IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 11 August 2025, accepted 27 August 2025, date of publication 2 September 2025, date of current version 8 September 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3605165

SURVEY

Advancing Federated Learning: A Systematic Literature Review of Methods, Challenges, and Applications

TAMANNA ZUBAIRI SANA[1], SHAHAB ABDULLA[2], ANINDYA NAG[3], (Member, IEEE), AYONTIKA DAS[4], (Member, IEEE), MD. MEHEDI HASSAN[5], (Member, IEEE), ZOYA ZUBAIRI FIZA[1], ASIF KARIM[6], (Member, IEEE), AND SHEIKH RIDWAN RAIHAN KABIR[5]

[1]Department of Computer Science and Engineering, East Delta University, Chattogram 4209, Bangladesh
[2]UniSQ College, University of Southern Queensland, Toowoomba, QLD 4350, Australia
[3]Department of Computer Science and Engineering, Northern University of Business and Technology Khulna, Khulna 9100, Bangladesh
[4]Department of Computer Science and Engineering, Adamas University, Kolkata 700126, India
[5]Computer Science and Engineering Discipline, Khulna University, Khulna 9208, Bangladesh
[6]Faculty of Science and Technology, Charles Darwin University, Casuarina, NT 0810, Australia

Corresponding authors: Shahab Abdulla (Shahab.Abdulla@unisq.edu.au), Md. Mehedi Hassan (mehedihassan@ieee.org), and Anindya Nag (anindyanag@ieee.org)

ABSTRACT Federated Learning (FL) has emerged as a cutting-edge paradigm in machine learning, showcasing remarkable advancements in recent years. This research paper delves into the dynamic landscape of FL by addressing four pivotal research questions. The study investigates the most recent advancements in implementing FL and explores additional applications that could benefit from this decentralized learning paradigm. This inquiry aims to provide an up-to-date overview of the evolving FL field and its potential cross-industry impact. The paper explores the integration of FL with various machine learning approaches to ensure optimal performance, privacy preservation, and scalability. By unraveling the collaborative aspects of FL with other machine learning paradigms, the research seeks to unveil novel strategies for enhancing efficiency in FL scenarios. The third research question focuses on the repercussions of scalability challenges and resource constraints in federated learning. This investigation aims to uncover the practical difficulties of implementing FL across diverse sectors, shedding light on potential barriers to its widespread adoption. The research probes into the future of federated learning by examining how it will be utilized in upcoming technological advancements and industries. This exploration aims to provide insights into the long-term viability and applicability of FL, anticipating its role in shaping the technological landscape across various sectors. Through a comprehensive analysis of these research questions, this paper contributes to the understanding of FL, providing valuable insights for researchers, practitioners, and decision-makers navigating the intricate intersection of FL, machine learning, and emerging technologies. This research paper aspires to provide a holistic overview of the advancements, integration possibilities, challenges, and prospects associated with federated learning, contributing to the ongoing discourse on the intersection of FL and machine learning in contemporary technological landscapes.

INDEX TERMS Federated learning, systematic literature review, machine learning, blockchain, Internet of Things, security.

I. INTRODUCTION

In recent years, the landscape of machine learning has been dynamically reshaped by the emergence of Federated Learning (FL), a paradigm that enables collaborative model training across decentralized devices. This innovative

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

approach has not only witnessed rapid advancements but has also opened new avenues for applications across diverse industries [2]. As the paradigm continues to evolve, understanding its latest developments, integration possibilities with other machine learning (ML) approaches, challenges in scalability, and its potential role in shaping upcoming technological advancements becomes imperative. This research endeavors to delve into the multifaceted domain of FL, aiming to answer key questions that are pivotal for comprehending its current state and future potential. Our exploration begins with an investigation into the most recent advancements in implementing FL, shedding light on cutting-edge technologies and the myriad industries that stand to benefit from its application. From collaborative healthcare solutions to privacy-preserving financial analytics, the scope of FL is expanding, making it imperative to explore the frontiers of its applicability [6]. Moving forward, the research focuses on the integration of FL with other machine learning approaches, emphasizing the importance of ensuring efficient performance, privacy preservation, and scalability. Understanding the synergy between FL and collaborative ML methodologies is crucial for harnessing their collective potential in addressing complex real-world challenges [27]. FL is a decentralized machine learning approach that enables model training across multiple edge devices or servers without exchanging raw data. The process begins with the distribution of a global model to individual devices, which locally computes updates based on its private data. These updates are then aggregated to form an improved global model without exposing sensitive information. This collaborative learning paradigm addresses privacy concerns associated with centralized data storage, as raw data remains on the local device, reducing the risk of data breaches. FL also promotes efficiency by allowing devices to learn from their unique datasets, enhancing model customization for diverse user profiles [16]. This emerging paradigm is particularly relevant in privacy-sensitive applications, such as healthcare and finance, where data security is paramount. In this paper, we explore the working procedure of FL, its applications, and the challenges it presents, emphasizing its potential to revolutionize collaborative and secure machine learning in various domains. Scalability challenges and resource constraints present substantial hurdles in the widespread adoption of FL [82]. This study aims to shed light on the repercussions of these challenges, providing insights into the difficulties associated with implementing FL across various sectors. By addressing these issues head-on, we aim to contribute to the refinement of FL methodologies, making them more robust and applicable in diverse environments. Lastly, our investigation extends to the prospects of FL, exploring how this paradigm will be utilized in upcoming technological advancements and industries [56]. As we stand at the intersection of technology and collaboration, understanding the trajectory of FL is instrumental in shaping the landscape of ML and artificial intelligence (AI) in the years to come. In summary, this research paper serves as a comprehensive exploration of FL, delving into its advancements, integration possibilities, challenges, and future applications. By addressing these key facets, we aim to contribute to the evolving discourse surrounding FL, providing valuable insights for researchers, practitioners, and stakeholders alike [109]. The paper is organized as follows: Section I introduces the background, prospects, approaches, and research application of FL. Section II presents the SLR, Research Questions, Search Strategy, Selection Procedure of Primary Studies, Inclusion and Exclusion Criteria, Snowballing, Results and Discussions, and Research studies associated with the research questions. Section III concludes the paper and provides some directions for future work.

II. SYSTEMATIC LITERATURE REVIEW

A systematic literature review (SLR) defines, chooses, and evaluates the literature to provide a solution to a specific topic. As per Kitchenham and Charters [206], an SLR is defined as "a type of secondary study employing a rigorous methodology to identify, analyze, and interpret all pertinent evidence concerning a specific research question in an unbiased and replicable manner." Before conducting the review, the systematic review must adhere to a well-defined protocol or strategy in which the criteria are clearly outlined. It is a thorough, transparent search of many databases and literature that other researchers can imitate and replicate. It entails developing a carefully thought-out search strategy that has a specified focus or solves a specific issue. The review identifies the sort of information sought, analyzed, and reported within specified deadlines. The review must include the search terms, search tactics (including platforms, database, names, and search dates), and limits. An SLR can show the present status of research on a topic while revealing gaps and areas that need more research about a specific research question. A rigorous methodological approach is used in SLR to eliminate distortions induced by an unduly narrow selection of available literature and to raise the dependability of the literature chosen as addressed by Tranfield et al., [207]. A unique feature in this respect is the definition of a research purpose for the search itself, as well as the criteria for choosing which results are to be included and rejected before completing the search.

A. RESEARCH QUESTIONS

The main objective of SLR conducted in this research is to provide a concise overview and enhance understanding of FL in terms of its utilization, applications, and challenges, to meet the study objectives. To achieve this purpose, four research questions (RQ's) have been designed which are illustrated in Table 1.

B. SEARCH STRATEGY

Within the existing body of literature, various types of review articles may be found that facilitate a more comprehensive exploration of a given topic. These include systematic reviews and narrative reviews, which serve distinct purposes in doing

TABLE 1. Research questions.

Sr. No	Research Questions	Motivation
RQ1	What are the state-of-the-art techniques and domain-specific implementations of FL, particularly in sectors with high demands for data privacy, scalability, or autonomy?	To identify and categorize advanced FL methods used in critical sectors that demand stringent requirements for privacy, performance, or real-time decision-making.
RQ2	In what ways has FL been combined with specific machine learning paradigms (e.g., transfer learning, reinforcement learning, and cryptographic learning) to improve performance, scalability, or privacy?	To evaluate synergies and integration patterns between FL and other ML paradigms, focusing on methodological innovations.
RQ3	What are the primary technical and infrastructural bottlenecks encountered when deploying FL at scale, and what mitigation strategies have been proposed?	To systematically assess real-world constraints that hinder FL scalability and analyze proposed solutions.
RQ4	What are the current and emerging application domains for FL, and what future research directions are evident from the literature?	To explore the forward-looking potential of FL in cutting-edge and rapidly evolving sectors.

in-depth research. Two primary methodologies are widely utilized in the field: Preferred Reporting Items for Systematic Reviews and Meta-Analyses (*PRISMA*) and Kitchenham's guidelines. To carry out this review, we adhered to the *PRISMA* 2020 methods, which are widely recognized as the standard method for conducting an SLR. In the context of an SLR, the initial step involves the identification of pertinent publications that specifically address a certain study field and its associated question(s). Subsequently, a critical evaluation is conducted to assess the methodological rigor and the evidential robustness of the studies encompassed within the selected papers. Finally, the gathered findings are synthesized to derive appropriate conclusions. The review follows the *PRISMA* 2020 three-phase structure: Identification, Screening, and Inclusion, as depicted in Figure 1.

Because FL was introduced for the very first time in 2016, the search procedure of the review was constrained to the period spanning 2017 to 2024. While IEEE Xplore yielded the largest share of initial records (representing 83% of all identified papers), we mitigated potential source imbalance during the review itself by (a) applying explicit domain-based inclusion filters at the title/abstract and full-text screening stages to ensure substantive retention from SpringerLink, ScienceDirect, and MDPI; (b) using systematic backward- and forward-snowballing to add relevant non-IEEE studies; and (c) resolving near-duplicates and methodologically overlapping works by retaining versions that preserved quality while improving venue and sector diversity (e.g., healthcare, finance, smart cities), thereby preventing a purely engineering-centric selection. We took famous digital libraries into consideration which are well-known for their extensive collections of papers, which are: *IEEE Xplore*, *SpringerLink*, *ScienceDirect*, and Multidisciplinary Digital Publishing Institute (*MDPI*). The search phrases analyzed all the databases thoroughly and examined the titles, abstracts, details, relevancy, and keywords of each one. In the Identification phase, a total of 591,007 records were identified across the selected digital libraries. The *PRISMA* flow diagram can be seen in Figure 1, which presents all of the aspects that were taken into consideration for the articles in this systematic review.

TABLE 2. Selected digital libraries.

Sr. No	Digital Library	Link
1	*IEEE Xplore*	https://ieeexplore.ieee.org/Xplore/home.jsp
2	*Springer Link*	https://link.springer.com/
3	*ScienceDirect*	https://www.sciencedirect.com/
4	*MDPI*	https://www.mdpi.com/

Following the completion of the search operation, the articles that were largely collected were put through a selection procedure. In the Screening phase, we first removed irrelevant research and titles, reducing the set to 174,418. After applying relevance-based domain filtering, we retained 7,010 papers for deeper review. Following de-duplication, we obtained 6,975 unique records. Full-text eligibility screening was performed on 202 articles, resulting in the exclusion of 16 papers due to irrelevance or being outside the defined scope. In the Included phase, after conducting an in-depth abstract and full-text analysis, a final set of 186 studies were included in the review.

C. SELECTION PROCEDURE OF PRIMARY STUDIES

This section outlines the search method for finding the material needed to analyze and respond to the mentioned research questions.

1) DATABASE

Our study conducts the SLR on the most well-known and reputable academic sources available. The digital libraries that are used in this study are presented in Table 2.

2) SEARCH STRING

To improve the number of results returned by the search, we used "federated learning" as the primary search phrase and added several synonyms and acronyms as additional terms. We constructed the search strings for each main source to examine the title, abstract, and keywords. These search strings included Boolean expressions with "AND"

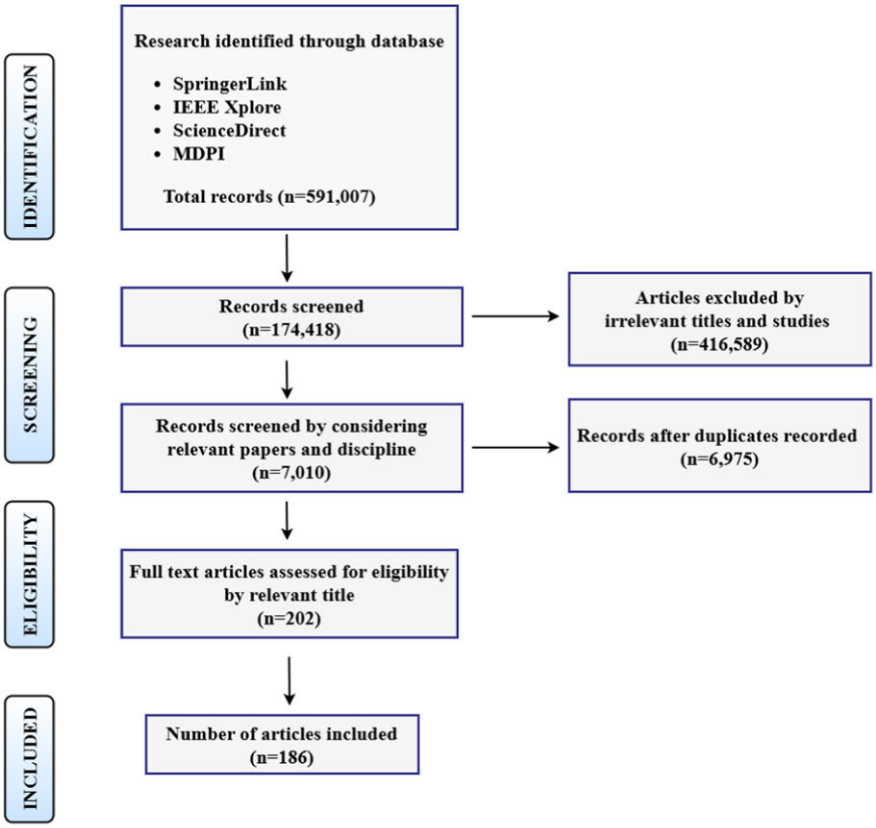


FIGURE 1. Methodology of *PRISMA* search.

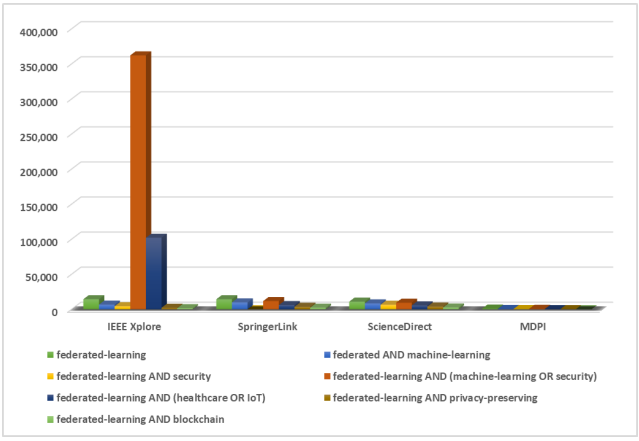


FIGURE 2. Number of papers found initially as per the search strings.

and "OR" operators. Following the completion of the initial drought of search strings, we checked the efficiency of the search strings by comparing the results obtained from each search string with the results obtained from each database. The following is a list of the search strings that were used for that initial search:

- federated-learning
- federated AND machine-learning

TABLE 3. Inclusion and exclusion criteria.

Inclusion Criteria	Ref	Exclusion Criteria	Ref
Search strings with the words or keywords in the title	[2]	Papers that don't include the search strings or the keywords	E1
English language	[3]	Preview only articles	E2
Content type (journals, articles, conference papers, books, chapters, etc.)	[4]	Duplicate articles	E3
Full paper	[5]		

- Federated learning AND security
- federated-learning AND (machine-learning OR security)
- federated-learning AND (healthcare OR IoT)
- federated-learning AND privacy-preserving
- Federated learning AND blockchain

With the help of the search strings, a total of 591,007 papers were discovered. We observed that *IEEE Xplore* contained the highest number of papers based on the search strings compared to *SpringerLink*, *ScienceDirect*, and *MDPI*. Figure 2 shows the number of papers initially found as per the search strings, without any filtering.

By considering the search strings, relevancy, content type (articles, journals, etc.), domains (Table 4), and

TABLE 4. Selected domains on the libraries.

Digital Library	Domain
Springer	Subjects: Machine learning, Artificial intelligence, Data privacy, Internet of Things, Cloud computing, Privacy, Blockchain, Data and information security, Health informatics; Discipline: Computer Science, Engineering, Medicine Public Health, Sub-discipline: Artificial Intelligence; Content type: Article, Conference Paper, Article, Research Article, Book
IEEE Xplore	Journals, Conferences, Books; Publication Topics: Federated Learning, Internet Of Things, Machine Learning, Data Privacy, Data Security, Deep Learning, Edge Computing, Internet of Things Devices, Cloud Computing, Differential Privacy
ScienceDirect	Article type: Review Articles, Research Articles, Book Chapters; Publication title: Future Generation Computer Systems, Procedia Computer Science, Medical Image Analysis, Internet of Things, Engineering Applications of Artificial Intelligence, Computer Security, Intelligent Systems with Applications, Vehicular Communications, Engineering Applications of Artificial Intelligence; Subject areas: Computer Science, Medicine & Dentistry, Engineering
MDPI	Subjects: Public Health Healthcare, Computer Science Mathematics, Engineering, Journals: Healthcare, Future Internet, Diagnostics, Network, IoT, Robotics, Vehicles, AI, Engineering Proceedings, Blockchains; Article types: Article, Proceeding Paper, Systematic Review

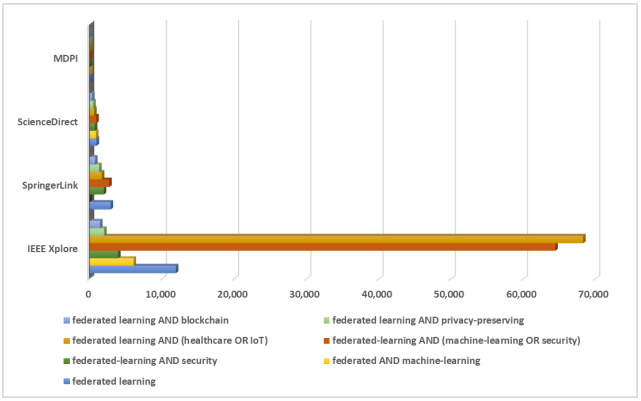


FIGURE 3. Number of papers as per the search strings through filtering as per the relevant domains.

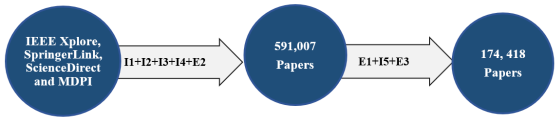


FIGURE 4. Filtering process using Inclusion and Exclusion Criteria.

other factors during this survey, at first, we discovered a total of 174,418 papers that were published in distinct four publisher websites. 158,114 papers were screened through *IEEE Xplore*, 11,252 on *SpringerLink*, 4,848 on *ScienceDirect*, and, 204 from *MDPI*. *IEEE Xplore* remains a significant contributor, as illustrated in Figure 3.

D. INCLUSION AND EXCLUSION CRITERIA

The criteria for inclusion and exclusion have been developed to pick relevant papers efficiently. During the search for relevant articles, there were a great number of ones that were irrelevant and required to be filtered away. In Table 3, the inclusion and exclusion criteria are used to illustrate how the filtering process was carried out and Figure 4 presents the filtering process using the inclusion and exclusion criteria.

