓				✓		✓			✓		✓	✓
[108]				✓			✓				✓	✓			✓								✓	✓		✓			
[109]				✓	✓					✓		✓				✓	✓			✓						✓			✓
[110]		✓			✓					✓		✓				✓	✓				✓					✓	✓		✓
[102]		✓					✓				✓		✓		✓			✓			✓					✓		✓	
[99]				✓			✓	✓				✓			✓		✓					✓				✓		✓	✓
[112]	✓						✓			✓			✓		✓	✓					✓		✓			✓	✓	✓	
[115]				✓			✓	✓					✓	✓				✓		✓				✓	✓	✓			
[120]				✓			✓			✓			✓		✓		✓			✓				✓		✓	✓		✓
[121]	✓						✓			✓			✓		✓					✓				✓	✓	✓	✓		
[116]	✓						✓			✓		✓			✓						✓			✓	✓	✓		✓	
[117]				✓			✓		✓				✓		✓		✓	✓		✓			✓		✓	✓	✓		✓
[118]	✓			✓			✓			✓		✓			✓						✓			✓		✓		✓	
[119]							✓			✓			✓		✓			✓			✓		✓			✓		✓	
[100]	✓						✓			✓		✓			✓					✓			✓			✓		✓	
[101]			✓				✓				✓	✓			✓			✓			✓			✓		✓	✓		

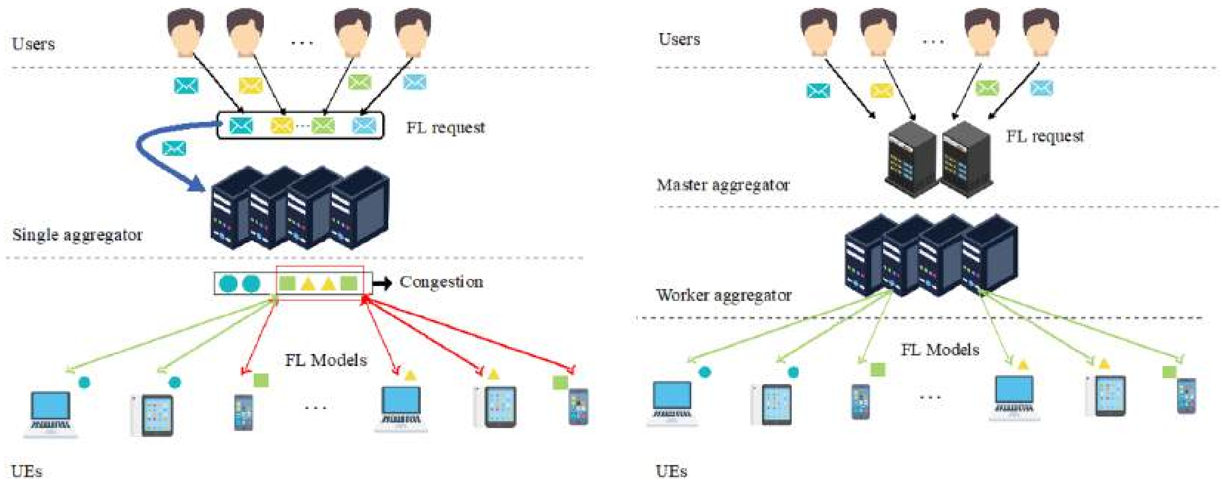

Fig. 10. the hierarchical structure of FL in [123].

missed detection and positional accuracy present avenues for further refinement. However, this paper have limitations in data collection, high system complexity, and real-world testing in varied conditions. Exploring the theoretical underpinnings of FL, Liu et al. [129], delved into the analysis of integration errors in deep FL networks. By examining the immediate and statistical errors in two-hop relaying channels, their study established the foundation for a deeper understanding of error propagation in FL networks, providing valuable insights for future research aimed at enhancing the integration of local and global training. Addressing the scalability of FL in large-scale MEC networks, You et al. [130], introduced the hierarchical PFL strategy. This approach segments user equipments into clusters, adopting a blend of synchronous and semi-asynchronous aggregation to optimize bandwidth allocation and edge server scheduling. The HPFL strategy adeptly navigates the trade-off between maximizing training loss reduction and minimizing communication latency, showcasing the potential of hierarchical aggregation in extensive MEC environments. Nevertheless, this study did not consider real-world conditions or different types of data, which could affect the results' applicability. In their publication, Nguyen et al. [131], explored the optimization of hyper-learning rates and resource allocation through their MS_FEDL design, which notably aims to minimize the learning time and energy consumption of mobile devices. Their method, combining centralized and distributed algorithms, marks a significant stride towards efficient FL. However, this venture raises questions about scalability in expansive network landscapes, paving the way for subsequent research to build upon. Progressing from this foundational work, He et al. [132], presented AceFL, customized specifically for the heterogeneous and resource-constrained environments of 6G-enabled MEC networks. Their strategy, employing the IFBA algorithm to counteract the straggler effect, showcases a pivotal advancement in accelerating the FL training process. This development not only complements the efficiency-focused endeavors of Nguyen et al. but also highlights the critical need for adaptive solutions capable of navigating the diverse challenges of modern MEC networks. Nonetheless, the resilience of AceFL against dynamic network conditions and unforeseen resource limitations remains an area ripe for further exploration. In parallel to these efficiency-enhancing strategies, Zheng et al. [133], explored ways to decrease communication costs in FL using a gradient reduction algorithm and introduced FT-IoMT Health mechanism for the IoMT. This approach, enhancing personalized model training while strictly adhering to privacy and security protocols, aligns with the overarching goal of optimizing FL deployments. Despite its promising performance, the effectiveness of the proposed methodology in data-heterogeneous environments beckons further scrutiny, suggesting a continuous loop of research and refinement. Moreover, Zhao et al. [134], explored the integration of blockchain technology into a crowdsourcing FL system, offering an approach to ensuring data integrity and privacy. This method not only builds upon the foundational work of Nguyen et al. and He et al. by introducing a robust security layer but also addresses the scalability concerns through a decentralized model aggregation framework. While the efficacy and viability of this

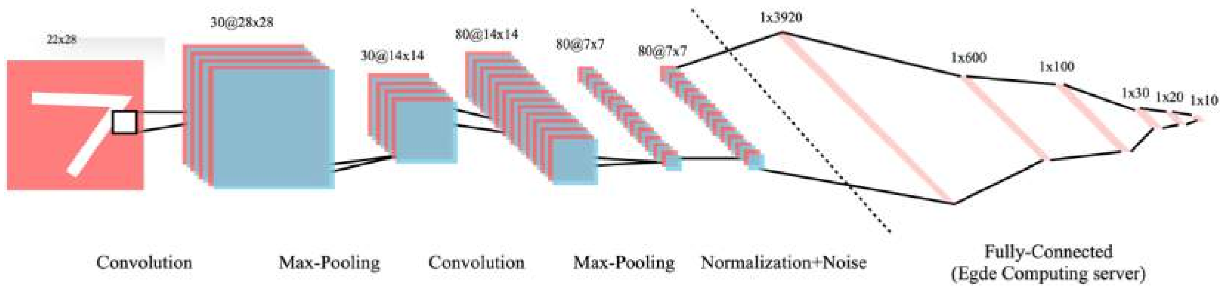

Fig. 11. Neural network used in experiments of [134].

blockchain-empowered system are well-documented, the computational and energy demands associated with blockchain adoption highlight a critical trade-off, underscoring the need for balanced solutions in FL implementations. Fig. 11 showcases a neural network model used in experiments of this scheme to validate the efficacy of approaches. The diagram details the layers and nodes involved, highlighting the complexity and depth of the neural architectures employed.

In their study, Tang et al. [135], introduced a resource allocation algorithm that leverages a two-layered Stackelberg game model, aiming to balance the trade-offs between local model precision, energy consumption, and system delay in MEC environments. By motivating EDs with rewards, their design not only motivates the contribution of computing resources but also maintains an balance between global model accuracy and operational efficiency. This approach demonstrates how strategic resource allocation and incentives can collectively enhance the performance of FL systems, reducing energy consumption and system delays, thereby promoting active participation from EDs. The results from their simulations confirm the algorithm's advantage in optimizing resource distribution, illustrating a significant step forward in FL efficiency. However, the study by the authors have limitations due to not applying their algorithm in real-world scenarios, which can often present unexpected challenges and variables not accounted for in simulations. Additionally, the reliance on the theoretical model might not perfectly capture the complex dynamics of actual MEC environments, possibly affecting the algorithm's practical effectiveness and scalability. Building on the theme of efficiency, Jin et al. [136], explored security considerations with their Edge QoS Per-PM approach, which integrates public and private model training to enable personalized forecasting while bolstering security measures. Their methodology ensures the confidentiality of private models, addressing the pivotal concern of data privacy in FL. By periodically updating the LSTM model with the latest private data, Edge QoS Per-PM strives to maintain real-time accuracy in QoS predictions within the ever-evolving edge environment. The approach's effectiveness, demonstrated through improvements in integration speed and prediction accuracy, highlights its potential in various scenarios requiring secure and precise QoS forecasting. However, the reliance on frequent data updates underscores a critical balance between enhancing security and managing the resultant computational and communication demands. Table 4 outlines the performance of CNN and gradient descent schemes across multiple evaluation parameters like accuracy, loss, and privacy. It details the application of each scheme in various settings using simulators like MATLAB and Python, and for different data types and deployment approaches.

4.3. Federated game theory-based schemes

The diverse and distributed characteristics of MEC environments present challenges for FL, including issues related to unreliable communication channels, user mobility, and resource limitations. Game theory has emerged as a potential solution for tackling these challenges and improving the performance of FL in MEC environments. In game theory, agents decide according to the strategies adopted by other agents in a specific scenario, aiming to maximize their collective and individual objectives. By combining FL with game theory, agents have the opportunity to cooperate and compete with each other, aiming to reach a state of Nash equilibrium. As stated in [142], no agent can enhance its utility in this balance state by independently modifying its strategy. Recent studies have illustrated how this approach improves FL's resilience, efficiency, and security in MEC environments.

Abou El Houda et al. introduced a pioneering framework named FedGame [143], which leverages MEC to defend IIoT applications by applying FL. The design enables secure collaboration among multiple MEC domains when keeping the privacy of IIoT devices. A non-cooperative game is constructed in the FedGame framework, allowing MEC nodes to gain virtual resources from a managed MEC orchestrator to address various IIoT attacks effectively. The authors assessed the performance of FedGame through practical experiments involving real-world IIoT attacks. The results of these experiments illustrated the effectiveness of their proposed model in offering the required MEC resources to counter IIoT attacks while ensuring the protection of privacy for industrial systems. The approach employs FL to construct a MEC-enabled model prediction for intrusion detection. Upon detecting an intrusion, FedGame uses a noncooperative game to allocate the required virtual resources for resisting the attack. FedGame can be considered a proficient design that enhances user privacy and safeguards industrial systems against attacks originating from the IIoT. However, the study did not test other ways to protect IIoT systems, so it's not clear if there are better options. Plus, the study's experiments were only on a few types of attacks, so we don't know how it does with others. Furthermore, Lee et al. introduced a combined mechanism for managing datasets and incentives in FL across MEC systems. This mechanism aims to decrease MDs' power usage in FL [144]. The suggested method enables each MEC to maximize revenue by offering comprehensive incentives to MDs, encouraging their participation in any FL task. This is achieved when considering the exchange between the costs of incentives and the estimated precision. The total allocated incentives were distributed based on the proportion of the dataset utilized for local training by MDs, which in turn influenced the overall accuracy. MDs leveraged these incentives to determine the dataset for local training, with the goal of optimizing their returns in terms of energy usage and expected incentives. The examination using game theory demonstrated that the suggested approach guaranteed a unique solution at equilibrium, optimizing the advantage for all participants. The outcomes demonstrated the benefits of implementing incentive-based mechanisms; the suggested approach ensures efficient FL dataset management for MDs and FL service providers, according to the findings. However, the study did not reflect the real-world variability as it assumes constant dataset quality across all MDs. Also, the impact of network delays on training times and costs wasn't explored. In other study, Li et al. [145], addressed the challenge of surging traffic demands near medical infrastructures during health emergencies and the need to protect patient data by proposing a UAV-assisted MEC system with hierarchical FL. They introduced a Stackelberg game and incentive mechanism to motivate user and UAV participation in FL, optimizing data usage, task, and reward allocation. This approach ensures efficient communication, safeguards patient privacy, enhances model training accuracy, and maximizes social welfare, as demonstrated by their experimental results. Nevertheless, FL model's performance can change with more users in the proposed method. Also, patient privacy methods need constant updates.

Table 4
Properties of the CNN and gradient descent schemes. See references [131-135,137-141].

