IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 2 July 2024, accepted 24 July 2024, date of publication 30 July 2024, date of current version 28 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3435968

RESEARCH ARTICLE

Unlocking a Promising Future: Integrating Blockchain Technology and FL-IoT in the Journey to 6G

FATEMAH H. ALGHAMEDY[1], NAHLA EL-HAGGAR[1], ALBANDARI ALSUMAYT[1], ZEYAD ALFAWAER[2], MAJID ALSHAMMARI[3], LOBNA AMOURI[1], SUMAYH S. ALJAMEEL[4], AND SARAH ALBASSAM[4]

[1]Computer Science Department, Applied College, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia
[2]Department of Science Technology and Mathematics, College of Arts and Sciences, Lincoln University, Jefferson City, MO 65101, USA
[3]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia
[4]Saudi Aramco Cybersecurity Chair, Department of Computer Science, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia

Corresponding author: Nahla El-Haggar (naelhaggar@iau.edu.sa)

This work was supported by the Saudi Aramco Cybersecurity Chair.

ABSTRACT The rapid advancement of technology has set higher standards for the next generation of wireless communication networks, known as 6G. These networks go beyond the simple task of connecting devices and aim to establish a self-sustaining system within society. One of the key factors in achieving this goal is the integration of AI services and apps through the Internet of Things (IoT), which will be made possible with the support of 6G technology. The advancement of artificial intelligence (AI) will play a crucial role in enhancing the protocols, architectures, and operations of 6G networks. To achieve collaborative AI in IoT applications, Federated Learning (FL) has emerged as a popular method. FL enables AI training without the need for data sharing, ensuring privacy and security. However, FL also faces challenges, such as the presence of malicious data and the risk of single-point failure. To address these concerns, blockchain technology (BCT) offers a secure and efficient solution. By leveraging blockchain, these issues can be effectively tackled, providing a reliable framework for implementing FL-IoT applications.

INDEX TERMS Internet of Things, 6G communication, federated learning, blockchain, security, privacy protection, FL-IoT.

I. INTRODUCTION

The Internet of Things (IoT) is a cutting-edge system that connects electronic devices to a smart network through the Internet, utilizing advanced communication systems to guarantee reliable and immediate connectivity. This seamless integration enables the gathering of data from sensors, computing devices, and actuating tools, unlocking a world of possibilities [1], [2]. With the rapid advancement of IoT technology, an expanding array of industries are diving into this realm, encompassing smart homes, smart cities, smart transportation, and intelligent logistics management. Projections indicate that by 2030, the worldwide deployment of IoT devices is expected to soar, reaching an astounding figure of almost 125 billion [3]. With the continuous development of the Internet of Things (IoT), the limitations of 5G technology will gradually hinder its ability to meet the requirements of large-scale IoT applications. Consequently, there is a growing necessity for advancements and progress in wireless communication and networking, leading to the emergence of the next generation of networks, namely 6G networks. These advanced networks are poised to bring about a revolutionary transformation in customer services and applications within the IoT realm, ultimately culminating in the establishment of a ubiquitous intelligent society where autonomous systems play a pivotal role [4], [5].

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

The widespread usage of IoT devices results in an immense volume of data, requiring the support of artificial intelligence (AI) for efficient analysis. The convergence of IoT and AI holds tremendous promise in revolutionizing various industries and unlocking new opportunities. However, in order to fully harness the potential of IoT devices, it will be imperative to invest in innovative technologies. The benefits derived from such investments will be significant, fundamentally transforming the operations of industries, businesses, and economies as a whole [6]. According to experts, the anticipated use cases of IoT can be broadly categorized into two main groups: critical IoT and Massive IoT (MIoT) [4].

In the realm of IoT, there exists a category known as Critical IoT, which demands a combination of robust bandwidth and minimal latency. This technological feat can be accomplished through cutting-edge innovations like 5G. Critical IoT encompasses a wide range of applications, such as industrial control systems, robotic machinery, autonomous vehicles, and various healthcare use cases that heavily rely on the seamless transmission of real-time data [7]. In contrast, the realm of Massive IoT has emerged as a burgeoning field within IoT connectivity technologies, captivating attention and interest. It encompasses an array of applications, such as smart city initiatives, environmental monitoring endeavors, and asset tracking solutions. The advent of Massive IoT has given rise to groundbreaking applications like holographic and five-sense communications, as well as wireless brain-computer interfaces. This expansive domain presents fresh opportunities for interconnecting diverse devices on a global scale, spanning an extensive array of applications, ranging from utility monitoring and industrial process optimization to asset management and the provision of intelligent lighting infrastructure for cities, all the way to energy consumption metering.

The convergence of AI and IoT, whether in critical or massive applications, holds immense potential for reaping substantial rewards. By incorporating AI capabilities, the processing and analysis of vast troves of data generated by IoT devices can be expedited, empowering real-time decision-making and facilitating predictive maintenance. In critical IoT scenarios, AI can play a pivotal role in ensuring reliability and minimizing downtime. In the context of massive IoT, AI's adeptness at discerning patterns and detecting anomalies within data sets can yield valuable insights, ultimately enhancing efficiency and streamlining costs [8]. Nonetheless, the successful implementation of AI services and applications via IoT encounters obstacles as a result of the existence of private datasets.

Back in 2016, Google unveiled Federated Learning (FL) as an innovative distributed machine learning (ML) technique. It empowers Internet of Things (IoT) devices to collaboratively learn a model without the need to transmit raw data to centralized nodes.

The remarkable communication efficiency and heightened data privacy offered by Federated Learning (FL) have garnered considerable attention and acclaim. By circumventing the need for raw data exchange, FL has emerged as a compelling solution in the realm of data privacy and communication efficiency [9], [10]. However, it is important to acknowledge that Federated Learning (FL) is not without its limitations. For instance, the presence of a single point of failure can potentially weaken the network's resilience against attacks such as DoS or DDoS, as well as the inclusion of malicious data. The FL paradigm revolves around a collaborative training process that involves the distribution of datasets among multiple participants. In this setup, each participant derives the benefits of other participants' datasets solely through the shared global model within the federation, without direct access to their sensitive data. With its distinctive attribute of collaborative training, whereby models are distributed, and predictions are made by participants, FL stands as an innovative approach to machine learning.

Blockchain technology (BCT) encompasses a decentralized and distributed digital database or ledger that is shared among various nodes within a peer-to-peer network. This innovative technology relies on cryptographic principles to uphold the integrity of the ledger, with each node maintaining its own copy. To ensure the accuracy of new transactions, a consensus protocol is followed before they are appended to the chain. By leveraging BCT, Federated Learning (FL) can be implemented in a secure and efficient manner, particularly in the vast landscape of the Internet of Things (IoT) [10]. The fusion of blockchain and Federated Learning (FL) opens up possibilities for the establishment of decentralized learning networks that exhibit robustness against attacks and failures. By leveraging blockchain technology, a secure and decentralized platform can be created for IoT devices to communicate and exchange data, guaranteeing data integrity and privacy protection. Additionally, the implementation of smart contracts can automate processes and foster trust between parties, eliminating the need for intermediaries. This not only leads to cost savings but also enhances overall efficiency [11].

The year 2030 is set to mark the launch of the first commercialized system for 6G technology, heralding a digital society that heavily relies on advanced and immediate wireless connectivity. 6G is poised to transcend the limitations of its predecessor, 5G, by offering unprecedented benefits. These include significantly higher data rates, reaching up to Terabits per second (Tbps), remarkably lower latency in the sub-millisecond range, three-dimensional coverage spanning space, sea, and undersea environments, more precise localization capabilities down to centimeter-level accuracy, and an array of enhanced privacy and security measures. Anticipated for 6G is an improved wireless network technology that will provide extended coverage, reduced energy consumption, extensive utilization of spectrum resources,

and cost-effectiveness, all while bolstering security measures [4], [12].

The foundation of 6G networks is expected to be built upon a range of cutting-edge technologies, including post-quantum cryptography, artificial intelligence (AI), machine learning (ML), enhanced edge computing, molecular communication, THz, visible light communication (VLC), and distributed ledger (DL) technologies like blockchain. However, these advancements also call for a reassessment of conventional security measures to safeguard privacy and data. The applications of 6G will extend across diverse domains such as automotive connectivity, drones, mobile devices, IoT devices, homes, industries, and more. Consequently, it becomes imperative to reevaluate existing security measures to ensure the utmost protection of privacy and data [13], [14].

The journey towards 6G can leverage the potential of blockchain technology to enable Federated Learning (FL) in the Internet of Things (IoT). However, there are challenges that must be overcome, including scalability and interoperability. By embracing blockchain, new levels of trust and security can be achieved in communication networks. It has the capability to facilitate decentralized sharing of resources and data, fostering innovation in the development of applications and services for IoT. Therefore, blockchain holds great promise in shaping the future of 6G and unlocking its full potential [1], [15]. The integration of blockchain, AI, and 6G with IoT networks is gaining popularity due to its potential for enhancing security. Blockchain technology is employed to securely store verified session keys in a decentralized manner. Additionally, it facilitates the distribution of computational load among edge devices with low battery levels, ensuring efficient utilization of resources. This convergence of technologies holds promise in fortifying the security measures of IoT networks and paving the way for more robust and reliable systems [16].

In the upcoming years, a remarkable opportunity emerges to transform the way we communicate, interact, and innovate. This is driven by the expanding complexity and scale of IoT networks, the advancements in 6G technology and its integration with AI, and the increasing prominence of blockchain technology. These factors converge to create a fertile ground for groundbreaking developments that have the potential to reshape various aspects of our lives. As we embrace this convergence, we open doors to new possibilities, propelling us towards a future characterized by enhanced connectivity, seamless interactions, and unprecedented innovation [17]. Emerging as a crucial component of the IoT's future, blockchain holds immense potential in addressing the diverse challenges faced by the industry. Its development requires the collaborative efforts and creative thinking of researchers, business executives, and decision-makers. Together, they must ensure that blockchain technology is nurtured in a responsible and sustainable manner. By fostering a collective commitment to innovation and ethical practices, we can unlock the full capabilities of blockchain and pave the way for a future where the IoT flourishes and thrives.

The Motivation for the Study: In this article, our goal is to present a comprehensive analysis of the latest research trends involving the combination of blockchain technology and AI. Specifically, we explore how this integration facilitates federated learning of Massive IoT, ultimately paving the way for the development of 6G. Throughout this article, we delve into the crucial aspects of security issues, recent advances, and future trends, shedding light on the path forward in this exciting field.

Contributions of this Work

- Exploring IoT and evaluating Fusion FL and IoT: Given machine learning's limitations regarding centralization and privacy, Federated learning FL is emerging with the ability to be fusion IoT.
- Discussing 6G Visions and Technical Requirements: The article delves into the visions and technical requirements of 6G, including modifications to existing network architecture and cloud computing technologies. In addition, 6G emerging technologies, 6G-enabled IoT, and the impact of 6G on the future of IoT are covered.
- Clarifying the Fundamentals of Blockchain Technology: This work aims to provide a comprehensive understanding of blockchain technology, covering its concept, characteristics, categories, benefits, challenges, and issues.
- Exploring Potential Benefits and Challenges: The integration of blockchain, MIoT (Massive Internet of Things), and FL in 6G networks is discussed, highlighting the potential advantages and challenges, such as security and scalability. Recent advances in this field are also examined.
- Illustrating the Motivations and Applications of Blockchain in Massive FL-IoT for 6G: The motivations for applying blockchain in massive IoT for 6G are illustrated, along with its applications and open issues. The role of 6G in supporting massive IoT is also explained.
- Exploring Future Research Directions: Future research directions are discussed, including further exploration of blockchain, MIoT, and FL in 6G applications, as well as the development of new tools and techniques to address integration challenges.

Organization of this Work: The structure of this paper is presented in Figure 1 and outlined as follows:

- Section I: Introduction - This section provides an overview of emerging technologies, including blockchain, federated learning, and Massive IoT. It sets the stage for understanding the roadmap towards 6G.
- Section II: Literature Review - In this section, a comprehensive review of relevant studies and research related to the topic is presented.
- Section III: Internet of Things (IoT) - This section provides a profound vision of IoT technology, including its architecture, enabling technologies, challenges, and potential solutions.

- Section IV: Federated Learning for Internet of Things and Their Fusion (FL-IoT) - This section focuses on the evaluation of the fusion between federated learning (FL) and IoT. It begins with the fundamentals and classification of FL. Then, the FL-IoT concept is introduced, including FL-IoT's key features and challenges. Related works of FL-IoT proposed methods are examined.
- Section V: 6G Technology. It delves into the fundamentals, visions, and technical requirements of 6G, including emerging technologies, potential modifications to existing network architecture, and cloud computing technologies.
- Section VI: Fundamentals of Blockchain Technology - This section dives into the fundamentals of blockchain technology, covering its characteristics, types, platform technology, and architectures. Additionally, it explores the role of blockchain in the context of 6G trends and challenges.
- Section VII: Motivations to Applying Blockchain in Massive FL-IoT for 6G - This section explores the motivations behind applying blockchain in the context of massive FL-IoT for 6G, highlighting its applications and key features, and identifying open issues. Additionally, it explains the role of 6G and blockchain in supporting massive FL-IoT.
- Section VIII: Conclusion - The study concludes in this section, summarizing the key findings and addressing open research gaps that can be explored in future work.

A. ABBREVIATIONS

The abbreviations used in this paper are shown in Table 1.

TABLE 1. Acronyms.

Notation	Description
5G	Fifth Generation
6G	Sixth Generation
6LoWPAN	Low Power Personal Area Network for IPv6
AI	Artificial Intelligence
AMQP	Advanced Message Queuing Protocol
BCT	Blockchain Technology
CA	Certificate Authority
CoAP	Constrained Application Protocol
DDS	Data Distribution Service
FL	Federated Learning
FL-IoT	Federated Learning for Internet of Things
FTL	Federated Transfer Learning
GD	Gradient Descent
HTTPS	Hypertext Transfer Protocol Secure
IIoT	Industrial Internet of Things
IoE	Internet of Everything
IoT	Internet of Things
LSTM	Long Short-Term Memory
MIMO	Multiple-Input Multiple-Output
MIoT	Massive Internet of Things
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
NOMA	Non-Orthogonal Multiple Access
non-Iid	non-Independent and Identically Distributed
P2P	Peer-to-Peer
QoS	Quality of Service
RFID	Radio Frequency Identification
RIS	Reconfigurable Intelligent Surface
SGD	Stochastic Gradient Descent
SVM	Support Vector Machine
THz	Terahertz
UAVs	Unmanned Aerial Vehicles
UE	User Equipment
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WSNs	Wireless Sensor Networks
XMPP	Extensible Messaging and Presence Protocol
ZIGBEE	Zonal Intercommunication Global-standard

II. LITERATURE REVIEW

In this section, past related surveys are studied. We use the Google Scholar database to search for relevant surveys by applying the following search syntax: ("FL" + "IoT" + "Blockchain" + "6G"). The results were sorted by relevance, and only surveys published in 2024 were considered. We selected the top 30 surveys for further examination. Firstly, we excluded papers that are not considered review articles. In addition, we considered only indexed Scopus journals, which yielded excluded conference papers, book chapters, and preprint papers. A total of 20 surveys were screened by carefully examining the abstracts and keyworks to identify the topics covered. The including and excluding process is illustrated in Figure 2.

Table 2 presents the previous surveys that have been included in our literature review with the main covered technologies: IoT, 6G, FL-IoT, and blockchain.

In [23], they reviewed comprehensively state-of-the-art proposed methods that integrate AI-enabled Digital Twin Networks (DTNs) with 6G networks. In addition, they discussed several related concepts, such as the role of AI-enabled DTN in 6G and key enabling technologies for accomplishing the capabilities of AI-enabled DTN in 6G. Various applications of AI-enabled DTN in 6G are analyzed practically in many industries, including healthcare, transportation, and smart cities.

In [25], they present a comprehensive review of enabling AI technologies in diverse wireless networks with various applications. Moreover, they show AI-driven applications that utilize AI's capacities to facilitate wireless network transformation. In addition to their goal of providing an understanding of recent AI-based wireless network research, they discussed unsolved issues as promising research coming research topics.

This article [27] is dedicated to conducting a comprehensive review of the integration of edge computing and blockchain in IoT systems by exploring architectures and categories of blockchain-based edge deployment with all security requirements including confidentiality, integrity, authentication, authorization, privacy, confidence, transparency, availability, secure automaticity, and tolerance. In addition, applications of blockchain-based edge potential usages with consideration of security requirements are reviewed.

In [29], the authors systematically reviewed the available literature on federated learning on the Internet of Things

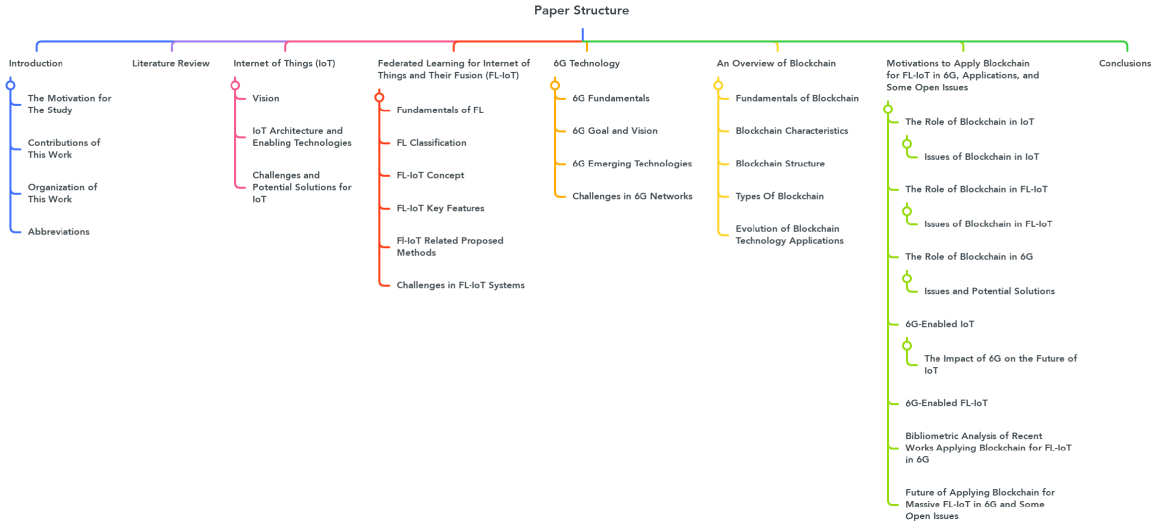

FIGURE 1. Paper structure.

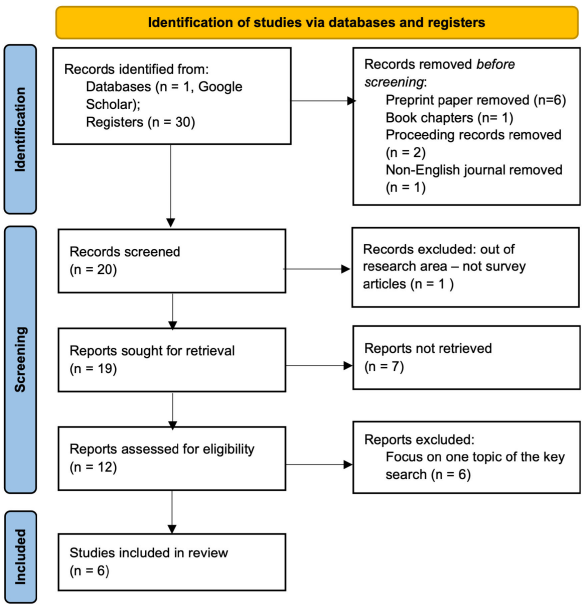

FIGURE 2. PRISMA 2020 flow diagram for the systematic reviews.

IoT. The primary objective of the review is to provide a thorough outline of the escalating utilization of FL in IoT networks, encompassing the architecture and challenges. After an overview of recent research in FL and the IoT, the integration of these two technologies is explored, specifically the capabilities of FL in the communication protocols, frameworks, and architecture. Then, a comprehensive analysis of the integration of FL in IoT applications, such as smart agriculture, finance, healthcare, transportation, cities, and industry are discussed.

This paper [32] examines the utilization of blockchain technology with cybersecurity within the Internet of Things (IoT) networks through a comprehensive review that focuses on the integration of blockchain technology with intrusion detection systems (IDS). Various articles from different fields, such as AI, blockchain, IDS, IoT, and Industrial IoT (IIoT), are investigated to pinpoint emerging trends and challenges in this domain. The exploration of different methodologies that merge AI and blockchain illustrates the capability of amalgamating these technologies to revolutionize IDS.

The previous research mentioned earlier generally presents comprehensive studies and analyses on specific technologies. However, none of these surveys simultaneously integrates the four element topics: IoT, 6G, Fl-IoT, and Blockchain. Therefore, our study distinguishes itself by comprehensively analysis the latest research trends involving the integration of blockchain technology and AI. Specifically, we explore how this integration facilitates federated learning of Massive IoT, ultimately paving the way for the development of 6G.

III. INTERNET OF THINGS (IoT)

A. VISION

The Internet of Things (IoT) is a singular concept to transform the world within the coming years. IoT is an innovative solution that allows devices in distant places to connect with the community frequently. The basic working precept of IoT revolves around wireless connections to facilitate ubiquitous computing. It is carried out for one-of-a-kind purposes and services together with remote sensing, automation, information analytics, and control [36]. The Internet of Things (IoT), the modern-day generation in the global virtual realm, consists of small smart devices mixed with sensors. IoT revolves around the connectivity and communique of objects to serve human desires. Wireless sensor networks have been designed to build up the core structure of the IoT aimed at better and solid overall performance [36].

TABLE 2. Comparison of existing surveys in 2024.