E. SNOWBALLING

To address our research inquiries, we have implemented the snowballing methodology as presented by Wohlin [208] to ascertain pertinent studies. The utilization of snowballing as a methodological approach is advantageous in the context of conducting a systematic review, as it serves to enhance the comprehensiveness of the review by mitigating the risk of overlooking pertinent studies that may not have been captured in the initial search process. Following the establishment of the original set of studies, we employed the snowballing technique, which encompasses both backward and forward searching, to identify supplementary studies that are pertinent to our research, with a start set of 186 papers, which is illustrated in Figure 5. This process entails conducting a comprehensive examination of the references cited in the included research, commonly referred to as backward snowballing. Additionally, it involves identifying and reviewing papers that have cited the included. Studies, known as forward snowballing.

1) BACKWARD SNOWBALLING

A backward snowballing search was conducted on the references of each paper in the initial batch. At first, the title and reference context of each cited publication were evaluated. In certain cases, additional elements of the referenced work, like the abstract and keywords, were also reviewed. Secondly, the inclusion and exclusion criteria were established using a full-text reading. Papers that were assessed to be pertinent were added to the initial collection after the process was repeated until no new articles could

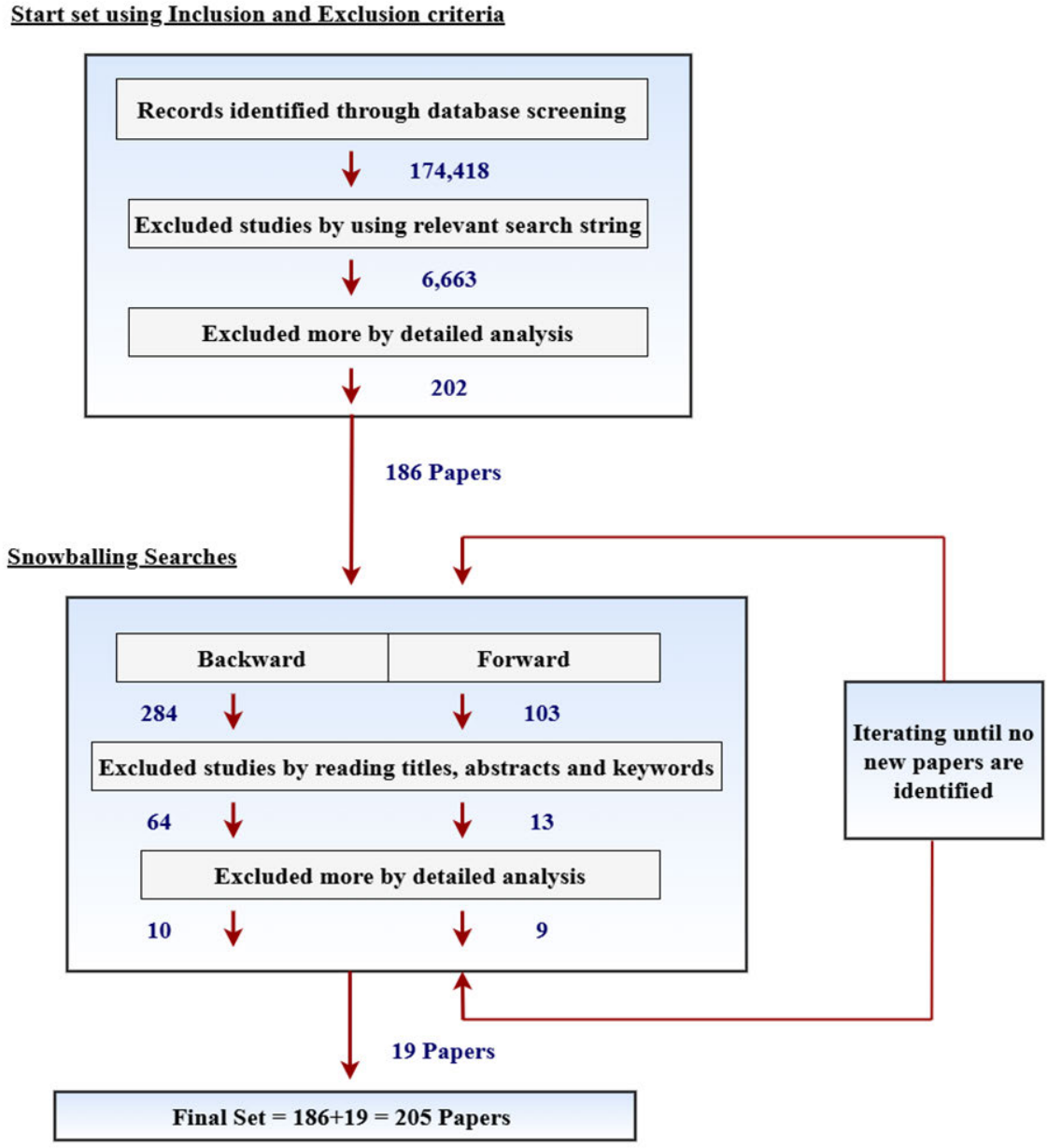


FIGURE 5. Snowballing Process.

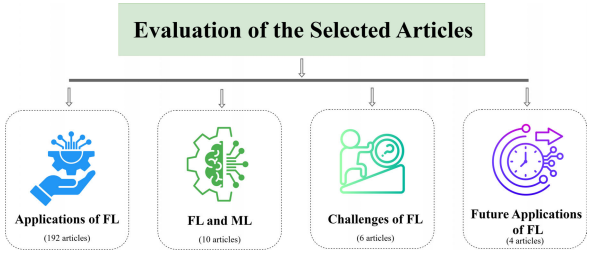


FIGURE 6. Primary article classification based on the research questions.

be found. We analyzed 284 articles during the iteration, of which 64 were relevant, and at last through detailed analysis, we observed that 10 papers were relevant.

2) FORWARD SNOWBALLING

We conducted a forward snowballing search using the citations of the start-set publications. We started by analyzing the titles of all the studies and their abstracts, keywords, and reference contexts. Selected items were added to the initial collection after the process was repeated until no new items were found. During the iteration, we examined over 103 articles and found 13 that were pertinent, but we only used 9 of them through detailed analysis. The snowballing procedure resulted in 19 more papers, 10 from backward snowballing along with 9 from forward snowballing. These 19 studies are then combined with the initial 186 papers from the database search, putting the

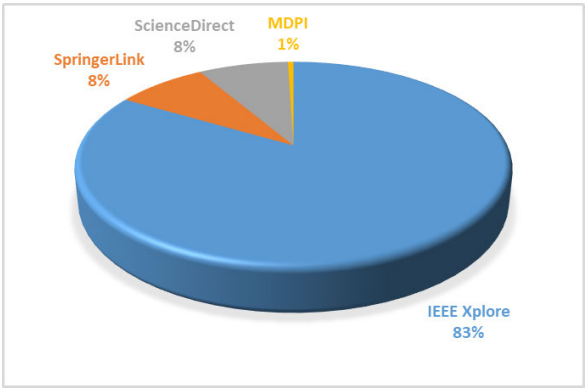


FIGURE 7. Percentage of publications in the digital libraries without any filtering.

overall number of papers included in the systematic review to 205.

F. SELECTION OF STUDIES AND FINAL INCLUSION

The final set of 205 papers was obtained through a rigorous multi-stage screening process. From an initial pool of 591,007 publications retrieved via broad search strings across four major digital libraries (*IEEE Xplore*, *SpringerLink*, *ScienceDirect*, and *MDPI*), we first applied strict inclusion and exclusion criteria to filter out non-pertinent works. This involved limiting results to English-language, full-text research papers containing the federated learning keywords in the title, and confining the scope to relevant domains (e.g., ML, data privacy, IoT, healthcare, etc.) as defined in the study's criteria (Table 4), while excluding any duplicates or off-topic entries. Through this process, the dataset was drastically narrowed (e.g., down to 174,418 after automated domain filtering and initial relevancy screening, then to 6,975 unique papers after consolidating duplicates). The titles of these remaining papers were then manually reviewed for relevance to the research questions, further reducing the candidates to 202, and subsequent in-depth abstract analysis refined the pool to 186 core studies that fully met all inclusion criteria. Finally, we employed snowballing, both backward and forward, to ensure comprehensiveness: they examined the reference lists of the 186 studies (backward snowballing) and identified newer works citing those studies (forward snowballing). This snowballing procedure yielded 19 additional relevant papers (10 via backward search and 9 via forward search), which were added to the initial set. By combining the 186 papers from the database search with these 19 snowballing discoveries, the review arrived at a total of 205 studies, all of which align with the defined inclusion criteria and are directly pertinent to the topic. Figure 6 illustrates the classification of the articles as per the research questions. Studies relevant to the query are grouped as one in Table 5.

G. QUALITY ASSESSMENT AND BIAS MITIGATION

To ensure the quality and relevance of the final set of studies, we conducted an informal quality assessment focused on three factors: (i) peer-reviewed status, (ii) relevance to the defined research questions, and (iii) citation or publication venue reputation. Only full-text, peer-reviewed conference or journal articles were included; preview articles, extended abstracts, non-English content, and duplicate studies were excluded.

While this study did not apply a formal scoring rubric (e.g., GRADE or CASP), the inclusion of studies from top-tier publishers (*IEEE Xplore*, *SpringerLink*, *ScienceDirect*, *MDPI*) and the use of domain filters helped mitigate quality-related bias. Furthermore, to reduce selection bias, both backwards and forward snowballing were applied independently on multiple rounds by different reviewers, increasing the diversity and representativeness of included literature.

H. COMPARATIVE ANALYSIS WITH PRIOR SYSTEMATIC REVIEWS

Several previous reviews have examined FL from various perspectives, including its technical foundations, domain-specific applications, and emerging challenges. Many of these works focus on targeted areas such as privacy preservation, communication efficiency, or deployment within a single field like healthcare or IoT. While these studies provide valuable contributions to the literature, there remains a need for a broader synthesis that captures the cross-domain implementation of FL and reflects its evolution across a wider set of contexts.

The present study addresses this need by offering a comprehensive and methodologically transparent review of FL applications and methodologies spanning multiple sectors, including healthcare, finance, industrial IoT, smart cities, autonomous systems, and mobile crowdsensing. This review employs a structured protocol informed by the *PRISMA* 2020 guidelines, beginning with the retrieval of over 590,000 records from four major academic databases and narrowing them through a multi-stage filtering process, including inclusion/exclusion criteria, manual screening, and snowballing, to a curated set of 205 primary studies.

Framed around four well-defined research questions, the review synthesizes findings related to technological advancements, integration strategies with other learning paradigms, scalability issues, and real-world application trends. By organizing and analyzing these diverse insights within a unified framework, this study contributes to a more integrative understanding of FL and provides a foundation for future theoretical and practical advancements in decentralized learning systems.

1) RESULTS AND DISCUSSIONS

To uncover the applications, methods, datasets, and obstacles that might be faced while utilizing FL, this study looked at the results of 205 separate research papers. A comprehensive review of the methods used and the results obtained by certain possible research is accomplished through the process of meticulously filtering and examining the studies that have been shortlisted. Figure 6 illustrates the classification of the

articles as per the research questions. During this survey, at first, without applying any filter, we discovered a total of 591,007 papers that were published in distinct four publisher websites, using the search strings. Figure 7 represents the percentage of the papers as per the search strings published till now on the utilized digital libraries. We found that *IEEE Xplore* is the largest contributor with 493,264 publications, followed by *Springer* and *ScienceDirect* as the next two major contributors with the counts 47,700 and 47,168, respectively. *MDPI*, on the other hand, only generated 2,875 papers.

The 205 studies included in this research span across various domains, with healthcare and medical applications being the most frequently explored. Approximately 25% of the studies are focused on healthcare, followed by the Internet of Things (IoT) and Industrial IoT (IIoT) at 18%, and blockchain at 12%. Smart cities, autonomous vehicles, edge computing, and cybersecurity (including intrusion and anomaly detection) also form substantial parts of the research landscape, contributing 10%, 8%, 7%, and 6%, respectively. Other emerging domains, including finance, mobile crowdsensing, and smart homes, make up the remaining 9%.

An analysis of the most frequent keywords reveals a clear emphasis on key aspects of FL. Terms like privacy preservation, scalability, and decentralization appear in 30%, 25%, and 20% of the studies, respectively. Security, optimization, and ML integration are also prominent themes, appearing in 18%, 15%, and 12% of the papers, reflecting the growing need for secure, efficient, and integrated systems in decentralized learning environments.

When examining the trends over the years from 2017 to 2024, it's evident that FL gained significant momentum from 2020 onwards. In the early years (2017-2019), the focus was primarily on healthcare and privacy concerns, with FL being applied predominantly in these fields. From 2020 to 2022, the adoption expanded significantly into domains like smart cities and blockchain, showing a 20% increase in papers dedicated to these areas. By 2023-2024, FL reached a broader set of applications, with an emphasis on addressing privacy and scalability issues, 50% of the papers published during this period highlighted these concerns, reflecting the growing maturity and challenges of FL in real-world deployments.

The chosen publications were grouped into clusters according to the research topics. Studies relevant to the query are grouped as one in Table 5.

I. RQ1:WHAT ARE THE STATE-OF-THE-ART TECHNIQUES AND DOMAIN-SPECIFIC IMPLEMENTATIONS OF FL, PARTICULARLY IN SECTORS WITH HIGH DEMANDS FOR DATA PRIVACY, SCALABILITY, OR AUTONOMY?

Blockchain The integration of blockchain technology with FL offers a significant advancement in enhancing data privacy and security via decentralized systems. Blockchain-based Federated Learning (BCFL), was first introduced by H. Kim et al., [1], is an innovative approach that addresses privacy concerns while promoting cooperation across several industries. This novel method effectively integrates the advantages of both technologies, guaranteeing safe data transmission and bolstering confidence in decentralized networks. In healthcare, BCFL improves data-sharing security by using immutable blockchain records. Rahman et al., [8] proposed a hybrid lightweight FL platform with smart blockchain contracts for the Internet of Health Things, which improved authentication, trust management, and encrypted dataset operations. Aich et al., [18] combined blockchain and AI technology to address data privacy concerns in healthcare, using blockchain for secure data access and FL for strong, global AI models. In the realm of IoT, BCFL handles growing dangers and assures secure device connectivity. Lu et al., [4] proposed a differential private multi-party data model-sharing method that combines FL to reduce data leakage risks. Majeed and Hong [5] presented FL chain, a blockchain-based FL system for multi-access edge computing that employs channels for learning global models and a global model state tree. Połap et al., [6] proposed privacy-preserving blockchain-based FL strategies for protecting the Internet of Medical Things (IoMT), resulting in efficient malware detection and security architecture. Zhao et al., [15] presented a hierarchical crowdsourced FL system for appliance makers using blockchain technology. Ning et al., [14] used BlockFed for data exchange and integrated FL into a blockchain's consensus process. A scalable security architecture based on permissioned blockchains was proposed by Lugan et al., [7], which ensured privacy-preserving data exchange and encouraged coalition involvement in the absence of a central authority. Zhang et al., [16] proposed a FL strategy that uses blockchain to identify device failures in Industrial IoT (IIoT). Their technique uses a platform architecture to maintain data integrity using Merkle trees stored on the blockchain. In permissionless blockchain-based solutions, Li et al., [9] proposed CrowdSFL, a crowdsourcing protocol that uses FL and blockchain to prevent harmful behavior in public blockchains. Liu et al., [10] developed a blockchain-based FL framework to prevent poisoning and membership inference attacks in 5G networks. A distributed computing defensive method for safeguarding the Internet of Battle Things was proposed by Sharma et al., [12] which used blockchain technology and FL to achieve high accuracy rates. Wang et al., [11] presented BEMA, a secure decentralized multiparty learning technique for edge computing-based IoT applications, which achieves high prediction accuracy under attack. The integration of blockchain and FL has benefitted decentralized health and EHR-sharing systems as well. Nguyen et al., [67] presented BEdgeHealth, a decentralized health architecture that combines MEC with blockchain for data offloading and sharing across hospital networks, along with a smart contract-based authentication mechanism. El Rifai et al., [17] used smart contracts with FL data aggregation to forecast diabetes risk. Nguyen et al., [68] developed a unique EHR sharing architecture that combines

TABLE 5. Research studies associated with the research questions.

Sr. No	Research Focus	Related Studies
1	Technological and methodological advancements in FL, including privacy, architecture, and optimization methods	[2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60], [61], [62], [63], [64], [65], [66], [67], [68], [69], [70], [71], [72], [73], [74], [75], [76], [77], [78], [79], [80], [81], [82], [83], [84], [85], [86], [87], [88], [89], [90], [91], [92], [93], [94], [95], [96], [97], [98], [99], [100], [101], [102], [103], [104], [105], [106], [107], [108], [109], [110], [111], [112], [113], [114], [115], [116], [117], [118], [119], [120], [121], [122], [123], [124], [125], [126], [127], [128], [129], [130], [131], [132], [133], [134], [135], [136], [137], [138], [139], [140], [141], [142], [143], [144], [145], [146], [147], [148], [149], [100], [150], [151], [152], [153], [154], [155], [156], [157], [158], [159], [160], [161], [162], [163], [164], [165], [166], [167], [168], [169], [170], [171], [172], [173], [174], [175], [176], [177], [178], [179], [180], [181], [182], [183], [184], [185], [186], [187], [188], [197], [199], [200], [205]
2	Integration of FL with other ML paradigms (e.g., transfer learning, reinforcement learning, cryptographic learning)	[4], [189], [190], [191], [192], [193], [194], [195], [196], [198]
3	Real-world implementation challenges in FL, including heterogeneity, scalability, and communication overhead	[26], [30], [197], [201], [202], [203]
4	Emerging application domains of FL and future directions in deployment and adoption	[30], [197], [203], [204]

blockchain and IPFS on a mobile cloud platform, using smart contracts to safeguard data transfers between patients and healthcare providers, and demonstrated successful, secure, and low-latency EHR sharing. FL integrated with blockchain has shown potential in a variety of different applications. Witt et al., [25] discovered that FL frameworks are feasible for handling financial information, with decentralized finance (DeFi) using blockchain to safeguard transactions and FL for risk assessment. Li et al., [120] introduced BFLC, a decentralized FL framework that utilizes blockchain and a committee consensus method to improve security and scalability. Liu et al., [121] proposed BFL-SA, a blockchain-based FL method that improves safe aggregation by using blockchain consensus and verified secret sharing. Wu et al., [13] offered an overview of combining FL with blockchains, assessing current frameworks, and proposing application opportunities and obstacles. BCFL is used in the Internet of Vehicles (IoV) to enable dependable communication and model upgrades for self-driving vehicles. Pokhrel et al., [19] provided a decentralized framework for on-vehicle machine learning, while Lu et al., [20] presented a BFL framework for efficient data sharing in IoV, which included an asynchronous FL technique based on edge data. Chai et al., [21] designed a blockchain-based hierarchical FL algorithm to improve in-vehicle network stability. Furthermore, Cui et al., [22] proposed a blockchain-assisted FL algorithm for content caching. Doku et al., [47] presented PoCI, a consensus process that combines blockchain and FL trust mechanisms to identify and store important data.