Ref	Operation methods				Security			Application				Cloud		Approach			Datasets			Simulator			Evaluation Parameters						
	Offloading	Scheduling	Load balancing	Resource allocation	Blockchain	Intrusion detection	Secure aggregation	Other	IoV	IoT	UAV	Without Cloud	With Cloud	Centralized	Distributed Edge Server	Distributed Edge Device	Benchmark	Real-world	Synthetic	NA	Python	MATLAB	Reward	Energy	Cost	Privacy	Delay	Loss	Accuracy
[131]				✓			✓			✓		✓						✓		✓				✓	✓	✓			
[132]				✓			✓			✓		✓			✓		✓		✓		✓					✓		✓	✓
[133]							✓	✓					✓		✓			✓		✓						✓			✓
[134]	✓				✓			✓				✓			✓		✓			✓			✓			✓			✓
[135]				✓			✓			✓		✓				✓					✓			✓		✓	✓		
[137]				✓			✓		✓			✓		✓				✓		✓						✓		✓	✓
[138]		✓	✓				✓			✓		✓			✓		✓				✓					✓			✓
[139]		✓					✓			✓		✓			✓		✓			✓				✓	✓	✓	✓	✓	✓
[140]							✓	✓				✓			✓		✓					✓				✓		✓	
[141]							✓	✓					✓	✓			✓				✓					✓			

Also, Zeng et al. proposed FMore, a system specifically designed to incentivize the involvement of superior edge nodes with minimal costs in FL. The objective is to enhance the system's overall performance [146]. This method employs a lightweight and incentive-compatible multi-dimensional procurement auction that selects K winners. Moreover, the authors provided a theoretical study of the Nash equilibrium strategy adopted by edge nodes. They utilized expected utility theory to guide the aggregator, drawing upon their research outcomes. Thorough real-world and simulation experiments have shown that FMore significantly reduces the number of training iterations and dramatically improves the accuracy of complex AI models.

In a practical system consisting of 32 nodes, the proposed design reduced training time and improved model precision. However, this work did not combine the budget constraint of the aggregator, leaving it as a subject for future investigation. The probability associated with each node also requires further examination. In their publication, Li et al. presented VARF [147], which is an incentive mechanism designed for MEC to facilitate cross-silo FL. VARF employs a heuristic algorithm to carefully select edge nodes with excellent reputations and quality for model training. Furthermore, VARF incentivizes these selected ENs to contribute their resources actively. By integrating the framework of an infinitely repeated game, VARF effectively grasps the persistent conduct of ENs in the context of cross-silo FL. It then formulates a stable and lasting cooperative strategy for clients while maximizing local data utilization for optimal model learning. The effectiveness of VARF is assessed using actual datasets from real-world scenarios, and the evaluation demonstrates its superior advantages over other benchmark approaches. Moreover, in the setting of cross-silo FL, VARF enriches learning task performance and reduces the loss associated with these tasks. Under the circumstances of trigger strategy, CPs and ENs establish a durable and enduring cooperative partnership. VARF boosts the effectiveness of learning tasks in cross-silo FL by incentivizing the consistent and engaged involvement of esteemed organizations with excellent quality and reputation. Nonetheless, this study may not account for changes in edge node quality over time or potential bias in selecting nodes with high reputations, which could affect the fairness and adaptability of the VARF system.

Deep learning methods used in FL and MEC apply adaptive algorithms that customize learning based on the specific abilities and limits of diverse edge devices, improving efficiency and preventing resource overload. Techniques such as model partitioning help spread out the computing work by moving parts of neural networks to edge servers, which speeds up training and cuts down on delay. Privacy is a key focus, using methods such as Differential Privacy that introduce noise to data or gradients to keep user information safe during the learning process. To address challenges such as energy consumption and fluctuating network conditions, optimization algorithms adjust in real-time by incorporating strategies like model compression to reduce communication needs. Hierarchical learning methods enable system scaling through local data aggregations followed by a global synthesis, effectively managing the unequal data distribution among devices. Additionally, techniques like unsupervised and semi-supervised learning utilize unlabeled data at edge nodes, enhancing the models' relevance and efficiency while maintaining data privacy.

4.4. Federated auction-based schemes

Auction-based mechanisms in MEC are mostly used for resource allocation and pricing in a distributed manner. In an auction-based system, service providers (SPs) and mobile users (MUs) interact in a competitive environment where the MUs bid for the resources needed to perform their tasks, and the SPs compete for the right to serve those tasks [148]. The auction can be designed as a sealed-bid second-price auction or an ascending auction. In a sealed-bid second-price auction, each MU submits a private bid, and the SP with the highest bid is selected to serve the task, but the price paid is the second-highest bid [149]. In an ascending auction, MUs can observe the current highest bid and decide whether to bid higher [150]. The auction-based mechanism is used to improve the efficiency of resource allocation and reduce the cost-of-service provisioning in MEC. In their research, Lu et al. introduced a client selection approach for FL in [151] to resolve the data heterogeneity issue in the system. The authors presented an idea of a federated virtual dataset created to create a dataset that aligns with the overall distribution pattern. Additionally, they formulated a clustering method to group the clients.

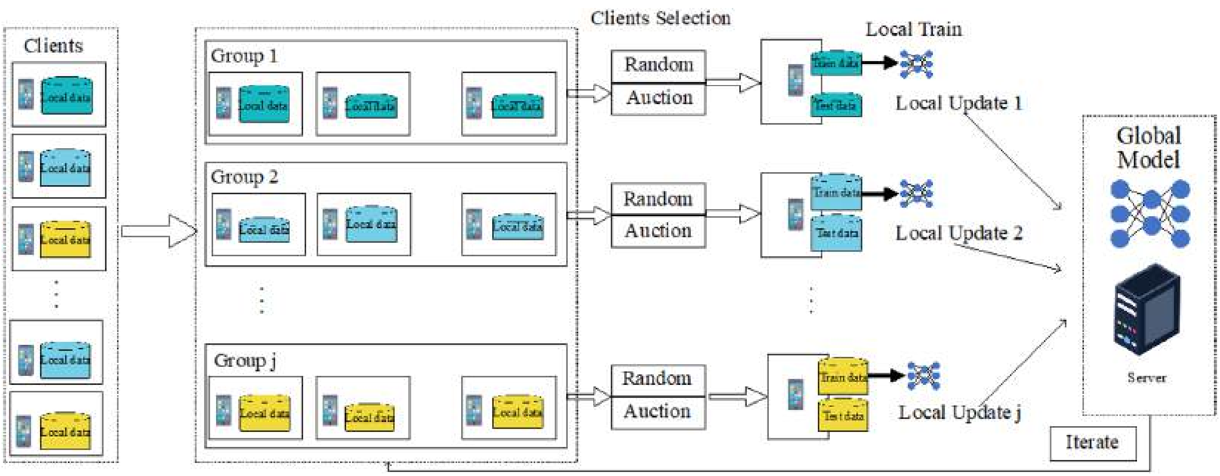

Fig. 12. An overview of action-based clustered FL [151].

The authors also suggested a sample windows framework to mitigate the effect of local data disparity on the precision of clustering. Furthermore, they offered a sample windows approach to tackle the influence of imbalanced local data on the precision of clustering. When merged with the stochastic gradient descent algorithm, the authors demonstrated that their client selection method exhibited integration toward an approximate favorable solution. In addition, in each cluster, a client selection algorithm was created according to auctions to ensure fair energy consumption distribution. When deploying the CNN model with varying data distributions, the simulation outcomes illustrated that the suggested client selection design and auction-based FL approach surpassed alternative methods in terms of performance. The findingsof this study mainly depend on simulations which might not represent real-world conditions. The effect of network issues on client coordination was not discussed. Additionally, the study does not address how the proposed method scales with extremely large datasets. Fig. 12 presents an auction-based client selection method within a FL scenario in MEC. This approach optimizes resource allocation by dynamically selecting clients based on their bids, enhancing overall system efficiency.

In other study, Lu et al. [152], proposed an Auction-based Cluster Federated Learning (ACFL) scheme to address challenges in MEC by enhancing data privacy and managing data heterogeneity and resource constraints. They introduced a clustered FL framework with a mean-shift clustering algorithm to group clients based on local data distribution. An auction-based client selection strategy was implemented to balance energy consumption and improve model convergence. Their approach, validated through experiments on real-world datasets, demonstrated optimized performance in convergence rate and energy efficiency compared to traditional FL methods.

4.5. Federated metaheuristic-based schemes

Metaheuristic-based schemes in MEC refer to the use of optimization algorithms inspired by natural phenomena and biological processes to solve complex problems [153]. These algorithms involve iteratively searching through a large search space to find an optimal solution. Examples of metaheuristic algorithms include Genetic Algorithms, Particle Swarm Optimization, Ant Colony Optimization, and Artificial Bee Colony Optimization [154]. In MEC, metaheuristic-based schemes can be used to optimize various aspects, such as task offloading, resource allocation, and energy consumption [155]. These strategies can enhance the efficiency and scalability of MEC systems by simplifying the computational complexity involved in optimization tasks. However, they may require significant computation and may not always converge to an optimal solution. Therefore, it is essential to carefully select and tune metaheuristic algorithms to achieve the desired performance. Moreover, Feng et al. [156], introduced an integrated optimization design for user selection and data sampling in the setting of FL deployed in MEC systems. The researchers developed a mathematical formulation to address the challenge of minimizing cost and precision loss, considering computation and communication resource constraints. Effectively converging the stationary optimal solution, they developed an optimization algorithm. The proposed optimization design was tested through real-world experiments and numerical simulations, showing significant improvements in the accuracy of FL. Moreover, the suggested algorithm effectively maintained low costs, as evidenced by the outcomes. Furthermore, the authors established a feasible upper limit on the extent of precision reduction to quantify the precision of the model, incorporating the costs related to computation and communication. By effectively managing the sample and user selection, the joint optimization algorithm successfully achieves a compromise between model precision and cost. However, this study limited by specific system settings and mathematical assumptions, results may not generalize to other contexts. In other study, Feng et al. [157], demonstrated an optimization design to enhance the precision of FL in MEC systems when maintaining low costs. They set up an optimization problem to strike a balance between reducing precision and managing costs, taking into account resource limitations and challenging wireless transmission conditions. A unified optimization algorithm was developed to optimize sample selection and the tactics of model compression and user selection, nearing the stable optimal resolution. The suggested algorithm and the evaluation were conducted using experiments and numerical simulations to assess its optimization design. The outcomes demonstrated notable precision decreases and costs in MEC systems. The authors underlined the importance of their study, which has the potential to improve the efficiency of FL in various MEC environments. Nevertheless, this research did not consider varying user behaviors and the unpredictable nature of real-time data. Table 5 evaluates DL, game theory-based, auction-based, and metaheuristic-based schemes across various parameters such as accuracy, loss, and privacy. The table also includes details on simulators, data types, deployment approaches, and security features used in these schemes.

4.6. Other FL schemes

In this section we investigate different algorithmic foundations that improve the effectiveness of FL, with a focus on enhancing communication efficiency, maintaining privacy, and adapting learning capabilities in MEC. These algorithms tackle the specific challenges found in MEC settings, such as restricted bandwidth, high mobility, and strict privacy needs. Our discussion covers various approaches like differential privacy, integrating blockchain, and stochastic optimization, which are crucial for furthering the use of FL in networks driven by edge computing. To start with, Lu et al. proposed a differentially private asynchronous FL model in [137], devised for resource allocation within vehicular networks. This framework incorporates Local Differential Privacy to protect the privacy of local models during updates. It introduces a new approach of random distributed updates to address security risks that might arise from having a centralized coordinator. Additionally, the framework speeds up convergence by verifying updates and using weighted consolidation. The effectiveness and accuracy of this approach were demonstrated through evaluations conducted on three real-world datasets, with an emphasis on preserving data privacy. The model presents a solid and reliable FL system suitable for edge computing within vehicular networks. The incorporation of local differential privacy in the gradient descent local training progression

Table 5
Properties of the DL, Game theory based, Auction based, and Metaheuristic based schemes. See references [128,129,143,144,146,147,151,156,157]

Ref	Operation methods				Security			Application				Cloud		Approach		
	Offloading	Scheduling	Load balancing	Resource allocation	Blockchain	Intrusion detection	Secure aggregation	Other	IoV	IoT	UAV	Without Cloud	With Cloud	Centralized	Distributed Edge Server	Distributed Edge Device
[128]		✓					✓	✓					✓		✓	
[129]										✓			✓			
[143]				✓		✓		✓				✓		✓		
[144]				✓			✓			✓		✓		✓		
[146]				✓			✓			✓			✓		✓	
[151]			✓				✓			✓			✓		✓	
[156]		✓								✓		✓				✓
[157]		✓								✓		✓		✓		
[147]				✓			✓	✓					✓			✓

Ref	Datasets			Simulator			Evaluation Parameters						
	Benchmark	Real-world	Synthetic	NA	Python	MATLAB	Reward	Energy	Cost	Privacy	Delay	Loss	Accuracy
[128]		✓		✓						✓			
[129]				✓						✓			
[143]	✓			✓						✓			
[144]			✓		✓					✓			
[146]	✓			✓						✓		✓	✓
[151]	✓				✓		✓	✓	✓	✓		✓	✓
[156]	✓			✓					✓	✓		✓	✓
[157]	✓			✓				✓	✓	✓		✓	✓
[147]	✓			✓						✓		✓	✓

ensures protection for the revised models of each participant. A traditional update method involving a centralized server and its clients is replaced with a random peer-to-peer mechanism. The proposed scheme emphasizes verifying the integrity of updates and subsequent weighted integration of the updated models, enhancing the convergence rate of the framework. Fig. 13 depicts a Differentially Private Asynchronous FL model used within vehicular networks. This model ensures strong privacy protections by incorporating local differential privacy techniques during data transmission and model updates.