Survey Title	IoT	6G	FL-IoT	Blockchain	Addition topic
Blockchain technology meets 6G wireless networks: A systematic survey [18]	-	✓	-	✓	-
Security of federated learning in 6G era: A review on conceptual techniques and software platforms used for research and analysis [19]	-	✓	-	-	FL
Exploring the Synergy of Fog Computing, Blockchain, and Federated Learning for IoT Applications: A Systematic Literature Review [20]	✓	-	-	✓	FL/Fog Computing (FC)
Federated Analytics for 6G Networks: Applications, Challenges, and Opportunities [21]	-	✓	-	-	Federated Analytics (FA)
Federated Learning for Computational Offloading and Resource Management of Vehicular Edge Computing in 6G-V2X Network [22]	-	✓	-	-	Vehicular Edge Computing (VEC)
A Comprehensive Survey on Revolutionizing Connectivity Through Artificial Intelligence-Enabled Digital Twin Network in 6G [23]	✓	✓	-	-	IoE/ Digital Twin Network (DTN) in 6G
Evolution toward intelligent communications: Impact of deep learning applications on the future of 6G technology [24]	-	✓	-	-	Deep Learning
Artificial Intelligence in 6G Wireless Networks: Opportunities, Applications, and Challenges [25]	✓	✓	-	-	AI
6G Networks and the AI Revolution—Exploring Technologies, Applications, and Emerging Challenges [26]	-	✓	-	-	AI
Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications [27]	✓	-	-	✓	Edge Computing
A Systematic Survey on 5G and 6G Security Considerations, Challenges, Trends, and Research Areas [28]	-	✓	-	-	-
Federated Learning on Internet of Things: Extensive and Systematic Review [29]	✓	-	✓	-	-
Explainable AI for 6G Use Cases: Technical Aspects and Research Challenges [30]	-	✓	-	-	Explainable AI (XAI)
Enhancing trust and privacy in distributed networks: a comprehensive survey on blockchain-based federated learning [31]	-	-	-	✓	FL
Beyond Flight: Enhancing the Internet of Drones with Blockchain Technologies [31]	-	-	-	✓	Internet of Drones (IoD)
Tides of Blockchain in IoT Cybersecurity [32]	✓	-	-	✓	-
A comprehensive survey on digital twin for future networks and emerging Internet of Things industry [33]	✓	-	-	-	Digital Twin/ Industrial IoT/ 5G
Federated Learning-Empowered Mobile Network Management for 5G and Beyond Networks: From Access to Core [34]	-	-	-	-	FL/5G
Artificial intelligence empowered physical layer security for 6G: State-of-the-art, challenges, and opportunities [35]	✓	✓	-	-	AI
Our study	✓	✓	✓	✓	MIoT

An IoT system contains four key elements: sensors, connectivity, statistics processing, and person interface. Initially, smart gadgets accumulate environmental records like temperature, humidity, GPS coordinates, and strength intake. After that, these facts are transmitted to the cloud using various methods, including cell, satellite, WiFi, or Bluetooth. In the cloud, the uncooked data undergoes processing and evaluation to extract insights, allow knowledgeable selections, and trigger suitable movements. Subsequently, processed statistics are added to give up end users through cellular apps, web interfaces, or wearable devices, facilitating human interplay with IoT structures. The adoption of

IoT packages across diverse domain names is regularly expanding. The boundless capacity of the era continues to introduce new use cases that revolutionize enterprise operations throughout various sectors. Currently, IoT packages are actively deployed in logistics, production, retail, healthcare, agriculture, transportation, smart cities, the strength region, and other industries [37], [38].

B. IoT ARCHITECTURE AND ENABLING TECHNOLOGIES

IoT technology has fundamental components such as hardware, software, sensors, and systems that allow the creation of smart objects and applications. As a result, this makes them smarter, regardless of whether these are medical equipment, a smartphone, a wristwatch, a surveillance camera, a car, a factory assembly line, or window shutters. They are also required to have integrated security mechanisms that prevent almost all security breaches on networked equipment. Establishing intelligent and innovative scalable networks together reduces system complexity and lowers operational costs while simultaneously opening up new financial opportunities via revenue and new business designs. Therefore, it allows businesses to stop inefficient processes, automates routine work, and enhances and individualizes services [39].

IoT technology is being gradually adopted by organizations across a wide variety of industries to improve their organizational performance and gain a deeper understanding of their customers [40]. This allows them to provide superior customer service, enhance their decision-making processes, and increase the value of their company.

The base technology for IoT is RFID, which enables microchips to transmit identifying information wirelessly to a reader. With RFID, individuals can analyze, track, and monitor objects equipped with RFID tags. Another key technology, Wireless Sensor Networks (WSNs), utilizes intelligent sensors for sensing and monitoring purposes. RFID has been utilized in various industries such as transportation, pharmaceutical production, and retail since the 1980s, while WSNs are commonly used in applications like traffic management, healthcare, and industrial monitoring. The progress in both technologies has driven the expansion of IoT. Additionally, all these elements are connected through communication protocol and a wide range of other technologies and devices like barcodes, location-based services, Service-Oriented Architecture (SOA), WiMAX, ZigBee, cloud computing, low-power Wi-Fi, Message Queuing Telemetry Transport (MQTT), Low Power Personal Area Network for IPv6 (6LoWPAN), Near Field Communication (NFC), Bluetooth Low Energy (BLE), to create a comprehensive network that empowers IoT [41], [42]. Figure 3 depicts the IoT architecture enabling technologies.

IoT is a system that brings together all the heterogeneous components of IoT in a managed way to build an efficient system. It is the integration of devices, operating systems, controllers, gateways, middleware, and platforms.

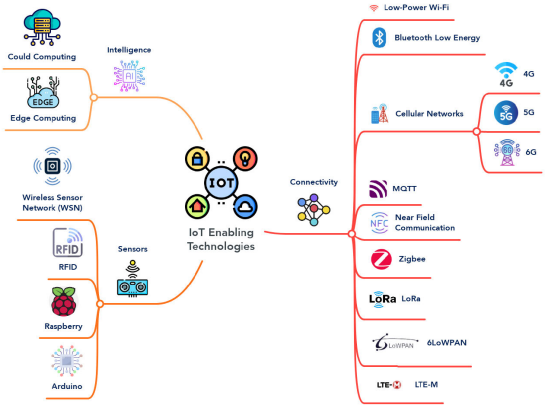

FIGURE 3. IoT enabling technologies.

IoT architecture is an organized network of interconnected devices, sensors, actuators, and cloud services that enable the flow of data. It is categorized based on functions, techniques, and devices. It consists of four key layers: perception/sensing, connectivity/network, middleware, and application. The desired features of architecture for IoT include scalability, interoperability, reliability, QoS, and decentralization of heterogeneous devices in IoT within design. As a result, breaking down the IoT architecture into four stages is seen as a more powerful way to facilitate interactions amongst IoT devices in real-time situations [41], [43], [44].

1) PERCEPTION/SENSING LAYER

The perception Layer is also known as the 'Device Layer' or the 'Sensing Layer'. It is also termed the Recognition Layer, which displays the properties of the objects and physical equipment of the objects within the network. Examples of the Perception Layer are Radio Frequency Identification (RFID) sensors, Wireless Sensor Network (WSN), and Global Positioning System (GPS). Furthermore, it is responsible for converting information into digital signals for easier transmission over a network. Nanotechnologies and embedded intelligence play a vital role in the physical layer [45], [46].

2) CONNECTIVITY/NETWORK LAYER

The network layer is also referred to as the transmission layer. This layer is responsible for the transfer of data from the perception relay to the next to establish connections between all IoT devices to share data between them. Furthermore, the network level enables transmission to different IoT gateways and switches positioned between numerous IoT devices to support the collection and transmission of data between them. For this purpose, the transmission medium may utilize wire or be wireless, including but not limited to 4G, 5G, 6G, WiFi, ZigBee, etc. [47], [48]. Depending on their adherence to the security protocols, latency and bandwidth between the

devices shall differ. These may be public, private, and hybrid systems.

3) MIDDLEWARE LAYER

The middleware layer, also known as the "service layer," provides integration services and application functionality in IoT systems. Middleware is a software or service programming that can provide an interface between the components of IoT. Also, connecting large numbers of individual devices and enabling communication between them through multiple communication protocols, networks, and platforms, resulting in complex interactions across heterogeneous IoT networks. The primary role of middleware is to act as an intermediary between devices, integrating data from the physical environment into IoT-connected devices, networks, and servers. This integration process encompasses tasks like storage, analytics, and implementation, providing interfaces between complex systems with flexibility not originally designed for this type of activity [49], [50].

4) APPLICATION LAYER

The application layer, also known as the business layer, is the highest layer of the IoT architecture and is visible to end users. Middleware manages applications based on the data processed by the layer. Application levels can be configured in different ways depending on the service provided. IoT applications such as smart buildings, health monitoring systems, and highway management systems have been developed [51]. Protocols are implemented at the application level and distributed to the end systems. These protocols include HTTPS, DDS, MQTT, Web Sockets, CoAP, XMPP, and AMQP [52].

C. CHALLENGES AND POTENTIAL SOLUTIONS FOR IoT

As with all emerging technologies, all the IoT features are surrounded by challenges. The most critical challenge could be listed as the following:

1) SECURITY, SECRECY, AND PRIVACY

IoT faces challenges from two main perspectives: IoT architecture and protocols. Further, each IoT layer confronts various types of threats. The threats of the sensing layer include node tampering, unauthorized access, malicious node injection, physical damage, RF interface on RFID, etc. In addition, some network and middleware layers threats are traffic analysis attack, RFID spoofing, malicious node injection, hello attack, ACK flooding, Data tampering, routing attack, etc. Finally, the application layer encounters many threats, including malicious code injection, DDoS, sniffers, spear-phishing, third-party relationships, intrusion, virtualization threats, etc. The latest technologies and methods can relieve this issue, including utilizing machine learning and deep learning to predict attacks in advance. In addition, blockchain is one of the bright methods that could make IoT networks more secure [53].

2) SCALABILITY

The IoT handles massive amounts of data generated from a vast number of IoT devices. In addition, the number of connected devices in the IoT increases exponentially, which requires increased bandwidth and data transmission rate. This problem is raised when IoT networks are integrated with blockchain technology. Due to the necessity of validating every transaction before incorporation into the block and subsequent storage at all nodes within the network, blockchains face challenges in scaling to meet the increasing volume of transactions arising from the Internet of Things. 6G can handle this issue with all promising features [54].

3) POWER MANAGEMENT

Power and energy usage are not just important but crucial factors that significantly influence an IoT device's performance. The ability to operate wirelessly for extended durations is a direct result of their effective management. A node within the IoT domain is deemed energy-efficient when it executes various functions while consuming minimal power. Several factors affect power consumption in an IoT network, including data communication among IoT nodes, microprocessors, associated peripherals, and sensing operations [55]. Several domains could be optimized to minimize energy consumption with IoT. Hardware components, including processors, displays, wireless radios, and memory/storage, could be essential to reduce energy consumption through modern components requiring low energy. Further, design and development applications should consider methods that could be used to minimize energy utilization. Moreover, cloud offloading is one of the promoting techniques that offer a huge relief in energy consumption, especially for IoT devices that use machine learning (ML) and deep learning (DL) by accomplishing computational operations on powerful cloud servers instead of IoT nodes [56].

4) CONNECTIVITY

Retaining consistent and reliable network connectivity for IoT devices, especially for applications in vital industries such as healthcare and transportation, is essential. New IoT applications require many connectivity requirements, such as low latency, ultra-high transmission reliability, and wide coverage. However, ensuring that IoT devices can connect remotely raises challenges. Several methods have been proposed to address this issue, including intelligent resource management, non-orthogonal multiple access (NOMA) technology, spectrum sharing, etc. [57].

IV. FEDERATED LEARNING FOR INTERNET OF THINGS AND THEIR FUSION (FL-IoT)

A. FUNDAMENTALS OF FL

AI plays a significant role in supporting real-time data analysis and facilitating efficient decision-making, making remarkable contributions to data organization. With its capability for real-time pattern and consistency detection,

AI algorithms can gather unstructured data from diverse sources and process it into a consistent format, significantly reducing task completion time. This streamlined data structuring process benefits stakeholders by saving laborious efforts.

Thanks to AI and real-time data, businesses now have exceptional visibility into the customer experience. This enables IT and support staff to proactively address issues, often fixing problems even before end users are aware of them. As a result, the support experience has been radically transformed, leading to improved customer satisfaction. IDC estimates that 45% of the data generated by the Internet of Things needs to be evaluated locally rather than sending it to the cloud for analysis. By distributing intelligence throughout the network, end devices can analyze data effectively and make near-instant decisions.

AI, especially machine learning and deep learning are utilized to analyze data, identify specific occurrences, reduce downtime, improve network performance, detect patterns and anomalies quickly, and identify trends before they impact the company. Machine learning also helps create a network baseline tailored to specific needs, reducing noise and false positives. This allows IT professionals to accurately detect problems, trends, anomalies, and their underlying causes, leading to enhanced network performance management.

However, despite machine learning's numerous benefits, it faces challenges in terms of privacy and scalability. The exponential growth of data presents limitations in applying machine learning due to resource constraints. Aggregating data from users to a central location for the machine learning process may also raise privacy concerns. To address these issues, federated learning (FL) has emerged as a solution.

FL, introduced by Google in 2016, focuses on preserving data privacy and enabling device learning. In FL, each IoT device trains its model using locally collected data, eliminating the need to transmit sensitive data to a centralized cloud station. The cloud station collects and updates local training models from individual devices, enabling distributed AI tasks at the network edge. FL finds applications in various fields, such as healthcare, smart cities, keyboard suggestions, and medicine. By allocating AI commands to local devices, FL creates a shared global model without the need to offload all raw data to a central data center for AI training. This approach overcomes the challenges of machine learning, ensuring privacy preservation and efficient distributed learning. Figure 4 visually represents the concept of FL-IoT - Federated Learning (FL) applied to the Internet of Things (IoT). In addition,

B. FL CLASSIFICATION

FL could be classified based on networking structure or data partitioning, which determines the distribution of training data over the feature spaces and samples [58]. Figure 5 shows the FL classification with more details.

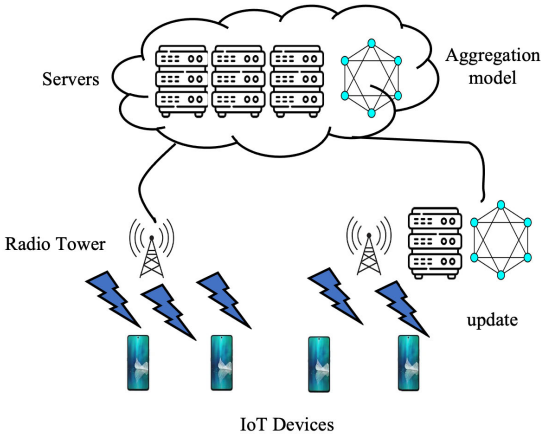

FIGURE 4. FL-IoT system.

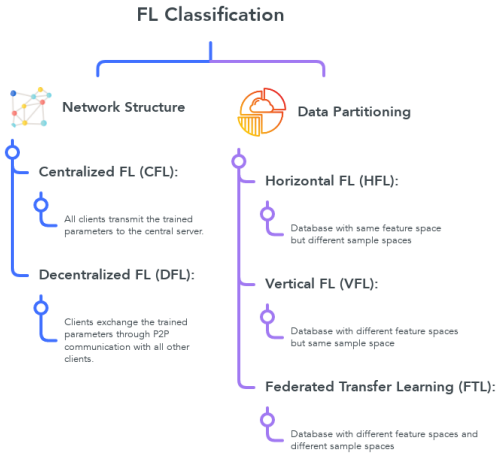

FIGURE 5. FL classification.

C. FL-IoT CONCEPT

Federated Learning FL could be integrated with any of the distinct categories of IoT: massive IoT, critical IoT, industrial IoT, and broadband IoT. Within the realm of IoT systems, Federated Learning FL plays a crucial role in enhancing privacy-preserving solutions. However, it is essential to note that FL also presents several significant challenges, including security, robustness, resource management, and incentive mechanisms. These challenges become even more complex when dealing with industrial IoT (IIoT), as it requires a higher level of security and reliability. IIoT is an extension of IoT technology designed explicitly for industrial sectors and applications. It heavily relies on machine-to-machine communications (M2M), machine learning, and big data analysis.

Typically, each IoT device possesses its own dataset, and the aggregation server can be located either in the virtual cloud or at the network edge. Different FL models have distinct features and limitations. For instance, FL with the server at the network edge is suitable for applications requiring location awareness, low latency, and network

contextual information. On the other hand, cloud-based FL is more appropriate for applications involving a large number of IoT devices across various regions, with storage requirements and powerful computing capabilities.

D. FL-IoT KEY FEATURES

When Federated Learning (FL) is integrated with the Internet of Things (IoT), their features are fusion also, which provides a powerful technology. The most significant features of FL-IoT are the following [58]:

1) DATA PRIVACY

Because the raw data are not required for the training at the aggregator with FL, issues like data leakage are minimized. Therefore, a degree of data privacy is enhanced.

2) SCALABILITY

As mentioned before, one of the biggest problems with machine learning is the struggle to handle the exponential growth of data. FL has emerged as a solution to this issue because machine learning models can be trained on various IoT devices.

3) LOW-LATENCY NETWORK COMMUNICATION

FL does not transmit IoT data to the server. Therefore, FL helps to save network resources and reduce latencies of communication that happen as a result of data offloading. In addition, it also saves network resources.

4) IMPROVE THE LEARNING

FL allows the utilization of various computation resources, including IoT nodes and diverse datasets from an IoT network. These resources enable FL to adapt models based on real-time data, which has the potential to improve accuracy and other measurement metrics.

E. FL-IoT RELATED PROPOSED METHODS

In recent years, numerous studies have focused on enabling FL in IIoT. For instance, Liu et al. conducted research on IIoT data-sharing applications, exploring the use of blockchain and FL. Their findings demonstrated that the proposed scheme could enhance security and performance utility without the need for a central server for training [59]. In a study similar to [59], Zhang et al. [60] utilized blockchain and Federated Learning (FL) to identify device failures in Industrial Internet of Things (IIoT) environments and secure the raw data of IIoT devices. More recently, Liu et al. [61] developed a communication-efficient FL approach that combines FL and the long-short-term memory (LSTM) model to detect device failures in IIoT. This approach offers the advantage of preserving data privacy through FL while efficiently handling time-series data in IIoT using the LSTM learning model. Despite the rapid progress of FL and the emergence of numerous IIoT applications, there is a lack of a comprehensive survey that provides a holistic overview of FL, IIoT, and the application of FL in IIoT domains. Motivated by this gap, our work focuses on delivering the fundamentals of FL and IIoT, as well as reviewing state-of-the-art research on FL for IIoT applications.

In 2019, a study [62] proposed a communication-efficient federated learning (FL) approach for IoT wireless edge intelligence. This approach reduced communication rounds and data uploads but did not incorporate compression techniques for downloaded data. In 2020, a novel multicriteria-based client selection model called FedMCCS [63] was introduced, which optimized client selection for FL-IoT by considering client heterogeneity and computation resources. However, it did not explore the efficiency of each client updating to the global model. In the same year, a study [64]introduced a privacy-preserving blockchain-based FL method for IoT devices. This method utilized blockchain and normalization techniques but lacked testing with real-world datasets and optimal settings for machine-learning models. Another study in 2021 proposed a blockchain-assisted secure framework for FL-IoT, utilizing FL and blockchain for secure big data analytics [65]. However, this framework lacked real-world testing.

In 2021, another study focused on an efficient FL algorithm for resource allocation in wireless IoT networks [66]. It addressed heterogeneity and minimized energy consumption and completion time but did not utilize next-generation wireless IoT networks. In 2022, a study enhanced FL with deep reinforcement learning to equip the Industrial IoT with digital twins [67]. The study developed an architecture and selection process for IIoT devices. However, the limitations were attributed to the limited sample size and the type of training samples used.

Another study in the same year focused on communication efficiency and resource optimization in FL over wireless IoT networks [68]. It proposed a communication-efficient approach that achieved favorable communication loads and demonstrated a strong linear convergence rate. However, the proposed approach was not tested with real-world datasets and relied on uniform resource allocation.

In 2023, a study [69] proposed a Q-learning-aided offloading strategy for edge-assisted federated learning (FL) in Industrial IoT (IIoT), aiming to improve training efficiency. However, it had the limitation of lacking heterogeneous resource allocation in edge-assisted FL.

In the same year, a study [70]focused on FL-based resource management in Smart IoT with blockchain trust assurance. It proposed an FL-based framework with a blockchain trust assurance algorithm but lacked an in-depth investigation of blockchain and FL techniques in future smart IoT.

Additionally, in the same year, another study [71] introduced an accuracy-based client selection mechanism for federated IIoT. This approach combined a secure FL approach with client evaluation accuracy consideration. However, the study did not incorporate blockchain technology for user authentication or crypto-based incentive mechanisms.

TABLE 3. The recent FL-IoT studies of the last five years.