1) HEALTHCARE AND MEDICAL

FL improves patient care, research, and data analysis in healthcare via collaborative and privacy-preserving approaches. According to Neto et al., [26], training an effective deep learning model requires a massive amount of data, however sending sensitive medical data to a centralized data center is prohibited by privacy rules. This collaborative method enhances diagnostic tools by preventing data centralization. Islam et al., [27] addressed centralized data collecting difficulties in brain tumor detection using MRI scans, proving FL's capacity to categorize tumors with high accuracy while respecting privacy. Aouedi et al. [28] emphasized the need for extensive databases for machine learning, and FL may aid by keeping patient data locally and protecting privacy. Korkmaz et al., [57] used CloudLab to evaluate FL on real-world medical datasets and found that Inception-v3 and *EfficientNetB0* performed best, with FedAvg being the most successful federated optimization approach, followed by FedAvgM. FL enhances healthcare cybersecurity threat identification. Taha et al., [29] conducted a comprehensive literature analysis and research on FL in healthcare. The solution analyzes cybersecurity data from several healthcare institutions to identify and correct security faults without disclosing vulnerabilities, hence making healthcare IT infrastructure safer. Wen et al., [30] demonstrated that FL is successful in developing detection models for COVID-19 and DNA sequencing. In customized medicine, Patel et al., [31] highlighted how FL might assist in customizing patient therapies while respecting privacy. They proposed a FL-based healthcare informatics architecture to improve patient well-being and data privacy. Brisimi et al., [64] developed a decentralized optimization framework for cardiac hospitalization prediction that preserves data privacy while achieving comparable accuracy to centralized approaches. Shickel et al., [61] examined deep learning applications in EHR data, identifying limits and potential future research approaches. Silva et al. [54] presented an FL architecture for safe, distributed biomedical data processing, which was evaluated on synthetic data and in many investigations. Li et al., [32] employed FL for fMRI analysis to diagnose neurological diseases, while Sheller et al., [54] obtained excellent accuracy via multi-institutional medical imaging partnerships. Sharghi et al., [56] presented a service-based middleware for federated diagnostic imaging systems that address both interoperability and security concerns. Zeng et al., [58] developed FMore, an innovative framework that increases model accuracy and decreases training cycles using an incentive mechanism. Liang et al., [59] proposed a FL

technique for dealing with label noise based on benchmark samples. Chen et al. [37] presented FedHealth for privacy and customization in smart healthcare. Hao et al., [63] presented PRCL to solve the privacy and computational problems associated with EHR data. Yan et al., [69] employed FL to identify COVID-19 using chest X-rays and compared the performance of several models. To improve model convergence and accuracy, Chen et al. [65] developed PFL-IU, an efficient and privacy-preserving FL system for E-Health. Thwal et al. [205] used FL to create a clinical decision support system that addresses privacy concerns and cyber dangers. Zhang et al. [118] developed Cov-Fed, which improves COVID-19 diagnosis using chest X-rays while protecting data privacy. Gupta et al. [119] combined Blockchain and FL for lung disease categorization, attaining 90% accuracy. Li et al., [122] adopted FedFocus for COVID-19 identification, which improved model performance and stability. Harerimana et al., [62] examined big data analytics difficulties in healthcare and provided a thorough roadmap for future study. Blanquer et al., [123] used FL on ATMOSPHERE to diagnose rheumatic heart disease early, using echocardiography films to ensure accurate categorization and secure model building. Li et al., [40] investigated the application of differential privacy in FL for brain tumor segmentation and demonstrated its efficacy in securing patient data while managing sensitive medical information.

2) LEVERAGING PATIENT CLUSTERING TO PREDICT HOSPITAL STAY TIME AND MORTALITY

FL is used in medicine to predict patient mortality and hospital stay duration using electronic medical records (EMRs). EMRs, which are crucial for healthcare insights, have challenges due to their sensitivity and decentralized construction, according to Aledhari et al., [156]. Traditional machine learning algorithms suffer from storage, security, and privacy challenges. To address these issues, Huang et al., [39] developed CBFL (Community Based FL), an algorithm that clusters data to generate personalized models and improves prediction performance.

3) IoT AND IIoT

FL is a crucial component in the realm of the Internet of Things (IoT) and Industrial IoT (IIoT) because it allows for decentralized data safety, communication efficiency, and adaptability. Nguyen et al., [141] investigated the possibilities of FL in several IoT applications, such as data sharing, attack detection, and mobile crowdsensing. Ferrag et al., [3] performed a thorough investigation on federated deep learning algorithms for IoT cybersecurity, revealing that federated models provide better protection and detection accuracy than centralized approaches. In the context of IoT data collaborations, Yin et al., [158] developed FDC, a secure data collaboration scheme that employs blockchain and data centers to assure privacy and efficiency in wearable sensor data processing. Salh et al., [138] investigated energy-efficient bandwidth allocation and CPU optimization for FL in IoT, using an Alternative Direction Algorithm (ADA) to reduce energy usage. Song et al., [144] improved FL reliability by using trust-weighted aggregation and adaptive calibration techniques. Yu et al., [159] proposed UDEC, a FL-based approach for privacy, security, and resource optimization, which uses deep reinforcement learning for data security. Math et al., [142] developed an intelligent SDN-based solution for managing FL communications across 5G/6G networks, with an emphasis on network stability and model correctness. An FL-based approach was Zhang et al., [143] for detecting machinery faults that incorporate dynamic verification and self-supervised learning. Mohammed et al., [147] proposed a heuristic for improving accuracy in FL, which improved the identification of illegitimate IoT devices.

In the context of secure IIoT, Khoa et al., [149] proposed a collaborative learning-based IDS for cyberattack prevention, while Kong et al., [148] developed FTM, a framework for data mining that uses homomorphic encryption. Hao et al., [100] presented PEFL, a privacy-enhanced FL system that uses differential privacy and homomorphic encryption. TrustFed, a decentralized system was proposed by Rehman et al., [150] which used blockchain to protect participant reputations. Hu et al., [36] developed a trend-following approach for multi-sensor time-series data in IIoT, while Zhao et al., [151] suggested employing proxy servers to decrease communication load and assure anonymity for participants in FL.

4) CLOUD COMPUTING

FL overcomes privacy problems in secure cloud computing by allowing for decentralized training on numerous devices simultaneously. Zhang et al., [152] developed a FL framework for AI IoT applications that improves the prediction accuracy of individual devices by training models without centralizing sensitive data. Similarly, Fang et al., [153] presented HFWP, a FL strategy that preserves strong privacy with lightweight encryption while achieving good accuracy on real-world datasets. Wu et al., [66] presented a customized FL approach that uses edge computing to mitigate the negative impacts of heterogeneity, resulting in high throughput and low latency. Wei et al., [154] expanded on this by proposing a FL method to improve cloud computing-based 5G heterogeneous networks, using end-edge-cloud collaboration and deploying attack detection systems across network nodes for increased security and efficiency.

5) EDGE NETWORK COMPUTING

Traditional cloud designs need data to be transported to centralized servers for processing, which may cause delays and latency. To overcome these difficulties, edge networks analyze data closer to the source, lowering reaction times and increasing efficiency. Lu et al., [116] presented the Privacy-Preserving Asynchronous FL Mechanism for Edge Network Computing (PAFLM), which reduces data traffic between edge nodes and the parameter server while enabling

nodes to participate or opt out of learning operations. Li et al., [117] addressed spectrum efficiency and energy consumption issues in FL on mobile devices by developing M-AirComp, a spectrum-efficient aggregation approach, and an energy-efficient FL architecture, which improved both spectrum use and learning accuracy. Ye et al., [124] presented EdgeFed, an edge FL system that offloads local model updates to an edge server, lowering computing and communication costs while exhibiting efficacy across a range of bandwidth circumstances.

Emerging technologies such as Mobile Edge Computing (MEC) and enhanced communication systems are critical to the expansion of IoT networks. Lu et al., [126] proposed DITEN, which combines blockchain with FL to protect data privacy and secure learning processes in edge networks. Qian et al., [127] developed a privacy-preserving data analytics system for centralized fog devices that use active learning in edge devices to increase privacy and minimize latency. Xiao et al., [128] presented FEI, a federated edge intelligence framework in which edge servers collaborate to train a model using data from IoT devices while optimizing resource allocation. Cui et al., [129] proposed SAPE, a secure, decentralized edge computing platform that uses federated deep reinforcement learning (DRL) and blockchain-based verification to improve system stability and protection against threats.

6) FRAUD DETECTION

FL's decentralized, privacy-preserving technique improves fraud detection by enabling financial institutions to train models on local devices, protecting transaction data privacy while enhancing model performance. Yang et al., [130] proposed FFD (FL for Fraud Detection), which trains fraud detection models utilizing local datasets rather than cloud-based Fraud Detection Systems (FDS). This approach combines locally generated model changes to create a common FDS. Ferreira et al., [139] presented a Federated ML architecture on 5G edge nodes, which showed enhanced privacy and latency in decentralized training. Their solution to fraud detection outperformed centralized algorithms and is relevant in real-world MEC settings.

Salam et al., [131] developed a FL strategy for credit card fraud detection that addresses data privacy and class imbalance problems. Their research emphasized the benefits of hybrid resampling strategies, notably with Random Forest, and discovered that PyTorch outperformed Tensorflow Federated in prediction accuracy, but with a longer processing time. Reddy et al., [132] proposed the Jellyfish Namib Beetle Optimization Algorithm-SpinalNet (JNBO-SpinalNet), a hybrid optimization-based deep learning method for identifying counterfeit credit card payments.

7) STOCKMARKET

FL's collaborative solutions, which combine collective insights with data privacy and security, have the potential to transform the stock market and finance sector. Financial institutions and traders may use historical stock price data to build machine learning models for stock price prediction analytics. This collaborative method enhances forecasts without disclosing trading techniques. Ardakani et al., [24] presented a FL architecture for stock market prediction based on Random Forest, Support Vector Machine, and Linear Regression model. In their research, they compare FL to centralized and decentralized learning frameworks to establish the best stock market prediction approach. Sakhare et al., [48] proposed a novel ensemble technique for predicting stock market trading decisions using a spatial federation of deep learning, machine learning, and dictionary-based approaches. The method maintained privacy and geographic diversity by federating models into five groups, generating a 5-bit pattern for decision-making.

8) SMART FINANCE AND INSURANCE

FL is transforming the financial and insurance industries by providing safe, collaborative data analysis while protecting privacy. It is very effective in marketing, risk management, and anti-money laundering. WeBank has effectively used FL for risk management in small company and personal loans. This program improves credit scoring and insurance claim forecasts by using third-party data while protecting user privacy. Cheng et al., [160] presented a privacy-preserving boosting tree architecture using vertical FL (VFL). This system enables secure cooperative machine learning on segmented credit score data, increasing the accuracy of credit evaluations and insurance forecasts. Liu et al., [46] developed FedCoin, a blockchain-based payment system that enables FL. FedCoin utilizes community computing resources for FL tasks and uses the Shapley value to precisely calculate each client's contribution to the global model.

9) RECOMMENDER SYSTEM

FL improves recommendation systems by allowing decentralized model training while maintaining user privacy. Harasic et al., [136] developed a federated recommender system that incorporates research into federated algorithms, architectural designs, and privacy techniques. This method provides highly tailored content recommendations without revealing user data by changing models locally on devices as users engage with the material. FL also promotes cross-platform cooperation across several sectors. Wu et al., [137] presented *FedDeepFM*, a deep recommender system built on FL. *FedDeepFM* uses model parameters rather than raw data to train a global model with generalization capabilities, and it includes a pseudo-interaction filling mechanism to shield true user input from indirect inference. This method enhances suggestions by using user preferences without explicitly gathering personal information. In contrast, Duan et al., [41] proposed JointRec, a cloud video recommendation system that uses deep learning and the JointCloud architecture for joint training across dispersed cloud servers. This system streamlines the recommendation process by

merging data from numerous cloud sources while remaining efficient and effective.

10) MOBILE KEYBOARD PREDICTION

FL was utilized for keyboard prediction and keyword detection, using a special kind of neural network known as CIFG trained inside FL, as discussed by Aledhari et al., [156]. This solution reduces computing strain on devices by using data from 7.5 billion phrases. Devices have to have 2GB of RAM, be charged, connected to a network, and idle during the procedure. FL-trained CIFG networks performed well. Leroy et al., [52] studied the use of FL for keyword detection using a Recurrent Neural Network (RNN). They used a Coupled Input and Forget Gate (CIFG) variation of LSTM RNN to improve performance on resource-constrained devices. They trained using Tensorflow and handled 7.5 billion phrases sent by Gboard users. Their approach addressed limits by using adaptive averaging algorithms to increase model efficiency.

11) INTRUSION DETECTION

FL substantially improves intrusion detection systems by increasing security and privacy while lowering communication overhead. Neto et al., [155] presented a score-based participant selection and global momentum technique to improve the resilience of FL-based intrusion detection systems by reducing the danger of malevolent participation and statistical discrepancies. Zhao et al., [146] developed a FL-based intrusion detection system that outperformed traditional approaches. Similarly, Li et al., [34] proposed DeepFed, a FL-based architecture for industrial cyber-physical systems that protects privacy via a secure communication protocol based on the Paillier cryptosystem. In terms of privacy-preserving intrusion detection, Al-Marri et al., [165] presented an IDS that used federated mimic learning and achieved a high accuracy of 98.11%. Li et al., [166] developed a distributed IDS for satellite-terrestrial networks that incorporates homomorphic encryption and CNN for successful DDoS detection. Rahman et al., [168] and Cetin et al., [169] investigated IoT intrusion detection via FL, stressing privacy protection and decreased communication overhead, respectively. Chen et al., [172] presented FedAGRU, an FL-based IDS that improves detection accuracy while lowering communication costs. In addition, McElwee et al., [174] presented FASTT, a solution for prioritizing and responding to IDS alarms that uses Tensorflow deep neural networks. Liu et al., [125] presented a cooperative intrusion detection system for automotive networks that offloads model training to distributed edge devices and uses blockchain for secure model storage, therefore improving privacy and lowering both communication overhead and computing costs.

12) ANOMALY DETECTION AND VOICE ASSISTANT IN SMART BUILDING

FL can improve anomaly detection and privacy in smart buildings and IoT systems, including voice assistants. Jithish et al., [162] proposed a FL-based strategy for detecting smart grid anomalies, in which ML models are trained locally in smart meters without data sharing, protecting user privacy. Their technique was tested against centralized ML models and proven to be successful at identifying abnormalities while maintaining privacy. Nguyen et al., [51] proposed DÏOT, a federated self-learning anomaly detection system for IoT utilizing unlabeled crowdsourcing data, and achieved a 95% detection rate with no false positives. Similarly, Cámara et al., [164] developed a training framework for unsupervised network anomaly detection models, which improved collaborative training while lowering network overhead in large IoT and IIoT installations. Liu et al., [33] addressed edge device failures in IIoT with their AMCNN-LSTM framework, which combines CNN and LSTM with attention mechanisms for accurate anomaly detection and improves transmission efficiency via gradient compression. Mothukuri et al., [167] presented an IoT IDS using FL to maintain data integrity. Wang et al., [175] proposed hierarchical FL for detecting anomalies in IoT networks. Cvitic et al., [170] investigated DDoS detection in IoT using logistic model trees. Moustafa et al., [171] developed the TON IoT dataset for Windows operating systems, which includes many threat families. Huong et al., [173] proposed LocKedge, an IoT IDS that prioritizes edge-layer detection accuracy. In addition, Huong et al., [163] introduced FedeX, which performed better than 14 previous anomaly detection algorithms with a Recall of 1 and an F1-score of 0.9857. FedeX's fast training time and low memory use make it ideal for real-time edge computing deployment.

13) LOCALIZATION AND LOCATION

FL enhances GPS accuracy by training models across several devices. GPS precision and location accuracy increase as devices learn from different local settings and signal circumstances. Yin et al., [188] proposed Federated Localization (FedLoc) which seeks to produce accurate location services while protecting user privacy, particularly with regard to sensitive geographical data. And it also improves GPS accuracy by allowing device-to-device model training. Their method enabled collaborative mobile users to reach near-centralized performance in data fitting and prediction. Gao et al., [200] presented FedLoc3D, a FL system for indoor localization. Their methods, FedDSC-BFC and FedADA-LLR are algorithms for building-floor classification and latitude-longitude regression that improve localization accuracy and efficiency in the face of data heterogeneity and network instability. Ciftler et al., [157] proposed a FL-based method for increasing RSS fingerprint-based localization accuracy while maintaining user privacy. Their solution improved accuracy by 1.8 meters and performed well in real-world circumstances.

14) FLOOD FORECASTING

FL improves flood predicting accuracy, flexibility, and privacy by using decentralized and collaborative methodologies.

It supports real-time updates and includes local meteorological data, which is critical for accurate flood forecasts. Farooq et al., [161] developed a model based on locally trained feed-forward neural network (FFNN) models from eighteen clients. This model analyzed station flooding and issued a five-day flood alarm. The FFNN models used geographical characteristics to estimate water levels, and they were 84% accurate in predicting floods in the investigated zone between 2010 and 2015. Nahak et al., [199] presented a FL framework for flood prediction that employs models from 18 stations and an advanced CNN2D algorithm. Their technology generates accurate flood notifications with a five-day advance time while protecting data privacy and lowering network latency.

15) SMART INDUSTRY

In the smart sector, AI is critical for process modeling and control, but data sharing raises privacy problems. FL provides a privacy-preserving method to intelligence that does not need the sharing of data. FL is important in robotics and Industry 4.0 because it optimizes industrial operations while protecting data privacy. Liu et al., [35] proposed LFRL, a lifelong federated reinforcement learning architecture for cloud robotic system navigation that uses past information to adapt to new settings via a knowledge fusion method. Tanwani et al., [96] developed a ''Fog Robotics'' solution that distributed resources across Cloud and Edge for low-latency robot learning and was used to surface cleaning with 86% success. Lim et al., [97] presented a federated reinforcement learning architecture in which agents communicate experiences and model parameters across devices via Actor-Critic PPO, hence speeding learning. Li et al., [98] introduced FC-SLAM, a collaborative system that employs FL to increase visual-LiDAR SLAM performance in cloud robotics via real-time feature extraction without picture transmission. Zhou et al., [94] proposed RT-robots, a real-time data processing system for many robots that uses differential FL to provide privacy and real-time recognition. Nguyen et al., [110] presented employing Deep Q-Network (DQN) for maximizing energy recharge to workers and choosing transmission channels in FL, displaying higher performance over traditional methods. In the larger context of Industry 4.0, Lu et al., [99] performed a thorough assessment of 88 publications, dividing them into important research topics and addressing interoperability issues. Hao et al., [100] presented PEFL, a privacy-enhanced FL strategy for Industrial Artificial Intelligence (IAI) that enhances accuracy and efficiency while preventing data breaches. Pokhrel et al., [101] developed a model to investigate C-TCP performance on Industry 4.0 WiFi infrastructure, exhibiting performance enhancements using cognitive radio and FL approaches. Arachchige et al., [102] proposed PriModChain, a system that combines differential privacy, FL, blockchain, and smart contracts to assure privacy in IIoT data, which was proven using simulations. Qu et al. [103] developed a decentralized paradigm for big data-driven cognitive computing that addresses privacy and security concerns by combining FL and blockchain. Qiu et al., [104] investigated the influence of edge computing on the Industrial Internet of Things (IIoT), emphasizing its ability to reduce latency, save bandwidth, and improve privacy. Sun et al., [106] presented a General Gradient Sparsification (GGS) framework for FL that decreases communication cost while retaining accuracy. Mills et al., [105] proposed CE-FedAvg, an upgraded FedAvg algorithm that uses distributed Adam optimization and innovative compression methods to improve communication efficiency. Zhai et al., [107] developed a delay-constrained FL framework to enable dynamic client selection in mobile edge computing scenarios. Wang et al., [108] presented Communication-Mitigated FL (CMFL), which minimizes communication by filtering out unnecessary updates while increasing efficiency by 13.97x. Yang et al. [109] investigated energy-efficient resource allocation in FL via wireless networks and proposed an optimization approach that decreases energy usage by 59.5 Imteaj et al., [111] presented a FL model for IoT devices that provides trust ratings depending on client behavior to ensure efficient learning. Aïvodji et al., [112] proposed a smart home design that combines FL with safe data aggregation to improve privacy. Fu et al., [113] presented VFL, a verifiable FL solution for privacy-preserving large data that relies on Lagrange interpolation to ensure gradient integrity. Zhang et al., [114] presented ''FengHuoLun,'' a FL-based edge computing platform for Cyber-Physical Systems (CPS) that ensures trustworthy services via model training in a trusted FL framework. A network-aware distributed learning strategy for fog computing was developed by Tu et al., [115] that maximizes network utility and minimizes energy usage, minimizing latency and improving communication efficiency.