In their publication cited as [138], Chen et al. introduced Fed-IR, a novel approach that improves the communication efficiency of standard FL methods. The suggested method achieves this by exchanging intermediate outcomes rather than exchanging the complete model. The authors conducted a theoretical analysis of Fed-IR and established a correlation between the frequency of intermediate result exchanges and the performance of the training process. Based on their results, the researchers proposed an algorithm that adaptively adjusts exchange intervals to balance training performance with communication costs. The outcomes from the simulation showed that the suggested approach effectively decreased communication traffic by a significant margin, with reductions ranging from approximately 42 % to 81 %. Remarkably, this reduction in traffic was achieved while maintaining similar levels of precision compared to the traditional methods of exchanging the entire model. The suggested approach improves distributed FL communication efficiency, addressing a critical need in large-scale and resource-limited systems such as MDs and IoT networks. However, this scheme might experience performance drops in highly unstable network conditions or when dealing with larger or more complex models. Zhu et al. [158], highlighted the privacy and security problems in UAV-utilized smart cities, particularly with UAV-MEC systems' centralized data processing exposing sensitive data to risks. To counter this, they introduced UBFL, a FL mechanism integrating blockchain for secure data sharing. This approach uses an adaptive nonlinear encryption function for privacy, outperforming traditional differential privacy methods. UBFL incorporates the random cut forest algorithm for anomaly detection, showing high resilience against data attacks in extensive tests, achieving notable accuracy and robustness in securing UAV data within MEC environments. Nevertheless, the authors did not check if using blockchain slows down data sharing or increases costs. Plus, they mainly focused on privacy, not other potential issues like how practical or cost-effective their system is in different settings.

According to the findings of Bai et al. in the study, a concept known as MC-FL was suggested. The primary objective of MC-FL is to improve the adaptability and resilience of FL in the context of MEC systems [139]. MC-FL manages and trains several GMs with varying learning performance and computational complexity tradeoffs. This approach is implemented to effectively handle the diversity of devices and the fluctuations in their statuses. Furthermore, MC-FL uses a partial client participation design, enabling the inclusion of different clients over time to accommodate the challenges posed by unpredictable mobile environments. The researchers provided a thorough mathematical demonstration of how the MC-FL framework can be integrated and developed an online client scheduling system to reduce the time needed for completion. Additionally, the authors demonstrated a service delivery scenario utilizing MC-FL to illustrate the enhanced Quality of Experience for service subscribers by leveraging multiple GMs. However, the MC-FL framework might suffer from scalability issues as the number of GMs and participating clients increase, potentially hindering performance. Fig. 14 illustrates the scheduling model used in a Multicore FL framework for MEC systems. This model facilitates efficient task distribution and resource management across multiple processing units, enhancing operational flexibility and performance.

In their study [140], Chen et al. suggested a communication-efficient design for FL aimed at minimizing the number of iterations

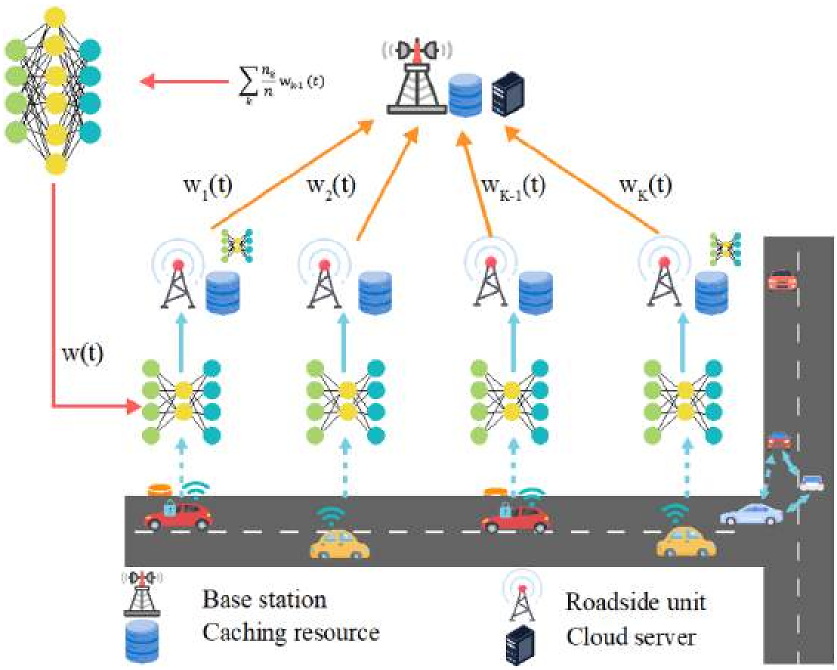

Fig. 13. FL-based vehicular networks presented in [137].

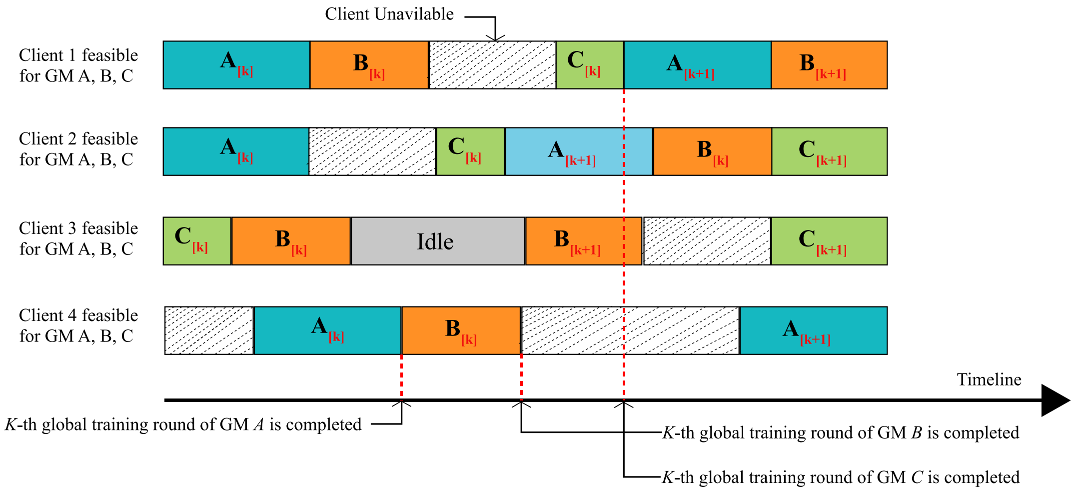

Fig. 14. Client scheduling model proposed in [139].

needed among all servers and participants, while maintaining precision. The researchers formulated the problem as an optimization problem with finite sums and suggested a method according to FedSVRG (Federated stochastic variance reduced gradient) to address it. The technique also includes an analysis of how it integrates. The suggested design was tested testing on linear and logistic regression problems, and the results demonstrate that FedSVRG achieves a significant reduction in communication costs compared to standard stochastic gradient descent-based FL approaches. To summarize, this study presents a communication-efficient solution that effectively minimizes communication costs in FL. However, the study could have limitations due to not applying their method to multiple data types beyond linear and logistic regression problems. In other study, Huang et al. [159], introduced a reliable and fair FL mechanism for MEC to address security and performance issues arising from the high mobility and vulnerability of mobile devices. They proposed a reputation-based node selection scheme, counter-strategies against attacks, and a new global model aggregation strategy to mitigate poisoning attacks. Additionally, a blockchain-based reward-penalty scheme was designed to ensure fairness and penalize malicious nodes. Nevertheless, this study did not consider all possible attack types. Also, the blockchain system could slow down the process, and real-world testing might show different results. Moreover, Houda et al. introduced DETECT, [141]. The suggested architecture facilitates the cooperative and secure mitigation of IoT attacks across various MEC domains, all while guaranteeing the MEC collaborator's privacy and the IoT devices involved. During the experimental evaluation on the NSL-KDD and Edge-IIoTset datasets, DETECT exhibited remarkable precision, as shown by the Precision and F1 score measurements. By utilizing the NSL-KDD dataset and conducting experiments involving actual IoT attacks, it was demonstrated that DETECT surpasses managed ML and DL approaches across multiple metrics, such as precision. This finding highlights the potential of DETECT as a promising architecture for safeguarding IoT applications while upholding the privacy of devices. Furthermore, Wang et al. proposed an FL system in their study, specifically designed for real-time target recognition in 5 G MEC networks [160]. To effectively send training models across a dynamically changing bandwidth, the design integrates a mechanism for selecting the compression mode adaptively. Compared to standard non-cooperative methods, the suggested model reduced training delay and achieved a higher precision when in contrast to the approach of managed processing approach. Additionally, the system guarantees user privacy. By introducing a mechanism for adaptive switching of lossless compression levels, the training efficiency is enhanced, particularly in wireless channels that exhibit time-varying characteristics. The authors conducted experimental tests to demonstrate the advantages of the proposed method over non-cooperative and managed methods, specifically focusing on improving accuracy and reducing delays. However, the scheme does not address possible data privacy risks inherent in real-time target recognition.

As noted Qian et al., presented a PSP design in [161], aiming to confront the problem of service placement, the authors devised a solution by incorporating privacy awareness into edge cloud systems. The authors transformed service placement into a binary (0–1) problem and constructed a hybrid service placement algorithm that combines managed greedy algorithms with distributed FL. This approach aims to safeguard users' privacy while ensuring enhanced QoS. The PSP design utilizes distributed FL to gain an understanding of users' preferences, employing a greedy algorithm to address the optimization challenge. The outcomes of the simulation experiments demonstrated that the PSP algorithm effectively safeguards users' privacy while fulfilling their service requirements by reducing the service load on the remote cloud. The outcomes of the simulation experiments substantiated that the PSP algorithm successfully ensures the privacy of users while fulfilling their service requirements needs by mitigating the service load on the remote cloud. However, the PSP design might face scalability issues when applied to larger, more complex networks.

Majeed et al. introduced FLchain in their paper [162], presenting a blockchain-powered framework designed to bolster the security of FL. The researchers employed channels to store numerous global models (GM). The researchers leveraged blockchain technology to store the local model parameters for every global iteration, documenting them as blocks on the channel-specific ledger. The concept of "the global model state trie" was introduced by the researchers. The trie plays a crucial role in storing and regularly updating the global model on the blockchain network. It achieves this by combining the individual model updates received from MDs. By a qualitative evaluation, the authors showcased the resilience of FLchain compared to standard FL approaches. FLchain guarantees the soundness of the FL model by preserving its provenance and enabling auditable features in an immutable fashion. Nevertheless, the efficacy of the suggested methodology depends on the dependability and credibility of the corresponding EDs when communicating transactions to the blockchain network. Nonetheless, the FLchain framework's performance could be affected by inherent blockchain limitations like transaction latency and scalability challenges in larger networks.

In [163], Yang et al. explained a design according to FL for controlling the power and local computing in a MEC system, aiming to minimize general power usage. The authors demonstrated that in scenarios involving maximum power transmission, the optimal solution lies in either the execution at the local or full offloading modes. They also provided analytical expressions for energy consumption. Usually, the objective function comprises a non-convex rate expression, which is streamlined through the implementation of the alternative optimization technique. The suggested design according to FL optimizes local computing and transmission power collaboratively. It effectively decreases energy consumption by leveraging the capabilities of the local devices and the communication channel's capacity. The design outperforms standard benchmarks, demonstrating at least a minimal improvement according to the numerical results, which suggest successful integration. Although this research significantly contributes to advancing energy-efficient FL in MEC systems, it does not consider the impact of potential network latency on the proposed energy-efficient design. In other paper, He et al. proposed an innovative federated optimization algorithm, named Adp-FedProx, in [164]. This was developed to maximize learning efficiency within the restrictive computation and communication resources found at the network periphery. The algorithm operates dynamically, modifying the precision of every client's localized solution as well as the count of local iterations within each global interval. Such a design ensures inclusive participation of all users in the training procedure, while also safeguarding model convergence. Their approach focuses on narrowing the discrepancy between the final loss function and the optimal one, working within the confines of the available resources to ensure peak learning performance. An innovative bound on the convergence of federated training loss in heterogeneous IoT contexts is also presented. They analyze the impact of global update frequency, time spent, and energy allocated for learning on the training loss per user. Experimental tests suggests that their proposed model can speed up FL and reduce energy utilization in training in comparison to FedProx, all the while taking into account heterogeneity and limited resource allocation. When matched against the same training duration as FedProx, Adp-FedProx attains a more precise model. However, Adp-FedProx's effectiveness might diminish in scenarios of extreme heterogeneity or when network instability affects communication between clients.