Year	Topic Title	Contributions	Limitations	IoT Network	FL Algorithm
2019	Communication-Efficient Federated Learning for Wireless Edge Intelligence in IoT [62]	Proposed CE-FedAvg (based on FedAvg) that uses distributed Adam optimization and compression techniques of uploaded models in order to reduce the communication total number of rounds that need to convergence and reduce the total data uploaded per round compared to uncompressed FedAvg.	The compressing models are used only for uploading data, not for downloaded data by clients from the server.	Not mentioned	DNN with distributed Adam SGD optimization
2020	FedMCCS: Multicriteria Client Selection Model for Optimal IoT Federated Learning [63]	Novel multicriteria-based optimization model that is efficiently able to select and maximize the number of clients to participate in FL, taking into account their heterogeneity and the computation resources; and it is efficient for intrusion detection.	The efficiency of each client updating to the global model hasn't been studied as a criterion to select client participation.	Consists of two components: the service provider, which provides various applications of ML-based services, and IoT devices which considers as clients,	Not Mentioned
2020	Privacy-Preserving Blockchain-Based Federated Learning for IoT Devices [64]	Proposed a blockchain-based crowdsourcing FL system for IoT devices to build the machine learning model in order to understand customers' consumption behaviors, which helps predict customers' requirements. For security, a new normalization technique is applied which increases the accuracy more than batch normalization while the differential privacy of extracted features of customer's data is preserved along with blockchain to prevent malicious updates.	It is not tested with real-world datasets, and the local and global machine learning model settings are not optimal (epochs).	Hierarchical Crowdsourcing FL	Not Mentioned
2021	Integration of Federated Machine Learning and Blockchain for the Provision of Secure Big Data Analytics for Internet of Things [65]	Proposed a blockchain-assisted secure framework for FL for IoT that utilizes FL to train the model locally. Then, the encrypted models are transferred to the edge-based AI service that merges the blockchain-verified local models into a global model. A fuzzy hashing is applied for trained FL on the blockchain to detect anomalies in FL-trained models against poisoning attacks.	It is not tested in the real world.	Peer-to-peer, based on the federation architecture.	SGD

TABLE 3. *(Continued.)* **The recent FL-IoT studies of the last five years.**

Year	Topic Title	Contributions	Limitations	IoT Network	FL Algorithm
2021	Efficient Federated Learning Algorithm for Resource Allocation in Wireless IoT Networks [66]	Proposed an extension of FedAvg that efficient FL algorithm based on a weight-based proximal term to 1) handle the problem of the heterogeneity across user equipment (UEs) data and characteristics in federated networks by allowing a small number of UEs per round to participate in the training process. 2) Minimizing total energy consumption and completion time by defining a wireless IoT resource allocation problem.	Missing of utilizing next-generation wireless IoT networks	FL-supported wireless IoT network consisting of one base station (BS) and users' equipments.	SGD
2022	Optimizing Federated Learning With Deep Reinforcement Learning for Digital Twin Empowered Industrial IoT [67]	Proposed new architecture of Digital Twin (DT) Empowered in Industrial (DTEI) IoT to capture the characteristics of IIoT devices for dynamic perception and intelligent decision by exploiting the optimized FL. Further, the DTEI-assisted deep reinforcement learning (DRL) method is developed for the selection process of IIoT devices in FL with high utility values to improve the efficiency of FL.	The performance of the locally optimal solution is lower than that of the global optimal solution because of an insufficient number of samples and the single type of samples used for local training.	Heterogeneous IIoT network that consists of two layers: the physical layer, which has BSs and client devices, and the digital twin (DT) layer.	Distributed SGD
2022	Federated Learning over Wireless IoT Networks with Optimized Communication and Resources [68]	To reduce communication costs and improve learning performance, a communication-efficient CEFL is proposed for wireless FL systems which is combined with a client scheduling policy and a linear search-based allocation method. By limiting communication exchanges and reusing the parameters of the stale local model, CEFL achieves a strong linear convergence rate and good communication loads, using uniform resource allocation.	It is not tested with real-world datasets.	General one-hop FL supported wireless IoT network beside a base station (BS) and distributed nodes.	GD
2023	Q-Learning-Aided Offloading Strategy in Edge-Assisted [69]	Federated Learning over Industrial IoT proposed a Q-learning-aided offloading strategy with an edge-assisted FL framework in conjunction with IIoT by utilizing a mobile edge computing (MEC) technique to improve the training efficiency of FL which its training loss function minimization problem is formulated by optimizing the offloading data size under the latency constraint in order to obtain the optimal offloading strategy.	Lack of heterogeneous resource allocation in edge-assisted FL	IIoT network has two layers: the end layer, which includes IIoT devices, and the edge layer, which consists of an edge server responsible for aggregating the local model from all IIoT devices.	Convolutional neural network (CNN), ReLu activation, and a softmax for the output layer.

TABLE 3. *(Continued.)* **The recent FL-IoT studies of the last five years.**

Year	Topic Title	Contributions	Limitations	IoT Network	FL Algorithm
2023	Federated Learning-Based Resource Management with Blockchain Trust Assurance in Smart IoT [70]	After an in-depth study of the FL-based resource management mechanism with blockchain trust assurance, they proposed an FL-based IoT resource management framework with a blockchain trust assurance algorithm. A support Vector Machine (SVM) classifier is used to detect malicious nodes to exclude the impact on the performance.	Lack of in-depth investigation of blockchain and federated learning techniques in the future smart IoT.	IoT applications deployed in Multi-access Edge Computing MEC servers.	SVM to detect malicious nodes.
2023	ACS Accuracy-based client selection mechanism for federated industrial IoT [71]	Proposed a novel client selection mechanism that merged with a proposed secure FL-based approach for IIoT by applying the certificate authority (CA), which authorizes each available participant before joining the FL process to avoid malicious participants and consider the client evaluation accuracy from the previous FL round to be selected the next round.	Not applying blockchain technology as an alternative to CA to authenticate users or guarantee operations security for updating parameters between local clients and servers and not include crypto-based incentive mechanisms in FL.	Proposed FL architecture with a certificate authority (CA) implementation on non-IID data in the IIoT	Lightweight DL

These discussed studies have made significant contributions to FL-IoT and industrial applications, including offloading strategies, resource allocation, privacy preservation, and secure frameworks. However, each study also has its own limitations, particularly in terms of testing on real-world datasets. Further research is needed to overcome these limitations and advance FL-IoT and industrial environments. Table 3 provides an overview of the recent studies on this topic.

F. CHALLENGES IN FL-IoT SYSTEMS

FL is a potential technology for Internet of Things systems and may offer multiple advantages, including lower data transmission, expansion, and privacy protection. Nevertheless, FL-IoT systems suffers several difficulties as follows [72], [73], [74]:

1) UPDATING MODELS

Varied IoT devices could contain varied volumes of data, and some might not always be available for training. Effective upgrading model strategies are necessary for a distributed system that uses fewer resources, interaction, and computing [75].

2) MALICIOUS USERS

Malicious users could gain access to the central FL aggregation server, which may lead to the end user's confidential information being leaked. Although some methods could be used to reduce the impact of leakage, such as adding noise to the parameters of the trained local model before sending it to the FL server, other issues arise, such as the high convergence time for the FL process.

3) FAIRNESS

Unbalanced or skewed data patterns may lead to fairness problems in trained models, which will raise issues in overall model performance. Fairness issues in FL must be addressed, and an efficient fairness strategy with a low number of IoT devices must be developed in order to implement it.

4) HETEROGENEOUSLY OF IoT GADGETS AND DATA

Federated Learning (FL) uses data from several IoT gadgets, each with potentially distinct hardware setups and data distributions, to train models. One of the primary research challenges in the FL method involves dealing with a variety of endpoints and data. Devices inside a federated network could have very different storage, computing, and transmission capacities. Variations in hardware (CPU, RAM), connectivity to the network (3G, 4G, 5G, WiFi), and the power source (power level) are typically the causes of variations.

5) CONSTRAINTS OF IoT DEVICES

Due to the high expense of FL computation, IoT gadgets with little processing power and resources might be unable to participate in the local training paradigm. Thus, lightweight-efficient FL strategies may be developed while maintaining high model reliability and precision. Notably for the training phase, and to minimize the amount of storage or power needed for training, as well as the quantity of transmitted data. By doing this, it will be possible for IoT devices with constrained processing power to nonetheless participate in the training procedure.

6) GENERALISATION

FL is frequently utilized to train models on a subset of machines that aren't really indicative of the public at large. The generalization problem may be resolved with the aid of the same methods that can resolve the non-independent and identically distributed (non-IID) problem. This strategy needs to be reliable and quick to guarantee that regionally trained models might be deployed to new equipment and communities with extreme precision and accuracy.

7) ALGORITHMS OPTIMISATION

Optimization techniques are used by trained regional frameworks at IoT/edge devices (decentralized). Nevertheless, given the dispersed form of the data and the computational and resource limitations of IoT devices, the optimization techniques now in use might not be appropriate for IoT. They are creating novel optimization methods that can efficiently train models with outstanding accuracy, clarity, and resolution rates using a small number of Internet of Things (IoT) gadgets and distributed data.

8) STANDARDISATION

Subsequently, FL is continuously a rising field, and there is a need for standardization in terms of conventions, systems, and assessment measurements. Hence, creating standardized conventions and systems for FL to facilitate its selection in numerous IoT spaces may be assumed as a central sector.

9) SECURITY TECHNIQUES

FL requires links between gadgets and the central server, which poses privacy and safety vulnerabilities at several levels (gadgets, servers, and connection). To further address the limitations of IoT devices, we must provide secure and efficient security features with the least amount of extraneous interaction, processing, and usage of resources. Furthermore, these approaches ought to maintain the model's functionality. Current security-preserving techniques face new hurdles in the context of Federated Learning security. Above all, privacy-preserving techniques must provide a strong confidentiality guarantee without unduly sacrificing accuracy. As a result, these techniques need to be communication-efficient, analytically inexpensive, and resistant to being dropped devices. Secrecy-preserving federated learning systems that are in use today usually start with traditional cryptographic techniques.

10) EXPLAINABILITY

Since the step of the training models depends on decentralized data, they are unable to account for the predictions made by the model. The challenge of fully understanding the trained local model's decision-making method in the absence of access to the particular information on each device is referred to as this obstacle. This problem is crucial in many programs, particularly those where delicate or essential decisions need to be made, like in banking or medical care, and it's crucial to comprehend the model's approach to decision-making. As a result, to produce comprehensible models–that is, models that explain the choices made by trained models it is essential to propose a novel, trustworthy, and powerful means of extraction without sacrificing confidentiality.

11) FEDERATED TRANSFER LEARNING

Using effective pre-trained models to build new, optimal models is known as Transfer Learning (TL), a well-liked machine learning strategy. By leveraging the pre-trained model from a source domain to establish the models on gadgets in the target domain, FTL–an emerging research direction–combines TL and FL techniques. FTL involves passing on information among machines in a federated context. This may enhance the model's rate of resolution and capacity for generalization. Constructing a fast FTL system that can locate an appropriate pre-trained model pertinent to the intended domain while weighing the trade-off between model relevance and privacy preservation. For Federated Learning to run better and be more scalable, reliability is a must. One of the many significant improvements needed in the area of FL is this aspect.

12) NON-IID AND IDENTICALLY DISTRIBUTED (IID) DATA

FL makes the assumption that all source IoT/edge device data is IID. But since every device's data isn't drawn from the exact same source, it can be non-IID in many real-world Internet of Things scenarios. Various device kinds, geographic regions, user characteristics, and even periodic differences in data collection can all contribute to this. Given that most ML solutions presume that the training data is IID, this is going to be a significant obstacle to FL. The conventional techniques, however, might not function well when the training data is non-IID because this would result in subpar performance of models (accuracy and resolution rates). Consequently, to address the problem of non-IID data, we must provide an easy remedy that considers both the diversity and the underlying data pattern. This might be done by using algorithm customization methods, the concept of meta, or clustering.

13) OVERHEAD

FL requires interaction, which may be costly in terms of computing power and time, across IoT/edge equipment and a centralized server. The development of effective compression and quantization techniques is essential to lowering the amount of data transmitted and, as a result, the associated costs associated with communication delays. This is necessary in order to adequately address the energy, computational, and memory restrictions of connected devices.

V. 6G TECHNOLOGY

A. 6G FUNDAMENTALS

With each passing generation, communication technologies experience revolutionary transformations driven by the rapid advancement of communication applications. To date, a total of five generations of cellular mobile communication systems have been developed. Each successive generation, from analog communications systems (1G) to digital communications systems (5G), introduces higher frequencies, wider bandwidths, and faster data rates. However, it is important to note that even with the capabilities of 5G networks, achieving a fully automated and intelligent network that offers comprehensive services and delivers an immersive experience may not be feasible [76]. While 5G communication systems have witnessed notable advancements compared to their predecessors, there are still several challenges that need to be addressed. These challenges include latency, reliability, throughput, and the ability to support a large number of connections. Furthermore, it is important to note that 5G systems may not be able to meet the future demands of intelligent and automated systems over the next decade [77]. Within the realm of 5G technology, various innovative techniques have emerged. These include the utilization of new frequency bands like millimeter-wave (mmWave) and optical spectrums, advanced spectrum usage and management, as well as the integration of licensed and unlicensed spectrums. However, the rapid growth of data-centric and automated systems may surpass the capabilities of 5G wireless networks. It is crucial to acknowledge that 5G communication falls short in terms of converging functionalities such as communication, intelligence, sensing, control, and computing. The convergence of Internet of Things (IoT) technologies becomes essential for future applications. Some devices, such as VR devices, require significantly more data than what 5G can currently provide, necessitating at least 10 Gbps speeds [78].

B. 6G GOAL AND VISION

- **Goal:** By the end of 2023, mobile telecommunications companies are aiming to transition to a 6G wireless network to overcome obstacles faced by 5G, such as latency and reliability issues. 6G is expected to offer advancements in energy efficiency and spectral capabilities, enabling new connected services like drones and tactile Internet. The goal of 6G is to revolutionize wireless access networks by improving spectrum distribution, increasing coverage, and implementing enhanced security protocols.
- **Vision:** 6G envisions a transformative shift in wireless access networks, encompassing spectrum allocation, application support, coverage expansion, and heightened

security measures. By the 2030s, 6G aims to expand coverage to include UAVs and satellite communications, creating a comprehensive 3D communication network across land, sea, and space. Worldwide research organizations are focusing on 6G networks to enhance performance with data rates up to 1 Tbps and ultra-low latency, as well as increasing capacity by 1000 times compared to 5G [79]. The integration of satellite and underwater communication networks will ensure global coverage, with new categories like the ubiquitous mobile ultra-broadband (uMUB), ultrahigh-speed-with-low-latency communications (uHSLLC), and ultrahigh data density (uHDD) [80], [81].

In anticipation of the final deployment phase of 5G, academic, regulatory, and industrial bodies have already embarked on research and development efforts for future 6G wireless networks. The period between 2020 and 2030 is projected to be dedicated to the advancement of these networks [80], [82], [83]. While 5G communication systems can support Ultra-Reliable Low Latency Communication (URLLC), their reliance on short packets and sensing-based URLLC limits their ability to deliver services with low latency, high reliability, and high data rates. As a result, multisensory Extended Reality (XR) applications, such as Augmented Reality (AR), Mixed Reality (MR), and Virtual Reality (VR), which demand such stringent requirements, cannot be fully leveraged on 5G cellular networks. Moreover, the emergence of the Internet of Everything (IoE) applications necessitates the convergence of communication, control, computing, and sensing functions. To enable the successful operation of IoE services and autonomous systems, 6G networks must provide heterogeneous devices with high data rates, reliability, and low latency for both uplinks and downlinks [84]. It is imperative that the design of 6G wireless networks takes into account these applications, as well as the technological trends anticipated from the evolving landscape of IoT services, in order to overcome these limitations. The evolution of cellular mobile communication systems, as depicted in Figure 6, illustrates the progressive refinement of functionalities and specifications over the years. Furthermore, Table 4 offers a comparison of the communication systems employed in 4G, 5G, and 6G. In contrast to 5G, 6G networks will provide significantly higher capacity, lower latency, and utilize higher frequencies. A key objective of 6G is to enable communication with latency as low as one microsecond. The unused band of frequencies in the terahertz range, situated between infrared and microwave waves on the electromagnetic spectrum, forms the foundation of 6G technology. Although terahertz waves are small and delicate, there exists a substantial amount of free spectrum above them, which holds the potential for remarkable data rates.

Presently, researchers worldwide are engaged in studying the future landscape of 6G communications, as well as the factors that will drive the development of 6G wireless networks. These networks have evolved in response to several

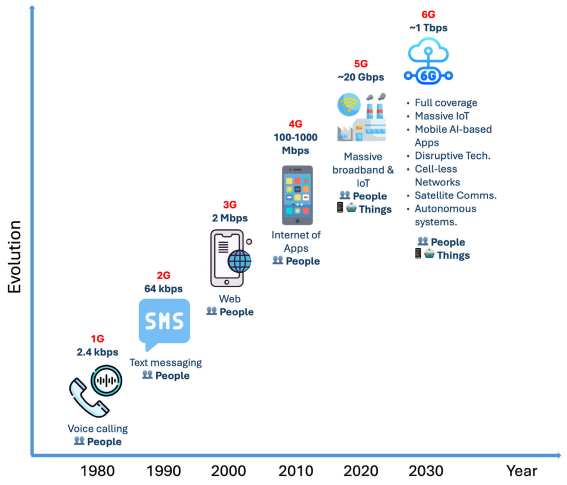

FIGURE 6. Cellular mobile communication systems evaluation (1G - 6G).

TABLE 4. Comparison between 4G, 5G, and 6G communication system.

Issue	4G	5G	6G
Per device peak data rate	1 Gbps	10 Gbps	1 Tbps
End-to-end latency	100 ms	10 ms	1 ms
Maximum spectral efficiency	15 bps/Hz	30 bps/Hz	100 bps/Hz
Mobile support	Up to 350 km/hr	Up to 500 km/hr	Up to 1000 km/hr
Satellite integration	No	No	Fully
Artificial intelligence	No	Partial	Fully
Autonomous vehicle	No	Partial	Fully
Extended reality (XR)	No	Partial	Fully
Haptic communication	No	Partial	Fully
Terahertz communication	No	Very limited	Widely
Service level	Video	VR, AR	Tactile
Architecture	MIMO	Massive MIMO	Intelligent surface
Maximum frequency	6 GHz	90 GHz	10 THz

crucial trends, including the demand for high bit rates, high reliability, low latency, high energy efficiency, high spectral efficiency, exploration of new spectra, green communication practices, intelligent networks, network availability, convergence in communications, localization capabilities, computation advancements, control enhancements, and sensing technologies. Consequently, it is anticipated that 6G will create a fully digital world, where connectivity is pervasive. This market evolution is expected to yield substantial improvements in imaging, presence technology, and location awareness. Sampling rates will be significantly faster, while data rates and throughput will experience substantial increases. Additionally, the future will witness the emergence of simple, portable devices with diverse digital capabilities, revolutionizing the way we interact with technology. Public transport optimization will enable more efficient utilization of limited rail, air, and road resources, thereby enhancing transportation efficiency. Artificial Intelligence (AI) and

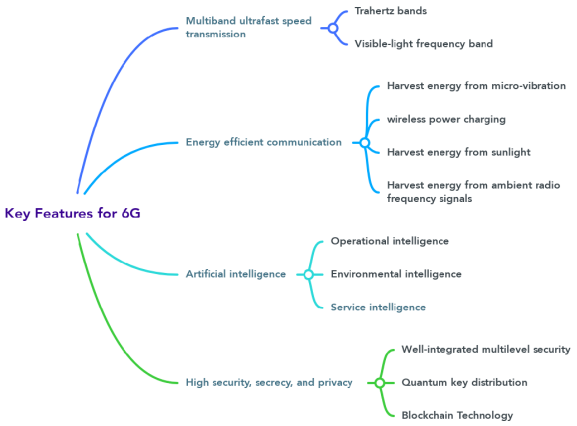

FIGURE 7. Key features for 6G.

massively parallel computing architectures will be leveraged to address transportation and scheduling operation research challenges. Below are some key featured services that are expected to be available in 6G communication systems [85], [86], [87] as shown in Fig. 7.

1) **Multiband ultrafast speed transmission:** It is feasible to transmit data at incredibly high speeds by harnessing multiple bands of terahertz frequencies alongside visible light frequencies.
2) **Energy efficient communication:** In order to achieve energy-efficient communication, it is possible to harness ambient radio frequency signals and sunlight for power generation, as well as utilize wireless power charging technology.
3) **Artificial intelligence:** Within the realm of artificial intelligence, various forms of intelligence, such as operational intelligence, environmental intelligence, and service intelligence, are employed.
4) **High security, secrecy, and privacy:** Blockchain technology, along with the integration of multiple levels of security and quantum key distribution, collectively contribute to achieving enhanced security, confidentiality, and privacy measures.

The characteristics of 6G networks, including satellite integration and ubiquitous connectivity, are essential for overcoming geographical constraints. This new generation of wireless communication will support seamless global coverage across various locations, such as land, sea, air, and skies, ensuring constant connectivity regardless of the user's location. To achieve this, the integration of terrestrial, satellite, and airborne systems is necessary, providing always-on broadband global mobile connectivity. This integration is crucial for meeting the demand for ubiquitous mobile ultra-broadband services [88]. 6G goes beyond previous wireless generations by evolving from connected things to connected intelligence. It requires a complete AI system to enable intelligent communication devices to acquire and allocate resources, similar to 5G. Additionally, 6G wireless networks are expected to transfer power wirelessly, allowing devices like smartphones and sensors to charge without physical connections. This wireless information and energy transfer (WIET) capability will be a prominent feature of 6G networks [89]. With 6G, super-3D connectivity will be universally accessible through drones and low-earth orbit satellites. Small cell networks are utilized to enhance signal quality and improve energy, throughput, and spectral efficiency in cellular systems. The integration of radar systems with 6G networks enables high-accuracy localization. Softwarization and virtualization play a vital role in the design of 6G networks, facilitating flexibility, reconfigurability, and programmability. Moreover, a shared physical infrastructure allows for the sharing of billions of devices [90], [91], [92]. 6G communication systems will benefit from ultra-dense heterogeneous networks. Multi-tier networks made up of heterogeneous networks will increase the quality of service and lower the costs [93]. Radar systems will be integrated with 6G networks because 6G wireless communication systems provide high-accuracy localization. During the design of 5GB networks, softwarization and virtualization are key features for ensuring flexibility, reconfigurability, and programmability. A shared physical infrastructure will also allow billions of devices to be shared.