16) SMART CITY

Smart City efforts encountered hurdles as stronger data privacy restrictions hampered cooperation and data exchange. Gharaibeh et al., [85] used a data-centric approach, concentrating on core data management approaches to assure consistency, interoperability, and privacy in IoT-generated data. They emphasized the successes and difficulties of combining data security, privacy, networking, and computing technologies for smart cities. Mukhametov et al., [87] investigated the integration of ubiquitous computing along with distributed machine learning, focusing on the role of technologies such as sensors, IoT, AI, and network robots, as well as methods such as stochastic gradient descent, K-means, and federated training for data compatibility and privacy. Mohammadi et al., [86] addressed large data underutilization in smart cities by presenting a scalable three-level learning system that optimizes services using semi-supervised deep reinforcement learning, demonstrating its applicability across several domains. Kumar et al. [88] codified the criteria for trustworthy AI systems, emphasizing data and algorithm ethics to boost confidence in AI applications, notably in smart

cities. Masera et al., [90] highlighted the importance of smart energy networks, calling for a thorough cost-benefit analysis (CBA) that takes into account environmental, economic, and social implications in order to make educated choices about smart grid installations in smart cities.

In terms of FL applications, Chiu et al., [89] presented an edge learning system that combined semi-supervised and FL to improve object identification and picture classification accuracy while dealing with data privacy concerns. Taïk and Cherkaoui [92] used FL and edge computing to enhance home load predictions, achieving encouraging results using data from 200 residences in Texas. Albaseer et al., [49] presented FedSem, a semi-supervised federated edge learning approach that used unlabeled data to increase performance in the face of inadequate labeled data. Pérez et al., [91] developed an ANN predictive power model that is tailored for GPU-based federated edge data centers, resulting in accurate power estimates and increased energy efficiency. Samarakoon et al., [42] introduced FL-JPRA, a distributed system for ultra-reliable, low-latency vehicular communication that employs FL and roadside units. FedGRU, a FL-based recurrent unit neural network for traffic flow prediction, was presented by Liu et al., [43], whereas Samarakoon et al., [72] proposed an FL approach for joint transmit power and resource allocation in vehicular networks, which used extreme value theory and Lyapunov optimization to minimize data exchange and improve queue length.

17) SMART TRANSPORTATION

FL tackles privacy concerns in smart transportation by providing decentralized learning and collaborative training while protecting user data. Nguyen et al., [74] presented a Mobile Edge Computing (MEC)-based blockchain network in which mobile users function as miners. Their solution treated workload offloading, user privacy, and mining profit as a combined optimization issue, using Markov decision processes and RL-based offloading systems like deep Q-networks. Simulations revealed increased privacy, lower energy usage, and lower offloading costs as compared to benchmarks. Cao et al., [75] used FL in MEC to improve Intelligent Transportation Systems, with an emphasis on privacy protection and efficient computing for smart cars. Their technique improved learning collaboration while lowering execution costs, proving success via numerical findings. Zhang et al., [73] proposed a DRL-based technique for joint transmission mode selection and resource allocation in cellular V2X communications. They structured it as a Markov decision process and used a two-timescale federated DRL method, which outperformed decentralized baselines.

Jin et al., [70] used Gaussian mixture models (GMMs) to locate breakpoints in fundamental diagrams (FDs), using MAP estimation for robust parameter estimation. Their technique efficiently separated traffic circumstances and selected essential parameters, which were confirmed using Caltrans Performance Measurement System (PMS) information. Jones et al., [76] presented an FL system running on an emulated wide-area communications network with dynamic and heterogeneous resource availability. Their decentralized framework enabled clients to help one another depending on availability, with a graphical interface that displayed network connections and training progress.

18) RESIDENTIAL LOAD FORECASTING

FL contributes significantly to residential load forecasting by offering a decentralized and collaborative method that enhances accuracy, privacy, and flexibility in predicting energy consumption patterns. Qu et al., [179] presented a Personalized FL (PFL)-based system for user-level load prediction. Their technique proved that a simultaneously generated global model could effectively anticipate regional power consumption statistics, expanding the scope of their load forecasting approach. They included GAN-DP into their system to improve privacy while reducing the effect on prediction accuracy. The results of their studies demonstrated that their technique accurately anticipated user-level load statistics while respecting user privacy.

19) AUTONOMOUS VEHICLES

Parekh et al., [140] used gradient encryption in FL to guarantee user privacy while requiring minimum extra processing. They developed a German traffic sign identification system employing a CNN-based classification system and GeFL, which was 2% more accurate than traditional FL approaches and decreased data transmission by around three times. Zhang et al., [44] used FL to predict wheel steering angle in autonomous cars, resulting in improved model quality and training time while keeping accuracy equivalent to centralized techniques. Lu et al., [182] presented CLONE, a collaborative edge learning architecture that uses FL and long-term memory networks to provide latency reduction, privacy protection, and tailored driving experiences. They also presented a federated peer-to-peer vehicle learning strategy for improved safety and dependability via asynchronous aggregation. Xiong et al., [77] proposed an intelligent task offloading architecture for heterogeneous vehicular networks using DSRC, C-V2X, and mmWave communication technologies. They employed stochastic network calculus to determine delay upper limits and devised a federated Q-learning strategy to reduce communication/computing costs and offloading failures, outperforming previous methods.

Du et al., [180] investigated FL's use in wireless IoT, concentrating on its potential for future automotive IoT systems such as cooperative autonomous driving and intelligent transportation systems (ITS). They addressed pertinent technological issues and laid out future research paths. Ye et al., [181] presented an FL system that employs two-dimensional contract theory to safeguard vehicle customers' privacy during model selection. This methodology solves knowledge asymmetry and enhances data privacy and security in vehicle networks.

20) INTERNET OF DRONES

FL improves UAV capabilities for mobile crowdsensing while also protecting privacy in the Secure Internet of Drones. Motlagh et al., [133] showed that UAVs can train AI models together while keeping local data private. Wang et al., [23] proposed SFAC, a FL system that combines blockchain, local differential privacy, and reinforcement learning to enable safe AI model training in UAV-assisted crowdsensing. Mowla et al., [84] developed an adaptive federated reinforcement learning system to enhance the detection of jamming assaults in flying ad hoc networks. To resist eavesdropping in fog-aided IoD networks, Yao et al., [134] presented a secure FL approach that optimizes safety rates while being bound by UAV battery capacity and QoS. Yazdinejadna et al., [135] developed an authentication system based on FL and RF characteristics, which achieved high true positive rates and outperformed competing systems.

In addition to privacy and security, FL applications in UAV networks tackle a variety of operational difficulties. Fotouhi et al., [78] investigated the integration of UAVs into cellular networks, including UAV types, interference, and security concerns. Lim et al., [71] presented an FL solution for collaborative machine learning across separate DaaS providers in IoV applications, which uses contracts and algorithms to solve information asymmetry and optimize profitability. Chen et al., [79] studied combined caching and resource allocation in cache-enabled UAV networks and discovered considerable improvements in user queue stability and convergence speed using an LSM-based method. Yuan et al., [81] presented a predictive beamforming system to reduce beam misalignment caused by UAV jittering while displaying reliable communication performance. Qu et al., [83] proposed AGIFL, which combines air-ground networks with FL to improve edge intelligence in 6G networks, emphasizing technological hurdles and future research objectives. Zeng et al., [80] presented a distributed FL system for UAV swarms that improves convergence and reduces communication rounds by combining power allocation and scheduling. Wang et al., [82] used a FL framework with convolutional auto-encoders to optimize UAV deployment in VLC-enabled networks, resulting in considerable savings in UAV transmission power.

21) IMITATION LEARNING AND COLLISION DETECTION FOR AUTONOMOUS DRIVING

Liang et al., [53] proposed an online federated reinforcement learning transfer technique for extracting information in real-time during autonomous driving. This technique enables participants to make educated judgments based on shared information, allowing for real-time adaptability and better decision-making in autonomous driving situations.

22) PREDICTION OF ENERGY DEMAND AND DRIVING RANGE OF ELECTRIC VEHICLES

Thorgeirsson et al., [178] used probabilistic neural networks and linear regression models as an extension of the federated averaging approach to solve the issues of estimating energy consumption and driving range for electric cars utilizing distributed systems. This method maintains communication and privacy while considering uncertainty from distributed data. Their research indicated that probabilistic prediction models outperform deterministic ones and that FL may improve conventional driver-specific learning. They obtained increased effective driving range and shorter route durations by using probabilistic estimates, with changeable safety margins dependent on destination attainability.

Saputra et al., [50] presented a federated energy demand learning system that enables charging stations to safely communicate data. Their cluster-based energy demand learning technique improves forecast accuracy.

23) VISUAL OBJECT DETECTION AND COMPUTER VISION

Computer vision depends significantly on deep learning for visual object detection, however, privacy problems limit the usage of centrally stored training datasets. Shenaj et al., [176] examined several FL settings in computer vision and identified major obstacles. They gave a complete review of FL algorithms used in vision tasks like image classification, object identification, semantic segmentation, and specialized fields like face recognition and medical imaging.

Zhang et al., [145] proposed FedVisionBC, a blockchain-based FL system aimed to tackle single points of failure, model poisoning, and membership inference weaknesses in conventional FL. FedVisionBC replaces a central server with aggregation and verification nodes, and model poisoning is combated using encryption, verification nodes, and smart contracts. FedVisionBC was able to recognize objects even when less than 60% of the clients were hostile.

24) IMAGE SENSING CLASSIFICATION

Image data sharing with central cloud servers for real-time categorization has prompted issues regarding client customization and network load. To solve these difficulties in privacy-sensitive businesses, optimal FL approaches are critical for ensuring data privacy while maintaining model accuracy and making effective use of communication and computing resources. Tam et al., [177] presented an adaptive model communication strategy for edge FL, which includes virtual resource optimization. Their solution uses a deep Q-learning algorithm to control a self-learning agent in conjunction with a network functions virtualization orchestrator and software-defined networking. The proposed FL classification model for IoT image sensing with varied spatial resolutions provides high accuracy and economical QoS metrics, effectively resolving future network congestion concerns.

25) AUGMENTED REALITY

To improve compute efficiency and latency in augmented reality (AR) applications, Chen et al., [60] introduced an architecture that combines mobile edge computing with FL. Their technique, which links AR operating principles to

object identification and categorization, was tested using CIFAR-10 data. It successfully decreased training iterations compared to centralized learning while resolving bandwidth and latency issues.

26) MOBILE PACKET CLASSIFICATION (MPC)

Bakopoulou et al., [45] used Federated Support Vector Machines (F-SVM) for Mobile Packet Classification, allowing mobile devices to train global models without sharing original data. Their strategy is leveraging a smaller feature area, notably the HTTP key, to minimize the sharing of sensitive data.

27) DISCOVERY OF DRUGS

FL has emerged as a useful method for drug development. FL solves the issues associated with skewed datasets in drug discovery, allowing the development of a universal FL framework. This system, which includes a server coordinator and collaborators for FL clients, enables model updates and training rounds. In comparison to centralized learning across seven drug-related datasets, the system performed better. Xiong et al., [38] developed a FATE-based cross-silo federal drug development model to mitigate data bias.

28) MOBILE CROWDSENSING

Mobile crowdsensing, a key component of IoT, utilizes people outfitted with devices to perform different sensing functions. To address difficulties like user dropout and forced aggregation, Liu et al., [184] developed FEDXGB, a federated extreme gradient boosting system. FEDXGB uses safe algorithms and aggregation protocols to construct XGBoost classification trees while maintaining dropout users' data via cryptographic methods. Evaluations of the ADULT and MNIST datasets showed that FEDXGB efficiently minimizes computing and communication expenses while minimizing performance loss.

Zhang et al., [185] introduced FedSky, a secure data aggregation solution for federated mobile crowdsensing. FedSky has an effective worker selection process based on consumers' local data and device computing capability. FedSky reduces the user's calculation time and system latency greatly when compared to FedAvg, as shown by MNIST dataset performance tests.

29) MALWARE DETECTION

The proliferation of unsecured IoT devices has exacerbated malware vulnerabilities, demanding robust detection strategies. Payne and Kundu [186] proposed a hierarchical deep federated protection strategy for cloud computing, presenting malware detection as a graph and hypergraph learning task. Taheri et al. [187] presented Fed-IIoT, a FL-based solution for Android malware detection that uses generative adversarial networks to simulate poisoned settings. When evaluated over several datasets, performance is better than local adversarial training.

30) CYBER-PHYSICAL SYSTEMS

FL is a viable method for safeguarding data privacy in cyber-physical systems, which often manage multi-source and large-scale data from several domains. Yang et al., [183] presented a privacy-preserving tensor completion technique based on a Gaussian mechanism and an improved federated soft-impute algorithm. This method protects the privacy of dispersed data by addressing partial and private information while retaining high accuracy, as proved by a formal recovery error boundary.

J. RQ2: IN WHAT WAYS HAS FL BEEN COMBINED WITH SPECIFIC MACHINE LEARNING PARADIGMS (E.G., TRANSFER LEARNING, REINFORCEMENT LEARNING, AND CRYPTOGRAPHIC LEARNING) TO IMPROVE PERFORMANCE, SCALABILITY, OR PRIVACY?

1) FL OVERVIEW

FL is a collaborative machine learning framework that enables multiple clients to train models locally on their private data and share only model updates, not raw data. To address challenges related to performance, scalability, and privacy in decentralized environments, FL has increasingly been integrated with other machine learning paradigms such as transfer learning, reinforcement learning, and cryptographic learning. These hybrid approaches leverage the strengths of complementary paradigms to enhance model adaptability across heterogeneous devices, improve data privacy, and enable more efficient and scalable deployments in real-world applications.

2) PRIVACY

FL prioritizes privacy by storing raw data locally and communicating only model changes. This strategy considerably lowers the danger of data breaches as compared to centralized training, which involves sharing data with a central server, posing privacy issues. Kaur et al., [190] highlighted FL's potential to protect data privacy, as opposed to centralized approaches, which present more dangers during data transfers. To improve privacy, Lu et al. [4] investigated merging blockchain and FL in industrial IoT applications. According to Ogundokun et al., [189], FL meets privacy regulations such as GDPR, which protects data more effectively than centralized solutions. Govindwar et al., [191] emphasized that traditional centralized learning presents privacy risks because of the exponential rise of data created by the Internet of Things. They identified problems with data collecting and user information sharing.

In contrast, FL's way of transmitting local updates keeps user data on the device. Fang and Qian et al., [198] introduced PFMLP, a privacy-preserving system that employs partly homomorphic encryption and FL. Their method communicates only encrypted gradients, attaining model accuracy with variations of less than 1% and increasing training time by 25-28% using an improved Paillier algorithm. FL has also

been combined with cryptographic learning techniques such as secure multiparty computation (SMPC) and homomorphic encryption to provide end-to-end encrypted model aggregation, further strengthening data privacy in sensitive domains like healthcare and finance.

3) PERFORMANCE

FL uses multiple data sources to improve model performance. However, it confronts issues with data dissemination and communication. FL distributes learning over several edge devices and might have performance concerns, especially with heterogeneous devices and non-IID data. Liu et al., [192] addressed these issues with approaches such as asynchronous FL and momentum gradient descent, which try to enhance speed but often result in delayed convergence. Kairouz et al., [193] examined innovations such as adaptive federated optimization and model compression, which assist minimize some of FL's performance limitations, such as sluggish convergence and increased processing load. Federated Transfer Learning (FTL) has been applied to improve model performance in cases where data distributions differ significantly across clients. In such scenarios, pre-trained models are fine-tuned locally, enhancing personalization and performance while avoiding the computational burden of training from scratch. This is particularly beneficial in domains like medical imaging and cross-silo learning, where institutions share only partial feature sets or operate with limited local data. Additionally, reinforcement learning has been integrated into FL to dynamically optimize communication frequency, client selection, and resource allocation. For instance, FL with reinforcement learning agents allows edge devices to learn scheduling policies that reduce communication overhead and increase training efficiency under constrained environments.

4) SCALABILITY

FL's decentralized design improves scalability over standard centralized learning by harnessing the processing capacity of local devices. Campolo et al., [194] highlighted how FL on IoT devices might limit data transmission to centralized servers, hence protecting privacy and reducing network congestion. They developed a system that uses the MQTT protocol with OMA LwM2M semantics to increase communication efficiency in IoT applications. Chen et al., [195] demonstrated that FL over wireless networks decreases network traffic and communication costs, although wireless impairments might affect performance, requiring network tuning. Abarghouyi et al., [196] proposed a two-level learning technique for hierarchical FL over wireless networks, which included scalable over-the-air aggregation and bandwidth-limited broadcast strategies. Their solution tackles scalability issues while efficiently managing data heterogeneity and interference, resulting in excellent learning accuracy and exceeding classic hierarchical learning algorithms. Moreover, reinforcement learning integrated within FL frameworks supports decision-making in decentralized and autonomous systems, such as fleets of autonomous vehicles or drones. These systems use federated deep reinforcement learning to share policy updates instead of raw experiences, maintaining scalability while enabling real-time learning across agents.

K. RQ3: WHAT ARE THE PRIMARY TECHNICAL AND INFRASTRUCTURAL BOTTLENECKS ENCOUNTERED WHEN DEPLOYING FL AT SCALE, AND WHAT MITIGATION STRATEGIES HAVE BEEN PROPOSED?

1) CHALLENGES AND SOLUTIONS IN FL

FL is a distributed learning paradigm that allows multiple devices to collaboratively learn a global model without sharing their local data. FL has many advantages in terms of data privacy, scalability, and efficiency, but it also faces some challenges and trade-offs, especially when implemented at the network edge with resource-constrained and heterogeneous devices. Some of the repercussions of scalability challenges and resource constraints in FL are:

- **Communication Overhead:** FL requires frequent communication between the devices and the central server to exchange model updates. This can incur high bandwidth and energy costs, especially for large-scale networks with many devices. Sean et al., [203] provide a comprehensive review of fairness in FL, focusing on its motivations, concepts, challenges, techniques, and future research directions for ensuring equitable decision-making in privacy-preserving distributed machine learning systems. Communication overhead can also affect the convergence and accuracy of FL, as devices may have different communication capabilities and delays.
- **System Heterogeneity:** FL devices may have different hardware specifications, software platforms, and computational resources. This can lead to imbalanced workloads, unfair resource allocation, and inconsistent performance among devices. Nader et al., [202] provide a comprehensive survey of the unique security vulnerabilities in FL, highlighting key attack vectors, defenses, and challenges, while proposing future research directions to enhance the robustness of FL systems. System heterogeneity can also make it difficult to design and evaluate FL algorithms, as existing simulation frameworks may not capture the realistic scenarios of FL deployment.
- **Data Heterogeneity:** FL devices may have different data distributions, sizes, and qualities. This can result in non-iid (independent and identically distributed) data, which can degrade the performance and robustness of FL. A.K.S et al., [201] propose a method to balance poisoning detection and accommodating data diversity in FL, ensuring fairer and more accurate models, particularly with non-i.i.d. data, by distinguishing between legitimate and malicious client updates. Data

heterogeneity can also raise privacy and security issues, as devices may have sensitive or malicious data that can affect the global model.