Finally, in [165], Wang et al. presented a method for safeguarding indoor positioning privacy, grounded in FL within a MEC setting. They undertook a comprehensive analysis and subsequent mathematical representation of the learning mechanisms of horizontal, vertical, and transfer FL. To mitigate potential data leakage threats, the incorporation of differential privacy was proposed. They then forwarded an indoor positioning privacy preservation model, premised on FL and corresponding algorithms within the MEC environment, aiming to enhance positioning performance, bolster privacy safeguards, and manage resource overhead. The proposed algorithm's performance was evaluated through simulation experiments, during which it was juxtaposed against three other algorithms using two analogous datasets. The findings suggested that the proposed algorithm outperformed in terms of convergence speed, time expenditure on localization, and localization accuracy, delivering an ultimate positioning accuracy and an average positioning time. However, the scheme may struggle to maintain privacy safeguards when faced with complex adversarial attacks, an aspect not thoroughly analyzed in the study. Table 6 compares neural network, deep neural network, and Table 7 outlines other schemes, detailing their performance across parameters like accuracy, loss, and privacy, and covering their applications, simulators used, data types, and deployment strategies.

5. Discussion

This section aims to address the research inquiries outlined in Section 2 while exploring various related issues. The findings here are anticipated to help identify new opportunities and ongoing challenges in merging MEC with FL. In synthesizing the findings from our comprehensive review, the assessment revealed a focus on specific operational tactics like resource allocation and data offloading, which reflect prevailing trends in Federated Learning and Mobile Edge Computing integration. This focus underscores the prevalent research direction and points to the potential efficiencies these tactics bring to IoT and MEC frameworks. The selection of these focal areas, while not indicative of bias, helps to highlight areas where significant contributions can be made. Variations in study outcomes are largely attributed to different architectural configurations and simulation tools, suggesting that enhancements in these areas could refine validation processes. The effectiveness of the methods reviewed, which have been tested in various simulation environments, supports well-known theories that show distributed architectures are effective at managing Federated Learning tasks in Mobile Edge Computing settings. Consistency across different data collection methods further supports the reliability of our conclusions, demonstrating a clear trajectory towards optimized resource management and system scalability.

In our detailed review, we explored how different FL frameworks are used in MEC settings and identified important trends. As depicted in Fig. 15, we identified four main operational tactics, with resource allocation being the most common at 46 %, followed by offloading at 27 %, scheduling at 19 %, and load balancing at 8 %. Resource allocation is crucial for efficiently distributing computing resources among FL participants, thereby improving collective learning efforts. Offloading, meanwhile, utilizes additional computing power to reduce the load on IoT devices. Though not as prevalent, scheduling and load balancing are vital for the effective management of tasks and even distribution of workloads.

Our systematic review explored various strategies used within the FL frameworks across different MEC settings. Specifically, as illustrated in Fig. 16, our analysis showed that 20 % of the frameworks utilized a Distributed Edge Device strategy, 60 % implemented a Distributed Edge Server strategy, and the remaining 20 % opted for a Centralized strategy. These findings emphasize the variety of

Table 6
Properties of the neural network, deep neural network, and other schemes. See references [122-126,130,160-162,166]

Ref	Operation methods				Security			Application				Cloud		Approach			Datasets			Simulator			Evaluation Parameters						
	Offloading	Scheduling	Load balancing	Resource allocation	Blockchain	Intrusion detection	Secure aggregation	Other	IoV	IoT	UAV	Without Cloud	With Cloud	Centralized	Distributed Edge Server	Distributed Edge Device	Benchmark	Real-world	Synthetic	NA	Python	MATLAB	Reward	Energy	Cost	Privacy	Delay	Loss	Accuracy
[122]			✓				✓			✓		✓			✓		✓			✓						✓			✓
[123]				✓			✓			✓			✓		✓		✓			✓					✓	✓		✓	✓
[124]				✓			✓	✓					✓			✓	✓				✓					✓		✓	
[125]	✓						✓			✓			✓		✓		✓			✓						✓			✓
[126]							✓			✓			✓			✓	✓				✓					✓			✓
[130]		✓					✓			✓			✓		✓		✓				✓					✓		✓	✓
[166]	✓						✓			✓			✓		✓		✓				✓					✓			✓
[160]				✓			✓			✓		✓		✓							✓				✓	✓			
[161]	✓									✓			✓			✓				✓						✓			
[162]					✓					✓		✓				✓				✓						✓			

Table 7
Properties of the FL schemes. See references [163-165]

Ref	Operation methods					Security			Application				Cloud		Approach			Datasets			Simulator			Evaluation Parameters						
	Power consumption	Offloading	Scheduling	Load balancing	Resource allocation	Blockchain	Intrusion detection	Secure aggregation	Other	IoV	IoT	UAV	Without Cloud	With Cloud	Centralized	Distributed Edge Server	Distributed Edge Device	Benchmark	Real-world	Synthetic	NA	Python	MATLAB	Reward	Energy	Cost	Privacy	Delay	Loss	Accuracy
[163]	✓	✓						✓			✓		✓		✓						✓				✓		✓			
[164]					✓			✓			✓		✓			✓		✓				✓					✓		✓	✓
[165]								✓			✓			✓		✓			✓			✓					✓			✓

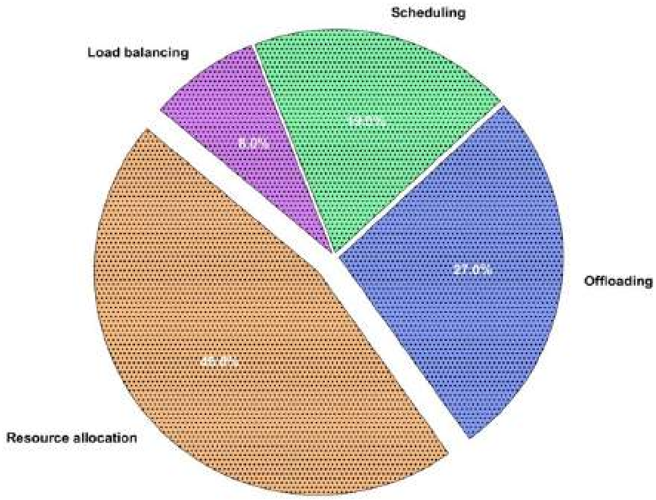

Fig. 15. Applied operation methods.

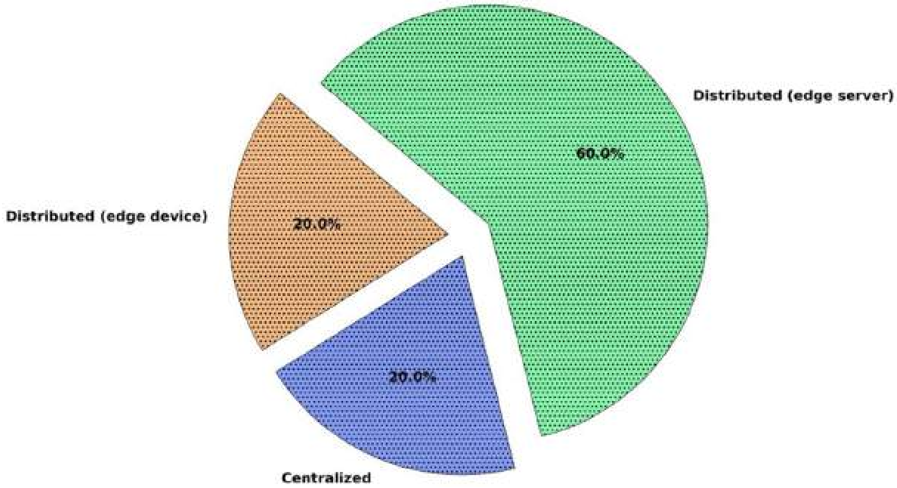

Fig. 16. Applied approaches.

strategies used in FL deployments across the IoT and MEC fields, where researchers clearly favor using distributed edge server setups. The distribution of these strategies enriches our comprehension of how FL is deployed in such contexts and points to potential avenues for further research and enhancement.

Fig. 17 displays the count of frameworks that have implemented various algorithms within the FL workflow. According to this figure, the majority of the examined frameworks prefer RL and DL techniques. RL models tend to yield favorable outcomes in distributed settings, like the 2-tier or 3-tier architectures employed in the frameworks under study. Similarly, DL techniques are effective in classification tasks and are widely used by numerous frameworks to tailor FL for the MEC context.

As previously mentioned, the FL frameworks proposed for MECs adhere to either a 2-tier or 3-tier structural design. Our analysis, depicted in Fig. 18, shows that 56 % of the frameworks employ a two-tier architecture, facilitating FL interactions between IoT devices and MECs. On the other hand, 44 % of the approaches utilize a 3-tier architecture, incorporating an IoT layer, a MEC layer, and a cloud computing layer into the FL processes. In such frameworks, the aggregation function typically resides in the cloud computing layer, leveraging its computational capacity for the aggregation task. Due to the additional computational resources provided by cloud data centers, 3-tier architectures can manage more complex classifiers and models, and support a larger number of participants.

Fig. 19 illustrates the different settings that the reviewed methodologies cater to. According to this figure, a significant 68 % of the frameworks are tailored for IoT applications, while 12 % are designated for IIoT environments. Additionally, UAV-based settings are the focus of 6 % of the frameworks. Furthermore, 4 % are developed for Internet of Vehicles (IoV) contexts, and another 4 % are dedicated to applications within smart homes and cities.

As depicted in Fig. 20, 44 % of these frameworks were implemented using the Python programming language, while 6 % took

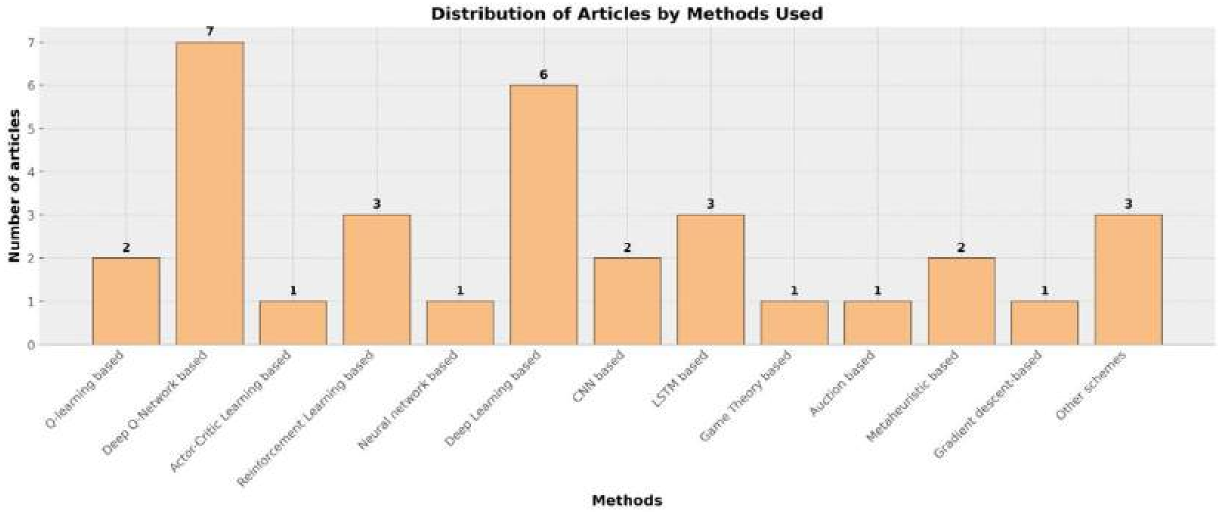

Fig. 17. Utilized algorithms.