In addition to offering many exciting applications and services, 6G presents a multitude of roadblocks and challenges that researchers must overcome to create a wireless network that meets expectations and delivers on its promises. These challenges such as the design of the transceiver front-end. Moreover, it is important to consider the type of materials and components being used when designing multi-antenna arrays used for THZ communication. Materials properties and the fabrication process used for these antennas might present complications at frequencies above 50 GHz. Transceivers and other devices in the 6G wireless network will need radical changes in their embedded systems and software [94]. While 6G presents exciting applications and services, researchers face numerous challenges. Designing the transceiver front-end and multi-antenna arrays for THZ communication requires careful consideration of materials and components. Complications may arise due to material properties and fabrication processes at frequencies above 50 GHz. Furthermore, embedded systems and software in transceivers and other devices within the 6G wireless network will require radical changes. Unlike 5G, which relies on predetermined frame structures and network parameters, 6G utilizes AI-driven protocols for scheduling, coordination, and signaling. Overcoming these challenges is crucial to fulfilling the promises and expectations of 6G wireless networks [84].

C. 6G EMERGING TECHNOLOGIES

The evolution towards 6G technology aims to enhance connectivity and efficiency across various devices and services in response to the growing demand for data and the rise of connected devices. 6G networking promises to bring significant advancements in security, privacy, and innovation

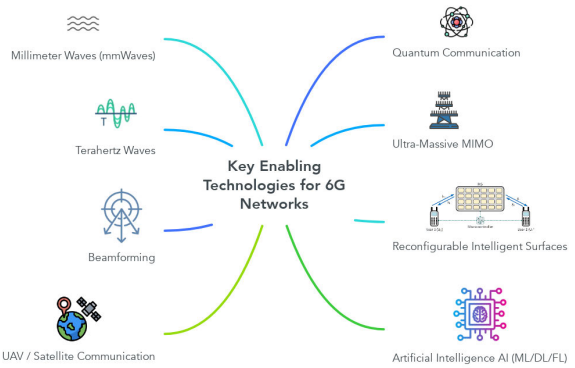

FIGURE 8. Key features for 6G.

through integrating current and emerging technologies [95]. Figure 8 presents several key technologies that are being explored and considered as potential components of 6G networks, including terahertz waves, quantum communication, beamforming, ultra-massive MIMO, reconfigurable intelligent surfaces, AI/ML, millimeter waves, and UAV or satellite communication. Each technology is crucial for enhancing future wireless communication systems' data rate, reliability, and overall efficiency [25], [26]:

1) TERAHERTZ COMMUNICATION

6G is anticipated to function within the terahertz frequency range, allowing for ultra-fast data transmission speeds and significantly reduced latency compared to current technologies. This enhanced efficiency in data transmission is supported by the utilization of AI to optimize signal processing and security measures. AI's capability to adjust transmission parameters in real-time improves network performance and minimizes signal weakening, ensuring reliable and secure wireless communication [96]. Terahertz communication has the potential to enable new applications like high-resolution imaging, remote sensing, and advanced medical imaging that necessitate higher data rates and lower latency [97]. By utilizing short wavelengths that are challenging to intercept or detect, terahertz communication can enhance wireless communication security, reducing the risk of cyber-attacks and unauthorized access [98].

2) ULTRA-MASSIVE MIMO

Massive Multiple Input Multiple Output (MIMO) technology, a crucial element in the advancement of 6G networks, brings about significant progress in network capacity, data rates, and coverage. By employing a vast array of antennas that can transmit and receive multiple data streams simultaneously, this technology not only speeds up data transmission but also greatly enhances data rates [99]. Moreover, ultra-massive MIMO improves signal processing and beamforming, resulting in increased energy efficiency and more efficient spectrum utilization. Additionally, ultra-massive MIMO plays a key role in supporting emerging applications that require higher data rates and lower latency, such as virtual reality, autonomous vehicles, and smart city infrastructure development [100]. AI algorithms adapt antenna configurations in real time and anticipate user demand patterns to optimize spectral efficiency and user throughput. This collaboration between AI and ultra-massive MIMO enhances network coverage and reliability while reducing interference for improved service quality [101].

3) BEAMFORMING

Beamforming is an essential technology that enhances the effectiveness and dependability of wireless communication, facilitating the evolution of 6G networks. This technique involves the precise targeting of radio waves in a particular direction to optimize spectrum utilization and network efficiency. In the context of 6G networks, beamforming plays a crucial role in concentrating wireless signals towards intended recipients, leading to reduced interference and enhanced signal strength [102]. Consequently, this results in increased data speeds, decreased latency, and the capability to facilitate real-time data transmission for innovative applications such as virtual reality, remote medical procedures, and autonomous vehicles. By directing radio waves to specific regions, beamforming technology allows for more efficient utilization of the frequency spectrum, thereby diminishing interference, boosting network capacity, alleviating congestion, and ultimately enhancing overall performance [103]. AI-driven beamforming techniques enhance spectral efficiency and mitigate multi-path fading, ensuring seamless connectivity and reliability in dynamic urban environments [104].

4) QUANTUM COMMUNICATION

Quantum communication, a technology that uses photons for data transmission, is ideal for 6G networks due to its high-security levels [105]. Quantum communication techniques are anticipated to be utilized to enhance security measures, ensuring unbreakable encryption for data transmission and safeguarding sensitive information from cyber threats. It's also suitable for military and government communications, as well as real-time data transmission applications like autonomous vehicles and smart cities. Quantum communication provides unparalleled security through quantum essential distribution methods that prevent data transmission from eavesdropping. Integrating quantum principles into 6G networks could bring additional privacy and data protection measures into play. Quantum technology integration improves system performance while increasing security and dependability; its potential is unrealized in future communication systems. The integration of AI into quantum communication within 6G networks optimizes protocols for quantum key distribution and enhances network management systems. AI algorithms streamline encoding strategies and automate key distribution processes, guaranteeing secure and dependable data transmission across quantum

communication channels [76]. However, its implementation faces challenges like specialized hardware and infrastructure, as well as substantial costs.

5) RECONFIGURABLE INTELLIGENT SURFACES (RIS)

RIS technology involves employing arrays of small, programmable reflectors that manipulate radio waves in real time for enhanced signal quality, coverage extension, and interference mitigation. RISs are expected to transform the propagation environment, creating an intelligent radio environment with dynamic capabilities for 6G wireless communications applications [106]. This transformation could radically reshape wireless communications landscapes and enable unprecedented capabilities and functionalities. Another significant advantage of RIS technology is its contribution to energy efficiency. By reflecting and focusing radio waves directionally, an RIS minimizes the energy required for transmitting signals over long distances [107]. This leads to lower power consumption, prolonged battery life for mobile devices, and a reduction in the overall energy footprint of the networkThe role of AI in reconfigurable intelligent surfaces (RISs) is instrumental in optimizing their configuration for efficient signal reflection and amplification, thereby enhancing network coverage and capacity. AI algorithms adaptively adjust RIS configurations based on changing environmental conditions and user demands, optimizing energy efficiency and spectral utilization for improved network performance [106].

6) INTEGRATED SATELLITE AND TERRESTRIAL NETWORKS (ISTN)

The seamless integration of satellite and terrestrial networks provides global coverage and reliable connectivity, closing the digital gap in remote and underserved regions. The Integrated Satellite-Terrestrial Network (ISTN) concept holds significant promise for offering universal broadband access to various user groups [25]. UAV/satellite communication technology, utilizing unmanned aerial vehicles (UAVs) and satellites, can advance the development of 6G networks [108]. By employing these aerial platforms, rapid data transfer and internet connectivity can be expanded to remote and underserved areas that are not reachable through traditional terrestrial networks. This technology has the potential to enhance network coverage, especially in remote and rural areas without standard infrastructure, thereby improving access to high-speed internet and data services. Furthermore, UAV/satellite communication supports new applications that require real-time data transmissions, such as remote medical procedures and disaster response efforts [109]. By employing AI-driven optimization for trajectory planning and resource allocation, UAV/satellite communication ensures continuous connectivity in remote regions by predicting user demand patterns and dynamically allocating resources. This improves network reliability and coverage, leading to enhanced access to high-speed internet and data services [110].

7) HYPERCONNECTED EDGE COMPUTING

The infrastructure of edge computing, combined with ultra-reliable low latency communication (URLLC), facilitates immediate data processing at the edges of networks to support applications such as autonomous vehicles, augmented reality, and industrial automation. AI-driven edge devices help decrease latency and traffic while enabling the functionalities of the Internet of Things (IoT) and augmented reality (AR). In the context of 6G, IoT devices will feature more powerful processors, enhancing their edge computing capabilities. This advancement will enable devices to process data locally, reducing latency and enhancing overall network efficiency. The interconnected nature of edge computing, powered by AI, plays a key role in transforming 6G networks by managing data and innovative applications locally to tackle issues related to latency and congestion [76], [105].

D. CHALLENGES IN 6G NETWORKS

6G poses numerous challenges that must be addressed by researchers to fulfill its promises and meet expectations. The main challenges in 6G Networks include [4], [26], [95], [111], [112]:

1) TRANSCEIVER FRONT END DESIGN

Developing efficient and high-performance transceiver front ends that can operate at frequencies above 50 GHz, which may introduce complications due to material properties and fabrication processes.

2) MULTI-ANTENNA ARRAY DESIGN

Selecting appropriate materials and components for multi-antenna arrays used in terahertz (THz) communication, considering the unique challenges posed by THz frequencies.

3) EMBEDDED SYSTEMS AND SOFTWARE

Making significant changes to the embedded systems and software of transceivers and other devices in the 6G network to support the advanced functionalities and requirements of 6G.

4) AI-DRIVEN PROTOCOLS

Implementing AI-driven protocols for scheduling, coordination, and signaling in 6G networks, unlike the predetermined network parameters and rigid frame structures used in 5G.

VI. AN OVERVIEW OF BLOCKCHAIN

A. FUNDAMENTALS OF BLOCKCHAIN

The blockchain is a decentralized database that facilitates the storage of transaction records shared among members. It operates on the principle of consensus, ensuring the prevention of fraudulent activity. Once a record is accepted by the blockchain, it becomes permanent and immutable, unable to be changed or lost.

The concept of blockchain involves a decentralized and encrypted database that utilizes shared ledger technology

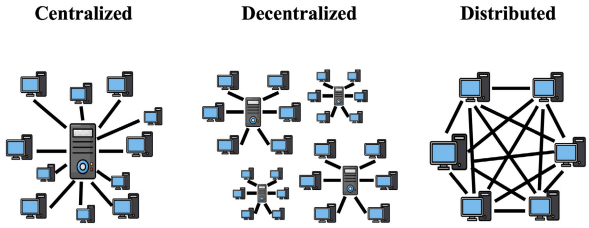

FIGURE 9. Centralised, decentralized versus distributed, peer-to-peer network.

to record and distribute data. This system functions as a distributed digital ledger (DLT), with each ledger representing a chain of blocks connected through hash capacity. Transactions are duplicated and distributed across a peer-to-peer (P2P) network of computers, known as nodes, as depicted in Figure 9 This process eliminates the need for central administration [11], [16].

The blockchain process begins with network participants verifying and sharing a new transaction using consensus mechanisms. These transactions are then time-stamped and grouped together to form a new block. The blocks are added to the existing chain in chronological order. Once added, a transaction is considered complete and becomes an immutable part of the ledger. This ensures the security of the stored information, as it requires the owner's digital signature to authorize a transaction, providing authenticity and protection against modifications [113].

The primary goal of blockchain technology is to enable secure and unalterable recording and distribution of digital data. This is accomplished through the use of robust cryptographic algorithms to protect transactions and consensus algorithms to maintain the integrity of the network. Blockchain technology has the potential to revolutionize various aspects of our lives, including transforming payment systems, managing global supply chains, and verifying authenticity. Its efficiency, transparency, and security have made it increasingly popular across different sectors, ranging from individuals and businesses to governments [113].

B. BLOCKCHAIN CHARACTERISTICS

In blockchain, the absence of a central authority or organization overseeing the system is a defining feature. Instead, the blockchain is maintained by a decentralized network of nodes. This characteristic is highly significant as it provides a viable alternative to centralized systems. Users in a blockchain are empowered with authority, allowing them to have direct access to the system and the ability to store assets without relying on a regulating body or third party.

The revolutionary nature of blockchain technology is driven by several key characteristics: [114], [115], [116]:

1) **Decentralization**: Blockchain technology eliminates the need for intermediaries or institutions in data interaction. Instead, it utilizes a peer-to-peer (P2P) network where all nodes are equal participants. There is no central server for data processing, storage, and updating. This decentralized nature ensures there is no single point of failure, as the entire blockchain network's data is distributed among multiple nodes globally.
2) **Non-Tampering:** Blockchain technology ensures the security and immutability of transaction data. Once encrypted into a block and added to the blockchain, the data becomes permanent and cannot be tampered with. The blocks are connected in a chain structure, with each block storing the hash value of the previous block. Any attempt to tamper with the data would require changing the hash values of the current and subsequent blocks, which would cause the entire chain structure to collapse. The cost of data tampering is prohibitively high, making it practically impossible to modify the blockchain without detection.
3) **Privacy and security:** Blockchain ensures security through individual encryption of all records. Each piece of information on the blockchain is cryptographically hashed, providing a unique identity. The blocks contain their own hash and the hash of the previous block, creating a cryptographic link between them. Immutability further enhances security, as modifying data would require changing all hash IDs, which is practically impossible. The absence of a central authority prevents easy data manipulation and adds an extra layer of protection to the network.
4) **Anonymity:** The blockchain network ensures the privacy and anonymity of every participant. Nodes are not required to reveal their identities to each other. Instead, pseudonyms, which are unique addresses, are used for conducting transactions. This anonymity feature allows participants to engage in a trusted manner without disclosing their real identities. Asymmetric encryption technology is utilized to establish trust in this anonymous setting.
5) **Traceability:** The blockchain network enables traceability of all transactions, as they are publicly available for any node to access. Although the private information of the involved parties is encrypted, other data on the blockchain can be accessed through public interfaces. The utilization of a chain block structure with timestamps introduces a time dimension to the stored data. Through cryptographic methods, each transaction is linked to two adjacent blocks, facilitating the tracing of transaction origins by users [117].

C. BLOCKCHAIN STRUCTURE

Figure 10 depicts a blockchain as a specific type of "data structure" comprising interconnected blocks that undergo encryption using mathematical algorithms. These blocks encompass various digital assets, including financial transactions, inventory records, and sensor data. Furthermore, each block contains metadata and a collection of transaction records from the same time period. The metadata usually

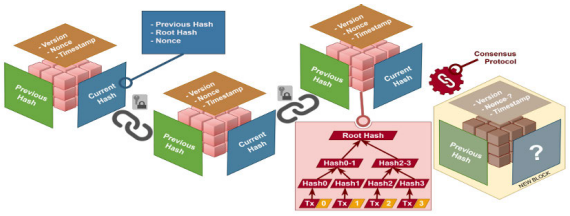

FIGURE 10. Blockchain's block connection and block structure design [121].

consists of a time stamp, a unique cryptographic fingerprint known as a ''hash,'' and the hash of the previous block, which establishes the linkage between blocks. The blockchain data structure operates on the principle of being ''append-only,'' meaning that once recorded, old entries are never deleted or modified. Consequently, a continuously expanding historical record of all transactions is maintained from the inception of the blockchain. This approach ensures data integrity, authenticity, and traceability within blockchain systems [118], [119], [120], [121].

Blockchain is a combination of four leading technologies [113]:

1) **P2P technology:** One of the fundamental and indispensable features of blockchain is the ability to create immutable ledgers, guaranteeing the structural immutability of each individual node's ledger. Unlike centralized databases that are susceptible to hacking and rely on trust in third parties for security, blockchain employs an immutable distributed ledger. This means that the ledgers within a blockchain consistently progress forward, only allowing data to be added in a time-sequential order. Once data is appended to the blockchain, modifying it becomes virtually impossible, ensuring its enduring structural immutability.
2) **Security technology:** Blockchain transactions benefit from a suite of security technologies, including encryption, cryptographic techniques like PKI, digital signatures, Merkle trees, and hashing algorithms. These technologies outlined in [122], play a crucial role in guaranteeing the privacy and security of transactions. Utilizing data encryption and cryptography mechanisms, blockchain prevents unauthorized tampering and forgery. These techniques ensure that data remains secure and unaltered throughout the transaction process. The implementation of a complex checksum sharing mechanism upholds the integrity, availability, and confidentiality of data. This mechanism ensures that data remains intact, accessible, and confidential, providing a robust foundation for secure transactions. Blockchain employs encryption standards, such as digital signatures, to detect multiple attackers. Each node possesses a unique key, and packet transmission occurs only when the key is in a valid state. This ensures that only authorized entities can engage in the transaction process [123]. By leveraging these security technologies, blockchain establishes a reliable framework for maintaining the privacy and security of transactions. Through data encryption, cryptography, checksum sharing, and attacker detection, blockchain ensures the integrity, availability, and confidentiality of data, safeguarding against tampering and unauthorized access attempts.
3) **Consensus algorithms:** Consensus mechanisms play a critical role in the blockchain network by providing a mathematical mechanism for nodes to synchronize and reach agreements on the current state of the distributed ledger. This ensures secure and transparent record-keeping within the network. The consensus mechanism enables nodes within the blockchain network to synchronize and agree on the current state of the distributed ledger. By reaching a consensus, all participating nodes can maintain a consistent and accurate view of the ledger. Several widely used and common consensus algorithms exist in the blockchain ecosystem. These include Proof of Work (PoW) which requires nodes to solve complex mathematical puzzles to validate transactions and add blocks to the blockchain. This algorithm is famously used in Bitcoin and Ethereum networks. Proof of Stake (PoS) selects validators to create new blocks based on their stake or ownership of the cryptocurrency. It reduces the energy consumption associated with PoW by removing the need for intensive computational tasks. Delegated Proof of Stake (DPoS) which introduces a voting system where stakeholders elect a limited number of delegates to validate transactions and produce blocks. This consensus algorithm aims to increase scalability and efficiency. Practical Byzantine Fault Tolerance (PBFT) is a consensus algorithm designed to tolerate Byzantine faults, where malicious nodes may behave arbitrarily. It ensures consensus even when there is a certain percentage of malicious actors in the network. These consensus algorithms enable blockchain networks to achieve agreement, security, and reliability in maintaining a distributed ledger. Each algorithm has its own strengths and trade-offs, catering to different requirements and use cases within the blockchain ecosystem [114].
4) **Smart contracts:** Smart contracts emerged from Nick Szabo's pioneering proposal in 1994 as a means to digitally execute agreement terms, eliminating the requirement for trusted intermediaries. These contracts bring forth a range of advantages, including reduced transaction costs, enhanced reliability, and increased efficiency when compared to traditional contracts [124], [125]. Smart contracts serve as digital counterparts to contractual terms, automatically enforced upon triggering and remaining unalterable once deployed. By leveraging this digital enforcement, smart contracts provide a secure and reliable execution framework for agreement terms [126]. Within the

blockchain ecosystem, smart contracts are written into blocks as program code, achieving consensus among network nodes. This integration ensures that every node agrees upon and enforces the logic encapsulated within the smart contract. By enabling seamless and automatic execution of agreement terms, smart contracts revolutionize the way digital agreements are handled. Their immutability and integration within blockchain networks offer a robust and efficient framework for executing and enforcing contractual obligations [127]. The operations of smart contracts can be inspected by all peer nodes in the P2P blockchain network.

D. TYPES OF BLOCKCHAIN

Differentiating between various types of blockchains can be challenging. To assist in this process, Table 5 showcases different blockchain categories based on two key factors: permission configuration (determining who can read, write, and commit transactions) [128], and server hosting type [129]. Blockchain types are categorized based on the authorization granted to read, write, and commit transactions on the blockchain. Read permission enables a node to access all past transactions, write permission allows nodes to create and share transactions with other network nodes, and commit permission enables a node to update the distributed ledger [128]. Choosing the appropriate type of blockchain depends on specific application requirements. Careful consideration is given to factors such as permissions, server hosting, and other unique characteristics to ensure the selected blockchain aligns with the desired use case.

Understanding these distinctions is essential in navigating the diverse landscape of blockchains and selecting the most suitable option for specific applications.

E. EVOLUTION OF BLOCKCHAIN TECHNOLOGY APPLICATIONS

Blockchain technology has evolved through different versions, from 1.0 to 5.0, to meet the varied requirements of industries and businesses. While the fundamental features of blockchain remain consistent, the underlying technologies continue to advance, reflecting the new and developing nature of this technology. Although there is no universally agreed-upon classification for the evolution of blockchain, the literature suggests five generations, which will be briefly outlined [14], [113], [119], [120], [130], [131]. Figure 11 depicts the extent of technical improvements in the blockchain.

1) BLOCKCHAIN 1.0 - 2009: CRYPTOCURRENCY

The initial phase of blockchain technology, known as Blockchain 1.0, established the essential building blocks of the technology platform, protocol, and digital currencies like Bitcoin and other tokens. This generation primarily focused on facilitating accurate monetary transactions and is exemplified by cryptocurrencies such as Litecoin, Dogecoin, and Reddcoin. The introduction of Blockchain 1.0 can be traced back to Satoshi Nakamoto's groundbreaking white paper, "Bitcoin: A Peer-to-Peer Electronic Cash System," which laid the groundwork for this technology. In 2009, the first Bitcoin transaction took place, marking a significant milestone. However, Blockchain 1.0 faced several limitations, including high energy consumption, costly hardware requirements, scalability issues, slow transaction processing, and small data/block size. Despite these challenges, Bitcoin emerged as a practical and tangible application of this technology, demonstrating its real-world feasibility. Although Blockchain 1.0 set the stage for digital currencies and highlighted the potential of decentralized transactions, subsequent generations of blockchain technology have since addressed these limitations, paving the way for even more innovative and transformative applications.