2) MITIGATION STRATEGIES

To address these challenges, researchers have proposed various solutions, such as:

- **Communication-efficient Methods:** These methods aim to reduce the communication overhead of FL by using techniques such as compression, quantization, sparsification, or encryption of model updates. They can also use adaptive or asynchronous communication schemes to cope with varying network conditions and device availability. However, these methods can slow convergence and may introduce biases, especially under non-IID data. K.M. et al., [197] provide a comprehensive review of FL research, categorizing existing studies based on challenges, design factors, and applications, while highlighting promising future research directions in the field.
- **Heterogeneity-aware Methods:** These methods aim to account for the system and data heterogeneity of FL devices by using techniques such as clustering, personalisation, or federated distillation. These methods ensure that models are better suited to the characteristics of individual devices, improving local utility while preserving global performance. Hierarchical FL architectures can also balance workloads across devices, though they may introduce multi-tier latency and failure modes at intermediate aggregators. Helio et al., [26] analyse the security vulnerabilities and privacy challenges of FL, review mitigation strategies, evaluate secure FL applications, and highlight future research directions to enhance user privacy and model performance. They can also use dynamic or hierarchical FL architectures to balance the workloads and resources among devices.
- **Privacy-preserving and Secure Methods** These methods aim to protect the data and model privacy and security of FL devices by using techniques such as differential privacy, homomorphic encryption, or secure multi-party computation. However, they impose substantial computational and memory overhead on edge-class hardware, reducing the frequency of training rounds and model sizes. Jie et al., [30] provide a systematic overview of FL, addressing its principles, privacy and security mechanisms, and challenges like communication overhead and heterogeneity, and highlight research advancements and future directions to enhance FL's application in privacy-sensitive domains. They can also use robust aggregation or anomaly detection methods to mitigate the effects of malicious or faulty devices.

3) CRITICAL APPRAISAL OF TRADE-OFFS IN FL

In contrast to the method inventory discussed above, a critical appraisal reveals persistent trade-offs that materially affect real-world FL deployments (e.g., [197], [201], [202], [203]).

- Communication-efficient schemes such as gradient sparsification, quantization, and over-the-air aggregation are effective in reducing uplink costs. However, they can slow convergence and bias updates, particularly when data is non-IID. Aggressive compression techniques may amplify model drift, while secure aggregation, though essential for maintaining confidentiality, limits adaptive weighting and per-client diagnostics during training.
- Heterogeneity-aware approaches (e.g., personalization, client clustering, FedProx-style regularization, and federated distillation) enhance local utility, especially with skewed data. However, these techniques risk fragmenting the global hypothesis class, leading to weaker generalization across clients and higher orchestration complexity. Hierarchical FL helps alleviate straggler effects but introduces multi-tier latency and potential failure modes at intermediate aggregators.
- Privacy-preserving mechanisms create a clear utility–cost frontier. Client- or record-level differential privacy offers formal privacy guarantees but degrades accuracy, particularly as the privacy budget tightens and compositions accumulate over multiple rounds. Meanwhile, homomorphic encryption and secure multi-party computation improve data protection but impose substantial computational and memory overhead on edge-class hardware. This overhead limits round frequency and model size.
- Robust aggregation rules (e.g., coordinate-wise median, trimmed mean, Krum) are designed with the assumption of near-IID gradients and bounded Byzantine failure rates. However, in the presence of realistic non-IID skew, they may suppress informative, albeit outlying, updates. Additionally, these methods remain vulnerable to Sybil amplification unless coupled with participation auditing and reputation systems.
- Fairness-aware client selection strategies aim to correct performance disparities by prioritizing underrepresented or challenging clients. While this can improve fairness, it typically increases the time-to-accuracy due to the additional focus on clients that may take longer to converge.

Empirically, many studies continue to rely on simulator-friendly benchmarks (e.g., MNIST, CIFAR) and fail to report multi-objective metrics (e.g., privacy, communication bytes, energy/J, and wall-clock latency), which limits the external validity of their findings.

Taken together, these observations suggest that no single mitigation strategy dominates across all settings. Instead, deployment-grade federated learning should combine techniques along a context-specific Pareto frontier. For example, pairing lightweight compression with secure aggregation as a default, incorporating personalization when non-IID skew is

high, reserving differential privacy for sensitive domains with calibrated, and primarily using cryptographic aggregation in cross-silo scenarios with moderate throughput demands.

L. RQ4: WHAT ARE THE CURRENT AND EMERGING APPLICATION DOMAINS FOR FL, AND WHAT FUTURE RESEARCH DIRECTIONS ARE EVIDENT FROM THE LITERATURE?

1) EMERGING AND FUTURE DIRECTIONS OF FL

FL has the potential to enable new applications and scenarios that are not feasible with traditional centralized ML approaches. In this section, we discuss some of the emerging and future directions of FL in various domains and industries, such as smart cities, autonomous vehicles, IoT, healthcare, and education. Tian et al., [205] discuss the concept of FL, highlighting its unique challenges in training models on decentralized, heterogeneous networks while preserving data privacy, and reviewing current methods and future research directions. We also highlight the challenges and opportunities of FL in these domains, and how FL can address the issues of data privacy, security, access, and heterogeneity.

- **Smart Cities:** FL can facilitate the development of smart city applications that leverage the data collected from various sources, such as sensors, cameras, traffic lights, and mobile devices, to improve the quality of life and services for citizens. For example, FL can enable smart parking, traffic management, waste management, and public safety applications, without compromising the privacy of the data owners or the efficiency of the communication network. Jie et al., [30] provide a systematic overview of FL, addressing its fundamental concepts, and challenges like privacy, security, communication, and heterogeneity, and exploring current research advancements and future directions for practical applications. However, FL in smart cities also faces challenges such as heterogeneity of devices, data, and tasks, scalability of the system, and robustness against malicious attacks.
- **Autonomous Vehicles:** FL can enhance the performance and safety of autonomous vehicles by allowing them to learn from the data generated by other vehicles, such as road conditions, traffic patterns, and driving behaviors, without sharing the raw data or compromising the privacy of the drivers. FL can also enable collaborative and cooperative driving among autonomous vehicles, such as platooning, lane changing, and intersection crossing. However, FL in autonomous vehicles also requires addressing the issues of latency, bandwidth, reliability, and security of the communication network, as well as the heterogeneity and distribution of the data and the models.
- **Internet of Things (IoT):** FL can enable IoT devices to learn from the data generated by other devices, such as sensors, smart meters, wearables, and smart home appliances, without sending the data to a central server or cloud. FL can also enable IoT devices to perform edge computing, such as inference, prediction, and decision-making, without relying on the cloud or the network. Sean et al., [203] review fairness in FL, covering its motivations, challenges, methods, and future research directions to ensure equitable decision-making while preserving data privacy. However, FL in IoT also poses challenges such as resource constraints, communication overhead, and synchronization issues of the devices, as well as the diversity and complexity of the data and the tasks.
- **Healthcare:** FL can enable healthcare applications that leverage the data collected from various sources, such as electronic health records, medical images, genomic data, and wearable devices, to improve the diagnosis, treatment, and prevention of diseases. FL can also enable personalized and precision medicine, such as drug discovery, disease risk prediction, and treatment recommendation, without violating the privacy or the regulations of the data owners or providers. K.M. et al., [197] discuss FL, a method for training algorithms across decentralized devices without sharing raw data, highlighting its challenges, design aspects, and applications, such as enabling privacy-preserving medical image analysis where patient data remains on local devices. However, FL in healthcare also faces challenges such as data quality, heterogeneity, imbalance, model complexity, and interpretability, and ethical and legal issues.
- **Education:** FL can enable education applications that leverage the data collected from various sources, such as online courses, learning platforms, and educational games, to improve the learning outcomes and experiences of students. FL can also enable personalized and adaptive learning, such as curriculum design, content recommendation, and feedback generation, without exposing the personal or sensitive information of the students or the teachers. However, FL in education also requires addressing the issues of data diversity, reliability, availability, model fairness, and accountability, and pedagogical and psychological factors.
- **Privacy-Preserving Personalization in Edge Environments:** The increasing adoption of edge AI in consumer devices (e.g., AR glasses, smart home assistants) demands on-device personalized models without compromising privacy. Future work can explore federated meta-learning and federated transfer learning to personalize global models using limited device-specific data while maintaining generalization.
- **Vertical FL (VFL) in Finance and Healthcare**: While horizontal FL is widely studied, VFL, where clients hold different feature sets over shared user IDs, is underexplored. Real-world implementations in credit scoring, insurance fraud detection, and patient-centric healthcare could benefit from secure multi-party

computation (SMPC) or split learning to combine vertically partitioned data across institutions.

- **Real-Time FL for Autonomous Systems:** Autonomous vehicles, UAVs, and robots must make low-latency collaborative decisions. Future work should target event-driven or asynchronous FL algorithms capable of real-time learning with non-iid and streaming data. Practical deployment requires adaptation to network jitter, unreliable links, and mobility.
- **Resource-Aware FL for Ultra-Low-Power Devices:** Federated optimization over battery-constrained microcontrollers and wearable's remains a major challenge. Advancing one-shot FL, quantized local updates, and adaptive client selection can unlock FL's potential in real-time health monitoring and remote sensing applications.
- **FL in Federated Cloud-Edge-Device Ecosystems**: Future networks (6G and beyond) will rely on a hierarchical compute continuum, integrating cloud, edge, and IoT devices. Practical research is needed on collaborative FL scheduling, privacy-preserving workload offloading, and hierarchical aggregation protocols that dynamically assign roles across this stack.
- **FL for Cross-Organization AI Governance and Compliance:** With global data regulations (e.g., GDPR, HIPAA), there is a rising need for auditable, explainable FL frameworks. Future work should explore FL with federated explainable AI (XAI) and blockchain-backed model provenance to ensure compliance, especially in sectors like digital forensics and smart law enforcement.

2) KEY RESEARCH GAPS

Despite the remarkable progress in FL, several research gaps remain that hinder its widespread adoption and efficiency. These gaps need to be addressed to ensure the long-term viability and scalability of FL systems. The following research gaps should be prioritized:

- **Data Heterogeneity and Non-IID Data:** Most FL models assume that data across devices are independent and identically distributed (IID). However, in real-world scenarios, data is often non-IID, leading to challenges in model accuracy and convergence. Developing FL algorithms that can efficiently handle non-IID data is a major research gap.
- **Optimization Techniques for Large-Scale Deployments:** As the number of devices participating in FL increases, the optimization of model updates becomes increasingly difficult. Current methods for optimizing FL, such as FedAvg, face scalability issues when applied to large-scale systems. Research into more efficient optimization techniques that minimize communication overhead and speed up convergence is crucial [209].
- **Model Personalization:** A key aspect of FL is the ability to personalize models on different devices. However, there is still a lack of efficient methods for achieving model personalization without sacrificing privacy or system performance. Research into federated meta-learning and advanced personalization algorithms will help address this gap.
- **Security and Privacy in Open Environments:** While FL inherently protects data privacy by keeping data localized, the communication and aggregation process still exposes models to potential attacks, such as model poisoning or inference attacks. More robust security mechanisms are needed to protect models against these vulnerabilities in open environments.

3) DEPLOYMENT CHALLENGES

The deployment of FL faces several significant challenges that need to be addressed before it can be fully adopted across various industries:

- **Scalability:** Scaling FL systems to handle millions of devices is a major challenge. Efficient communication protocols and aggregation methods need to be developed to ensure the scalability of FL systems without overburdening the network or computational resources. This involves optimizing both the communication infrastructure and the model aggregation techniques.
- **Resource Constraints:** Many devices participating in FL, such as IoT devices or mobile phones, have limited computational power, memory, and battery life. Designing lightweight FL models that can operate efficiently on such resource-constrained devices is critical. Future research should focus on developing FL algorithms that minimize resource consumption while maintaining model accuracy [210].
- **Communication Overhead:** One of the most significant challenges in FL is the high communication overhead due to the frequent exchange of model updates between devices and the central server. Research on communication-efficient FL techniques, such as compression, quantization, and sparsification of model updates, is needed to reduce this overhead.
- **Device Heterogeneity:** Devices involved in FL may have different hardware capabilities, operating systems, and network conditions. This heterogeneity poses challenges in ensuring equal participation and fairness in the learning process. Developing techniques to handle device diversity, including dynamic client selection and adaptive aggregation strategies, is essential for successful deployment.

4) UNDEREXPLORED DOMAINS

While FL has been applied to a variety of domains, there are several emerging areas where its potential remains largely untapped. These underexplored domains could significantly benefit from the adoption of FL:

- **FL for Edge and Fog Computing:** Edge and fog computing environments are becoming increasingly prevalent, but they are underutilized in FL research.

Federated learning can greatly enhance the capabilities of edge devices by enabling them to collaboratively learn models while preserving privacy. Further exploration of FL in edge and fog computing systems, especially in resource-constrained environments, is an exciting research avenue.

- **FL in Healthcare Beyond Diagnosis:** While FL has made strides in medical image analysis and diagnostic applications, its potential in other areas of healthcare remains largely unexplored. For instance, FL could be leveraged for personalized treatment plans, drug discovery, and epidemiological studies without exposing sensitive patient data. Research into how FL can enhance healthcare beyond diagnosis is a promising, underexplored domain.
- **FL for Financial Services:** The financial sector has not yet fully embraced the potential of FL. There is an opportunity to deploy FL in areas such as fraud detection, credit scoring, and financial risk assessment while ensuring data privacy. Further research on how FL can be integrated into financial models, particularly in the context of secure, decentralized data sharing, is needed.
- **FL for Smart Grids and Energy Systems:** Smart grids, which involve decentralized power generation, distribution, and consumption, could benefit significantly from FL. The ability to use FL for optimizing power distribution, load balancing, and predictive maintenance in smart grids could reduce energy consumption and improve efficiency. Research into FL applications for smart grids is a largely underexplored domain with great potential [211].
- **FL for Autonomous Systems:** While FL has been explored for autonomous vehicles, its use in other autonomous systems such as drones, robotics, and industrial machines is still in its infancy. These systems require real-time, distributed decision-making and could benefit from FL models that learn from decentralized data while preserving privacy. Research in this space is crucial for advancing FL in autonomous technologies.

III. CONCLUSION

The future research trajectory in FL should focus on addressing several key aspects identified in this study. Firstly, there is a need to explore innovative techniques for enhancing the integration of FL with diverse machine-learning approaches to ensure not only efficient performance but also robust privacy preservation and scalability. Research efforts should delve into developing advanced algorithms and frameworks that strike a balance between model accuracy and privacy protection in federated environments. Additionally, investigating solutions to mitigate scalability challenges and resource constraints in FL is imperative, with a particular emphasis on designing more resource-efficient algorithms and protocols. Future work should also extend beyond the current industries implementing FL and explore novel applications, harnessing the potential of FL in upcoming technological advancements and emerging sectors. In conclusion, this research paper has provided a comprehensive examination of FL, delving into its recent advancements, integration with machine learning approaches, scalability challenges, and potential applications in various industries. The findings underscore the significance of FL in addressing privacy concerns while fostering collaborative learning across decentralized networks. As industries increasingly adopt FL, it is crucial to continue advancing the field by developing more sophisticated integration strategies, overcoming scalability issues, and exploring uncharted territories for FL applications. The path forward involves interdisciplinary collaboration, combining expertise from machine learning, privacy preservation, and domain-specific fields to unlock the full potential of FL in shaping the future of secure and collaborative machine learning.

DATA AVAILABILITY STATEMENT

This research does not contain any associated data.

AUTHOR CONTRIBUTION

All authors have contributed equally.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DECLARATIONS

The authors declare that this manuscript has not been submitted to other journals for consideration.

REFERENCES

[1] H. Kim, J. Park, M. Bennis, and S.-L. Kim, "Blockchained on-device federated learning," *IEEE Commun. Lett.*, vol. 24, no. 6, pp. 1279–1283, Jun. 2020, doi: 10.1109/LCOMM.2019.2921755.

[2] D. Li, D. Han, T.-H. Weng, Z. Zheng, H. Li, H. Liu, A. Castiglione, and K.-C. Li, "Blockchain for federated learning toward secure distributed machine learning systems: A systemic survey," *Soft Comput.*, vol. 26, no. 9, pp. 4423–4440, Nov. 2021, doi: 10.1007/s00500-021-06496-5.

[3] M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, "Federated deep learning for cyber security in the Internet of Things: Concepts, applications, and experimental analysis," *IEEE Access*, vol. 9, pp. 138509–138542, 2021, doi: 10.1109/ACCESS.2021.3118642.

[4] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4177–4186, Jun. 2020, doi: 10.1109/TII.2019.2942190.

[5] U. Majeed and C. S. Hong, "FLchain: Federated learning via MEC-enabled blockchain network," in *Proc. 20th Asia–Pacific Netw. Oper. Manag. Symp. (APNOMS)*, Sep. 2019, pp. 1–4. [Online]. Available: https://ieeexplore.ieee.org/document/8892848

[6] D. Polap, G. Srivastava, A. Jolfaei, and R. M. Parizi. (2020). *Blockchain Technology and Neural Networks for the Internet of Medical Things*. Accessed: Jul. 3, 2021. [Online]. Available: https://researchers.mq.edu.au/en/publications/blockchain-technology-and-neural-networks-for-the-internet-of-med

[7] S. Lugan, P. Desbordes, E. Brion, L. X. Ramos Tormo, A. Legay, and B. Macq, "Secure architectures implementing trusted coalitions for blockchained distributed learning (TCLearn)," *IEEE Access*, vol. 7, pp. 181789–181799, 2019, doi: 10.1109/ACCESS.2019.2959220.

[8] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, "Secure and provenance enhanced Internet of Health Things framework: A blockchain managed federated learning approach," *IEEE Access*, vol. 8, pp. 205071–205087, 2020, doi: 10.1109/ACCESS.2020.3037474.

[9] Z. Li, J. Liu, J. Hao, H. Wang, and M. Xian, "CrowdSFL: A secure crowd computing framework based on blockchain and federated learning," *Electronics*, vol. 9, no. 5, p. 773, May 2020, doi: 10.3390/electronics9050773.

[10] Y. Liu, J. Peng, J. Kang, A. M. Iliyasu, D. Niyato, and A. A. A. El-Latif, "A secure federated learning framework for 5G networks," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 24–31, Aug. 2020, doi: 10.1109/MWC.01.1900525.

[11] Q. Wang, Y. Guo, X. Wang, T. Ji, L. Yu, and P. Li, "AI at the edge: Blockchain-empowered secure multiparty learning with heterogeneous models," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9600–9610, Oct. 2020, doi: 10.1109/JIOT.2020.2987843.

[12] P. K. Sharma, J. H. Park, and K. Cho, "Blockchain and federated learning-based distributed computing defence framework for sustainable society," *Sustain. Cities Soc.*, vol. 59, Aug. 2020, Art. no. 102220, doi: 10.1016/j.scs.2020.102220.

[13] L. Wu, W. Ruan, J. Hu, and Y. He, "A survey on blockchain-based federated learning," *Future Internet*, vol. 15, no. 12, p. 400, Dec. 2023, doi: 10.3390/fi15120400.

[14] R. Ning, C. Wang, X. Li, R. Gazda, and H. Wu, "BlockFed: A high-performance and trustworthy blockchain-based federated learning framework," in *Proc. IEEE Global Commun. Conf.*, Dec. 2023, pp. 892–897, doi: 10.1109/GLOBECOM54140.2023.10437623.