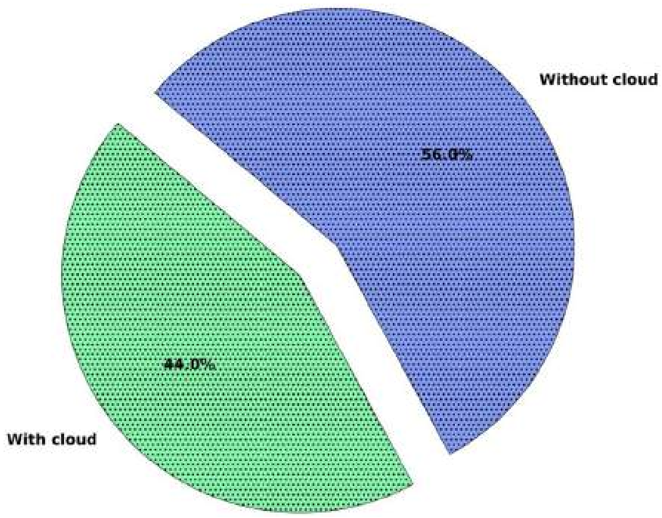

Fig. 18. Organization of schemes architecture.

advantage of the MATLAB software tool. However, half of the frameworks did not disclose the tools they used, casting a significant shadow on the transparency of their results. This lack of transparency is a concern that needs to be addressed, as it can affect the reliability and reproducibility of the outcomes. Moreover, none of the FL frameworks under review employed specialized simulators tailored for IoT and MEC environments, complicating the simulation of FL processes in MEC contexts. Therefore, there's a clear need for the creation of dedicated simulation tools in the future. These tools should be capable of accommodating various ML algorithms, including FL, and provide FL developers with pre-set and standardized aggregation techniques. They should also be versatile enough to support different IoT and MEC environments, as well as various cloud computing technologies, enabling the simulation of both 2-tier and 3-tier FL frameworks.

Fig. 21 outlines the metrics utilized to assess the FL frameworks under investigation. The figure shows that these frameworks mainly concentrate on assessing metrics like accuracy, energy efficiency, cost, and latency. However, the performance evaluations conducted by these studies tend to be limited, often only addressing specific aspects of their proposed solutions without providing a comprehensive assessment of all features. While evaluating FL frameworks is inherently complex, a thorough evaluation should encompass a broad spectrum of issues, including the model's performance, security, reliability, and various overheads. For a holistic assessment, a diverse set of metrics is essential, as focusing solely on accuracy is insufficient for system-wide evaluations. It's important to consider the total computational, communicational, and storage burdens, which encompass the FL system's intrinsic overheads and those associated with security protocols and infrastructure required for secure FL operations. Despite this, as indicated in Fig. 14, overheads have not been prominently featured in the quantitative analyses of the proposed frameworks, highlighting an area for

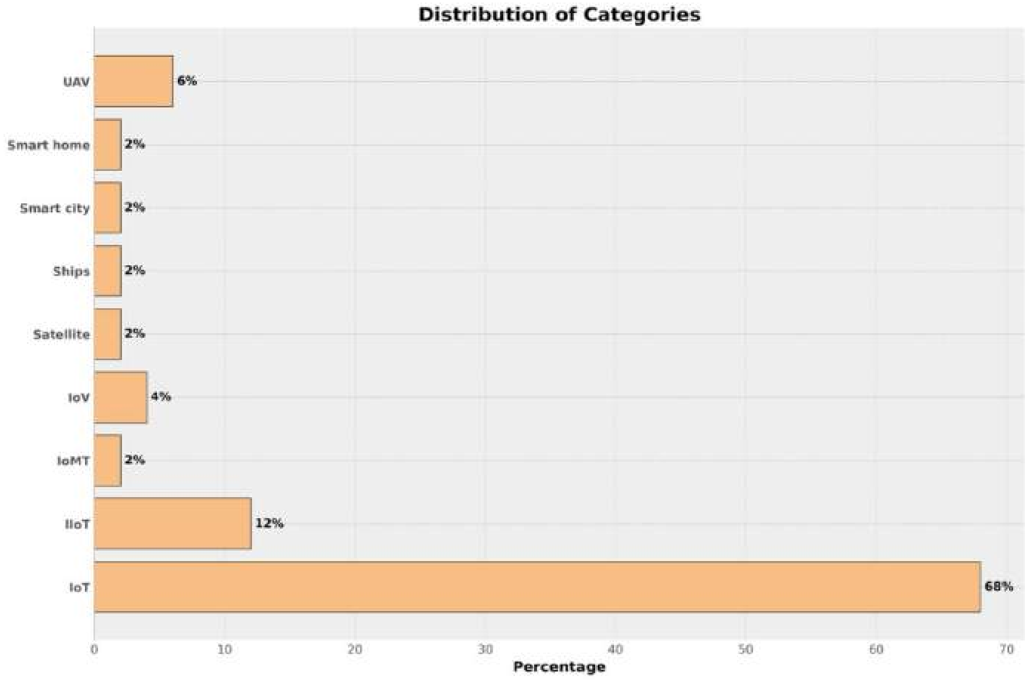

Fig. 19. Supporting environments.

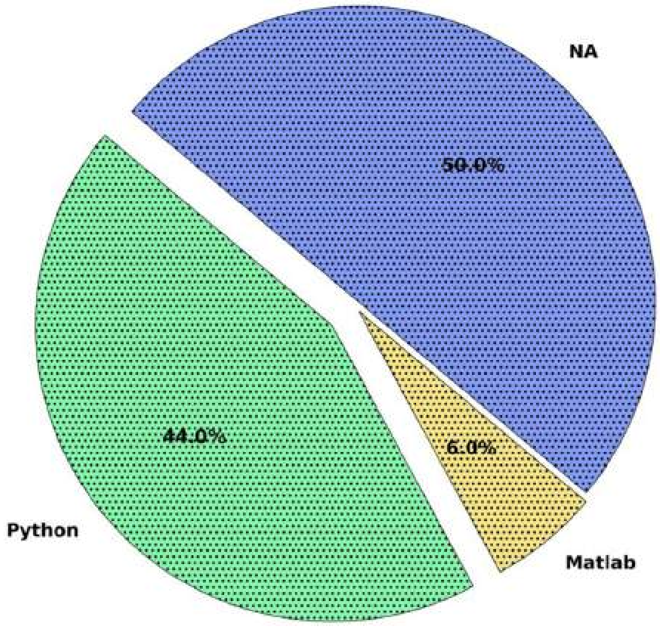

Fig. 20. Simulation tools.

improvement in future FL research.

Considering the intricacies of MEC environments where data is processed at the edge, metrics such as data freshness and context awareness become crucial. These metrics help understand how current and relevant the data processed by FL algorithms remains throughout operations, which is vital for dynamic environments like intelligent cities or real-time health monitoring systems. Additionally, scalability metrics are essential to evaluate how well an FL system can expand in terms of a number of nodes without degrading performance, reflecting the distributed nature of edge computing. Furthermore, resource utilization metrics, which include energy consumption, bandwidth usage, and computational overhead, are vital for assessing the sustainability and efficiency of FL

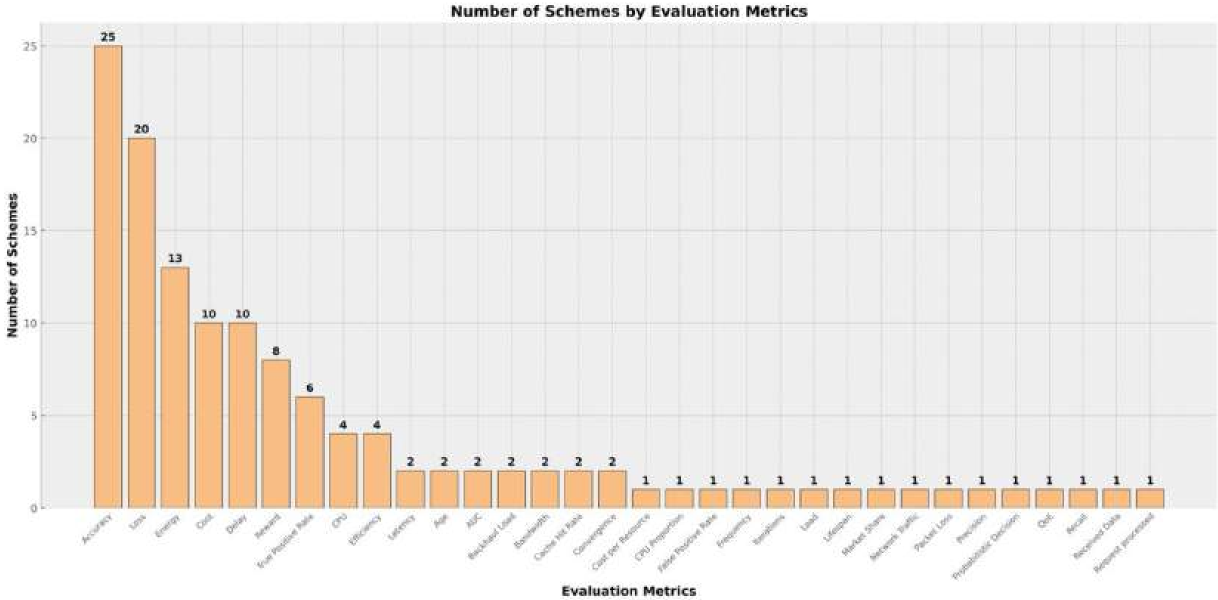

Fig. 21. Evaluation metrics.

implementations in resource-constrained edge devices. Security metrics such as intrusion detection rate and data privacy measures are also paramount, given edge devices' distributed and potentially vulnerable nature. Incorporating these diverse metrics into the evaluation framework will provide a more thorough understanding of the system performance and highlight potential areas for optimization and innovation in FL and MEC integration, guiding future research toward developing more robust, efficient, and secure systems.

Fig. 22 showcases the distribution of datasets utilized across different FL frameworks. According to the figure, popular datasets like MNIST, Real-World, and Cifar-10 are frequently used in these studies. The MNIST dataset, a standard benchmark in DL research, consists of 70,000 images of handwritten digits (0–9) in grayscale, each sized at 28 × 28 pixels, divided into 60,000 training and 10,000 testing images. Similarly, the CIFAR-10 dataset, which is also widely used, comprises 60,000 color images of 32 × 32 pixels, evenly distributed across ten categories, with each category containing 6000 images. This dataset is split into 50,000 training images and 10,000 test images.

This figure also reveals that 91 % of the examined frameworks rely on benchmark datasets, while only 4 % use synthetic datasets and 5 % utilize real-world data. Despite the widespread use of these datasets, there's a call for developing specialized workloads and benchmark datasets tailored to the unique requirements of FL frameworks in emerging domains like IoT and MECs. Additionally, many frameworks limit themselves to one or two datasets designed for specific tasks, highlighting the need for broader testing across diverse

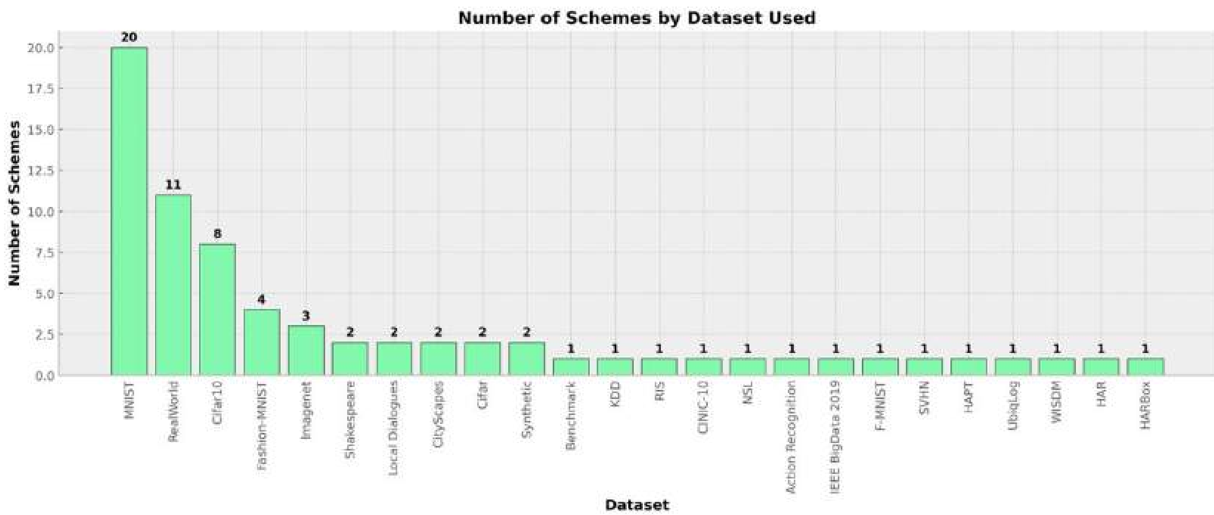

Fig. 22. Applied datasets.

datasets to ensure more comprehensive simulations and performance evaluations of proposed FL solutions.