2) BLOCKCHAIN 2.0 - 2015: SMART CONTRACTS AND ASSET TOKENIZATION

The second generation of blockchain technology goes beyond the functionalities of cryptocurrencies, offering a wider range of capabilities. This advancement was made possible by the emergence of trusted code platforms like Ethereum and Hyperledger. These platforms introduced groundbreaking concepts such as smart contracts and the digital tokenization of physical assets. Smart contracts have become a crucial element of many blockchain platforms and applications. They enable the creation of decentralized autonomous organizations (DAOs) and facilitate automated, self-executing agreements. Additionally, the concept of tokenization plays a significant role in Blockchain 2.0. It involves converting assets and rights into digital tokens on a blockchain network, allowing for the representation and transfer of various types of value. Despite these advancements, Blockchain 2.0 still faces certain limitations. Scalability issues, high energy consumption, vulnerabilities in smart contract code, and the risk of a 51% attack remain challenges that need to be addressed. Nonetheless, the second generation of blockchain technology has laid the foundation for more sophisticated and diverse applications, expanding the possibilities beyond cryptocurrency transactions.

3) BLOCKCHAIN 3.0 - 2018: ENTERPRISE BLOCKCHAIN

The year 2018 witnessed substantial advancements and widespread integration of blockchain technology across diverse industries. As the calendar turned to 2019, it was hailed as the year when enterprise blockchain adoption took center stage. This new era brought forth the emergence of the third generation of blockchain technology, equipped with unique attributes designed to surpass the constraints of its predecessors. Notable features of this latest generation encompass:

- **Decentralized applications (dApps):** The third generation of blockchain technology has ushered in a range of novel features aimed at addressing the limitations of its predecessors. One notable advancement is the proliferation of decentralized applications (dApps) that leverage

TABLE 5. Comparison between the different types of blockchain.

Property	Public	Private	Consortium (Hybrid Blockchains)
Consensus process	Permissionless	Permissioned	Permissioned and semiprivate
Operate permission (add, read, and write)	Anyone can join and maintain the shared ledger	Only authorized entities join and maintain the block	Jointly maintained by an authorized pre-selected group of nodes from multiple organizations or individuals
Consensus determination	Not controlled and allow anyone to join and remain anonymous to protect their privacy	Fully controlled by one organization and its nodes are not anonymous	Fully controlled by controlled nodes from multiple organizations
Consensus protocols	Proof-of-work (PoW), Proof of stake(PoS),etc	Multi-party	Multi-party
Transaction approval	Low efficiency as Transaction throughput is limited and high latency and large energy consumption	High efficiency as verification is done by just the owner of the blockchain, low latency, and low energy consumption	High efficiency as verification is done just by a pre-selected group of nodes from multiple organizations, slower than private ones, and low energy consumption
Immutability	Impossible to tamper due to the large number of participants	Easily tampered with due to the limited number of participants	Based on better security measures due to participants from multiple organizations
Network type	Completely Decentralized	Fully Centralized	Partially Centralized
Use Cases	Cryptocurrency	Finance and Supply chain management	Banking and Insurance
Application	Bitcoin	Ethereum	Edexa
Security and Privacy	Low privacy and anonymity	High Privacy, No anonymity, and Lower Security	High Privacyand Better Security
Cost	Costive	Costive	Costive
Example	Bitcoin and Ethereum (ETH) blockchains	Hyperledger is a private, permissioned blockchain	Energy Web Foundation, Dragonchain, and R3

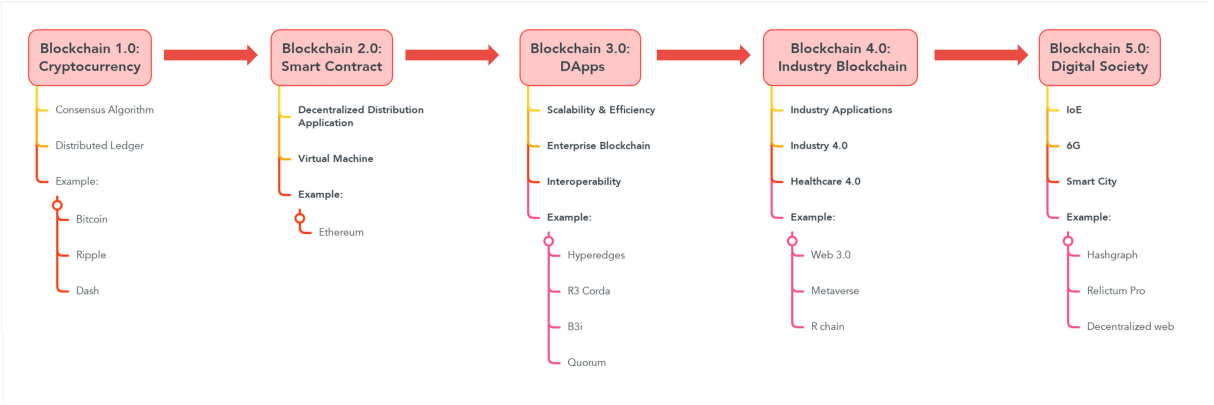

FIGURE 11. The scope of technical improvement in the blockchain.

blockchain infrastructure and employ smart contracts for seamless execution. Prominent examples of these dApps include Ethereum's decentralized autonomous organization (DAO), Hyperledger's chain codes, and Namecoin's domain name service (DNS). The advent of Blockchain 3.0 strives to augment the applicability

of blockchain technology to dApps, boasting increased storage capacity and scalability while upholding robust security and privacy measures. This facilitates effortless integration of data from diverse sources without compromising ownership confidentiality and fosters interoperability without unnecessary complexities. The inherent flexibility and capabilities of blockchain technology hold immense promise for fostering innovation, integration, and sustainability within the healthcare industry [113].

- **Inter-blockchain:**The inter-blockchain feature, also referred to as blockchain-to-blockchain (BC2BC) or relational blockchain, revolutionizes transaction processing by enabling seamless interaction between different blockchains, thereby enhancing the system's scalability. Cross-chain communication technologies, such as sidechains and sub-blockchains, have made significant strides in this domain, facilitating interoperability across blockchains. Sidechains empower independent transactions across multiple chains, while sub-chain technology enables the extraction of autonomous functions from the main chain. These advancements effectively eliminate network bottlenecks, bolstering system throughput, availability, and scalability. However, it is important to acknowledge the key limitations of Blockchain 3.0, including the need for back-end control to ensure system integrity and security, as well as the associated costs and complexities of implementation.

4) BLOCKCHAIN 4.0 - 2019: INDUSTRY

Blockchain 4.0 represents a significant leap forward from its predecessors, as it focuses on rendering decentralized applications (DApps) more viable and functional in real-time business scenarios, aligning with the principles of the Industrial Revolution 4.0. This remarkable progress is made possible through the implementation of a consensus protocol that effectively governs the network, ensuring seamless operation and reliability. By harnessing this enhanced protocol, Blockchain 4.0 empowers businesses to leverage DApps in a practical and efficient manner, unlocking new possibilities and opportunities in the ever-evolving landscape of the fourth industrial revolution.

5) BLOCKCHAIN 5.0 AI-ENABLED, IoT-CONVERGED BLOCKCHAIN

The convergence of Blockchain 4.0 with AI, 6G, and IoT technologies paves the way for Blockchain 5.0, an era where the Internet of Everything is seamlessly accommodated, and human involvement in the blockchain is superseded by AI-powered consensus algorithms for transaction validation and block addition. Anticipated as the next generation, Blockchain 5.0 aims to overcome the limitations of traditional blockchain systems, boosting processing speed and security through virtual connections.

However, the widespread adoption of blockchain technology in 6G networks faces a significant hurdle in the form of scalability. The slow processing speed inherent in blockchain may not align with the ultra-fast connectivity offered by 6G. For instance, established systems like Bitcoin and Ethereum can only handle a limited number of transactions per second, while Visa can process tens of thousands of transactions in the same timeframe. Addressing this challenge is crucial for unlocking the full potential of blockchain in the context of 6G networks.

VII. MOTIVATIONS TO APPLY BLOCKCHAIN FOR FL-IoT IN 6G, APPLICATIONS, AND SOME OPEN ISSUES

A. THE ROLE OF BLOCKCHAIN IN IoT

As mentioned before, blockchain technology provides a decentralized and encrypted database. It could be considered one of the most promising technologies for maximizing IoT capabilities [132].

Firstly, securing IoT devices and networks against cyber-attacks is a concern. Due to the heterogeneity of the IoT network and devices, managing security vulnerabilities is a significant challenge. Blockchain naturally supports security through immutable and decentralized characters, which can complement the security deficiency in IoT [132].

On the other hand, the nature of the information transmission through the IoT network and its devices makes the information susceptible to privacy breaches, including identity, data, and location [133]. Through BC and IoT integration, all interactions between the participants are done by using a unique address that is generated by blockchain and allocated to each participant [132].

By ensuring the security and privacy provided by blockchain features, the trust between participants regarding data integrity is improved. In addition, the validation process of adding new transactions in the blockchain involves a consensus by the participants, which consequently increases transparency and trust among the users. Furthermore, due to the blockchain's decentralization, there is no need for a centralized server, which decreases the overall cost of the IoT network. [132], [134].

1) ISSUES OF BLOCKCHAIN IN IoT

Scalability is one of the most crucial blockchain issues that will subsequently impact IoT performance in terms of throughput and storage [132]. The limitation on block size hampers the simultaneous processing of a significant number of transactions, leading to potential delays [135]. Even though blockchain supports security through immutability and decentralization, these features are double-edged. With the exponential increase in IoT devices, the demand for storage will increase over time. The fact that blockchain transactions cannot be deleted ever again burdens IoT data storage [132].

In addition, consensus algorithms are required to perform the validation process of new transactions. Consensus algorithms may face challenges regarding resources wasted on upgrading hardware and consuming a lot of energy to

solve puzzles [132]. In addition, one of the most popular used consensus algorithms, PoW, does not work well for real-time payments because of the speed of block creation [136].

Finally, even though blockchain-generated addresses are utilized to perform transactions to keep users' identification anonymous, privacy could be violated regarding transactions privacy. This issue appears because of blockchain transparency, which claims all the transactions are visible to all the participants in the IoT network, which can lead to revealing users' identification [132]. In addition, maintaining the private key of the blockchain secure is one of the most significant concerns because if the key is compromised, all the transactions will be leaked [137].

B. THE ROLE OF BLOCKCHAIN IN FL-IoT

In addition to the method features of blockchain in IoT in Subsection VII-A, blockchain improves security, privacy, integrity, and reliability of datasets used for training FL and parameters of the model [138], [139].

In order to support optimal decision-making in complex industrial systems, algorithms are required to handle both raw data and spatiotemporal data flows. It is generally not advisable to rely on a single, centralized database solution for such systems. As a result, we explore the use of decentralized or federated architectures that integrate IoT and blockchain with secure big data analytics services. This approach ensures a robust and secure framework for handling data in industrial systems, allowing for efficient and reliable decision-making processes. In [140], Rieken et al. propose a study highlighting the suitability of Federated Learning (FL) for digital medical use cases with data limitations. By combining FL, IoT, and blockchain, the level of privacy and protection is increased while minimizing latency and communication pressure. Blockchain provides more powerful and appropriate data sharing for FL compared to traditional FL methods. Additionally, another study [65] demonstrates the scalability and the elimination of single points of failure using blockchain technology. It ensures coherency between local models and simplifies data flow and access control without requiring a fully distributed topology. The proposed anomaly detection algorithm securely stores template parameters on the blockchain using a one-way fuzzy hash function, preserving privacy.

Advanced architectures of blockchain, such as dual-blockchain systems, handle issues of data heterogeneity of FL and FL model staleness by grouping and synchronizing training tasks [141].

1) ISSUES OF BLOCKCHAIN IN FL-IoT

In addition to the mentioned problems in Subsection VII-A1 regarding the issue of integrating blockchain with IoT, other matters will be raised by incorporating blockchain with FL-IoT, including the overhead on communication and computation. FL requires computation to update the local model; and communication to share the updated parameters with FL servers and receive parameters of the globe model from FL servers. On the other hand, blockchain technology demands computation, e.g., executing consensus algorithms for the mining process and Proof of Work (PoW). From a communication perspective, there are many processes that need to be accomplished for example, miners are required to propagate the local parameters to the whole network and send verified transactions [142].

Further, Due to the immutability of blockchain technology, model updates are stored permanently, costing a huge amount of storage space. However, the FL parameters tend to change over time, depending on the datasets used to train the models [143].

C. THE ROLE OF BLOCKCHAIN IN 6G

The world is currently undergoing a significant transformation into the intelligent information era, poised to elevate user experiences across diverse domains such as healthcare, transportation, entertainment, and smart cities. However, the telecommunication infrastructure must rise to meet the unprecedented service level requirements of future applications, including Virtual Reality (VR), holographic communications, and massive Machine Type Communications (mMTC). This presents substantial challenges for the communication network. Figure 12 presents a comprehensive overview of the role that blockchain plays in the context of 6G technology [144], [145], [146].

In order to address these limitations and establish functional standards for the forthcoming 6G era, blockchain technology has emerged as a disruptive enabler [147]. The integration of blockchain and 6G technology is set to revolutionize communication systems, ushering in a new era of efficiency, reliability, and accessibility. By harnessing the secure and transparent network of blockchain and the fast and dependable connectivity of 6G, this technological fusion will facilitate the advent of novel business models and services, including decentralized applications, smart contracts, and secure and automated transactions. This convergence will open up limitless possibilities, empowering individuals and organizations to explore new horizons in the realm of communication [12]. Moreover, this integration will significantly bolster data privacy and security measures, granting users greater control over their personal information. Additionally, it will pave the way for the emergence of innovative use cases, including autonomous vehicles, smart cities, and virtual reality experiences. The combined impact of blockchain and 6G on future communication systems promises to be transformative, shaping a more interconnected and secure world.

However, it is imperative to address key challenges pertaining to standardization, interoperability, and scalability. This necessitates collaborative efforts and relentless innovation from governments, industry leaders, and academia to fully unlock the vast potential of this groundbreaking technology combination. By actively working together, we can ensure

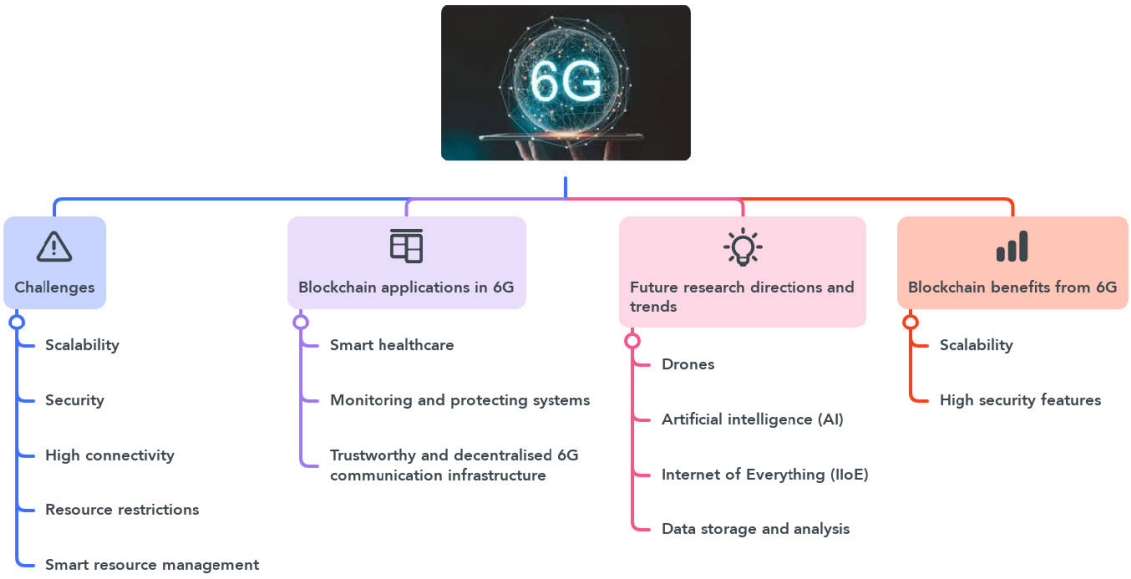

FIGURE 12. An overview of the role of blockchain in 6G.

that the benefits of blockchain and 6G are harnessed to their fullest extent, driving us towards a future where communication is seamless, secure, and limitless in its possibilities [13], [15], [148].

1) ISSUES AND POTENTIAL SOLUTIONS

In the realm of 6G network development, B. Aazhang, et al. in [149] have identified a range of challenges, including scalability, low latency, integration, higher throughput, confidentiality, and the looming threat of DDoS attacks. To effectively evaluate and monitor the behavior of a multitude of tenants and devices within the network system, standard security measures will be essential. While some countries are still focused on 5G, certain research groups have already initiated projects related to 6G, with expectations of revolutionizing communication technologies by 2030.

Blockchain technology holds immense potential in facilitating trust within future networks, offering faster processing times and lower costs compared to alternative technologies. By 2025, mobile traffic for 6G is projected to reach 607 Exabytes per month, further surging to 5016 Exabytes per month by 2030. This exponential growth necessitates exceptional service levels with high data rates and application traffic volume. However, the integration of blockchain with 6G presents its own set of challenges that require careful consideration and resolution, which include [145], [147], [150]:

1) **Throughput:** With the proliferation of connected Internet of Everything (IoE) devices and data-intensive applications within a high-speed communication infrastructure, a DLT-based 6G system will be tasked with processing a substantial volume of transactions. This necessitates a high throughput, where the system must efficiently handle a significant number of transactions within a given timeframe. However, storing verified transactions separately at each node presents challenges in terms of storage capacity. Furthermore, as the size of the database (ledger) expands, the time required to verify new transactions increases, resulting in higher latency. This limitation becomes particularly problematic for devices with limited resources that aim to participate in the blockchain network. To overcome these challenges, potential solutions can be explored. One such solution is the implementation of sharding or hierarchical blockchain structures, which enhance throughput by dividing the workload across multiple nodes. This approach enables parallel processing and improves the overall transaction processing speed. Additionally, utilizing off-chain storage or sidechains can address storage concerns, allowing for more efficient utilization of resources. By leveraging blockchain technology to provide a transparent and decentralized ledger for monitoring network resources and usage, 6G networks can achieve efficient network management. This, in turn, can lead to optimized network performance and reduced operational costs. By addressing the issues related to throughput, storage, and latency, blockchain technology offers a promising solution to enable effective transaction processing and resource management in the context of 6G networks.
2) **Exchange in security exploits:** The inherent transparency of blockchain technology exposes it to potential security attacks, such as selfish mining and Sybil attacks, which allow attackers to exploit the

resources of honest miners or manipulate multiple blockchain accounts. To mitigate these vulnerabilities, intelligent contracts can be employed to facilitate secure exchanges among participants. Enhanced security measures can be implemented by incorporating homomorphic signatures and Trusted Execution Environments (TEEs). These mechanisms bolster the security of blockchain transactions, ensuring that sensitive information remains protected. Additionally, Privacy Enhancing Technologies (PETs) and Attribute-Based Encryption (ABE) can be leveraged to safeguard privacy, enabling participants to maintain anonymity and confidentiality throughout the blockchain ecosystem. By integrating these advanced security and privacy-enhancing techniques, blockchain can effectively mitigate the risks associated with transparency and provide a more secure and confidential environment for transactions and interactions among participants.

3) **Scalability:** The issue of scalability poses a significant challenge in the cryptocurrency industry, particularly when it comes to transaction speeds. It is crucial for blockchain technology to efficiently handle a large volume of transactions, but achieving this remains a complex task. In order to tackle this challenge, researchers have explored various techniques, including sidechains, lightning networks, sharding, pruning, and directed acyclic graphs. However, these methods still encounter obstacles, such as determining the optimal allocation of tasks and deciding which transactions to prune. One potential solution to enhance scalability involves limiting data replication among nodes. By implementing this approach, blockchain technology can facilitate the development of scalable and adaptable network architectures for 6G networks. This would effectively support the growing number of connected devices and meet the increasing demand for high-speed data transfer. By employing innovative approaches and continually refining scalability techniques, the cryptocurrency industry can overcome the challenges of transaction speed and pave the way for a more scalable and efficient blockchain ecosystem. This will enable seamless integration with 6G networks and empower the smooth operation of a multitude of connected devices.
4) **Seamless Interoperability:** Interoperability within the blockchain industry entails the seamless exchange of data between diverse blockchain networks. This encompasses actions such as replicating data from one blockchain to another or executing functions based on information derived from another blockchain. However, achieving interoperability poses challenges due to the differing protocols and standards employed by various blockchain platforms, which in turn hinders integration with 6G networks. To address this challenge, blockchain technology can play a pivotal role in enabling smooth interoperability between 6G networks and devices. By leveraging blockchain's inherent characteristics, such as decentralization and transparency, it becomes possible to establish a more connected and integrated communication ecosystem. This allows for the secure and efficient sharing of data and information across diverse blockchain networks, ultimately fostering seamless interactions and collaborations within the 6G landscape. By promoting interoperability, blockchain technology not only facilitates the exchange of value and data but also enhances the overall functionality and effectiveness of 6G networks. This integration holds the potential to unlock new possibilities and drive innovation in the realm of communication technologies, ultimately leading to a more cohesive and interconnected future.
5) **Trustworthy Transactions:** Intelligent contracts emerge as a robust solution to address security vulnerabilities inherent in blockchain technology, particularly concerning exploits like selfish mining and Sybil attacks. These contracts effectively mitigate the risks associated with the transparent nature of blockchain by facilitating secure transactions among participants. By doing so, they provide a safeguard against the manipulation and exploitation of multiple blockchain accounts. The adoption and utilization of intelligent contracts within blockchain systems are on the rise. These contracts enable software-based agreements, such as exchanges, among members, bolstering the overall viability and reliability of blockchain technology. With their ability to enforce secure and transparent transactions, intelligent contracts contribute to the strengthening of trust and security within the blockchain ecosystem. As the prevalence of intelligent contracts continues to expand, they play a pivotal role in enhancing the efficiency and integrity of blockchain systems. By providing a secure framework for reliable and enforceable agreements, intelligent contracts contribute to the growth and development of blockchain technology, further solidifying its position as a transformative force in various industries.