[15] Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, and Y. Liu, "Privacy-preserving blockchain-based federated learning for IoT devices," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1817–1829, Feb. 2021, doi: 10.1109/JIOT.2020.3017377.

[16] W. Zhang, Q. Lu, Q. Yu, Z. Li, Y. Liu, S. K. Lo, S. Chen, X. Xu, and L. Zhu, "Blockchain-based federated learning for device failure detection in industrial IoT," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5926–5937, Apr. 2021, doi: 10.1109/JIOT.2020.3032544.

[17] O. El Rifai, M. Biotteau, X. de Boissezon, I. Megdiche, F. Ravat, and O. Teste, "Blockchain-based federated learning in medicine," in *Proc. Int. Conf. Artif. Intell. Med.*, 2020, pp. 214–224, doi: 10.1007/978-3-030-59137-3_20.

[18] S. Aich, N. K. Sinai, S. Kumar, M. Ali, Y. R. Choi, M. I. L. Joo, and H. C. Kim, "Protecting personal healthcare record using blockchain & federated learning technologies," in *Proc. 24th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2022, pp. 109–112, doi: 10.23919/ICACT53585.2022.9728772.

[19] S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4734–4746, Aug. 2020, doi: 10.1109/TCOMM.2020.2990686.

[20] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4298–4311, Apr. 2020, doi: 10.1109/TVT.2020.2973651.

[21] H. Chai, S. Leng, Y. Chen, and K. Zhang, "A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 3975–3986, Jul. 2020, doi: 10.1109/TITS.2020.3002712.

[22] L. Cui, X. Su, Z. Ming, Z. Chen, S. Yang, Y. Zhou, and W. Xiao, "CREAT: Blockchain-assisted compression algorithm of federated learning for content caching in edge computing," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14151–14161, Aug. 2022, doi: 10.1109/JIOT.2020.3014370.

[23] Y. Wang, Z. Su, N. Zhang, and A. Benslimane, "Learning in the air: Secure federated learning for UAV-assisted crowdsensing," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1055–1069, Apr. 2021, doi: 10.1109/TNSE.2020.3014385.

[24] S. Pourroostaei Ardakani, N. Du, C. Lin, J.-C. Yang, Z. Bi, and L. Chen, "A federated learning-enabled predictive analysis to forecast stock market trends," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 4, pp. 4529–4535, Feb. 2023, doi: 10.1007/s12652-023-04570-4.

[25] L. Witt, M. Heyer, K. Toyoda, W. Samek, and D. Li, "Decentral and incentivized federated learning frameworks: A systematic literature review," *IEEE Internet Things J.*, vol. 10, no. 4, pp. 3642–3663, Feb. 2023, doi: 10.1109/JIOT.2022.3231363.

[26] H. N. C. Neto, J. Hribar, I. Dusparic, D. M. F. Mattos, and N. C. Fernandes, "A survey on securing federated learning: Analysis of applications, attacks, challenges, and trends," *IEEE Access*, vol. 11, pp. 41928–41953, 2023, doi: 10.1109/ACCESS.2023.3269980.

[27] M. Islam, M. T. Reza, M. Kaosar, and M. Z. Parvez, "Effectiveness of federated learning and CNN ensemble architectures for identifying brain tumors using MRI images," *Neural Process. Lett.*, vol. 55, no. 4, pp. 3779–3809, Aug. 2022, doi: 10.1007/s11063-022-11014-1.

[28] O. Aouedi, A. Sacco, K. Piamrat, and G. Marchetto, "Handling privacy-sensitive medical data with federated learning: Challenges and future directions," *IEEE J. Biomed. Health Informat.*, vol. 27, no. 2, pp. 790–803, Feb. 2023, doi: 10.1109/JBHI.2022.3185673.

[29] Z. K. Taha, C. T. Yaw, S. P. Koh, S. K. Tiong, K. Kadirgama, F. Benedict, J. D. Tan, and Y. A. Balasubramaniam, "A survey of federated learning from data perspective in the healthcare domain: Challenges, methods, and future directions," *IEEE Access*, vol. 11, pp. 45711–45735, 2023, doi: 10.1109/ACCESS.2023.3267964.

[30] J. Wen, Z. Zhang, Y. Lan, Z. Cui, J. Cai, and W. Zhang, "A survey on federated learning: Challenges and applications," *Int. J. Mach. Learn. Cybern.*, vol. 14, no. 2, pp. 513–535, Nov. 2022, doi: 10.1007/s13042-022-01647-y.

[31] V. A. Patel, P. Bhattacharya, S. Tanwar, R. Gupta, G. Sharma, P. N. Bokoro, and R. Sharma, "Adoption of federated learning for healthcare informatics: Emerging applications and future directions," *IEEE Access*, vol. 10, pp. 90792–90826, 2022, doi: 10.1109/ACCESS.2022.3201876.

[32] X. Li, Y. Gu, N. Dvornek, L. H. Staib, P. Ventola, and J. S. Duncan, "Multi-site fMRI analysis using privacy-preserving federated learning and domain adaptation: ABIDE results," *Med. Image Anal.*, vol. 65, Oct. 2020, Art. no. 101765, doi: 10.1016/j.media.2020.101765.

[33] *Request Rejected*. [Online]. Available: https://ieeexplore.ieee.org/document/9146846

[34] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5615–5624, Aug. 2021, doi: 10.1109/TII.2020.3023430.

[35] B. Liu, L. Wang, and M. Liu, "Lifelong federated reinforcement learning: A learning architecture for navigation in cloud robotic systems," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst. (IROS)*, Nov. 2019, pp. 1688–1695, doi: 10.1109/IROS40897.2019.8967908.

[36] Y. Hu, X. Sun, Y. Chen, and Z. Lu, "Model and feature aggregation based federated learning for multi-sensor time series trend following," in *Proc. Int. Work-Conf. Artif. Neural Netw.*, Jan. 2019, pp. 233–246, doi: 10.1007/978-3-030-20521-8_20.

[37] Y. Chen, X. Qin, J. Wang, C. Yu, and W. Gao, "FedHealth: A federated transfer learning framework for wearable healthcare," *IEEE Intell. Syst.*, vol. 35, no. 4, pp. 83–93, Jul. 2020, doi: 10.1109/MIS.2020.2988604.

[38] Z. Xiong, Z. Cheng, X. Lin, C. Xu, X. Liu, D. Wang, X. Luo, Y. Zhang, H. Jiang, N. Qiao, and M. Zheng, "Facing small and biased data dilemma in drug discovery with enhanced federated learning approaches," *Sci. China Life Sci.*, vol. 65, no. 3, pp. 529–539, Mar. 2022, doi: 10.1007/s11427-021-1946-0.

[39] L. Huang, A. L. Shea, H. Qian, A. Masurkar, H. Deng, and D. Liu, "Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records," *J. Biomed. Informat.*, vol. 99, Nov. 2019, Art. no. 103291, doi: 10.1016/j.jbi.2019.103291.

[40] W. Li, F. Milletarí, D. Xu, N. Rieke, J. Hancox, W. Zhu, M. Baust, Y. Cheng, S. Ourselin, M. J. Cardoso, and A. Feng, "Privacy-preserving federated brain tumour segmentation," in *Proc. Int. Workshop Mach. Learn. Med. Imag.*, Jan. 2019, pp. 133–141. [Online]. Available: https://kclpure.kcl.ac.uk/portal/en/publications/privacypreserving-federated-brain-tumour-segmentation(93e7026d-927e-4b77-bd13-7463b161e910)/export.html

[41] S. Duan, D. Zhang, Y. Wang, L. Li, and Y. Zhang, "JointRec: A deep-learning-based joint cloud video recommendation framework for mobile IoT," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1655–1666, Mar. 2020, doi: 10.1109/JIOT.2019.2944889.

[42] S. Samarakoon, M. Bennis, W. Saad, and M. Debbah, "Distributed federated learning for ultra-reliable low-latency vehicular communications," *IEEE Trans. Commun.*, vol. 68, no. 2, pp. 1146–1159, Feb. 2020, doi: 10.1109/TCOMM.2019.2956472.

[43] *Privacy-Preserving Traffic Flow Prediction: A Federated Learning Approach | IEEE Journals & Magazine | IEEE Xplore*. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9082655

[44] H. Zhang, J. Bosch, and H. H. Olsson. (Jul. 1, 2021). *End-to-End Federated Learning for Autonomous Driving Vehicles*. [Online]. Available: https://ieeexplore.ieee.org/document/9533808

[45] E. Bakopoulou, B. Tillman, and A. Markopoulou, "FedPacket: A federated learning approach to mobile packet classification," *IEEE Trans. Mobile Comput.*, vol. 21, no. 10, pp. 3609–3628, Oct. 2022, doi: 10.1109/TMC.2021.3058627.

[46] Y. Liu, Z. Ai, S. Sun, S. Zhang, Z. Liu, and H. Yu, "FedCoin: A peer-to-peer payment system for federated learning," in *Federated Learning: Privacy and Incentive* (Lecture Notes in Computer Science), 2020, pp. 125–138.

[47] R. Doku, D. B. Rawat, and C. Liu. (Jul. 1, 2019). *Towards Federated Learning Approach To Determine Data Relevance in Big Data*. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8843451

[48] N. N. Sakhare and I. S. Shaik, "Spatial federated learning approach for the sentiment analysis of stock news stored on blockchain," *Spatial Inf. Res.*, vol. 32, no. 1, pp. 13–27, Jun. 2023, doi: 10.1007/s41324-023-00529-x.

[49] A. Albaseer, B. S. Ciftler, M. Abdallah, and A. Al-Fuqaha, "Exploiting unlabeled data in smart cities using federated edge learning," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 1666–1671, doi: 10.1109/IWCMC48107.2020.9148475.

[50] Y. M. Saputra, D. T. Hoang, D. N. Nguyen, E. Dutkiewicz, M. D. Mueck, and S. Srikanteswara, "Energy demand prediction with federated learning for electric vehicle networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/9013587/

[51] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A.-R. Sadeghi, "DÏoT: A federated self-learning anomaly detection system for IoT," in *Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2019, pp. 756–767, doi: 10.1109/ICDCS.2019.00080.

[52] D. Leroy, A. Coucke, T. Lavril, T. Gisselbrecht, and J. Dureau, "Federated learning for keyword spotting," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2019, pp. 6341–6345, doi: 10.1109/ICASSP.2019.8683546.

[53] X. Liang, Y. Liu, T. Chen, M. Liu, and Q. Yang, "Federated transfer reinforcement learning for autonomous driving," in *Adaptation, Learning, and Optimization*, 2022, pp. 357–371.

[54] M. J. Sheller, G. A. Reina, B. Edwards, J. Martin, and S. Bakas, "Multi-institutional deep learning modeling without sharing patient data: A feasibility study on brain tumor segmentation," in *Proc. Int. MICCAI Brainlesion Workshop*, 2019, pp. 92–104, doi: 10.1007/978-3-030-11723-8_9.

[55] S. Silva, B. A. Gutman, E. Romero, P. M. Thompson, A. Altmann, and M. Lorenzi, "Federated learning in distributed medical databases: Meta-analysis of large-scale subcortical brain data," in *Proc. IEEE 16th Int. Symp. Biomed. Imag. (ISBI)*, Apr. 2019, pp. 270–274. [Online]. Available: https://ieeexplore.ieee.org/document/8759317

[56] H. Sharghi, W. Ma, and K. Sartipi, "Federated service-based authentication provisioning for distributed diagnostic imaging systems," in *Proc. IEEE 28th Int. Symp. Comput.-Based Med. Syst.*, Jun. 2015, pp. 344–347, doi: 10.1109/CBMS.2015.85.

[57] A. Korkmaz, A. Alhonainy, and P. Rao, "An evaluation of federated learning techniques for secure and privacy-preserving machine learning on medical datasets," in *Proc. IEEE Appl. Imag. Pattern Recognit. Workshop (AIPR)*, Oct. 2022, pp. 1–7, doi: 10.1109/AIPR57179.2022.10092212.

[58] R. Zeng, S. Zhang, J. Wang, and X. Chu, "FMore: An incentive scheme of multi-dimensional auction for federated learning in MEC," in *Proc. IEEE 40th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, pp. 278–288, Nov. 2020, doi: 10.1109/ICDCS47774.2020.00094.

[59] Y. Chen, X. Yang, X. Qin, H. Yu, P. Chan, and Z. Shen, "Dealing with label quality disparity in federated learning," in *Federated Learning: Privacy and Incentive*, (Lecture Notes in Computer Science), 2020, pp. 108–121, doi: 10.1007/978-3-030-63076-8_8.

[60] D. Chen, L. J. Xie, B. Kim, L. Wang, C. S. Hong, L.-C. Wang, and Z. Han, "Federated learning based mobile edge computing for augmented reality applications," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2020, pp. 767–773, doi: 10.1109/ICNC47757.2020.9049708.

[61] B. Shickel, P. J. Tighe, A. Bihorac, and P. Rashidi, "Deep EHR: A survey of recent advances in deep learning techniques for electronic health record (EHR) analysis," *IEEE J. Biomed. Health Informat.*, vol. 22, no. 5, pp. 1589–1604, Sep. 2018, doi: 10.1109/JBHI.2017.2767063.

[62] G. Harerimana, B. Jang, J. W. Kim, and H. K. Park, "Health big data analytics: A technology survey," *IEEE Access*, vol. 6, pp. 65661–65678, 2018, doi: 10.1109/ACCESS.2018.2878254.

[63] M. Hao, H. Li, G. Xu, Z. Liu, and Z. Chen, "Privacy-aware and resource-saving collaborative learning for healthcare in cloud computing," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6, doi: 10.1109/ICC40277.2020.9148979.

[64] T. S. Brisimi, R. Chen, T. Mela, A. Olshevsky, I. C. Paschalidis, and W. Shi, "Federated learning of predictive models from federated electronic health records," *Int. J. Med. Informat.*, vol. 112, pp. 59–67, Apr. 2018, doi: 10.1016/j.ijmedinf.2018.01.007.

[65] H. Chen, H. Li, G. Xu, Y. Zhang, and X. Luo, "Achieving privacy-preserving federated learning with irrelevant updates over e-health applications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6, doi: 10.1109/ICC40277.2020.9149385.

[66] Q. Wu, K. He, and X. Chen, "Personalized federated learning for intelligent IoT applications: A cloud-edge based framework," *IEEE Open J. Comput. Soc.*, vol. 1, pp. 35–44, 2020, doi: 10.1109/OJCS.2020.2993259.

[67] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "BEdge-Health: A decentralized architecture for edge-based IoMT networks using blockchain," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11743–11757, Jul. 2021, doi: 10.1109/JIOT.2021.3058953.

[68] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based e-health systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019, doi: 10.1109/ACCESS.2019.2917555.

[69] B. Yan, J. Wang, J. Cheng, Y. Zhou, Y. Zhang, Y. Yang, L. Liu, H. Zhao, C. Wang, and B. Liu, "Experiments of federated learning for COVID-19 chest X-ray images," in *Proc. Int. Conf. Artif. Intell. Secur.*, in Communications in computer and information science, Jan. 2021, pp. 41–53, doi: 10.1007/978-3-030-78618-2_4.

[70] S. Jin, X. Luo, and D. Ma, "Determining the breakpoints of fundamental diagrams," *IEEE Intell. Transp. Syst. Mag.*, vol. 12, no. 1, pp. 74–90, Oct. 2020, doi: 10.1109/MITS.2018.2876576.

[71] W. Y. B. Lim, J. Huang, Z. Xiong, J. Kang, D. Niyato, X.-S. Hua, C. Leung, and C. Miao, "Towards federated learning in UAV-enabled Internet of Vehicles: A multi-dimensional contract-matching approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5140–5154, Aug. 2021, doi: 10.1109/TITS.2021.3056341.

[72] S. Samarakoon, M. Bennis, W. Saad, and M. Debbah. (2018). *Federated Learning for Ultra-Reliable Low-Latency V2V Communications*. Accessed: Oct. 11, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8647927

[73] X. Zhang, M. Peng, S. Yan, and Y. Sun, "Deep-reinforcement-learning-based mode selection and resource allocation for cellular V2X communications," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6380–6391, Jul. 2020, doi: 10.1109/JIOT.2019.2962715.

[74] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Privacy-preserved task offloading in mobile blockchain with deep reinforcement learning," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 4, pp. 2536–2549, Dec. 2020, doi: 10.1109/TNSM.2020.3010967.

[75] J. Cao, K. Zhang, F. Wu, and S. Leng, "Learning cooperation schemes for mobile edge computing empowered Internet of Vehicles," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, May 2020, pp. 1–6, doi: 10.1109/WCNC45663.2020.9120493.

[76] D. Conway-Jones, T. Tuor, S. Wang, and K. K. Leung, "Demonstration of federated learning in a resource-constrained networked environment," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Jun. 2019, pp. 484–486, doi: 10.1109/SMARTCOMP.2019.00095.

[77] K. Xiong, S. Leng, C. Huang, C. Yuen, and Y. L. Guan, "Intelligent task offloading for heterogeneous V2X communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 4, pp. 2226–2238, Apr. 2021, doi: 10.1109/TITS.2020.3015210.

[78] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodriguez, and J. Yuan, "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3417–3442, 4th Quart., 2019, doi: 10.1109/COMST.2019.2906228.

[79] M. Chen, W. Saad, and C. Yin, "Liquid state machine learning for resource and cache management in LTE-U unmanned aerial vehicle (UAV) networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 3, pp. 1504–1517, Mar. 2019, doi: 10.1109/TWC.2019.2891629.

[80] T. Zeng, O. Semiari, M. Mozaffari, M. Chen, W. Saad, and M. Bennis, "Federated learning in the sky: Joint power allocation and scheduling with UAV swarms," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6, doi: 10.1109/ICC40277.2020.9148776.

[81] W. Yuan, C. Liu, F. Liu, S. Li, and D. W. K. Ng, "Learning-based predictive beamforming for UAV communications with jittering," *IEEE Wireless Commun. Lett.*, vol. 9, no. 11, pp. 1970–1974, Nov. 2020, doi: 10.1109/LWC.2020.3009951.

[82] Y. Wang, Y. Yang, and T. Luo, "Federated convolutional auto-encoder for optimal deployment of UAVs with visible light communications," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2020, pp. 1–6, doi: 10.1109/ICCWORKSHOPS49005.2020.9145090.

[83] Y. Qu, C. Dong, J. Zheng, H. Dai, F. Wu, S. Guo, and A. Anpalagan, "Empowering edge intelligence by air-ground integrated federated learning," *IEEE Netw.*, vol. 35, no. 5, pp. 34–41, Sep. 2021, doi: 10.1109/MNET.111.2100044.

[84] N. I. Mowla, N. H. Tran, I. Doh, and K. Chae, "Federated learning-based cognitive detection of jamming attack in flying ad-hoc network," *IEEE Access*, vol. 8, pp. 4338–4350, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8945183

[85] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, "Smart cities: A survey on data management, security, and enabling technologies," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2456–2501, 4th Quart., 2017, doi: 10.1109/COMST.2017.2736886.

[86] M. Mohammadi and A. Al-Fuqaha, "Enabling cognitive smart cities using big data and machine learning: Approaches and challenges," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 94–101, Feb. 2018, doi: 10.1109/MCOM.2018.1700298.

[87] D. R. Mukhametov, "Ubiquitous computing and distributed machine learning in smart cities," in *Proc. Wave Electron. its Appl. Inf. Telecommun. Syst. (WECONF)*, Jun. 2020, pp. 1–5, doi: 10.1109/WECONF48837.2020.9131518.