In the next section, we will propose several gaps that future research should address. This discussion highlights the areas within MEC and FL integration that require further exploration to enhance system effectiveness and reliability. By identifying these gaps, we intend to guide future research directions that could lead to significant advancements in the field, ensuring more robust, scalable, and secure MEC and FL systems.

6. Future directions and challenges

The integration of FL with the MEC and cloud computing signals a transformative phase in distributed learning. However, this integration is accompanied by multifaceted challenges and open issues requiring meticulous exploration and innovative solutions. This section aims to clarify these challenges and propose future research directions to enhance the strength and practicality of MEC-based FL schemes.

6.1. Innovative theoretical frameworks for FL and MEC

FL and MEC involve many interacting components, where devices compute and continuously interact and evolve. Applying complex systems theory could provide new insights into how these interactions can be optimized for better learning outcomes and system robustness. For example, graph theory. Given that FL inherently involves a distributed node network, graph theory can offer profound advantages. New frameworks could model the FL process as a graph, where nodes represent devices and edges represent communication paths. This approach can optimize data flow and learning processes based on the properties of the graph, such as centrality and connectivity.

6.2. Quantum ML algorithms

Integrating quantum computing principles with FL could potentially lead to significant processing speed and security advancements. Quantum algorithms could enhance the encryption methods used in FL, making the model updates faster and more secure against cyber threats.

6.3. Federated transfer learning algorithms

These algorithms could be particularly beneficial in environments with diverse data distributions across devices. Federated transfer learning can leverage pre-trained models on related tasks to enhance learning efficiency and effectiveness in new but similar environments.

6.4. Meta-Learning algorithms in FL

Meta-learning approaches can be adapted for FL to enable models to learn how to learn effectively from decentralized data sources. These algorithms could quickly adjust to new data or tasks with minimal data transfer, which is crucial for MEC scenarios where bandwidth and latency are concerns.

6.5. Expanding learning paradigms

The current landscape of FL predominantly revolves around supervised learning, leaving semi-supervised and unsupervised learning paradigms underexplored in the context of IoT and MEC. The scarcity of labeled data in various applications underscores the necessity of integrating these learning paradigms into FL frameworks. Future research should delve into novel methodologies that combine semi-supervised or unsupervised learning with FL, potentially reducing reliance on labeled datasets and enhancing the versatility and applicability of FL in diverse domains.

6.6. Architectural evolution of FL

Much FL research has been anchored in centralized architectures characterized by a singular aggregator node orchestrating the learning process. While this centralized approach simplifies the aggregation of model updates, it raises concerns regarding scalability, reliability, and security. Future studies should venture into decentralized or federated architectures, exploring the dynamics of multiple collaborative aggregators and peer-to-peer learning models. Such architectural innovations could offer enhanced fault tolerance, scalability, and resistance to adversarial attacks, paving the way for more resilient FL systems.

6.7. Strengthening system reliability

The reliability of FL systems, particularly those following to centralized architectures, is important, especially in scenarios where FL is deployed for industrial or mission-critical purposes. The literature lacks comprehensive strategies for addressing potential faults within aggregator nodes, an oversight that could lead to significant disruptions. Future work should incorporate advanced fault tolerance mechanisms, such as sophisticated checkpointing and replication strategies, to ensure the continuity and integrity of the FL process, even in the face of hardware failures, network disruptions, or malicious attacks.

6.8. Advancing security measures

As FL systems become increasingly integrated with IoT and MEC environments, they become vulnerable to many security threats. Future FL frameworks must prioritize developing and integrating advanced security measures to safeguard against a spectrum of cyber threats, including but not limited to DDoS attacks, man-in-the-middle attacks, data poisoning, and model inversion attacks. Given the constrained resources typical of IoT devices and MEC nodes, these security solutions must be designed to be resource-efficient, ensuring that they do not overly burden the system while providing robust protection. For instance, homomorphic encryption allows FL nodes to train models on encrypted data, providing privacy without compromising the learning process. Moreover, integrating blockchain technology could further enhance security by creating decentralized and transparent logs of model updates, making unauthorized alterations easily detectable. These measures protect data integrity and ensure compliance with stringent privacy regulations such as GDPR.

6.9. Adaptive and compliant Fl frameworks

The adherence to regulatory standards, data privacy laws, and organizational policies is increasingly critical in deploying FL systems. Future FL schemes must be inherently adaptable and capable of operating within the stringent confines of legal and regulatory frameworks. This includes ensuring data privacy, securing data transmission, and adhering to cross-border data-sharing regulations. Research should focus on developing FL frameworks that are not only technologically advanced but also compliant with existing and emerging regulations, ensuring that FL deployments are both practical and legally sound.

6.10. Energy-Efficient FL implementations

The energy consumption of FL processes, especially in resource-constrained IoT and MEC environments, is a critical concern that requires further investigation. Future research should explore energy-efficient FL algorithms and communication protocols that minimize energy usage without compromising the learning performance. This includes the development of lightweight model architectures, efficient data compression techniques, and energy-aware resource allocation strategies.

6.11. Human-in-the-loop FL systems

Integrating human feedback and expertise into the FL process can significantly enhance the quality and reliability of the learned models. Future FL systems could benefit from human-in-the-loop approaches, where human experts periodically review and adjust model parameters, provide additional annotations, or validate model outputs. This collaboration between human expertise and automated learning processes could lead to more accurate, reliable, and interpretable FL models, particularly in complex or sensitive applications.

6.12. Interoperability and standardization

A critical challenge emerges as FL continues to evolve: the lack of compatibility among diverse FL frameworks and the absence of standardized protocols. This can hinder seamless collaboration between different systems and devices, particularly in heterogeneous IoT and MEC environments. Future research should focus on developing standardized FL protocols and interfaces that ensure compatibility across various platforms and devices, facilitating easier integration and broader adoption of FL technologies.

6.13. Scalability in heterogeneous networks

The scalability of FL systems in heterogeneous networks, where devices vary widely in terms of computational capabilities, network connectivity, and energy resources, remains a significant challenge. Future works should explore scalable FL algorithms that can efficiently handle the dynamic nature of IoT and MEC networks, ensuring that all devices, regardless of their capabilities, can participate in the learning process without overwhelming the network or degrading the overall system performance.

6.14. Personalization and fairness

While FL aims to develop generalized models, the need for personalized models that cater to specific user preferences or regional characteristics is becoming increasingly evident. Future studies should investigate mechanisms for achieving model personalization within FL frameworks, ensuring that the learning process accounts for individual differences. Addressing algorithmic fairness to prevent biases in the learned models is crucial, ensuring equitable model performance across diverse user groups and scenarios.

6.15. Dynamic data and concept drift

In many real-world applications, the underlying data distribution can change over time, a phenomenon known as concept drift. This challenges FL systems, as models may become outdated or less accurate as the data evolves. Future research should develop strategies for detecting and adapting to concept drift within FL systems, ensuring that models remain relevant and precise over time.

6.16. Integration with edge AI

The convergence of FL with Edge AI presents a promising avenue for enabling intelligent decision-making at the network edge. Future research should explore integrated frameworks that leverage FL for model training and Edge AI for real-time inference, optimizing computational resources and reducing latency in decision-making processes.

6.17. Incentive mechanisms for participant engagement

Maintaining sustained participant engagement in FL processes is critical for continuous model improvement. Future work should design effective incentive mechanisms that motivate users and devices to contribute their data and computational resources to FL tasks, ensuring a diverse and representative dataset for model training.

6.18. Robustness to adversarial attacks

As FL systems become more prevalent, they become attractive targets for adversarial attacks that aim to compromise model integrity or steal sensitive information. Future research must prioritize the development of robust defense mechanisms against such attacks, ensuring the integrity and confidentiality of FL models and participant data.

6.19. Environmental impact and sustainability

The environmental impact of deploying large-scale FL systems, particularly regarding energy consumption and carbon footprint, is an emerging concern. Future research should advocate for sustainable FL practices, optimizing energy usage and leveraging renewable energy sources where possible to minimize the environmental impact of FL deployments.

Addressing these complex challenges and investigating various future possibilities will be important for the progress of FL and MEC. This will help ensure that it keeps up with current technological and operational needs while considering wider societal, ethical, and environmental factors.

7. Conclusion

This review paper systematically explores the integration of FL with MEC, an area rich with innovation but also facing significant challenges in efficiency, privacy, and scalability. Our study shows substantial progress in refining FL frameworks and enhancing data security. However, important issues remain unresolved, such as the need for interoperable standards and effective management of dynamic data landscapes. Future research needs to focus on developing adaptable and robust architectural designs. This includes implementing advanced security protocols and integrating sustainable practices considering environmental impacts. Developing FL systems that are not only effective but also capable of functioning across diverse platforms is critical. These systems are poised to significantly influence distributed learning paradigms and the broader IoT and MEC ecosystems. Although the path forward is complex, it presents significant potential benefits that could fundamentally enhance how distributed computing is performed.

Author statement

Dear Prof. Eduardo Cabal-Yepez
Editor-in-Chief of the Computers and Electrical Engineering

As the corresponding author, I confirm that this manuscript, 'The Role of Mobile Edge Computing in Advancing Federated Learning Algorithms and Techniques: A Systematic Review of Applications, Challenges, and Future Directions,' is an original work. It has not been published previously nor is it under consideration elsewhere. All authors have contributed significantly to the research and are in agreement with the content of the manuscript. We have no conflicts of interest to declare.

Let me know if you need any further modifications!

Sincerely,

Mehdi Hosseinzadeh
Director, DTU AI & Data Science Hub (DAIDASH), Duy Tan University
mehdihosseinzadeh@duytan.edu.vn

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to

influence the work reported in this paper.

Acknowledgment

This study is supported via funding from Prince Satam bin Abdulaziz University project number (PSAU/2024/R/1446).

The authors extend their appreciation to the Deanship of Research and Graduate Studies at King Khalid University for funding this work through Large Research Project under grant number RGP2/384/45.

Data availability

No data was used for the research described in the article.