D. 6G-ENABLED IoT

The 6G is essential to enabling future IoT networks and their applications. This is due to the features and emerging technologies of 6G that fulfill the IoT network requirements. In addition, 6G features could be promising solutions to IoT challenges and issues. For example, 6G is expected to provide tremendous coverage and enhanced adaptability, which could lead to support IoT connectivity and service delivery [81].

In addition, 6 G's multiband ultrafast-speed transmission feature allows the scalability of an IoT network in terms of connected IoT devices and transmitted data. IoT-connected devices are required to accomplish many tasks, such as collecting data by utilizing emerging technology in connectivity. This certainly demands energy. On the other hand, 6G is promises energy-efficient communication that can handle the

energy required by IoT devices. One of the most challenging aspects of the IoT is its security, secrecy, and privacy. The IoT allows devices in distant places to connect with the community frequently, so it is susceptible to all known security breaches. By adopting 6G security technologies such as blockchain, IoT networks can enrich their security, secrecy, and privacy.

1) THE IMPACT OF 6G ON THE FUTURE OF IoT

The integration of 6G technology with IoT presents a wide array of opportunities for innovation, connectivity, security, intelligence, immersive experiences, sustainability, and efficiency across industries and sectors. Embracing these opportunities can unlock new possibilities for digital transformation, economic growth, and societal advancement in the era of 6G Integrated IoT. Here are some key opportunities that can arise from the integration of 6G technology with IoT [81], [151]:

1) Massive IoT Connectivity: The 6G is likely to provide even faster and more reliable connectivity for IoT devices compared to 5G, potentially reaching up to 1 million devices per square kilometer. 6G IoT networks will support a wide range of connectivity options, including 5G, terrestrial, and satellite networks, to provide seamless connectivity across different environments, including urban, rural, remote areas, and even underwater communication technologies. This will allow for seamless integration of IoT technologies into everyday life, smart cities, industrial automation, and more.
2) Ultra-Reliable Low Latency Communication (URLLC): The 6G is expected to operate in terahertz frequencies, offering higher data rates, lower latency compared to 5G, and enhanced reliability in communication, which will be crucial for time-sensitive IoT applications such as autonomous vehicles, remote surgery, and real-time monitoring. This will enable more responsive and secure interactions between devices and systems.
3) Energy Efficiency and Sustainability: 6G could introduce more energy-efficient communication protocols and technologies, promoting sustainable practices in connectivity. This may involve optimizing power consumption, extending the battery life of IoT devices [152], leveraging renewable energy sources, developing eco-friendly IoT solutions to reduce environmental impact, and promoting sustainability. This could make it easier and more cost-effective to deploy IoT networks in remote or hard-to-reach locations.
4) Enhanced Security and Privacy: With the increasing number of connected devices and data exchanges in IoT ecosystems, 6G will place a greater emphasis on robust security and privacy measures. This may involve implementing advanced encryption techniques like quantum encryption and blockchain technology where Each IoT device will have a unique identity stored on the blockchain, ensuring secure communication and data exchange., and secure authentication mechanisms to protect IoT data and networks from cyber threats, ensuring a more secure IoT ecosystem [18].
5) Integration of AI and ML: The 6G is likely to incorporate advanced artificial intelligence (AI) and machine learning capabilities directly into IoT devices and networks. This will enable IoT systems to become more intelligent, adaptive, and autonomous, leading to enabling smarter decision-making, predictive analytics based on real-time data, and personalized services. With the integration of federated learning FL techniques, 6G IoT networks will be able to perform advanced data analytics while ensuring data privacy and security. This will enable more accurate insights and predictions from IoT data streams.
6) Immersive Experiences and Augmented Reality: The 6G Integrated IoT can enable immersive experiences through augmented reality (AR) and virtual reality (VR) applications in many sectors, such as gaming, entertainment, education, and healthcare. In addition, high-speed connectivity and low latency will support real-time rendering of AR/VR content, interactive experiences, and collaborative environments powered by IoT devices.
7) Sustainable and Smart Infrastructure: The 6G Integrated IoT can assist the development of sustainable and smart infrastructure solutions by optimizing resource utilization, energy efficiency, and environmental monitoring. In addition, IoT-enabled smart cities, buildings, transportation systems, and energy grids can benefit from 6G technology to create eco-friendly, interconnected ecosystems that enhance the quality of life and sustainability.

E. 6G-ENABLED FL-IoT

Moreover, the integration of IoT and machine learning plays a crucial role in the design of future wireless networks. It has permeated various network domains such as access, core, device, and edge, enabling the development of new smart applications. The combination of big data and deep learning further enhances automation, network management, and efficiency. While 5G primarily relies on radio frequency (RF) and millimeter wave bands, the limitations of these bands necessitate a shift to higher frequencies in 6G for the advancement of wireless networks. 6G, the next generation of wireless network systems, is being developed to support the technology era of smart devices and artificial intelligence models. It enables automation, digitization, and integration of heterogeneous networks. 6G surpasses conventional RF-based communications and encompasses various propagation media, including sonar waves. As the number of connected devices grows, 6G will cater more to machine-centric communication rather than human-centric communication. It will be characterized by virtualization, cloudification, intelligence, self-sustainability, and

software-driven features. Hence, security becomes essential, considering the increasing adoption of technologies like artificial intelligence and blockchain. The proliferation of ubiquitous devices and the associated data generation raise significant security concerns. With the capability to handle massive amounts of data, 6G elevates network performance by providing lower latency, enhanced privacy, more spectrum, increased data capacity, accurate localization, and better coverage. 6G plays a pivotal role in supporting massive IoT, facilitating connectivity among billions of devices across various environments such as oceans, skies, and earth.

F. BIBLIOMETRIC ANALYSIS OF RECENT WORKS APPLYING BLOCKCHAIN FOR FL-IoT IN 6G

This section is dedicated to presenting the researches that employ the four topics in their proposed model: IoT, FL-IoT, 6G, and blockchain. We used the Scopus dataset to search for ''IoT AND federated AND 6g AND blockchain'' in the title, abstract, and keywords. In addition, any research that has review or survey words in the title, abstract, or keywords is excluded. Furthermore, the search includes articles only which means conference papers, conference reviews, books, and review researches were excluded. The search query is TITLE-ABS-KEY (iot AND federated AND 6g AND blockchain AND NOT review AND NOT survey) AND (LIMIT-TO (DOCTYPE, ''ar'')). There was no limitation on the publication's year. Table 6 presents the researches of the executed query. As we noticed, only one of them is focusing on 5G instead of 6G [153].

In [154], a two-phased method was proposed for a dynamic gateway scheduling method based on multi-criteria for data transmission in blockchain and IoT-FL networks. Besides the LSTM approach employed to predict the forthcoming traffic on the links, statistical techniques are utilized to determine the optimal link. The 6G network standards are satisfied by the proposed method, which uses 6G features such as connectivity and uninterrupted services. The proposed method's efficiency is proven with respect to data transfer fairness and energy consumption by minimizing the queuing delays, maximizing the throughput, and maximizing the packet delivery rate and data transmission rate.

This study [155] presents a resource scheduling method by scanning resources, deadlines, delays, and costs associated with resources. The proposed scheme operates for various missions with preferences, such as blockchain and FL. This approach can handle the high latency and massive energy loss at local user devices caused by federated learning (FL). Their simulation results demonstrate that 45% running time and 53% cost gain are achieved compared with the baseline methods.

In [156], they proposed a blockchain-based hierarchical federated learning (HFL) framework for UAV-enabled IoT networks to handle data volume and privacy problems. They claimed that the traditional UAV transmission of data is not suitable for sensitive applications due to latency caused by non-IID data, which is collected by edge devices, and the trust threat caused by the FL decentralized global aggregation model. They integrated a lightweight blockchain with FL through an optimization scheme that integrates device association, wireless resource allocation, and UAV deployment cohesively to strike an equilibrium between learning latency and model accuracy. While local models are trained in devices and then form clusters based on data distance and communication channel quality, UAVs are in charge of edge and global aggregation, employing a lightweight blockchain consensus method to enhance global aggregation security. Their experiments' result outperforms state-of-the-art methods in terms of accuracy and learning utility.

A novel framework for dynamic authentication is proposed to facilitate User Equipment (UE) interaction with different base stations within the 6G wireless network in [157]. They use blockchain and federated learning to deliver Quality-of-Services and preserve privacy on 6G networks. At the distributed federated layer, user equipment (UE) is trained with a machine learning model to safeguard user privacy by masking sensitive data from service providers and masqueraders. This process aids in achieving convergence on a global model through local gradient updates. Their results in terms of average computation, aggregation and response time, and throughput are promising.

In Figure 13, the bibliometric analysis presents the author's keywords of the four researches in Table 6. The data was extracted from Scopus. Data was prepossessed for the author keywords extracted by Scopus to unify the keywords regarding the abbreviation.

As we see, the center keywords are blockchain, FL, and IoT. In the visualization map, items with more occurrences of keywords are shown more prominently than items with fewer occurrences. Therefore, blockchain and federated learning are the most common occurrences, followed by the Internet of Things (IoT) then 6G. This is because the 6G technology is the newest compared to others.

The links that connect two keywords represent that these keywords have been appearing in the same publication. The number of publications in which two keywords occur together increases the link strength. Four keywords have more than one occurrence in two or more publications, which are our search keywords.

In addition, there are three clusters, each represented by a different color. The clusters were generated by VOSviewer using the association strength method proposed in [158]. The clusters form based on the association strength between the keywords, calculated using the number of co-occurrence links between keywords. In addition, Figure 14 shows the keywords over the years.

The purpose of the analysis is to discover related topics and applications. For example, integrating FL with blockchain in IoT networks implies more tasks and burdens on IoT devices and 6G networks, which leads to high latency and energy consumption, affecting performance. These issues should be

TABLE 6. Recent works applying blockchain for FL-IoT in 6G.

Title	Pup. Year	Author Keywords	Aim	Target
Pandemic Management for Diseases Similar to COVID-19 Using Deep Learning and 5G Communications [153]	2021	Out of Scope		
Multi-criteria Approach for Handling Sophisticated Data Transmission over Gateways in Blockchain and Internet of Things (IoT) Federated Networks [154]	2022	blockchain; Internet of Things (IoT); IoT gateways (IGWs); sixth generation (6G) networks; solution specific gateways (SSGWs)	Enhance resource scheduling	Gateway
Merit: An on-demand IoT Service Delivery and Resource Scheduling Scheme for Federated Learning and Blockchain Empowered 6G Edge Networks with Reduced Time and Energy cost [155]	2023	BC; blockchain; energy loss; federated learning; FL; MEC; mobile edge computing; multi-task execution; resource scheduling; resource utilisation cost; saturation throughput; task running time; trust score; utility	Enhance resource scheduling	Running time
Blockchain-Based Trustworthy and Efficient Hierarchical Federated Learning for UAV-Enabled IoT Networks [156]	2024	Autonomous aerial vehicles; blockchain; Blockchains; Computational modeling; Data models; deep reinforcement learning; Federated learning; Hierarchical federated learning (HFL); Internet of Things; IoT; Training; UAV networks	Enhance latency and privacy	UAV
6G-DeFLI: Enhanced Quality-of-Services Using Distributed Hash Table and Blockchain-Enabled Federated Learning Approach in 6G IoT Networks [157]	2024	6G networks; Blockchain; Federated learning; Internet of Things; Quality of service	Enhance Quality-of-Services and preserve privacy	UE

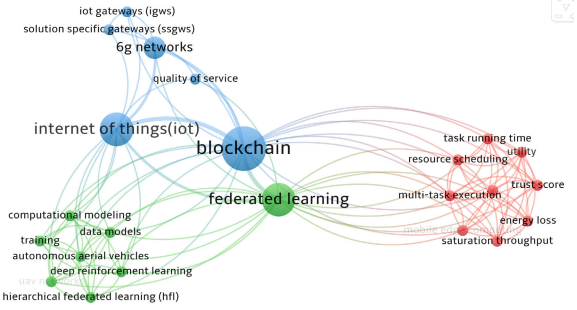

FIGURE 13. The network visualization bibliometric analysis of the author's keywords (co-occurrence) based on Table 6.

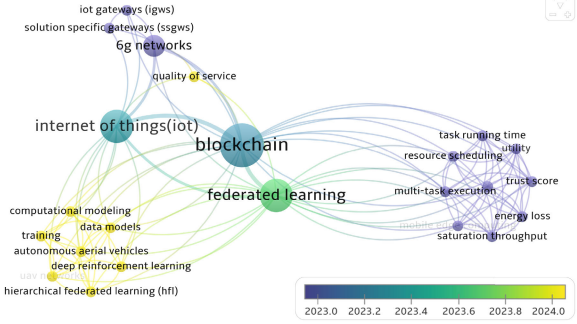

FIGURE 14. The bibliometric analysis of published years and the co-occurrence of the author's keywords based on Table 6.

handled using effective resource allocation algorithms as mentioned in [154], [155], and [156]. In addition, handling massive amounts of data to preserve privacy and transmission is critical. This problem could be solved using privacy techniques [156], [157].

As we see in Figure 13, the FL keyword is related more to training, Dl, HFL, and data modeling. On the other hand, 6G is related to gateways and IoT. Furthermore, we noticed from Figure 14 that quality-of-service, data modeling, and DL are some topics researchers commenced a discussion regarding the subject in 2024.

G. FUTURE OF APPLYING BLOCKCHAIN FOR MASSIVE FL-IoT IN 6G AND SOME OPEN ISSUES

We aim to inspire researchers and industry fields to develop applications for integrating blockchain, FL-IoT, and 6G, elevating the IoT to Massive IoT. Applications incorporating these technologies will benefit from their features and provide a wide range of services for their clients. Figure 15 presents an overview of blockchain FL-IoT integration over 6G networks. An infinite number of applications can apply the blockchain FL-IoT integration on 6G, including logistics, transportation, agriculture, education, manufacturing, shopping, healthcare, and homes.

The advent of 6G wireless networks promises to revolutionize the way we communicate, particularly in the realm of the Internet of Things (IoT). With its capability to support massive IoT deployments, 6G technology holds immense transformative potential. However, unlocking this potential requires overcoming various challenges, including data security and scalability concerns. In this regard, blockchain technology emerges as a highly promising solution.

This section delves into the motivations behind integrating blockchain with large-scale IoT and FL-IoT in the 6G era.

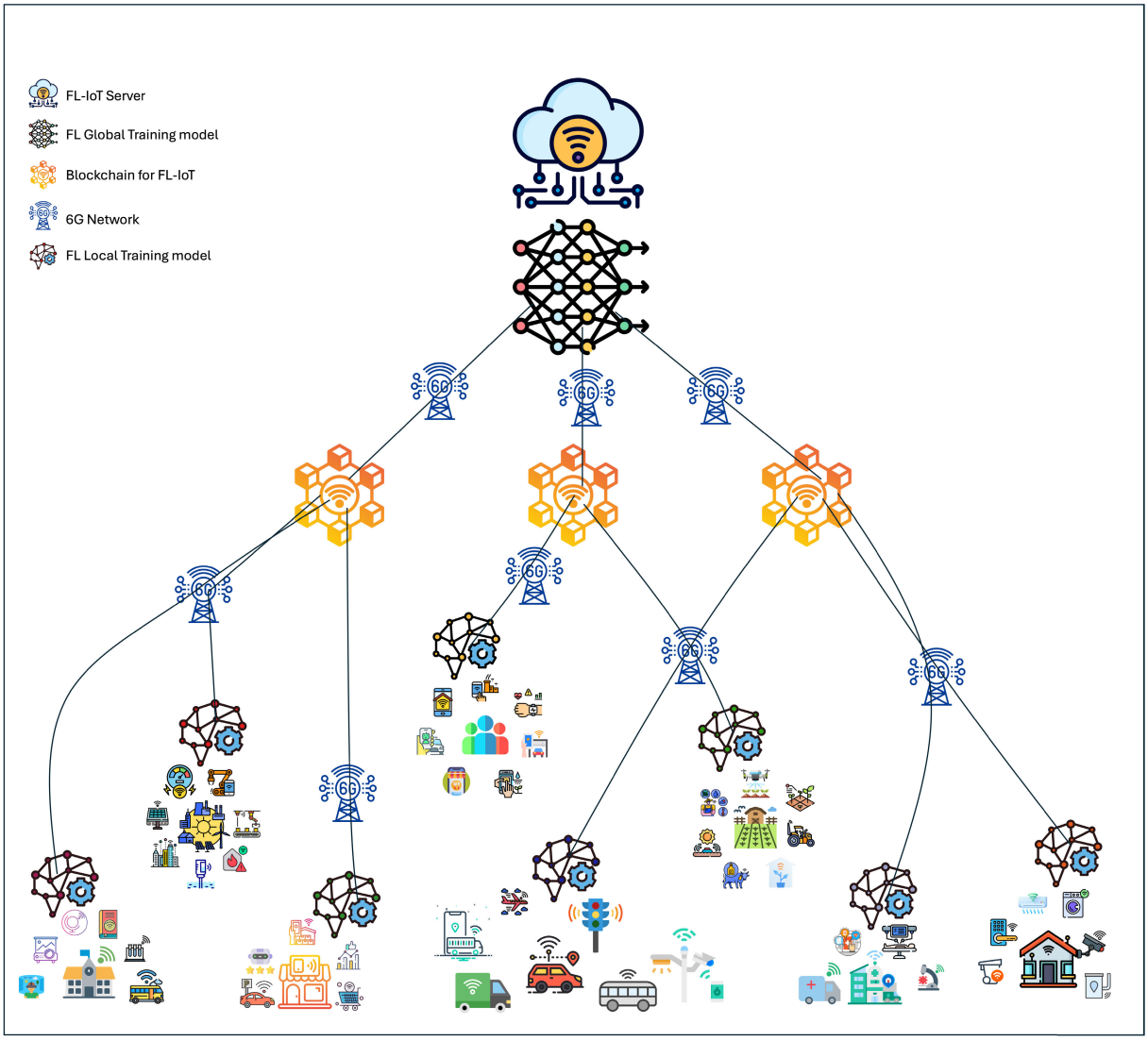

FIGURE 15. An overview of blockchain FL-IoT integration over 6G networks.

One key advantage lies in the decentralized architecture offered by blockchain, eliminating the need for a central authority and mitigating risks associated with single points of failure. Consequently, data security is significantly enhanced, ensuring the integrity and confidentiality of IoT data [132]. The decentralization of extensive IoT networks plays a pivotal role in empowering edge devices with greater autonomy, thereby enhancing the resilience and robustness of their operations. Moreover, the immutable and transparent nature of blockchain technology further bolsters the integrity and traceability of data. In an era where the number of IoT devices continues to surge, ensuring the authenticity of generated data remains of utmost significance [159]. By employing an immutable ledger, blockchain technology can effectively reduce the vulnerabilities associated with data tampering and cyber intrusions.

Another crucial objective is to enable secure and efficient data exchange among IoT devices. Through the implementation of blockchain-based smart contracts, processes can be automated, fostering trust among parties and facilitating seamless data sharing and collaboration [160]. Consequently, the integration of blockchain technology within the IoT ecosystem has the potential to introduce innovative business models and create new avenues for generating revenue. Additionally, the emergence of 6G networks will play a vital role in supporting the scalability of massive IoT. With enhanced data rates, ultra-low latency, improved network efficiency, and other advancements, 6G will enable seamless communication among billions of interconnected IoT devices [84]. Furthermore, the integration of cutting-edge technologies, such as artificial intelligence and machine learning, will lay the foundation for intelligent IoT networks that possess the ability to self-optimize, self-heal, and make autonomous decisions.

In addition, blockchain technology holds immense potential across various IoT applications. For instance, in supply

chain management, implementing blockchain ensures comprehensive visibility and traceability throughout the entire process, effectively mitigating the risks associated with counterfeiting, fraud, and theft [161]. Moreover, blockchain technology can be leveraged in smart city initiatives to bolster security, privacy, and efficiency across multiple sectors, such as energy management, transportation, and waste management. By implementing blockchain, smart cities can enhance data integrity, streamline processes, and promote seamless collaboration among stakeholders. This, in turn, leads to optimized resource allocation, improved sustainability, and a higher quality of life for residents [162].

Despite the potential of these applications, there are still several challenges that need to be addressed. One major concern is scalability, as conventional blockchain implementations may face difficulties in handling the high transaction throughput required by large-scale IoT networks [163]. Privacy represents another critical challenge in blockchain implementation. While the transparency of blockchain can be advantageous in various contexts, there is a risk of inadvertently exposing sensitive information. Striking the right balance between transparency and privacy is essential to ensure the secure and responsible use of blockchain technology [164]. Developing privacy-preserving techniques that do not compromise the fundamental principles of blockchain is crucial for promoting its adoption in IoT networks, especially those handling confidential data.

Unlike the traditional centralized radio access network (C-RAN) that lacks a robust authentication mechanism, blockchain-based architectures are considered secure and reliable in the industry. Blockchain technology is regarded as one of the supporting technologies in the post-5G era, offering a decentralized peer-to-peer network and wireless communication ecosystem. It operates as a decentralized and distributed ledger, where data is stored across multiple nodes. There is no central authority, and each node or block maintains a copy of the ledger. Blockchain ensures security through powerful cryptographic methods and offers key features such as transparency, non-repudiation, decentralization, immutability, and resilience to cyber attacks.

Therefore, blockchain holds potential solutions for 6G networks, such as ''intelligent resource management,'' and can enhance safety across various application sectors, including transparent environments, surveillance, protection, industrial applications, and healthcare.