[88] *Trustworthy AI in the Age of Pervasive Computing and Big Data*. [Online]. Available: https://ieeexplore.ieee.org/document/9156127

[89] T.-C. Chiu, Y.-Y. Shih, A.-C. Pang, C.-S. Wang, W. Weng, and C.-T. Chou, "Semisupervised distributed learning with non-IID data for AIoT service platform," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9266–9277, Oct. 2020, doi: 10.1109/JIOT.2020.2995162.

[90] M. Masera, E. F. Bompard, F. Profumo, and N. Hadjsaid, "Smart (electricity) grids for smart cities: Assessing roles and societal impacts," *Proc. IEEE*, vol. 106, no. 4, pp. 613–625, Apr. 2018, doi: 10.1109/JPROC.2018.2812212.

[91] S. Pérez, J. Pérez, P. Arroba, R. Blanco, J. L. Ayala, and J. M. Moya, "Predictive GPU-based ADAS management in energy-conscious smart cities," in *Proc. IEEE Int. Smart Cities Conf. (ISC)*, Oct. 2019, pp. 349–354, doi: 10.1109/ISC246665.2019.9071685.

[92] A. Taïk and S. Cherkaoui, "Electrical load forecasting using edge computing and federated learning," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6, doi: 10.1109/ICC40277.2020.9148937.

[93] Z. Ge, Z. Song, S. X. Ding, and B. Huang, "Data mining and analytics in the process industry: The role of machine learning," *IEEE Access*, vol. 5, pp. 20590–20616, 2017, doi: 10.1109/ACCESS.2017.2756872.

[94] W. Zhou, Y. Li, S. Chen, and B. Ding, "Real-time data processing architecture for multi-robots based on differential federated learning," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Oct. 2018, pp. 462–471, doi: 10.1109/SMARTWORLD.2018.00106.

[95] B. Liu, L. Wang, M. Liu, and C.-Z. Xu, "Federated imitation learning: A novel framework for cloud robotic systems with heterogeneous sensor data," *IEEE Robot. Autom. Lett.*, vol. 5, no. 2, pp. 3509–3516, Apr. 2020, doi: 10.1109/LRA.2020.2976321.

[96] A. K. Tanwani, N. Mor, J. Kubiatowicz, J. E. Gonzalez, and K. Goldberg, "A fog robotics approach to deep robot learning: Application to object recognition and grasp planning in surface decluttering," in *Proc. Int. Conf. Robot. Autom. (ICRA)*, May 2019, pp. 4559–4566, doi: 10.1109/ICRA.2019.8793690.

[97] H.-K. Lim, J.-B. Kim, C.-M. Kim, G.-Y. Hwang, H.-B. Choi, and Y. Han, "Federated reinforcement learning for controlling multiple rotary inverted pendulums in edge computing environments," in *Proc. Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC)*, Feb. 2020, pp. 463–464, doi: 10.1109/icaiic48513.2020.9065233.

[98] Z. Li, L. Wang, L. Jiang, and C.-Z. Xu, "FC-SLAM: Federated learning enhanced distributed visual-LiDAR SLAM in cloud robotic system," in *Proc. IEEE Int. Conf. Robot. Biomimetics (ROBIO)*, Dec. 2019, pp. 1995–2000, doi: 10.1109/ROBIO49542.2019.8961798.

[99] Y. Lu, "Industry 4.0: A survey on technologies, applications and open research issues," *J. Ind. Inf. Integr.*, vol. 6, pp. 1–10, Jun. 2017, doi: 10.1016/j.jii.2017.04.005.

[100] M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, "Efficient and privacy-enhanced federated learning for industrial artificial intelligence," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6532–6542, Oct. 2020, doi: 10.1109/TII.2019.2945367.

[101] S. R. Pokhrel and S. Singh, "Compound TCP performance for Industry 4.0 WiFi: A cognitive federated learning approach," *IEEE Trans. Ind. Informat.*, vol. 17, no. 3, pp. 2143–2151, Mar. 2021, doi: 10.1109/TII.2020.2985033.

[102] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, "A trustworthy privacy preserving framework for machine learning in industrial IoT systems," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6092–6102, Sep. 2020, doi: 10.1109/TII.2020.2974555.

[103] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao, and Y. Xiang, "A blockchained federated learning framework for cognitive computing in Industry 4.0 networks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2964–2973, Apr. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9134967

[104] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, and D. O. Wu, "Edge computing in industrial Internet of Things: Architecture, advances and challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2462–2488, 4th Quart., 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9139976

[105] J. Mills, J. Hu, and G. Min, "Communication-efficient federated learning for wireless edge intelligence in IoT," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 5986–5994, Jul. 2020, doi: 10.1109/JIOT.2019.2956615.

[106] H. Sun, S. Li, F. R. Yu, Q. Qi, J. Wang, and J. Liao, "Toward communication-efficient federated learning in the Internet of Things with edge computing," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 11053–11067, Nov. 2020, doi: 10.1109/JIOT.2020.2994596.

[107] S. Zhai, X. Jin, L. Wei, H. Luo, and M. Cao, "Dynamic federated learning for GMEC with time-varying wireless link," *IEEE Access*, vol. 9, pp. 10400–10412, 2021, doi: 10.1109/ACCESS.2021.3050172.

[108] L. Wang, W. Wang, and B. Li. (Jul. 1, 2019). *CMFL: Mitigating Communication Overhead for Federated Learning*. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8885054?casa_token=o82a5mcscF4AAAAA:Ad5c5VNfj-16CJX8VvvD8N2B066iINlX9hewz_I2gLZ5-JGxrNF1R6SiP4znNHVpCzWctELCTh0

[109] Z. Yang, M. Chen, W. Saad, C. S. Hong, and M. Shikh-Bahaei, "Energy efficient federated learning over wireless communication networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 3, pp. 1935–1949, Mar. 2021, doi: 10.1109/TWC.2020.3037554.

[110] H. T. Nguyen, N. Cong Luong, J. Zhao, C. Yuen, and D. Niyato, "Resource allocation in mobility-aware federated learning networks: A deep reinforcement learning approach," in *Proc. IEEE 6th World Forum Internet Things (WF-IoT)*, Jun. 2020, pp. 1–6, doi: 10.1109/WF-IoT48130.2020.9221089.

[111] A. Imteaj and M. Hadi Amini, "FedAR: Activity and resource-aware federated learning model for distributed mobile robots," in *Proc. 19th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2020, pp. 1153–1160, doi: 10.1109/ICMLA51294.2020.00185.

[112] U. M. Aïvodji, S. Gambs, and A. Martin. (May 1, 2019). *IOTFLA: A Secured and Privacy-Preserving Smart Home Architecture Implementing Federated Learning*. [Online]. Available: https://ieeexplore.ieee.org/document/8844592

[113] A. Fu, X. Zhang, N. Xiong, Y. Gao, H. Wang, and J. Zhang, "VFL: A verifiable federated learning with privacy-preserving for big data in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3316–3326, May 2022, doi: 10.1109/TII.2020.3036166.

[114] C. Zhang, X. Liu, X. Zheng, R. Li, and H. Liu, "FengHuoLun: A federated learning based edge computing platform for cyber-physical systems," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2020, pp. 1–4, doi: 10.1109/PERCOMWORKSHOPS48775.2020.9156259.

[115] Y. Tu, Y. Ruan, S. Wagle, C. G. Brinton, and C. Joe-Wong, "Network-aware optimization of distributed learning for fog computing," in *Proc. IEEE Conf. Comput. Commun.*, Jul. 2020, pp. 2509–2518, doi: 10.1109/INFOCOM41043.2020.9155372.

[116] X. Lu, Y. Liao, P. Lio, and P. Hui, "Privacy-preserving asynchronous federated learning mechanism for edge network computing," *IEEE Access*, vol. 8, pp. 48970–48981, 2020, doi: 10.1109/ACCESS.2020.2978082.

[117] L. Li, C. Huang, D. Shi, H. Wang, X. Zhou, M. Shu, and M. Pan, "Energy and spectrum efficient federated learning via high-precision over-the-air computation," *IEEE Trans. Wireless Commun.*, vol. 23, no. 2, pp. 1228–1242, Feb. 2024, doi: 10.1109/TWC.2023.3287549.

[118] I. Adjei-Mensah, X. Zhang, I. O. Agyemang, S. B. Yussif, A. A. Baffour, B. M. Cobbinah, C. Sey, L. D. Fiasam, I. A. Chikwendu, and J. R. Arhin, "Cov-Fed: Federated learning-based framework for COVID-19 diagnosis using chest X-ray scans," *Eng. Appl. Artif. Intell.*, vol. 128, Feb. 2024, Art. no. 107448, doi: 10.1016/j.engappai.2023.107448.

[119] M. Gupta, M. Kumar, and Y. Gupta, "A blockchain-empowered federated learning-based framework for data privacy in lung disease detection system," *Comput. Hum. Behav.*, vol. 158, Sep. 2024, Art. no. 108302, doi: 10.1016/j.chb.2024.108302.

[120] Y. Li, C. Chen, N. Liu, H. Huang, Z. Zheng, and Q. Yan, "A blockchain-based decentralized federated learning framework with committee consensus," *IEEE Netw.*, vol. 35, no. 1, pp. 234–241, Jan. 2021, doi: 10.1109/MNET.011.2000263.

[121] Y. Liu, Z. Jia, Z. Jiang, X. Lin, J. Liu, Q. Wu, and W. Susilo, "BFL-SA: Blockchain-based federated learning via enhanced secure aggregation," *J. Syst. Archit.*, vol. 152, Jul. 2024, Art. no. 103163, doi: 10.1016/j.sysarc.2024.103163.

[122] Z. Li, X. Xu, X. Cao, W. Liu, Y. Zhang, D. Chen, and H. Dai, "Integrated CNN and federated learning for COVID-19 detection on chest X-ray images," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, vol. 24, no. 4, pp. 835–845, Jan. 2022, doi: 10.1109/TCBB.2022.3184319.

[123] I. Blanquer, F. Brasileiro, A. Brito, A. Calatrava, A. Carvalho, C. Fetzer, F. Figueiredo, R. P. Guimarães, L. Marinho, W. Meira, A. Silva, Á. Alberich-Bayarri, E. Camacho-Ramos, A. Jimenez-Pastor, A. L. L. Ribeiro, B. R. Nascimento, and F. Silva, "Federated and secure cloud services for building medical image classifiers on an intercontinental infrastructure," *Future Gener. Comput. Syst.*, vol. 110, pp. 119–134, Sep. 2020, doi: 10.1016/j.future.2020.04.012.

[124] Y. Ye, S. Li, F. Liu, Y. Tang, and W. Hu, "EdgeFed: Optimized federated learning based on edge computing," *IEEE Access*, vol. 8, pp. 209191–209198, 2020, doi: 10.1109/ACCESS.2020.3038287.

[125] H. Liu, S. Zhang, P. Zhang, X. Zhou, X. Shao, G. Pu, and Y. Zhang, "Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 6073–6084, Jun. 2021, doi: 10.1109/TVT.2021.3076780.

[126] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Communication-efficient federated learning and permissioned blockchain for digital twin edge networks," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2276–2288, Feb. 2021, doi: 10.1109/JIOT.2020.3015772.

[127] J. Qian and M. Barzegaran. (Dec. 1, 2021). *A Decomposed Deep Training Solution for Fog Computing Platforms*. Accessed: Sep. 17, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9709003/

[128] Y. Xiao, X. Zhang, Y. Li, G. Shi, M. Krunz, D. N. Nguyen, and D. T. Hoang, "Time-sensitive learning for heterogeneous federated edge intelligence," *IEEE Trans. Mobile Comput.*, vol. 23, no. 2, pp. 1–18, Feb. 2024, doi: 10.1109/TMC.2023.3237374.

[129] L. Cui, Z. Chen, S. Yang, R. Chen, and Z. Ming, "A secure and decentralized DLaaS platform for edge resource scheduling against adversarial attacks," *IEEE Trans. Comput.*, vol. 73, no. 3, pp. 631–644, Jan. 2021, doi: 10.1109/TC.2021.3074806.

[130] W. Yang, Y. Zhang, K. Ye, L. Li, and C. Xu, "FFD: A federated learning based method for credit card fraud detection," in *Proc. Int. Conf. big data*, 2019, pp. 18–32, doi: 10.1007/978-3-030-23551-2_2.

[131] M. Abdul Salam, K. M. Fouad, D. L. Elbably, and S. M. Elsayed, "Federated learning model for credit card fraud detection with data balancing techniques," *Neural Comput. Appl.*, vol. 36, no. 11, pp. 6231–6256, Jan. 2024, doi: 10.1007/s00521-023-09410-2.

[132] V. V. K. Reddy, R. V. K. Reddy, M. S. K. Munaga, B. Karnam, S. K. Maddila, and C. S. Kolli, "Deep learning-based credit card fraud detection in federated learning," *Expert Syst. Appl.*, vol. 255, Dec. 2024, Art. no. 124493, doi: 10.1016/j.eswa.2024.124493.

[133] N. Hossein Motlagh, T. Taleb, and O. Arouk, "Low-altitude unmanned aerial vehicles-based Internet of Things services: Comprehensive survey and future perspectives," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 899–922, Dec. 2016, doi: 10.1109/JIOT.2016.2612119.

[134] J. Yao and N. Ansari, "Secure federated learning by power control for Internet of Drones," *IEEE Trans. Cognit. Commun. Netw.*, vol. 7, no. 4, pp. 1021–1031, Dec. 2021, doi: 10.1109/TCCN.2021.3076167.

[135] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and H. Karimipour, "Federated learning for drone authentication," *Ad Hoc Netw.*, vol. 120, Sep. 2021, Art. no. 102574, doi: 10.1016/j.adhoc.2021.102574.

[136] M. Harasic, F.-S. Keese, D. Mattern, and A. Paschke, "Recent advances and future challenges in federated recommender systems," *Int. J. Data Sci. Anal.*, vol. 17, no. 4, pp. 337–357, Aug. 2023, doi: 10.1007/s41060-023-00442-4.

[137] Y. Wu, L. Su, L. Wu, and W. Xiong, "FedDeepFM: A factorization machine-based neural network for recommendation in federated learning," *IEEE Access*, vol. 11, pp. 74182–74190, 2023, doi: 10.1109/ACCESS.2023.3295894.

[138] A. Salh, R. Ngah, L. Audah, K. S. Kim, Q. Abdullah, Y. M. Al-Moliki, K. A. Aljaloud, and H. N. Talib, "Energy-efficient federated learning with resource allocation for green IoT edge intelligence in B5G," *IEEE Access*, vol. 11, pp. 16353–16367, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10041930

[139] L. Ferreira, L. Silva, F. Morais, C. M. Martins, P. M. Pires, H. Rodrigues, P. Cortez, and A. Pilastri, "International revenue share fraud prediction on the 5G edge using federated learning," *Computing*, vol. 105, no. 9, pp. 1907–1932, Mar. 2023, doi: 10.1007/s00607-023-01174-w.

[140] R. Parekh, N. Patel, R. Gupta, N. K. Jadav, S. Tanwar, A. Alharbi, A. Tolba, B.-C. Neagu, and M. S. Raboaca, "GeFL: Gradient encryption-aided privacy preserved federated learning for autonomous vehicles," *IEEE Access*, vol. 11, pp. 1825–1839, 2023, doi: 10.1109/ACCESS.2023.3233983.

[141] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. V. Poor, "Federated learning for Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1622–1658, 3rd Quart., 2021, doi: 10.1109/COMST.2021.3075439.

[142] S. Math, P. Tam, and S. Kim, "Reliable federated learning systems based on intelligent resource sharing scheme for big data Internet of Things," *IEEE Access*, vol. 9, pp. 108091–108100, 2021, doi: 10.1109/ACCESS.2021.3101871.

[143] W. Zhang, X. Li, H. Ma, Z. Luo, and X. Li, "Federated learning for machinery fault diagnosis with dynamic validation and self-supervision," *Knowledge-Based Syst.*, vol. 213, Feb. 2021, Art. no. 106679, doi: 10.1016/j.knosys.2020.106679.

[144] Q. Song, S. Lei, W. Sun, and Y. Zhang, "Adaptive federated learning for digital twin driven industrial Internet of Things," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2021, pp. 1–6, doi: 10.1109/WCNC49053.2021.9417370.

[145] J. Zhang, J. Zhou, J. Guo, and X. Sun, "Visual object detection for privacy-preserving federated learning," *IEEE Access*, vol. 11, pp. 33324–33335, 2023, doi: 10.1109/ACCESS.2023.3263533.

[146] R. Zhao, Y. Yin, Y. Shi, and Z. Xue, "Intelligent intrusion detection based on federated learning aided long short-term memory," *Phys. Commun.*, vol. 42, Oct. 2020, Art. no. 101157, doi: 10.1016/j.phycom.2020.101157.

[147] I. Mohammed, S. Tabatabai, A. Al-Fuqaha, F. E. Bouanani, J. Qadir, B. Qolomany, and M. Guizani, "Budgeted online selection of candidate IoT clients to participate in federated learning," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5938–5952, Apr. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9249424

[148] L. Kong, X.-Y. Liu, H. Sheng, P. Zeng, and G. Chen, "Federated tensor mining for secure industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2144–2153, Mar. 2020, doi: 10.1109/TII.2019.2937876.

[149] T. V. Khoa, Y. M. Saputra, D. T. Hoang, N. L. Trung, D. Nguyen, N. V. Ha, and E. Dutkiewicz, "Collaborative learning model for cyberattack detection systems in IoT Industry 4.0," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, May 2020, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9120761

[150] M. H. U. Rehman, A. M. Dirir, K. Salah, E. Damiani, and D. Svetinovic, "TrustFed: A framework for fair and trustworthy cross-device federated learning in IIoT," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8485–8494, Dec. 2021, doi: 10.1109/TII.2021.3075706.

[151] B. Zhao, K. Fan, K. Yang, Z. Wang, H. Li, and Y. Yang, "Anonymous and privacy-preserving federated learning with industrial big data," *IEEE Trans. Ind. Informat.*, vol. 17, no. 9, pp. 6314–6323, Sep. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9325934

[152] X. Zhang, M. Hu, J. Xia, T. Wei, M. Chen, and S. Hu, "Efficient federated learning for cloud-based AIoT applications," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 40, no. 11, pp. 2211–2223, Nov. 2021, doi: 10.1109/TCAD.2020.3046665.