References

[1] Ahmed SF, et al. Towards a secure 5G-enabled internet of things: A survey on requirements, privacy, security, challenges, and opportunities, 12. IEEE Access; 2024. p. 13125–45.
[2] Gharehchopogh FS, et al. A multi-objective mutation-based dynamic Harris Hawks optimization for botnet detection in IoT. Internet Things 2023;24:100952.
[3] Humayun M, et al. Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey. IEEE Access 2024;12:25469–90.
[4] Alwahedi F, et al. Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. Internet Things Cyber-PhysSyst 2024;4:167–85.
[5] Katal A, Dahiya S, Choudhury T. Energy efficiency in cloud computing data centers: A survey on software technologies. Clust Comput 2023;26(3):1845–75.
[6] Indrason N, Saha G. Exploring Blockchain-driven security in SDN-based IoT networks. J Network Comput Appl 2024;224:103838.
[7] Moghaddasi K, Masdari M. Blockchain-driven optimization of IoT in mobile edge computing environment with deep reinforcement learning and multi-criteria decision-making techniques. Cluster Comput 2023;27:4385–413.
[8] Asghari A, Sohrabi MK. Server placement in mobile cloud computing: A comprehensive survey for edge computing, fog computing and cloudlet. Comput Sci Rev 2024;51:100616.
[9] Dhar S, et al. Securing IoT devices: A novel approach using blockchain and quantum cryptography. Internet Things 2024;25:101019.
[10] Moghaddasi K, Rajabi S, Gharehchopogh FS. Multi-Objective Secure Task Offloading Strategy for Blockchain-Enabled IoV-MEC Systems: A Double Deep Q-Network Approach. IEEE Access 2024;12:3437–63.
[11] Moghaddasi K, Rajabi S. Double Deep Q-Learning Networks for Energy-Efficient IoT Task Offloading in D2D MEC Environments. In: 2023 7th International Conference on Internet of Things and Applications (IoT). IEEE; 2023. p. 1–6.
[12] Moghaddasi K, Rajabi S, Gharehchopogh FS. Multi-Objective Secure Task Offloading Strategy for Blockchain-Enabled IoV-MEC Systems: A Double Deep Q-Network Approach. IEEE Access 2024;12:3437–63.
[13] Choudhury A, Ghose M, Islam A. Machine learning-based computation offloading in multi-access edge computing: A survey. J Syst Architecture 2024;148: 103090.
[14] Moghaddasi K, et al. An Energy-Efficient Data Offloading Strategy for 5G-Enabled Vehicular Edge Computing Networks Using Double Deep Q-Network. Wirel Pers Commun 2023;133(3):2019–64.
[15] Alkaabi S, Gregory M, Li S. Multi-Access Edge Computing Handover Strategies, Management, and Challenges: A Review. IEEE Access 2024;12:4660–73.
[16] Hasan MK, et al. Federated Learning for Computational Offloading and Resource Management of Vehicular Edge Computing in 6G-V2X Network. IEEE Trans Consum Electron 2024;70:3827–47.
[17] Moghaddasi K, Rajabi S, Gharehchopogh FS. An enhanced asynchronous advantage actor-critic-based algorithm for performance optimization in mobile edge computing -enabled internet of vehicles networks. Peer Peer Netw Appl 2024;17:1169–89.
[18] Xie X, et al. A survey on vulnerability of federated learning: A learning algorithm perspective. NeuroComput 2024;573:127225.
[19] Ahmed M, et al. A survey on vehicular task offloading: Classification, issues, and challenges. J King Saud University-Comput Inf Sci 2022;34(7):4135–62.
[20] Li L, et al. A review of applications in federated learning. Comput Ind Eng 2020;149:106854.
[21] Lim WYB, et al. Federated learning in mobile edge networks: A comprehensive survey. IEEE Commun Surv Tutorials 2020;22(3):2031–63.
[22] Li Q, et al. A survey on federated learning systems: vision, hype and reality for data privacy and protection. IEEE Trans Knowl Data Eng 2021;35:3347–66.
[23] Kaur MJJECFHtR. A comprehensive survey on architecture for big data processing in mobile edge computing environments. Edge Comput 2019:33–49.
[24] Abreha HG, Hayajneh M, Serhani MA. Federated learning in edge computing: A systematic survey. Sensors 2022;22(2):450.
[25] Brecko A, et al. Federated Learning for Edge Computing: A Survey. Appl Sci 2022;12(18):9124.
[26] Duan Q, et al. Combining Federated Learning and Edge Computing Toward Ubiquitous Intelligence in 6G Network: challenges, Recent Advances, and Future Directions. IEEE Commun Surv Tutorials 2023;25(4):2892–950.
[27] Abimannan S, et al. Towards Federated Learning and Multi-Access Edge Computing for Air Quality Monitoring: Literature Review and Assessment. Sustainability 2023;15(18):13951.
[28] Yan K, et al. A survey of energy-efficient strategies for federated learning inmobile edge computing. Frontiers Inf Technol Electron Eng 2024;25(5):645–63.
[29] Nguyen DC, et al. Federated learning meets blockchain in edge computing: Opportunities and challenges. IEEE Internet Things J 2021;8(16):12806–25.
[30] Lim WYB, et al. Federated learning in mobile edge networks: A comprehensive survey. IEEE Commun Surv Tutorials 2020;22(3):2031–63.
[31] Zhu C, et al. Blockchain-enabled federated learning for uav edge computing network: issues and solutions, 10. IEEE Access; 2022. p. 56591–610.
[32] Ko S, et al. Asynchronous federated learning with directed acyclic graph-based blockchain in edge computing: Overview, design, and challenges. Expert Syst Appl 2023;223:119896.
[33] Liao B, et al. Security analysis of IoT devices by using mobile computing: A systematic literature review. IEEE Access 2020;8:120331–50.
[34] Carvalho G, et al. Edge computing: Current trends, research challenges and future directions. Comput 2021;103:993–1023.
[35] Nguyen DC, et al. Federated learning meets blockchain in edge computing: Opportunities and challenges. IEEE Internet Things J 2021;8(16):12806–25.
[36] Huang S-Y, et al. A Survey on Resource Management for Cloud Native Mobile Computing: Opportunities and Challenges. Symmetry (Basel) 2023;15(2):538.
[37] Signoretti G, et al. An evolving tinyml compression algorithm for iot environments based on data eccentricity. Sensors 2021;21(12):4153.
[38] Shuja J, et al. Applying machine learning techniques for caching in next-generation edge networks: A comprehensive survey. J Network Comput Appl 2021; 181:103005.
[39] Ghaznavi M, et al. Content delivery network security: A survey. IEEE Commun Surv Tutorials 2021;23(4):2166–90.
[40] Hoque MA, et al. Context-driven encrypted multimedia traffic classification on mobile devices. Pervasive Mob Comput 2022;88:101737.
[41] Mahmood A, et al. Weighted utility aware computational overhead minimization of wireless power mobile edge cloud. Comput Commun 2022;190:178–89.
[42] Tun YK, et al. Energy-efficient resource management in UAV-assisted mobile edge computing. IEEE Commun Letters 2020;25(1):249–53.
[43] Cui Y-y, et al. A novel offloading scheduling method for mobile application in mobile edge computing. Wireless Networks 2022;28(6):2345–63.
[44] Koe ASV, Lin YJP, Computing M. Offline privacy preserving proxy re-encryption in mobile cloud computing. Pervasive Mob Comput 2019;59:101081.
[45] Ferrag MA, et al. Authentication and authorization for mobile iot devices using biofeatures: recent advances and future trends. Security and communication networks; 2019. 2019.

[46] Zaman SKu, et al. LiMPO: Lightweight mobility prediction and offloading framework using machine learning for mobile edge computing. Cluster Comput 2023;26(1):99–117.
[47] Sarker HJScs. Machine learning: Algorithms, real-world applications and research directions. SN Comput Sci 2021;2(3):160.
[48] Jiang T, Gradus JL, Rosellini AJJBT. Supervised machine learning: a brief primer. Behav Ther 2020;51(5):675–87.
[49] Boobalan P, et al. Fusion of federated learning and industrial Internet of Things: A survey. Comput Netw 2022;212:109048.
[50] Wahab OA, et al. Federated machine learning: survey, multi-level classification, desirable criteria and future directions in communication and networking systems. IEEE Commun Surv Tutorials 2021;23(2):1342–97.
[51] Unal D, et al. Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things. Comput Secur 2021;109:102393.
[52] Jahromi AN, Karimipour H, Dehghantanha A. An ensemble deep federated learning cyber-threat hunting model for Industrial Internet of Things. Comput Commun 2023;198:108–16.
[53] Merin Joshiba J, Judson D, Bhaskar V. A Comprehensive Review on NOMA Assisted Emerging Techniques in 5G and Beyond 5G Wireless Systems. Wirel Pers Commun 2023;130:2385–405.
[54] Khan M, Glavin FG, Nickles M. Federated Learning as a Privacy Solution - An Overview. Procedia Comput Sci 2023;217:316–25.
[55] Wen J, et al. A survey on federated learning: challenges and applications. Int J Mach Learn Cybern 2023;14(2):513–35.
[56] Issa W, et al. Blockchain-Based Federated Learning for Securing Internet of Things: A Comprehensive Survey. ACM Comput Surv 2023;55(9):1–43.
[57] Qi P, et al. Model aggregation techniques in federated learning: A comprehensive survey. Future Gen Comput Syst 2024;150:272–93.
[58] Beltrán ETM, et al. Decentralized Federated Learning: Fundamentals, State of the Art, Frameworks, Trends, and Challenges. IEEE Commun Surv Tutorials 2023;25(4):2983–3013.
[59] Chen H, et al. Privacy and Fairness in Federated Learning: On the Perspective of Tradeoff. ACM Comput Surv 2023;56(2):1–37.
[60] Xu C, et al. Asynchronous federated learning on heterogeneous devices: A survey. Comput Sci Rev 2023;50:100595.
[61] Alotaibi B, Khan FA, Mahmood S. Communication Efficiency and Non-Independent and Identically Distributed Data Challenge in Federated Learning: A Systematic Mapping Study. Applied Sci 2024;14(7):2720.
[62] Neto HNC, et al. A survey on securing federated learning: analysis of applications, attacks, challenges, and trends, 11. IEEE Access; 2023. p. 41928–53.
[63] Guendouzi BS, et al. A systematic review of federated learning: Challenges, aggregation methods, and development tools. J Network Comput Appl 2023;220: 103714.
[64] Pfeiffer K, et al. Federated Learning for Computationally Constrained Heterogeneous Devices: A Survey. ACM Comput. Surv. 2023;55(14s):1–27.
[65] Han Q, et al. Privacy preserving and secure robust federated learning: A survey. Concurrency Comput 2024;36:e8084.
[66] Coelho KK, et al. A survey on federated learning for security and privacy in healthcare applications. Comput Commun 2023;207:113–27.
[67] Brecko A, et al. Federated Learning for Edge Computing: A Survey. Applied Sci 2022;12(18):9124.
[68] Varghese B, et al. Challenges and opportunities in edge computing. In: 2016 IEEE international conference on smart cloud (SmartCloud). IEEE; 2016. p. 20–6.
[69] Zhang J, et al. Energy-latency tradeoff for energy-aware offloading in mobile edge computing networks. IEEE Internet Things J 2017;5(4):2633–45.
[70] Xia J, et al. Opportunistic access point selection for mobile edge computing networks. IEEE Trans Wirel Commun 2020;20(1):695–709.
[71] Zhang C, et al. A survey on federated learning. Knowl Based Syst 2021;216:106775.
[72] Abreha HG, Hayajneh M, Serhani MAJS. Federated learning in edge computing: a systematic survey. Sensors 2022;22(2):450.
[73] Ma X, Sun H, Hu RQ. Scheduling policy and power allocation for federated learning in NOMA based MEC. In: GLOBECOM 2020-2020 IEEE Global Communications Conference. IEEE; 2020. p. 1–7.
[74] Wang X, et al. CFLMEC: Cooperative federated learning for mobile edge computing. In: ICC 2022-IEEE International Conference on Communications. IEEE; 2022. p. 86–91.
[75] Cheng Z, et al. Joint client selection and task assignment for multi-task federated learning in MEC networks. In: 2021 IEEE Global Communications Conference (GLOBECOM). IEEE; 2021. p. 1–6.
[76] Fantacci R, Picano B. Federated learning framework for mobile edge computing networks. CAAI Trans Intell Technol 2020;5(1):15–21.
[77] Cai S, et al. Multi-granularity Weighted Federated Learning in Heterogeneous Mobile Edge Computing Systems. In: 2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS). IEEE; 2022. p. 436–46.
[78] Chen D, et al. Matching-theory-based low-latency scheme for multitask federated learning in MEC networks. IEEE Internet Things J 2021;8(14):11415–26.
[79] Zhang W, et al. Client selection for federated learning with non-iid data in mobile edge computing. IEEE Access 2021;9:24462–74.
[80] Zhang X, et al. D2D-assisted federated learning in mobile edge computing networks. In: 2021 IEEE Wireless Communications and Networking Conference (WCNC). IEEE; 2021. p. 1–7.
[81] Jing Y, et al. Satellite MEC with Federated Learning: Architectures, Technologies and Challenges. IEEE Netw 2022;36(5):106–12.
[82] Kim J, et al. A novel joint dataset and computation management scheme for energy-efficient federated learning in mobile edge computing. IEEE Wirel Commun Lett 2022;11(5):898–902.
[83] Lin Z, et al. Learning based efficient federated learning for object detection in mec against jamming. In: 2021 IEEE/CIC International Conference on Communications in China (ICCC). IEEE; 2021. p. 115–20.
[84] Liu T, Hu X, Shu T. Assisting Backdoor Federated Learning with Whole Population Knowledge Alignment in Mobile Edge Computing. In: 2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). IEEE; 2022. p. 416–24.
[85] Luo X, Zhao Z, Peng M. Tradeoff between Model Accuracy and Cost for Federated Learning in the Mobile Edge Computing Systems. In: 2021 IEEE Wireless Communications and Networking Conference Workshops (WCNCW). IEEE; 2021. p. 1–6.
[86] Hong W, et al. Optimal design of hybrid federated and centralized learning in the mobile edge computing systems. In: 2021 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE; 2021. p. 1–6.
[87] Ou R, Ayepah–Mensah D, Liu G. MEC-enabled Federated Learning for Network Slicing. In: 2022 International Conference on Computing, Communication, Perception and Quantum Technology (CCPQT). IEEE; 2022. p. 249–54.
[88] Shi T, et al. Task Scheduling with Collaborative Computing of MEC System Based on Federated Learning. In: 2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring). IEEE; 2022. p. 1–5.
[89] Wang X, et al. Distributed Task Scheduling for Wireless Powered Mobile Edge Computing: A Federated-Learning-Enabled Framework. IEEE Netw 2021;35(6): 27–33.
[90] Wang Y, Kantarci B. A novel reputation-aware client selection scheme for federated learning within mobile environments. In: 2020 IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). IEEE; 2020. p. 1–6.
[91] Xu Z, et al. Energy or accuracy? Near-optimal user selection and aggregator placement for federated learning in MEC. IEEE Trans Mob Comput 2023;23(3): 2470–85.
[92] Zhang Y, Zhang X, Cai Y. Multi-task Federated Learning based on Client Scheduling in Mobile Edge Computing. In: 2022 IEEE/CIC International Conference on Communications in China (ICCC). IEEE; 2022. p. 185–90.
[93] Zheng J, et al. Federated learning for energy-balanced client selection in mobile edge computing. 2021 International wireless communications and mobile computing (IWCMC). IEEE; 2021. p. 1942–7.
[94] Nishio T, Yonetani R. Client selection for federated learning with heterogeneous resources in mobile edge. In: ICC 2019-2019 IEEE international conference on communications (ICC). IEEE; 2019. p. 1–7.
[95] Liu J, et al. Enhancing Federated Learning with Intelligent Model Migration in Heterogeneous Edge Computing. In: 2022 IEEE 38th International Conference on Data Engineering (ICDE). IEEE; 2022. p. 1586–97.
[96] Lu Y, et al. Communication-efficient federated learning and permissioned blockchain for digital twin edge networks. IEEE Internet Things J 2020;8(4): 2276–88.