VIII. CONCLUSION

In summary, this research article has delved into the convergence of blockchain technology and AI through the application of federated learning in the Massive IoT landscape, with a specific emphasis on advancing towards the realm of 6G technology. By combining the inherent security and transparency of blockchain with the remarkable speed and reliability of 6G, a plethora of unprecedented opportunities emerge. These opportunities encompass the exploration of decentralized applications, smart contracts, and secure transactions, paving the way for innovation and growth. The incorporation of blockchain technology in 6G networks promises a host of advantages. It serves as a catalyst for heightened security, empowering the creation of a decentralized and tamper-proof ledger that is profoundly resilient against various forms of threats. Moreover, it fosters privacy enhancements, ensuring that sensitive information is securely stored and selectively shared among authorized entities. Additionally, blockchain facilitates the efficient management of networks, streamlining communication processes and optimizing overall system performance. Trustworthy and reliable transactions within 6G communication systems can be achieved, guaranteeing the integrity and authenticity of data exchanges. Before the proposed solution can be seamlessly implemented, it is imperative to address pertinent challenges that lie ahead. These challenges encompass scalability, storage constraints, interoperability, security threats, and energy consumption. By methodically tackling these obstacles, we can lay a solid foundation for the successful integration of blockchain in 6G networks. The proposed solution not only addresses the aforementioned challenges but also unlocks the potential for the development of novel business models and the optimization of network performance. By capitalizing on the synergies between blockchain and 6G, we can foster a more connected and secure communication ecosystem, driving innovation and cultivating a thriving digital landscape.

In conclusion, the integration of blockchain technology and AI within the context of 6G technology ushers in a promising future. By diligently addressing challenges, optimizing performance, and harnessing the transformative potential of this amalgamation, we can forge a path toward enhanced security, improved privacy, and a more efficient and interconnected communication landscape.

ACKNOWLEDGMENT

The authors would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this paper.

REFERENCES

[1] S. Iyer, R. Jashvantbhai Pandya, R. Kallimani, K. Pai, R. Khanai, D. Torse, and S. Mavinkattimath, ''Survey on Internet of Things enabled by 6G wireless networks,'' 2022, *arXiv:2203.08426*.

[2] I. Rafiq, A. Mahmood, S. Razzaq, S. H. M. Jafri, and I. Aziz, ''IoT applications and challenges in smart cities and services,'' *J. Eng.*, vol. 2023, no. 4, Apr. 2023, Art. no. e12262.

[3] A. Li, M. Fujisawa, I. Urabe, R. Kitagawa, S.-J. Kim, and M. Hasegawa, ''A lightweight decentralized reinforcement learning based channel selection approach for high-density LoRaWAN,'' in *Proc. IEEE Int. Symp. Dyn. Spectr. Access Netw. (DySPAN)*, Dec. 2021, pp. 9–14.

[4] F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji, and V. C. M. Leung, ''Enabling massive IoT toward 6G: A comprehensive survey,'' *IEEE Internet Things J.*, vol. 8, no. 15, pp. 11891–11915, Aug. 2021.

[5] 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.

[6] S. Kumar, W. M. Lim, U. Sivarajah, and J. Kaur, ''Artificial intelligence and blockchain integration in business: Trends from a bibliometric-content analysis,'' *Inf. Syst. Frontiers*, vol. 25, no. 2, pp. 871–896, Apr. 2022.

[7] M. Vaezi, A. Azari, S. R. Khosravirad, M. Shirvanimoghaddam, M. M. Azari, D. Chasaki, and P. Popovski, "Cellular, wide-area, and non-terrestrial IoT: A survey on 5G advances and the road toward 6G," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 1117–1174, 2nd Quart., 2022.

[8] M. Mnyakin, "Applications of AI, IoT, and cloud computing in smart transportation: A review," *Artif. Intell. Soc.*, vol. 3, no. 1, pp. 9–27, 2023.

[9] H. G. Abreha, M. Hayajneh, and M. A. Serhani, "Federated learning in edge computing: A systematic survey," *Sensors*, vol. 22, no. 2, p. 450, Jan. 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/2/450

[10] Z. Chen, H. Cui, E. Wu, and X. Yu, "Dynamic asynchronous anti poisoning federated deep learning with blockchain-based reputation-aware solutions," *Sensors*, vol. 22, no. 2, p. 684, Jan. 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/2/684

[11] A. Afaq, Z. Ahmed, N. Haider, and M. Imran, "Blockchain-based collaborated federated learning for improved security, privacy and reliability," 2022, *arXiv:2201.08551*.

[12] A. Jahid, M. H. Alsharif, and T. J. Hall, "The convergence of blockchain, IoT and 6G: Potential, opportunities, challenges and research roadmap," *J. Netw. Comput. Appl.*, vol. 217, Aug. 2023, Art. no. 103677. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804523000966

[13] S. A. A. Hakeem, H. H. Hussein, and H. Kim, "Security requirements and challenges of 6G technologies and applications," *Sensors*, vol. 22, no. 5, p. 1969, Mar. 2022.

[14] Y. Zuo, J. Guo, N. Gao, Y. Zhu, S. Jin, and X. Li, "A survey of blockchain and artificial intelligence for 6G wireless communications," 2023, *arXiv:2305.08604*.

[15] A. Alkandari and M. A. AlAhmad, "Overview on 5G and 6G wireless communication with IoT technology," *J. Eng. Sci. Technol.*, vol. 17, no. 1, pp. 95–105, 2022.

[16] A. Attkan and V. Ranga, "Cyber-physical security for IoT networks: A comprehensive review on traditional, blockchain and artificial intelligence based key-security," *Complex Intell. Syst.*, vol. 8, no. 4, pp. 3559–3591, Aug. 2022.

[17] H. H. Pajooh, S. Demidenko, S. Aslam, and M. Harris, "Blockchain and 6G-enabled IoT," *Inventions*, vol. 7, no. 4, p. 109, Nov. 2022. [Online]. Available: https://www.mdpi.com/2411-5134/7/4/109

[18] K. M. B. Hasan, M. Sajid, M. A. Lapina, M. Shahid, and K. Kotecha, "Blockchain technology meets 6G wireless networks: A systematic survey," *Alexandria Eng. J.*, vol. 92, pp. 199–220, Apr. 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1110016824001704

[19] S. H. A. Kazmi, F. Qamar, R. Hassan, K. Nisar, and M. A. Al-Betar, "Security of federated learning in 6G era: A review on conceptual techniques and software platforms used for research and analysis," *Comput. Netw.*, vol. 245, May 2024, Art. no. 110358. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128624001907

[20] W. V. Solis, J. M. Parra-Ullauri, and A. Kertesz, "Exploring the synergy of fog computing, blockchain, and federated learning for IoT applications: A systematic literature review," *IEEE Access*, vol. 12, pp. 68015–68060, 2024.

[21] J. M. Parra-Ullauri, X. Zhang, A. Bravalheri, S. Moazzeni, Y. Wu, R. Nejabati, and D. Simeonidou, "Federated analytics for 6G networks: Applications, challenges, and opportunities," *IEEE Netw.*, vol. 38, no. 2, pp. 9–17, Mar. 2024.

[22] M. K. Hasan, N. Jahan, M. Z. A. Nazri, S. Islam, M. A. Khan, A. I. Alzahrani, N. Alalwan, and Y. Nam, "Federated learning for computational offloading and resource management of vehicular edge computing in 6G-V2X network," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 3827–3847, Feb. 2024.

[23] M. Sheraz, T. C. Chuah, Y. L. Lee, M. M. Alam, A. Al-Habashna, and Z. Han, "A comprehensive survey on revolutionizing connectivity through artificial intelligence-enabled digital twin network in 6G," *IEEE Access*, vol. 12, pp. 49184–49215, 2024.

[24] M. A. Elaziz, M. A. A. Al-Qaness, A. Dahou, S. H. Alsamhi, L. Abualigah, R. A. Ibrahim, and A. A. Ewees, "Evolution toward intelligent communications: Impact of deep learning applications on the future of 6G technology," *WIREs Data Mining Knowl. Discovery*, vol. 14, no. 1, Jan. 2024, Art. no. e1521.

[25] A. Alhammadi, I. Shayea, A. A. El-Saleh, M. H. Azmi, Z. H. Ismail, L. Kouhalvandi, and S. A. Saad, "Artificial intelligence in 6G wireless networks: Opportunities, applications, and challenges," *Int. J. Intell. Syst.*, vol. 2024, pp. 1–27, Mar. 2024.

[26] R. Chataut, M. Nankya, and R. Akl, "6G networks and the AI revolution—Exploring technologies, applications, and emerging challenges," *Sensors*, vol. 24, no. 6, p. 1888, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/6/1888

[27] T. Nguyen, H. Nguyen, and T. Nguyen Gia, "Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications," *J. Netw. Comput. Appl.*, vol. 226, Jun. 2024, Art. no. 103884. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804524000614

[28] P. Scalise, M. Boeding, M. Hempel, H. Sharif, J. Delloiacovo, and J. Reed, "A systematic survey on 5G and 6G security considerations, challenges, trends, and research areas," *Future Internet*, vol. 16, no. 3, p. 67, Feb. 2024. [Online]. Available: https://www.mdpi.com/1999-5903/16/3/67

[29] M. Aggarwal, V. Khullar, S. Rani, T. A. Prola, S. B. Bhattacharjee, S. M. Shawon, and N. Goyal, "Federated learning on Internet of Things: Extensive and systematic review," *Comput., Mater. Continua*, vol. 79, no. 2, pp. 1795–1834, 2024. [Online]. Available: http://www.techscience.com/cmc/v79n2/56449

[30] S. Wang, M. A. Qureshi, L. Miralles-Pechuán, T. Huynh-The, T. R. Gadekallu, and M. Liyanage, "Explainable AI for 6G use cases: Technical aspects and research challenges," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 2490–2540, 2024.

[31] J. Liu, C. Chen, Y. Li, L. Sun, Y. Song, J. Zhou, B. Jing, and D. Dou, "Enhancing trust and privacy in distributed networks: A comprehensive survey on blockchain-based federated learning," *Knowl. Inf. Syst.*, vol. 66, no. 8, pp. 4377–4403, Aug. 2024.

[32] L. A. C. Ahakonye, C. I. Nwakanma, and D.-S. Kim, "Tides of blockchain in IoT cybersecurity," *Sensors*, vol. 24, no. 10, p. 3111, May 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/10/3111

[33] A. Hakiri, A. Gokhale, S. B. Yahia, and N. Mellouli, "A comprehensive survey on digital twin for future networks and emerging Internet of Things industry," *Comput. Netw.*, vol. 244, May 2024, Art. no. 110350. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128624001828

[34] J. Lee, F. Solat, T. Y. Kim, and H. V. Poor, "Federated learning-empowered mobile network management for 5G and beyond networks: From access to core," *IEEE Commun. Surveys Tuts.*, early access, Jan. 16, 2024, doi: 10.1109/COMST.2024.3352910.

[35] S. Zhang, D. Zhu, and Y. Liu, "Artificial intelligence empowered physical layer security for 6G: State-of-the-art, challenges, and opportunities," *Comput. Netw.*, vol. 242, Apr. 2024, Art. no. 110255. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128624000872

[36] J. Naulegari, S. Reddy, G. S. Babu, and L. Abualigah, "Machine learning approach to fix routing problems in IoT networks," 2024.

[37] S. K. Pattnaik, S. R. Samal, S. Bandopadhaya, K. Swain, S. Choudhury, J. K. Das, A. Mihovska, and V. Poulkov, "Future wireless communication technology towards 6G IoT: An application-based analysis of IoT in real-time location monitoring of employees inside underground mines by using BLE," *Sensors*, vol. 22, no. 9, p. 3438, Apr. 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/9/3438

[38] A. R. Anorboyevich, "Exploring the evolutionary path: A historical analysis of Internet of Things (IoT) technologies,". Toronto, ON, Canada: Global Book Publishing, 2024, pp. 1–70.

[39] M. Ahmid, O. Kazar, and E. Barka, "Internet of Things overview: Architecture, technologies, application, and challenges," in *Decision Making and Security Risk Management for IoT Environments*. USA: Springer, 2024, pp. 1–19.

[40] J. Héctor, *Understanding Nanoelectromechanical Quantum Circuits and Systems (NEMX) for the Internet of Things (IoT) Era*. Aalborg, Denmark: River Publishers, 2022.

[41] R. Mehta, J. Sahni, and K. Khanna, "Internet of Things: Vision, applications and challenges," *Proc. Comput. Sci.*, vol. 132, pp. 1263–1269, Jan. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050918307749

[42] M. Mahbub, "An overview of IoT infrastructure architecture, enabling technologies, issues, integration of cloud, and simulation tools," in *Proc. Emerging Trends in IoT and Integration with Data Science, Cloud Computing, and Big Data Analytics*. Hershey, PA, USA: IGI Global, 2022, pp. 20–38.

[43] L. Atzori, A. Iera, and G. Morabito, "Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm," *Ad Hoc Netw.*, vol. 56, pp. 122–140, Mar. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870516303316

[44] M. Ahmid and O. Kazar, "A comprehensive review of the Internet of Things security," *J. Appl. Secur. Res.*, vol. 18, no. 3, pp. 289–305, Jul. 2023, doi: 10.1080/19361610.2021.1962677.

[45] C. Bayılmış, M. A. Ebleme, Ü. Çavuşoğlu, K. Küçük, and A. Sevin, "A survey on communication protocols and performance evaluations for Internet of Things," *Digit. Commun. Netw.*, vol. 8, no. 6, pp. 1094–1104, Dec. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864822000347

[46] D. Sun, J. Hu, H. Wu, J. Wu, J. Yang, Q. Z. Sheng, and S. Dustdar, "A comprehensive survey on collaborative data-access enablers in the IIoT," *ACM Comput. Surv.*, vol. 56, no. 2, pp. 1–37, Sep. 2023, doi: 10.1145/3612918.

[47] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," in *Proc. Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)*, Feb. 2017, pp. 492–496.

[48] S.-L. Peng, S. Pal, and L. Huang, *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*. USA: Springer, 2020.

[49] M. Lombardi, F. Pascale, and D. Santaniello, "Internet of Things: A general overview between architectures, protocols and applications," *Information*, vol. 12, no. 2, p. 87, Feb. 2021. [Online]. Available: https://www.mdpi.com/2078-2489/12/2/87

[50] Q. Alfalouji, T. Schranz, A. Kümpel, M. Schraven, T. Storek, S. Gross, A. Monti, D. Müller, and G. Schweiger, "IoT middleware platforms for smart energy systems: An empirical expert survey," *Buildings*, vol. 12, no. 5, p. 526, Apr. 2022. [Online]. Available: https://www.mdpi.com/2075-5309/12/5/526

[51] F. J. Ferrández-Pastor, J. M. García-Chamizo, M. Nieto-Hidalgo, and J. Mora-Martínez, "Precision agriculture design method using a distributed computing architecture on Internet of Things context," *Sensors*, vol. 18, no. 6, p. 1731, May 2018. [Online]. Available: https://www.mdpi.com/1424-8220/18/6/1731

[52] J. A. Scheibmeir and Y. K. Malaiya, "Social media analytics of the Internet of Things," *Discover Internet Things*, vol. 1, no. 1, p. 16, Dec. 2021.

[53] J. Mohanty, S. Mishra, S. Patra, B. Pati, and C. R. Panigrahi, "IoT security, challenges, and solutions: A review," in *Proc. ICACIE*, vol. 2, 2019, pp. 493–504.

[54] M. Kokila and K. S. Reddy, "Authentication, access control and scalability models in Internet of Things security—A review," *Cyber Secur. Appl.*, vol. 3, Dec. 2025, Art. no. 100057. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2772918424000237

[55] P. Y. Dibal, E. N. Onwuka, S. Zubair, E. I. Nwankwo, S. A. Okoh, B. A. Salihu, and H. B. Mustaphab, "Processor power and energy consumption estimation techniques in IoT applications: A review," *Internet Things*, vol. 21, Apr. 2023, Art. no. 100655. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660522001366

[56] S. Pasricha, R. Ayoub, M. Kishinevsky, S. K. Mandal, and U. Y. Ogras, "A survey on energy management for mobile and IoT devices," *IEEE Design Test.*, vol. 37, no. 5, pp. 7–24, Oct. 2020.

[57] J. Ding, M. Nemati, C. Ranaweera, and J. Choi, "IoT connectivity technologies and applications: A survey," *IEEE Access*, vol. 8, pp. 67646–67673, 2020.

[58] Q. Li, Z. Wen, Z. Wu, S. Hu, N. Wang, Y. Li, X. Liu, and B. He, "A survey on federated learning systems: Vision, hype and reality for data privacy and protection," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 4, pp. 3347–3366, Apr. 2023.

[59] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, Jan. 2019, doi: 10.1145/3298981.

[60] L. Zhang, J. Xu, P. Vijayakumar, P. K. Sharma, and U. Ghosh, "Homomorphic encryption-based privacy-preserving federated learning in IoT-enabled healthcare system," *IEEE Trans. Netw. Sci. Eng.*, vo. 10, no. 5, pp. 2864–2880, Sep./Oct. 2022.

[61] 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, May 2022.

[62] 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.

[63] S. Abdulrahman, H. Tout, A. Mourad, and C. Talhi, "FedMCCS: Multicriteria client selection model for optimal IoT federated learning," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4723–4735, Mar. 2021.

[64] 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.

[65] D. Unal, M. Hammoudeh, M. A. Khan, A. Abuarqoub, G. Epiphaniou, and R. Hamila, "Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things," *Comput. Secur.*, vol. 109, Oct. 2021, Art. no. 102393. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821002170

[66] V.-D. Nguyen, S. K. Sharma, T. X. Vu, S. Chatzinotas, and B. Ottersten, "Efficient federated learning algorithm for resource allocation in wireless IoT networks," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3394–3409, Mar. 2021.

[67] W. Yang, W. Xiang, Y. Yang, and P. Cheng, "Optimizing federated learning with deep reinforcement learning for digital twin empowered industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 1884–1893, Feb. 2023.

[68] H. Chen, S. Huang, D. Zhang, M. Xiao, M. Skoglund, and H. V. Poor, "Federated learning over wireless IoT networks with optimized communication and resources," *IEEE Internet Things J.*, vol. 9, no. 17, pp. 16592–16605, Sep. 2022.

[69] S. Wu, H. Xue, and L. Zhang, "Q-learning-aided offloading strategy in edge-assisted federated learning over industrial IoT," *Electronics*, vol. 12, no. 7, p. 1706, Apr. 2023. [Online]. Available: https://www.mdpi.com/2079-9292/12/7/1706

[70] X. Fu, R. Peng, W. Yuan, T. Ding, Z. Zhang, P. Yu, and M. Kadoch, "Federated learning-based resource management with blockchain trust assurance in smart IoT," *Electronics*, vol. 12, no. 4, p. 1034, Feb. 2023. [Online]. Available: https://www.mdpi.com/2079-9292/12/4/1034

[71] M. A. P. Putra, A. R. Putri, A. Zainudin, D.-S. Kim, and J.-M. Lee, "ACS: Accuracy-based client selection mechanism for federated industrial IoT," *Internet Things*, vol. 21, Apr. 2023, Art. no. 100657. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S254266052200138X

[72] D. Chai, L. Wang, L. Yang, J. Zhang, K. Chen, and Q. Yang, "A survey for federated learning evaluations: Goals and measures," *IEEE Trans. Knowl. Data Eng.*, early access, Mar. 27, 2024, doi: 10.1109/TKDE.2024.3382002.

[73] S. K. Grewal and G. Kaur, "Aggregation techniques in wireless communication using federated learning: A survey," *Int. J. Wireless Mobile Comput.*, vol. 26, no. 2, pp. 115–126, 2024.

[74] S. S. Khalil, N. S. Tawfik, and M. Spruit, "Exploring the potential of federated learning in mental health research: A systematic literature review," *Appl. Intell.*, vol. 54, no. 2, pp. 1619–1636, Jan. 2024.

[75] M. Ali, H. Karimipour, and M. Tariq, "Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges," *Comput. Secur.*, vol. 108, Sep. 2021, Art. no. 102355. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821001796

[76] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future," *IEEE Access*, vol. 7, pp. 46317–46350, 2019.

[77] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G networks: Use cases and technologies," *IEEE Commun. Mag.*, vol. 58, no. 3, pp. 55–61, Mar. 2020.

[78] S. Mumtaz, J. M. Jornet, J. Aulin, W. H. Gerstacker, X. Dong, and B. Ai, "Terahertz communication for vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 5617–5625, Jul. 2017.

[79] A. Yastrebova, R. Kirichek, Y. Koucheryavy, A. Borodin, and A. Koucheryavy, "Future networks 2030: Architecture & requirements," in *Proc. 10th Int. Congr. Ultra Modern Telecommun. Control Syst. Workshops (ICUMT)*, Nov. 2018, pp. 1–8.

[80] B. Zong, C. Fan, X. Wang, X. Duan, B. Wang, and J. Wang, "6G technologies: Key drivers, core requirements, system architectures, and enabling technologies," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 18–27, Sep. 2019.

[81] Z. Qadir, K. N. Le, N. Saeed, and H. S. Munawar, "Towards 6G Internet of Things: Recent advances, use cases, and open challenges," *ICT Exp.*, vol. 9, no. 3, pp. 296–312, Jun. 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959522000959

[82] E. Calvanese Strinati, S. Barbarossa, J. L. Gonzalez-Jimenez, D. Ktenas, N. Cassiau, L. Maret, and C. Dehos, "6G: The next frontier: From holographic messaging to artificial intelligence using subterahertz and visible light communication," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 42–50, Sep. 2019.

[83] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6G wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 28–41, Sep. 2019.

[84] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May 2020.

[85] B. Li, Z. Fei, and Y. Zhang, "UAV communications for 5G and beyond: Recent advances and future trends," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2241–2263, Apr. 2019.

[86] F. Tariq, M. R. A. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A speculative study on 6G," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 118–125, Aug. 2020.

[87] *White Paper 5G Evolution and 6G*, NTT DOCOMO, Tokyo, Japan, Jan. 2020.