[153] C. Fang, Y. Guo, N. Wang, and A. Ju, "Highly efficient federated learning with strong privacy preservation in cloud computing," *Comput. Secur.*, vol. 96, Sep. 2020, Art. no. 101889, doi: 10.1016/j.cose.2020.101889.
[154] Y. Wei, S. Zhou, S. Leng, S. Maharjan, and Y. Zhang, "Federated learning empowered end-edge-cloud cooperation for 5G HetNet security," *IEEE Netw.*, vol. 35, no. 2, pp. 88–94, Mar. 2021, doi: 10.1109/MNET.011.2000340.
[155] H. N. Cunha Neto, J. Hribar, I. Dusparic, N. C. Fernandes, and D. M. F. Mattos, "FedSBS: Federated-learning participant-selection method for intrusion detection systems," *Comput. Netw.*, vol. 244, May 2024, Art. no. 110351, doi: 10.1016/j.comnet.2024.110351.
[156] M. Aledhari, R. Razzak, R. M. Parizi, and F. Saeed, "Federated learning: A survey on enabling technologies, protocols, and applications," *IEEE Access*, vol. 8, pp. 140699–140725, 2020, doi: 10.1109/ACCESS.2020.3013541.
[157] B. S. Ciftler, A. Albaseer, N. Lasla, and M. Abdallah, "Federated learning for RSS fingerprint-based localization: A privacy-preserving crowdsourcing method," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 2112–2117, doi: 10.1109/IWCMC48107.2020.9148111.
[158] B. Yin, H. Yin, Y. Wu, and Z. Jiang, "FDC: A secure federated deep learning mechanism for data collaborations in the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6348–6359, Jul. 2020, doi: 10.1109/JIOT.2020.2966778.
[159] S. Yu, X. Chen, Z. Zhou, X. Gong, and D. Wu, "When deep reinforcement learning meets federated learning: Intelligent multitimescale resource management for multiaccess edge computing in 5G ultradense network," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2238–2251, Feb. 2021, doi: 10.1109/JIOT.2020.3026589.
[160] K. Cheng, T. Fan, Y. Jin, Y. Liu, T. Chen, D. Papadopoulos, and Q. Yang, "SecureBoost: A lossless federated learning framework," *IEEE Intell. Syst.*, vol. 36, no. 6, pp. 87–98, Nov. 2021, doi: 10.1109/MIS.2021.3082561.
[161] M. S. Farooq, R. Tehseen, J. N. Qureshi, U. Omer, R. Yaqoob, H. A. Tanweer, and Z. Atal, "FFM: Flood forecasting model using federated learning," *IEEE Access*, vol. 11, pp. 24472–24483, 2023, doi: 10.1109/ACCESS.2023.3252896.
[162] J. Jithish, B. Alangot, N. Mahalingam, and K. S. Yeo, "Distributed anomaly detection in smart grids: A federated learning-based approach," *IEEE Access*, vol. 11, pp. 7157–7179, 2023, doi: 10.1109/ACCESS.2023.3237554.
[163] T. T. Huong, T. P. Bac, K. N. Ha, N. V. Hoang, N. X. Hoang, N. T. Hung, and K. P. Tran, "Federated learning-based explainable anomaly detection for industrial control systems," *IEEE Access*, vol. 10, pp. 53854–53872, 2022, doi: 10.1109/ACCESS.2022.3173288.
[164] X. Sáez-de-Cámara, J. L. Flores, C. Arellano, A. Urbieta, and U. Zurutuza, "Clustered federated learning architecture for network anomaly detection in large scale heterogeneous IoT networks," *Comput. Secur.*, vol. 131, Aug. 2023, Art. no. 103299, doi: 10.1016/j.cose.2023.103299.
[165] N. A. Al-Athba Al-Marri, B. S. Ciftler, and M. M. Abdallah, "Federated mimic learning for privacy preserving intrusion detection," in *Proc. IEEE Int. Black Sea Conf. Commun. Netw. (BlackSeaCom)*, May 2020, pp. 1–6, doi: 10.1109/BLACKSEACOM48709.2020.9234959.
[166] K. Li, H. Zhou, Z. Tu, W. Wang, and H. Zhang, "Distributed network intrusion detection system in satellite-terrestrial integrated networks using federated learning," *IEEE Access*, vol. 8, pp. 214852–214865, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9274426
[167] *Federated-Learning-Based Anomaly Detection for IoT Security Attacks*. [Online]. Available: https://ieeexplore.ieee.org/document/9424138
[168] S. A. Rahman, H. Tout, C. Talhi, and A. Mourad, "Internet of Things intrusion detection: Centralized, on-device, or federated learning?" *IEEE Netw.*, vol. 34, no. 6, pp. 310–317, Nov. 2020, doi: 10.1109/MNET.011.2000286.
[169] B. Cetin, A. Lazar, J. Kim, A. Sim, and K. Wu, "Federated wireless network intrusion detection," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2019, pp. 6004–6006, doi: 10.1109/BIGDATA47090.2019.9005507.
[170] I. Cvitic, D. Perakovic, B. B. Gupta, and K. R. Choo, "Boosting-based DDoS detection in Internet of Things systems," *IEEE Internet Things J.*, vol. 9, no. 3, pp. 2109–2123, Feb. 2022, doi: 10.1109/JIOT.2021.3090909.
[171] N. Moustafa, M. Keshky, E. Debiez, and H. Janicke, "Federated TON_IoT windows datasets for evaluating AI-based security applications," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 848–855, doi: 10.1109/TRUSTCOM50675.2020.00114.
[172] Z. Chen, N. Lv, P. Liu, Y. Fang, K. Chen, and W. Pan, "Intrusion detection for wireless edge networks based on federated learning," *IEEE Access*, vol. 8, pp. 217463–217472, 2020, doi: 10.1109/ACCESS.2020.3041793.
[173] T. T. Huong, T. P. Bac, D. M. Long, B. D. Thang, N. T. Binh, T. D. Luong, and T. K. Phuc, "LocKedge: Low-complexity cyberattack detection in IoT edge computing," *IEEE Access*, vol. 9, pp. 29696–29710, 2021, doi: 10.1109/ACCESS.2021.3058528.
[174] S. McElwee, J. Heaton, J. Fraley, and J. Cannady, "Deep learning for prioritizing and responding to intrusion detection alerts," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2017, pp. 1–5, doi: 10.1109/MILCOM.2017.8170757.
[175] X. Wang, S. Garg, H. Lin, J. Hu, G. Kaddoum, M. J. Piran, and M. S. Hossain, "Toward accurate anomaly detection in industrial Internet of Things using hierarchical federated learning," *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7110–7119, May 2022, doi: 10.1109/JIOT.2021.3074382.
[176] *Federated Learning in Computer Vision*. [Online]. Available: https://ieeexplore.ieee.org/document/10234425
[177] P. Tam, S. Math, C. Nam, and S. Kim, "Adaptive resource optimized edge federated learning in real-time image sensing classifications," *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.*, vol. 14, pp. 10929–10940, 2021, doi: 10.1109/JSTARS.2021.3120724.
[178] A. T. Thorgeirsson, S. Scheubner, S. Funfgeld, and F. Gauterin, "Probabilistic prediction of energy demand and driving range for electric vehicles with federated learning," *IEEE Open J. Veh. Technol.*, vol. 2, pp. 151–161, 2021, doi: 10.1109/OJVT.2021.3065529.
[179] X. Qu, C. Guan, G. Xie, Z. Tian, K. Sood, C. Sun, and L. Cui, "Personalized federated learning for heterogeneous residential load forecasting," *Big Data Mining Analytics*, vol. 6, no. 4, pp. 421–432, Dec. 2023, doi: 10.26599/bdma.2022.9020043.
[180] Z. Du, C. Wu, T. Yoshinaga, K.-L.-A. Yau, Y. Ji, and J. Li, "Federated learning for vehicular Internet of Things: Recent advances and open issues," *IEEE Open J. Comput. Soc.*, vol. 1, pp. 45–61, 2020. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9086790
[181] D. Ye, R. Yu, M. Pan, and Z. Han, "Federated learning in vehicular edge computing: A selective model aggregation approach," *IEEE Access*, vol. 8, pp. 23920–23935, 2020, doi: 10.1109/ACCESS.2020.2968399.
[182] S. Lu, Y. Yao, and W. Shi, "CLONE: Collaborative learning on the edges," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10222–10236, Jul. 2021, doi: 10.1109/JIOT.2020.3030278.
[183] J. Yang, C. Fu, and H. Lu, "Optimized and federated soft-impute for privacy-preserving tensor completion in cyber-physical-social systems," *Inf. Sci.*, vol. 564, pp. 103–123, Jul. 2021, doi: 10.1016/j.ins.2021.02.028.
[184] Y. Liu, Z. Ma, X. Liu, S. Ma, S. Nepal, R. H. Deng, and K. Ren, "Boosting privately: Federated extreme gradient boosting for mobile crowdsensing," in *Proc. IEEE 40th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Nov. 2020, pp. 1–11, doi: 10.1109/ICDCS47774.2020.00017.
[185] X. Zhang, R. Lu, J. Shao, F. Wang, H. Zhu, and A. A. Ghorbani, "FedSky: An efficient and privacy-preserving scheme for federated mobile crowdsensing," *IEEE Internet Things J.*, vol. 9, no. 7, pp. 5344–5356, Apr. 2022, doi: 10.1109/JIOT.2021.3109058.
[186] J. Payne and A. Kundu, "Towards deep federated defenses against malware in cloud ecosystems," in *Proc. 1st IEEE Int. Conf. Trust*, Dec. 2019, pp. 92–100, doi: 10.1109/TPS-ISA48467.2019.00020.
[187] R. Taheri, M. Shojafar, M. Alazab, and R. Tafazolli, "Fed-IIoT: A robust federated malware detection architecture in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8442–8452, Dec. 2021, doi: 10.1109/TII.2020.3043458.
[188] F. Yin, Z. Lin, Q. Kong, Y. Xu, D. Li, S. Theodoridis, and S. R. Cui, "FedLoc: Federated learning framework for data-driven cooperative localization and location data processing," *IEEE Open J. Signal Process.*, vol. 1, pp. 187–215, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9250516
[189] R. O. Ogundokun, S. Misra, R. Maskeliunas, and R. Damasevicius, "A review on federated learning and machine learning approaches: Categorization, application areas, and blockchain technology," *Information*, vol. 13, no. 5, p. 263, May 2022, doi: 10.3390/info13050263.

[190] H. Kaur, V. Rani, M. Kumar, M. Sachdeva, A. Mittal, and K. Kumar, "Federated learning: A comprehensive review of recent advances and applications," *Multimedia Tools Appl.*, vol. 83, no. 18, pp. 54165–54188, Nov. 2023, doi: 10.1007/s11042-023-17737-0.

[191] G. D. Govindwar and S. S. Dhande, "A review on federated learning approach in artificial intelligence," in *Proc. 6th Int. Conf. Comput., Commun., Control Autom. (ICCUBEA*, Aug. 2022, pp. 1–5, doi: 10.1109/ICCUBEA54992.2022.10010798.

[192] W. Liu, L. Chen, Y. Chen, and W. Zhang, "Accelerating federated learning via momentum gradient descent," *IEEE Trans. Parallel Distrib. Syst.*, vol. 31, no. 8, pp. 1754–1766, Aug. 2020, doi: 10.1109/TPDS.2020.2975189.

[193] *Advances and Open Problems in Federated Learning*. [Online]. Available: https://ieeexplore.ieee.org/document/9464278

[194] C. Campolo, G. Genovese, G. Singh, and A. Molinaro, "Scalable and interoperable edge-based federated learning in IoT contexts," *Comput. Netw.*, vol. 223, Mar. 2023, Art. no. 109576, doi: 10.1016/j.comnet.2023.109576.

[195] M. Chen and S. Cui, *Communication Efficient Federated Learning for Wireless Networks*. Cham, Switzerland: Springer, 2024, doi: 10.1007/978-3-031-51266-7.

[196] S. M. Azimi-Abarghouyi and V. Fodor, "Scalable hierarchical over-the-air federated learning," *IEEE Trans. Wireless Commun.*, vol. 23, no. 8, pp. 8480–8496, Aug. 2024, doi: 10.1109/TWC.2024.3350923.

[197] K. M. J. Rahman, F. Ahmed, N. Akhter, M. Hasan, R. Amin, K. E. Aziz, A. K. M. M. Islam, M. S. H. Mukta, and A. K. M. N. Islam, "Challenges, applications and design aspects of federated learning: A survey," *IEEE Access*, vol. 9, pp. 124682–124700, 2021, doi: 10.1109/ACCESS.2021.3111118.

[198] H. Fang and Q. Qian, "Privacy preserving machine learning with homomorphic encryption and federated learning," *Future Internet*, vol. 13, no. 4, p. 94, Apr. 2021, doi: 10.3390/fi13040094.

[199] S. K. Nahak, S. K. Acharya, and D. Padhy, "Enhanced flood forecasting: Revolutionizing prediction with federated learning," in *Proc. Int. Conf. Smart Comput. Commun.*, Jan. 2024, pp. 457–467, doi: 10.1007/978-981-97-1323-3_39.

[200] B. Gao, F. Yang, N. Cui, K. Xiong, Y. Lu, and Y. Wang, "A federated learning framework for fingerprinting-based indoor localization in multibuilding and multifloor environments," *IEEE Internet Things J.*, vol. 10, no. 3, pp. 2615–2629, Feb. 2023, doi: 10.1109/JIOT.2022.3214211.

[201] A. K. Singh, A. Blanco-Justicia, and J. Domingo-Ferrer, "Fair detection of poisoning attacks in federated learning on non-i.i.d. data," *Data Mining Knowl. Discovery*, vol. 37, no. 5, pp. 1998–2023, Jan. 2023, doi: 10.1007/s10618-022-00912-6.

[202] N. Bouacida and P. Mohapatra, "Vulnerabilities in federated learning," *IEEE Access*, vol. 9, pp. 63229–63249, 2021, doi: 10.1109/ACCESS.2021.3075203.

[203] S. Vucinich and Q. Zhu, "The current state and challenges of fairness in federated learning," *IEEE Access*, vol. 11, pp. 80903–80914, 2023, doi: 10.1109/ACCESS.2023.3295412.

[204] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50–60, May 2020, doi: 10.1109/MSP.2020.2975749.

[205] C. M. Thwal, K. Thar, Y. L. Tun, and C. S. Hong, "Attention on personalized clinical decision support system: Federated learning approach," in *Proc. IEEE Int. Conf. Big Data Smart Comput. (BigComp)*, Jan. 2021, pp. 141–147, doi: 10.1109/BIGCOMP51126.2021.00035.

[206] Kitchenham. (2007). *Guidelines for Performing Systematic Literature Reviews in Software Engineering*. [Online]. Available: https://www.elsevier.com/_data/promis_misc/525444systematicreviewsguide.pdf

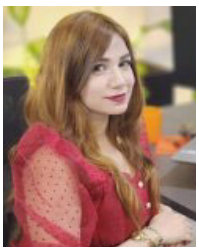
[207] D. Tranfield, D. Denyer, and P. Smart, "Towards a methodology for developing evidence-informed management knowledge by means of systematic review," *Brit. J. Manag.*, vol. 14, pp. 207–222, Sep. 2003. [Online]. Available: https://josephmahoney.web.illinois.edu/BADM504_Fall%202019/6_Tranfield,%20Denyer%20and%20Smart%20(2003).pdf

[208] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proc. 18th Int. Conf. Eval. Assessment Softw. Eng.*, May 2014, pp. 1–10, doi: 10.1145/2601248.2601268.

[209] A. Tariq, M. A. Serhani, F. M. Sallabi, E. S. Barka, T. Qayyum, H. M. Khater, and K. A. Shuaib, "Trustworthy federated learning: A comprehensive review, architecture, key challenges, and future research prospects," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 4920–4998, 2024, doi: 10.1109/OJCOMS.2024.3438264.

[210] C. Meese, H. Chen, S. A. Asif, W. Li, C.-C. Shen, and M. Nejad, "BFRT: Blockchained federated learning for real-time traffic flow prediction," in *Proc. 22nd IEEE Int. Symp. Cluster, Cloud Internet Comput. (CCGrid)*, Taormina, Italy, May 2022, pp. 317–326, doi: 10.1109/CCGRID54584.2022.00041.

[211] C. Meese, H. Chen, W. Li, D. Lee, H. Guo, C.-C. Shen, and M. Nejad, "Adaptive traffic prediction at the ITS edge with online models and blockchain-based federated learning," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 9, pp. 10725–10740, Sep. 2024, doi: 10.1109/TITS.2024.3391053.



TAMANNA ZUBAIRI SANA received the B.Sc. degree in computer science and engineering from East Delta University, Chattogram. She is currently an E-Commerce Manager and a Software QA Engineer with a private IT company, focusing on overseeing e-commerce operations and ensuring the delivery of high-quality, reliable, and user-friendly digital platforms through rigorous software testing and quality assurance.

SHAHAB ABDULLA received the Ph.D. degree. He is currently an Associate Professor of mathematics/communication. His interdisciplinary interest is in biomedical engineering, complex medical engineering, networked systems, intelligent control, computer control systems, robotics, artificial intelligence: machine learning, neural networks, deep learning, human impacts of climate change and human adaptation, natural resource management, environmental assessment and monitoring, reinforcement learning, and environmental management, mathematical sciences, and information and computing sciences. Designing expert systems for his research interests, including deep learning, convolutional neural, and long-short-term memory networks. His leadership was recognized by many awards. He served on several committees. He was the Chair of the IEEE Conference. He collaborates with researchers in the Middle East, U.S., Japan, Europe, China, and Canada, delivering more than 30 seminars. In the last three years, his articles have been cited more than 1000 times. With more than 55 publications (largely in Q1 journals), he leads the Advanced Data Analytics Modeling Research Simulation Group, as a Principal and an Associate Supervisor of more than 20 Ph.D. and master's degree students. Expressions of interest from potential higher degree applicants to study in his group are particularly welcome.

ANINDYA NAG (Member, IEEE) received the M.Sc. degree in computer science and engineering from Khulna University, Khulna, Bangladesh, and the B.Tech. degree in computer science and engineering from Adamas University, Kolkata, India. He is currently a Lecturer with the Department of Computer Science and Engineering, Northern University of Business and Technology Khulna, Khulna. He serves as a reviewer for numerous prestigious journals and international conferences. He has authored and co-authored about 47 publications, including journal articles, conference papers, and book chapters, and has co-edited nine books. His research interests include health informatics, the medical Internet of Things, neuroscience, and machine learning.

AYONTIKA DAS (Member, IEEE) received the Bachelor of Technology (B.Tech.) degree from Adamas University, India. She is currently a Software QA Engineer with a private IT company, where she focuses on software testing and quality assurance to help deliver reliable and high-performing applications.

MD. MEHEDI HASSAN (Member, IEEE) received the B.Sc. degree in computer science and engineering from Northwestern University, in 2022, and the M.Sc. degree in computer science and engineering from Khulna University, Bangladesh, in 2024. He is currently a Ph.D. Researcher in STEM (computer and information science) with the University of South Australia, working on a fully funded research project. He started his Ph.D., in 2025, building on a strong academic background in computer science and engineering. His research spans computer science engineering and data science, with a strong focus on predictive analysis and expert system development. He has authored 73 research articles and edited five books, actively contributing to the academic community. He serves as a peer reviewer for more than 80 prestigious journals and collaborates extensively in interdisciplinary research. As a trainer for the VCourse platform, he has educated more than 250 students over the past two years, sharing knowledge in emerging technologies and research methodologies. Beyond publications, he has actively engaged in intellectual property development, with several patents filed and three already granted in his name. His current research interests include computational neuroscience, machine learning for healthcare, and predictive modeling for biometrics.

ZOYA ZUBAIRI FIZA is currently pursuing the Bachelor of Science degree in computer science and engineering with the Department of Computer Science and Engineering, East Delta University, Chattogram, Bangladesh.

ASIF KARIM (Member, IEEE) received the Ph.D. degree. He is currently a Research-Active Lecturer with Charles Darwin University, Australia. His research interests include applying machine intelligence to areas, such as smart contracts and health informatics. In addition to his active research involvement, he has substantial industry experience in IT, particularly in software engineering.

SHEIKH RIDWAN RAIHAN KABIR received the B.Sc. degree in computer science and engineering from Northwestern University, Khulna, Bangladesh. He is currently pursuing the M.Sc. degree in computer science and engineering with Khulna University, Bangladesh. His research interests include across a range of fields, including healthcare, industrial applications, computer vision, the Internet of Things (IoT), natural language processing, machine learning, deep learning, and blockchain. With a strong belief in the power of collaborative innovation, he is dedicated to creating solutions that bridge the intersection of technology and human welfare. His work is driven by the goal of making meaningful contributions to groundbreaking advancements, whether it involves applying machine learning to explore the complexities of healthcare or using deep learning to address emerging challenges.