[97] Lu Y, et al. Federated learning for data privacy preservation in vehicular cyber-physical systems. IEEE Netw 2020;34(3):50–6.
[98] Pham Q-V, et al. Aerial access networks for federated learning: Applications and challenges. IEEE Netw 2022;36(3):159–66.
[99] Jing Y, et al. Resource optimization for signal recognition in satellite MEC with federated learning. In: 2021 13th International Conference on Wireless Communications and Signal Processing (WCSP). IEEE; 2021. p. 1–5.
[100] Huang H, et al. Worker-Centric Model Allocation for Federated Learning in Mobile Edge Computing. IEEE Trans Green Commun Netw 2022;7(2):869–80.
[101] Shin A, Lim YJE. Federated-learning-based energy-efficient load balancing for uav-enabled mec system in vehicular networks. Energies (Basel) 2023;16(5):2486.
[102] Zhu Z, et al. Federated multiagent actor–critic learning for age sensitive mobile-edge computing. IEEE Internet Things J 2021;9(2):1053–67.
[103] Xia Q, et al. A survey of federated learning for edge computing: Research problems and solutions. High-Confid Comput 2021;1(1):100008.
[104] Xiong X, et al. Resource allocation based on deep reinforcement learning in IoT edge computing. IEEE J Selected Areas in Commun 2020;38(6):1133–46.
[105] Zhang P, et al. Deep reinforcement learning assisted federated learning algorithm for data management of IIoT. IEEE Trans Industr Inform 2021;17(12):8475–84.
[106] Yang Z, et al. Federated Reinforcement Learning for RIS-Aided Non-Orthogonal Multiple Access MEC. In: 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall). IEEE; 2022. p. 1–5.
[107] Sun W, et al. Accelerating Convergence of Federated Learning in MEC with Dynamic Community. EEE Trans Mobile Comput 2023;23(2):1769–84.
[108] Nie Y, et al. Semi-distributed resource management in UAV-aided MEC systems: A multi-agent federated reinforcement learning approach. IEEE Trans Veh Technol 2021;70(12):13162–73.
[109] Huang X, et al. A reliable and fair federated learning mechanism for mobile edge computing. Comput Netw 2023;226:109678.
[110] Feng L, et al. Two-layered blockchain architecture for federated learning over the mobile edge network. IEEE Netw 2021;36(1):45–51.
[111] Zhang R, et al. Federated deep reinforcement learning for multimedia task offloading and resource allocation in MEC networks. IEICE Trans Commun 2024;E107-B(6):446–57.
[112] Liu S, et al. A Federated learning and deep reinforcement learning-based method with two types of agents for computation offload. Sensors 2023;23(4):2243.
[113] Consul P, et al. Federated reinforcement learning based task offloading approach for MEC-assisted WBAN-enabled IoMT. Alexandria Eng J 2024;86:56–66.
[114] Consul P, et al. A hybrid task offloading and resource allocation approach for digital twin-empowered uav-assisted mec network using federated reinforcement learning for future wireless network. IEEE Trans Consum Electron 2024;70(1):3120–30.
[115] Guo Y, et al. Efficient and flexible management for industrial internet of things: A federated learning approach. Comput Netw 2021;192:108122.
[116] Li J, et al. Task offloading mechanism based on federated reinforcement learning in mobile edge computing. Digit Commun Netw 2022;9(2):492–504.
[117] Li C, Zhang Y, Luo YJIToITS. A federated learning-based edge caching approach for mobile edge computing-enabled intelligent connected vehicles. IEEE Trans Intelligent Transportation Syst 2022;24(3):3360–9.
[118] Zang L, Zhang X, Guo BJIA. Federated deep reinforcement learning for online task offloading and resource allocation in WPC-MEC networks. IEEE Access 2022;10:9856–67.
[119] Li YJE. Federated deep reinforcement learning-based caching and bitrate adaptation for VR panoramic video in clustered MEC networks. Electron (Basel) 2022;11(23):3968.
[120] Zhang H, et al. Adaptive client selection in resource constrained federated learning systems: A deep reinforcement learning approach. IEEE Access 2021;9:98423–32.
[121] Shahidinejad A, et al. Context-aware multi-user offloading in mobile edge computing: A federated learning-based approach. J Grid Comput 2021;19:1–23.
[122] Li Y, et al. Adaptive vertical federated learning via feature map transferring in mobile edge computing. Comput 2022;106:1081–97.
[123] Xu Z, et al. HierFedML: Aggregator placement and UE assignment for hierarchical federated learning in mobile edge computing. EEE Trans Parallel Distributed Syst 2022;34(1):328–45.
[124] Zheng C, et al. Unsupervised recurrent federated learning for edge popularity prediction in privacy-preserving mobile-edge computing networks. IEEE Internet Things J 2022;9(23):24328–45.
[125] Zhang J, et al. An efficient federated learning scheme with differential privacy in mobile edge computing. In: Machine Learning and Intelligent Communications: 4th International Conference, MLICOM 2019. Springer; 2019. p. 538–50. August 24–25Proceedings 4. 2019.
[126] Wu W, et al. Accelerating federated learning over reliability-agnostic clients in mobile edge computing systems. IEEE Trans Parallel Distributed Syst 2020;32(7):1539–51.
[127] Lin Q, et al. Fed-PEMC: A Privacy-Enhanced Federated Deep Learning Algorithm for Consumer Electronics in Mobile Edge Computing. IEEE Trans Consum Electron 2024;70(1):4073–86.
[128] Hammedi W, Brik B, Senouci SMJIToITS. Toward optimal MEC-based collision avoidance system for cooperative inland vessels: A federated deep learning approach. IEEE Trans Intelligent Transportation Syst 2022;24(2):2525–37.
[129] Liu J, et al. Deep federated learning based convergence analysis in relaying-aided MEC-IoT networks. J Eng 2022;(1):8425975. **2022**.
[130] You C, et al. Hierarchical personalized federated learning over massive mobile edge computing networks. IEEE Trans Wirel Commun 2023;22(11):8141–57.
[131] Nguyen MN, et al. Toward multiple federated learning services resource sharing in mobile edge networks. IEEE Trans Mob Comput 2021;22(1):541–55.
[132] He J, et al. AceFL: Federated learning accelerating in 6g-enabled mobile edge computing networks. IEEE Trans Netw Sci Eng 2022;10(3):1364–75.
[133] Zheng X, et al. Mobile edge computing enabled efficient communication based on federated learning in internet of medical things. Wireless Commun Mobile Comput 2021;(1):4410894. 2021.
[134] Zhao Y, et al. Privacy-preserving blockchain-based federated learning for IoT devices. IEEE Internet Things J 2020;8(3):1817–29.
[135] Tang X, et al. Stackelberg game based resource allocation algorithm for federated learning in MEC systems. In: 2023 6th World Conference on Computing and Communication Technologies (WCCCT. IEEE; 2023. p. 7–12.
[136] Jin H, Zhang P, Dong H. Security-aware QoS forecasting in mobile edge computing based on federated learning. In: 2020 IEEE International Conference on Web Services (ICWS). IEEE; 2020. p. 302–9.
[137] Lu Y, et al. Differentially private asynchronous federated learning for mobile edge computing in urban informatics. EE Trans Industrial Informatics 2019;16(3):2134–43.
[138] Chen S, et al. Decentralized federated learning with intermediate results in mobile edge computing. IEEE Trans Mob Comput 2022;23(1):341–58.
[139] Bai Y, et al. Multi-Core federated learning for mobile edge computing platforms. IEEE Internet Things J 2022;10(7):5940–52.
[140] Chen D, et al. FedSVRG based communication efficient scheme for federated learning in MEC networks. IEEE Trans Veh Technol 2021;70(7):7300–4.
[141] Abou El Houda Z, et al. A MEC-based architecture to secure IoT applications using federated deep learning. IEEE Internet Things Magazine 2023;6(1):60–3.
[142] Tu X, et al. Incentive mechanisms for federated learning: from economic and game theoretic perspective. IEEE Trans Cogn Commun Netw 2022;8(3):1566–93.
[143] Abou El Houda Z, et al. When federated learning meets game theory: a cooperative framework to secure iiot applications on edge computing. IEEE Trans Industr Inform 2022;18(11):7988–97.
[144] Lee J, Kim D, Niyato DJIA. A novel joint dataset and incentive management mechanism for federated learning over MEC. IEEE Access 2022;10:30026–38.
[145] Li C, Song M, Luo Y. Federated learning based on Stackelberg game in unmanned-aerial-vehicle-enabled mobile edge computing. Expert Syst Appl 2024;235:121023.
[146] Zeng R, et al. Fmore: An incentive scheme of multi-dimensional auction for federated learning in mec. In: 2020 IEEE 40th international conference on distributed computing systems (ICDCS). IEEE; 2020. p. 278–88.
[147] Li Y, et al. VARF: An incentive mechanism of cross-silo federated learning in MEC. IEEE Internet Things J 2023;10(17):15115–32.
[148] Zhou H, et al. Reverse auction-based computation offloading and resource allocation in mobile cloud-edge computing. IEEE Trans Mob Comput 2022;22(10):6144–59.
[149] Besharati R, Rezvani MH, Sadeghi MMGJJoGC. An incentive-compatible offloading mechanism in fog-cloud environments using second-price sealed-bid auction. J Grid Comput 2021;19:1–29.

[150] Khezr P, Cumpston AJJoES. A review of multiunit auctions with homogeneous goods. J Econ Surv 2022;36(4):1225–47.
[151] Lu R, et al. Auction-Based cluster federated learning in mobile edge computing systems, 34. IEEE Transactions on Parallel and Distributed Systems; 2023. p. 1145–58.
[152] Lu R, et al. Auction-based cluster federated learning in mobile edge computing systems. IEEE Trans Parallel Distributed Syst 2023;34(4):1145–58.
[153] Peres F, Castelli MJAS. Combinatorial optimization problems and metaheuristics: Review, challenges, design, and development. Applied Sci 2021;11(14):6449.
[154] Wong W, Ming CI. A review on metaheuristic algorithms: Recent trends, benchmarking and applications. In: 2019 7th International Conference on Smart Computing & Communications (ICSCC). IEEE; 2019. p. 1–5.
[155] He W, Wu S, Sun J. An effective metaheuristic for partial offloading and resource allocation in multi-device mobile edge computing. In: 2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys). IEEE; 2021. p. 1419–26.
[156] Feng C, et al. Joint optimization of data sampling and user selection for federated learning in the mobile edge computing systems. In: 2020 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE; 2020. p. 1–6.
[157] Feng C, et al. On the design of federated learning in the mobile edge computing systems. IEEE Trans Commun 2021;69(9):5902–16.
[158] Zhu C, Zhu X, Qin T. An efficient privacy protection mechanism for blockchain-based federated learning system in UAV-MEC networks. Sensors 2024;24(5):1364.
[159] Huang X, et al. A reliable and fair federated learning mechanism for mobile edge computing. Comput Netw 2023;226:109678.
[160] Wang H, et al. A federated learning system for target recognition over 5G MEC networks. In: Artificial Intelligence in China: Proceedings of the 3rd International Conference on Artificial Intelligence in China. Springer; 2022. p. 704–11.
[161] Qian Y, et al. Privacy-aware service placement for mobile edge computing via federated learning. Inf Sci (Ny) 2019;505:562–70.
[162] Majeed U, Hong CS. FLchain: Federated learning via MEC-enabled blockchain network. In: 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE; 2019. p. 1–4.
[163] Yang T, Li X, Shao H. Federated learning-based power control and computing for mobile edge computing system. In: 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall). IEEE; 2021. p. 1–6.
[164] He J, et al. HeteFL: Network-aware federated learning optimization in heterogeneous MEC-enabled Internet of Things. IEEE Internet Things J 2022;9(15):14073–86.
[165] Wang J, et al. Indoor positioning privacy protection method based on federated learning in mec environment. Mobile Inf Syst 2022;(1):2311264. 2022.
[166] Zhang J, et al. FedMEC: improving efficiency of differentially private federated learning via mobile edge computing. Mobile Networks Appl 2020;25:2421–33.