[88] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y. A. Zhang, "The roadmap to 6G: AI empowered wireless networks," *IEEE Commun. Mag.*, vol. 57, no. 8, pp. 84–90, Aug. 2019.

[89] H. Zhang, M. Feng, K. Long, G. K. Karagiannidis, and A. Nallanathan, "Artificial intelligence-based resource allocation in ultradense networks: Applying event-triggered Q-learning algorithms," *IEEE Veh. Technol. Mag.*, vol. 14, no. 4, pp. 56–63, Dec. 2019.

[90] A. S. M. Z. Shifat, M. Z. Chowdhury, and Y. M. Jang, "Game-based approach for QoS provisioning and interference management in heterogeneous networks," *IEEE Access*, vol. 6, pp. 10208–10220, 2018.

[91] M. Z. Chowdhury, Md. T. Hossan, and Y. M. Jang, "Interference management based on RT/nRT traffic classification for FFR-aided small cell/macrocell heterogeneous networks," *IEEE Access*, vol. 6, pp. 31340–31358, 2018.

[92] A. J. Mahbas, H. Zhu, and J. Wang, "Impact of small cells overlapping on mobility management," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 1054–1068, Feb. 2019.

[93] S. Andreev, V. Petrov, M. Dohler, and H. Yanikomeroglu, "Future of ultra-dense networks beyond 5G: Harnessing heterogeneous moving cells," *IEEE Commun. Mag.*, vol. 57, no. 6, pp. 86–92, Jun. 2019.

[94] M. Katz, M. Matinmikko-Blue, and M. Latva-Aho, "6Genesis flagship program: Building the bridges towards 6G-enabled wireless smart society and ecosystem," in *Proc. IEEE 10th Latin-Amer. Conf. Commun. (LATINCOM)*, Nov. 2018, pp. 1–9.

[95] H. Hafi, B. Brik, P. A. Frangoudis, A. Ksentini, and M. Bagaa, "Split federated learning for 6G enabled-networks: Requirements, challenges, and future directions," *IEEE Access*, vol. 12, pp. 9890–9930, 2024.

[96] A. Farhad and J.-Y. Pyun, "Terahertz meets AI: The state of the art," *Sensors*, vol. 23, no. 11, p. 5034, May 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/11/5034

[97] W. Jiang, Q. Zhou, J. He, M. A. Habibi, S. Melnyk, M. El-Absi, B. Han, M. D. Renzo, H. D. Schotten, F.-L. Luo, T. S. El-Bawab, M. Juntti, M. Debbah, and V. C. M. Leung, "Terahertz communications and sensing for 6G and beyond: A comprehensive review," *IEEE Commun. Surveys Tuts.*, 2024.

[98] T. Aslam, I. Ahmed, S. Ali, and M. I. Aslam, "TeraHertz communication and associated challenges in 6G cellular networks," in *Proc. 4th Int. Conf. Comput. Inf. Sci. (ICCIS)*, Nov. 2021, pp. 1–6.

[99] R. Chataut and R. Akl, "Massive MIMO systems for 5G and beyond networks—Overview, recent trends, challenges, and future research direction," *Sensors*, vol. 20, no. 10, p. 2753, May 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/10/2753

[100] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 957–975, 2020.

[101] M. M. Khan, S. Hossain, P. Mozumdar, S. Akter, and R. H. Ashique, "A review on machine learning and deep learning for various antenna design applications," *Heliyon*, vol. 8, no. 4, Apr. 2022, Art. no. e09317. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405844022006053

[102] B. Ning, Z. Tian, W. Mei, Z. Chen, C. Han, S. Li, J. Yuan, and R. Zhang, "Beamforming technologies for ultra-massive MIMO in terahertz communications," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 614–658, 2023.

[103] J. Pérez Santacruz, E. Meyer, R. X. F. Budé, C. Stan, A. Jurado-Navas, U. Johannsen, I. Tafur Monroy, and S. Rommel, "Outdoor mm-wave 5G/6G transmission with adaptive analog beamforming and IFoF fronthaul," *Sci. Rep.*, vol. 13, no. 1, p. 13945, Aug. 2023.

[104] N. A. Alhaj, M. F. Jamlos, S. A. Manap, S. Abdelsalam, A. A. Bakhit, R. Mamat, M. A. Jamlos, M. S. M. Gismalla, and M. Hamdan, "Integration of hybrid networks, AI, ultra massive-MIMO, THz frequency, and FBMC modulation toward 6G requirements: A review," *IEEE Access*, vol. 12, pp. 483–513, 2024.

[105] P. S. R. Henrique and R. Prasad, "6G networks orientation by quantum mechanics," *J. ICT Standardization*, vol. 10, no. 1, pp. 39–62, Feb. 2022.

[106] Y. Lu, H. Jiang, and L. Dai, "Artificial intelligence for RIS-aided wireless communications," *ITU J. Future Evolving Technol.*, vol. 4, no. 1, pp. 70–77, 2023.

[107] T. Sharma, A. Chehri, and P. Fortier, "Reconfigurable intelligent surfaces for 5G and beyond wireless communications: A comprehensive survey," *Energies*, vol. 14, no. 24, p. 8219, Dec. 2021. [Online]. Available: https://www.mdpi.com/1996-1073/14/24/8219

[108] R. Shrestha, R. Bajracharya, and S. Kim, "6G enabled unmanned aerial vehicle traffic management: A perspective," *IEEE Access*, vol. 9, pp. 91119–91136, 2021.

[109] S. Kukliński, K. Szczypiorski, and P. Chemouil, "UAV support for mission critical services," *Energies*, vol. 15, no. 15, p. 5681, Aug. 2022. [Online]. Available: https://www.mdpi.com/1996-1073/15/15/5681

[110] S. Yin, S. Zhao, Y. Zhao, and F. R. Yu, "Intelligent trajectory design in UAV-aided communications with reinforcement learning," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 8227–8231, Aug. 2019.

[111] A. Alotaibi and A. Barnawi, "Securing massive IoT in 6G: Recent solutions, architectures, future directions," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100715. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660523000380

[112] M. A. Haque, S. Ahmad, A. J. Abboud, M. A. Hossain, K. Kumar, S. Haque, D. Sonal, M. Rahman, and S. Marisennayya, "6G wireless communication networks: Challenges and potential solution," *Int. J. Bus. Data Commun. Netw.*, vol. 19, no. 1, pp. 1–27, 2024.

[113] Z. Wenhua, F. Qamar, T.-A.-N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, "Blockchain technology: Security issues, healthcare applications, challenges and future trends," *Electronics*, vol. 12, no. 3, p. 546, Jan. 2023. [Online]. Available: https://www.mdpi.com/2079-9292/12/3/546

[114] H. Xiong, M. Chen, C. Wu, Y. Zhao, and W. Yi, "Research on progress of blockchain consensus algorithm: A review on recent progress of blockchain consensus algorithms," *Future Internet*, vol. 14, no. 2, p. 47, Jan. 2022. [Online]. Available: https://www.mdpi.com/1999-5903/14/2/47

[115] J. Zarrin, H. W. Phang, L. B. Saheer, and B. Zarrin, "Blockchain for decentralization of internet: Prospects, trends, and challenges," *Cluster Comput.*, vol. 24, no. 4, pp. 2841–2866, Dec. 2021.

[116] H. Hassani, K. Norouzi, A. Ghodsi, and X. Huang, "Revolutionary dentistry through blockchain technology," *Big Data Cogn. Comput.*, vol. 7, no. 1, p. 9, Jan. 2023. [Online]. Available: https://www.mdpi.com/2504-2289/7/1/9

[117] I. S. Bayrakdar, Y. Yasa, S. B. Duman, and K. Orhan, "What can blockchain technology bring to oral and maxillofacial radiology?" *Oral Surgery, Oral Med., Oral Pathol. Oral Radiol.*, vol. 130, no. 2, pp. 225–226, Aug. 2020.

[118] I. Priyadarshini, "Introduction to blockchain technology," in *Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies*. Hoboken, NJ, USA: Wiley, 2019, pp. 91–107.

[119] S. Tracey and K. Ruamsook, "Blockchain fundamentals and enterprise applications," Center Supply Chain Res., Pennsylvania State Univ., University Park, PA, USA, White Paper, 2021.

[120] S. K. Dewangan, A. Pathak, V. Raheja, H. Shende, C. Verma, and S. Jain, "A comprehensive study on blockchain technology," *Math. Statistician Eng. Appl.*, vol. 72, no. 1, pp. 462–469, 2023. [Online]. Available: https://www.philstat.org/index.php/MSEA/article/view/1899

[121] F. Zantalis, G. Koulouras, and S. Karabetsos, "Blockchain technology: A framework for endless applications," *IEEE Consum. Electron. Mag.*, vol. 13, no. 2, pp. 61–71, Mar. 2024.

[122] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, "A blockchain based truthful incentive mechanism for distributed P2P applications," *IEEE Access*, vol. 6, pp. 27324–27335, 2018.

[123] M. I. Talukdar, R. Hassan, M. S. Hossen, K. Ahmad, F. Qamar, and A. S. Ahmed, "Performance improvements of AODV by black hole attack detection using IDS and digital signature," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–13, Mar. 2021.

[124] W. Deng, H. Wei, T. Huang, C. Cao, Y. Peng, and X. Hu, "Smart contract vulnerability detection based on deep learning and multimodal decision fusion," *Sensors*, vol. 23, no. 16, p. 7246, Aug. 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/16/7246

[125] H. Taherdoost, "Smart contracts in blockchain technology: A critical review," *Information*, vol. 14, no. 2, p. 117, Feb. 2023. [Online]. Available: https://www.mdpi.com/2078-2489/14/2/117

[126] D. B. Rawat, "Fusion of software defined networking, edge computing, and blockchain technology for wireless network virtualization," *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 50–55, Oct. 2019.

[127] S. Yrjölä, "How could blockchain transform 6G towards open ecosystemic business models?" in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2020, pp. 1–6.

[128] G. Hileman and M. Rauchs, "2017 global cryptocurrency benchmarking study," SSRN, 2017.

[129] B. Carson, G. Romanelli, P. Walsh, and A. Zhumaev, "Blockchain beyond the hype: What is the strategic business value," McKinsey & Company, New York, NY, USA, Tech. Rep., 2018, vol. 1, pp. 1–13.

[130] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, "A survey on blockchain technology: Evolution, architecture and security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021.

[131] S. M. A. Ali, M. N. Yusoff, and H. F. Hasan, "Redactable blockchain: Comprehensive review, mechanisms, challenges, open issues and future research directions," *Future Internet*, vol. 15, no. 1, p. 35, Jan. 2023. [Online]. Available: https://www.mdpi.com/1999-5903/15/1/35

[132] S. Mathur, A. Kalla, G. Gür, M. K. Bohra, and M. Liyanage, "A survey on role of blockchain for IoT: Applications and technical aspects," *Comput. Netw.*, vol. 227, May 2023, Art. no. 109726. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128623001718

[133] H. Wang, Y. Wang, T. Taleb, and X. Jiang, "Special issue on security and privacy in network computing," *World Wide Web*, vol. 23, pp. 951–957, Jul. 2020.

[134] T. Alam, "Blockchain and its role in the Internet of Things (IoT)," *Int. J. Sci. Res. Comput. Sci., Eng. Inf. Technol.*, vol. 1, no. 5, pp. 151–157, Jan. 2019.

[135] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019.

[136] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 101–128, 2018.

[137] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 107, pp. 841–853, Jun. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X17318332

[138] M. Antal, V. Mihailescu, T. Cioara, and I. Anghel, "Blockchain-based distributed federated learning in smart grid," *Mathematics*, vol. 10, no. 23, p. 4499, Nov. 2022. [Online]. Available: https://www.mdpi.com/2227-7390/10/23/4499

[139] 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. [Online]. Available: https://www.mdpi.com/1999-5903/15/12/400

[140] N. Rieke, J. Hancox, W. Li, F. Milletari, H. R. Roth, S. Albarqouni, S. Bakas, M. N. Galtier, B. A. Landman, K. Maier-Hein, S. Ourselin, M. Sheller, R. M. Summers, A. Trask, D. Xu, M. Baust, and M. J. Cardoso, "The future of digital health with federated learning," *NPJ Digit. Med.*, vol. 3, no. 1, p. 119, 2020.

[141] X. Wang, H. Zhang, H. Wu, and H. Yu, "Dual-blockchain based multi-layer grouping federated learning scheme for heterogeneous data in industrial IoT," *Blockchain, Res. Appl.*, Feb. 2024, Art. no. 100195. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2096720924000083

[142] Y. Qu, M. P. Uddin, C. Gan, Y. Xiang, L. Gao, and J. Yearwood, "Blockchain-enabled federated learning: A survey," *ACM Comput. Surv.*, vol. 55, no. 4, pp. 1–35, Nov. 2022, doi: 10.1145/3524104.

[143] A. Qammar, A. Karim, H. Ning, and J. Ding, "Securing federated learning with blockchain: A systematic literature review," *Artif. Intell. Rev.*, vol. 56, no. 5, pp. 3951–3985, May 2023.

[144] M. Z. Asghar, S. A. Memon, and J. Hämäläinen, "Evolution of wireless communication to 6G: Potential applications and research directions," *Sustainability*, vol. 14, no. 10, p. 6356, May 2022. [Online]. Available: https://www.mdpi.com/2071-1050/14/10/6356

[145] A. Kalla, C. de Alwis, P. Porambage, G. Gür, and M. Liyanage, "A survey on the use of blockchain for future 6G: Technical aspects, use cases, challenges and research directions," *J. Ind. Inf. Integr.*, vol. 30, Nov. 2022, Art. no. 100404. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2452414X22000711

[146] P. Whig, A. Velu, and R. R. Naddikatu, "The economic impact of AI-enabled blockchain in 6G-based industry," in *AI and Blockchain Technology in 6G Wireless Network*. USA: Springer, 2022, pp. 205–224.

[147] T. Hewa, G. Gur, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6G: Challenges, opportunities and research directions," in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, Mar. 2020, pp. 1–5.

[148] J. Wang, X. Ling, Y. Le, Y. Huang, and X. You, "Blockchain-enabled wireless communications: A new paradigm towards 6G," *Nat. Sci. Rev.*, vol. 8, no. 9, Sep. 2021, Art. no. nwab069, doi: 10.1093/nsr/nwab069.

[149] *Key Drivers and Research Challenges for 6G Ubiquitous Wireless Intelligence (White Paper)*, Univ. Oulu, Oulu, Finland, 2019.

[150] R. Voleti, "Study of efficacious use of blockchain in 6G technology-path for the future," *Int. J. Eng. Res.*, vol. 9, no. 6, p. 1048, Jun. 2020.

[151] S. Polymeni, S. Plastras, D. N. Skoutas, G. Kormentzas, and C. Skianis, "The impact of 6G-IoT technologies on the development of agriculture 5.0: A review," *Electronics*, vol. 12, no. 12, p. 2651, Jun. 2023. [Online]. Available: https://www.mdpi.com/2079-9292/12/12/2651

[152] C.-X. Wang, X. You, X. Gao, X. Zhu, Z. Li, C. Zhang, H. Wang, Y. Huang, Y. Chen, H. Haas, J. S. Thompson, E. G. Larsson, M. D. Renzo, W. Tong, P. Zhu, X. Shen, H. V. Poor, and L. Hanzo, "On the road to 6G: Visions, requirements, key technologies, and testbeds," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 905–974, 2nd Quart., 2023.

[153] G. Muhammad, S. Alqahtani, and A. Alelaiwi, "Pandemic management for diseases similar to COVID-19 using deep learning and 5G communications," *IEEE Netw.*, vol. 35, no. 3, pp. 21–26, May 2021.

[154] S. Patil and P. Gokhale, "Multi-criteria approach for handling sophisticated data transmission over gateways in blockchain and Internet of Things (IoT) federated networks," *Expert Syst.*, vol. 39, no. 10, Dec. 2022, Art. no. e13127.

[155] M. Chowdhury, "Merit: An on-demand IoT service delivery and resource scheduling scheme for federated learning and blockchain empowered 6G edge networks with reduced time and energy cost," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 44, no. 2, pp. 79–103, 2023.

[156] Z. Tong, J. Wang, X. Hou, J. Chen, Z. Jiao, and J. Liu, "Blockchain-based trustworthy and efficient hierarchical federated learning for UAV-enabled IoT networks," *IEEE Internet Things J.*, early access, Feb. 28, 2024, doi: 10.1109/JIOT.2024.3370964.

[157] J. C. Priya, G. Nanthakumar, T. Choudhury, and K. Karthika, "6G-DeFLI: Enhanced quality-of-services using distributed hash table and blockchain-enabled federated learning approach in 6G IoT networks," *Wireless Netw.*, pp. 1–15, May 2024.

[158] L. Waltman, N. J. van Eck, and E. C. M. Noyons, "A unified approach to mapping and clustering of bibliometric networks," *J. Informetrics*, vol. 4, no. 4, pp. 629–635, Oct. 2010. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1751157710000660

[159] M. Aazam, S. Zeadally, and K. A. Harras, "Deploying fog computing in industrial Internet of Things and industry 4.0," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4674–4682, Oct. 2018.

[160] N. Kshetri, "Can blockchain strengthen the Internet of Things?" *IT Prof.*, vol. 19, no. 4, pp. 68–72, 2017.

[161] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldú, "The rise of blockchain technology in agriculture and food supply chains," *Trends Food Sci. Technol.*, vol. 91, pp. 640–652, Sep. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0924224418303686
[162] P. Bellini, P. Nesi, and G. Pantaleo, "IoT-enabled smart cities: A review of concepts, frameworks and key technologies," *Appl. Sci.*, vol. 12, no. 3, p. 1607, Feb. 2022. [Online]. Available: https://www.mdpi.com/2076-3417/12/3/1607
[163] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of IoT data," in *Proc. Cloud Comput. Secur. Workshop*. New York, NY, USA: Association for Computing Machinery, Nov. 2017, pp. 45–50, doi: 10.1145/3140649.3140656.
[164] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges," *Mech. Syst. Signal Process.*, vol. 135, Jan. 2020, Art. no. 106382. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S088832701930603X

FATEMAH H. ALGHAMEDY received the B.S. degree (Hons.) in computer science from King Faisal University, Saudi Arabia, in 2006, the M.S. (Outstanding) degree in computer science from Arkansas State University, USA, in 2013, and the Ph.D. degree in computer science from the University of Kentucky, USA, in 2019. She is currently an Assistant Professor in computer science with Imam Abdulrahman Bin Faisal University, Saudi Arabia. Her research interests include recommendation systems, machine learning, data mining, and deep learning.

NAHLA EL-HAGGAR received the B.Sc. and M.Sc. degrees in mathematics and in computer science from Ain Shams University, Cairo, Egypt, and the Ph.D. degree in scientific computing from Cairo University, Egypt. She is currently an Associate Professor with the Computer Science Department, Applied College, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia. She worked for nine years with the Information Technology Department, Faculty of Computing and Artificial Intelligence, Helwan University, Cairo. She worked for 20 years with the National Research Institute of Astronomy and Geophysics (NRIAG), Artificial Satellites Department, Helwan, Cairo. Her research interests include natural language processing (NLP), image processing, educational technology, information security, machine learning, drones, the IoT, blockchain, and cyber security.

ALBANDARI ALSUMAYT received the master's degree in computer security from The University of Manchester, in 2012, and the Ph.D. degree in computer security and networks from Nottingham Trent University, in 2017. She is currently an Assistant Professor and the Head of the Computer Science Department, Applied College, Imam Abdulrahman Bin Faisal University. Her research interests include security, wireless network security, drones, and blockchain.

ZEYAD ALFAWAER received the bachelor's degree in computer information systems from Applied Science University and the master's and Ph.D. degrees in computer application technology from Central South University, China. Currently, he is an Assistant Professor with the Science Technology and Mathematics Department, Lincoln University, Jefferson City, MI, USA. With a passion for advancing the field of computer science, he dedicates his efforts to teaching and conducting research in various areas, including wireless sensor networks, the Internet of Things (IoT), and cyber security.

MAJID ALSHAMMARI received the M.S. degree in computer science along with a Graduate Certificate in information protection and security from the University of New Haven, Connecticut, and the Ph.D. degree in computer science and engineering from the University of Bridgeport, Connecticut.

He is currently an Associate Professor in cybersecurity and computer science with the College of Computer Science and Information Technology, Taif University. He is certified in CompTIA Security+, Certified Ethical Hacker (CEH), Certified Computer Hacking Forensic Investigator (CHFI), and Microsoft Certified Systems Engineer: Security (MCSE: Security). He has published numerous papers in both conferences and journals. His research interests include machine learning, cybersecurity, cryptology, and the design and verification of cryptographic protocols. In addition to his academic roles, he is also a Cybersecurity and Digital Forensic Training Consultant, developing and training courses aligned with local and international workforce frameworks. At Taif University, he also holds the position of the Vice Dean of Development and Quality, contributing significantly to academic accreditation and curriculum development. His professional experience includes applying machine learning in cybersecurity, designing and implementing security systems, verifying cryptographic protocols, and enhancing cybersecurity education and practices.

LOBNA AMOURI is currently an Assistant Professor in industrial computing. Her research interests include artificial intelligence, robotics, network security, the Internet of Things, and multidisciplinary research.

SUMAYH S. ALJAMEEL received the B.S. degree (Hons.) in computer science from King Faisal University, Saudi Arabia, in 2004, the M.S. degree (Hons.) in software engineering from The University of Manchester, U.K., in 2013, and the Ph.D. degree in artificial intelligence from Manchester Metropolitan University, U.K., in 2018. She is currently an Assistant Professor in computer science and the Chair of the Computer Science Department, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Saudi Arabia. Her research interests include machine learning, deep learning, data mining, and specifically the application of AI with other fields, such as health, energy, and oil pipelines.

SARAH ALBASSAM, photograph and biography not available at the time of publication.