Received 27 September 2024; revised 10 November 2024; accepted 30 November 2024. Date of publication 9 December 2024; date of current version 8 January 2025.

Digital Object Identifier 10.1109/OJCOMS.2024.3513832

Federated Learning for 6G Networks: Navigating Privacy Benefits and Challenges

CHAMARA SANDEEPA [1] (Student Member, IEEE), ENGIN ZEYDAN [2] (Senior Member, IEEE), THARAKA SAMARASINGHE [3] (Senior Member, IEEE), AND MADHUSANKA LIYANAGE [1] (Senior Member, IEEE)

[1]School of Computer Science, University College Dublin, Dublin 4, D04 V1W8 Ireland
[2]Services as Networks (SaS) Research Unit, Centre Tecnològic de Telecomunicacions de Catalunya, 08860 Barcelona, Spain
[3]Department of Electronic and Telecommunication Engineering, University of Moratuwa, Moratuwa 10400, Sri Lanka

CORRESPONDING AUTHOR: M. LIYANAGE (e-mail: madhusanka@ucd.ie)

This work was supported in part by the European Union through the Project Confidential-6G under Grant 101096435, through the Project Robust-6G under Grant 101139068, and the Science Foundation Ireland under the CONNECT Phase 2 under Grant 13/RC/2077_P2; in part by the Spanish Ministry of Economy and Competitiveness (MINECO)—Program UNICO I+D under Grant TSI-063000-2021-54 and Grant TSI-063000-2021-55; in part by the "ERDF A Way of Making Europe" Project funded by MCIN/AEI/10.13039/501100011033 under Grant PID2021-126431OB-I00; and in part by the Generalitat de Catalunya under Grant 2021 SGR 00770.

ABSTRACT The upcoming Sixth Generation (6G) networks aim for fully automated, intelligent network functionalities and services. Therefore, Machine Learning (ML) is essential for these networks. Given stringent privacy regulations, future network architectures should use privacy-preserved ML for their applications and services. Federated Learning (FL) is expected to play an important role as a popular approach for distributed ML, as it protects privacy by design. However, many practical challenges exist before FL can be fully utilized as a key technology for these future networks. We consider the vision of a 6G layered architecture to evaluate the applicability of FL-based distributed intelligence. In this paper, we highlight the benefits of using FL for 6G and the main challenges and issues involved. We also discuss the existing solutions and the possible future directions that should be taken toward more robust and trustworthy FL for future networks.

INDEX TERMS Privacy, federated learning, 6G, beyond 5G, AI, distributed learning, machine learning.

I. INTRODUCTION

THE INTRODUCTION of Beyond 5G (B5G) and 6G networks opens a new era of connectivity characterized by immersive communication, integrated Artificial Intelligence (AI), massive, hyper-reliable and low-latency communication, ubiquitous connectivity, and integrated sensing. These advances promise to revolutionize various sectors, including healthcare, industrial automation, smart cities, and autonomous vehicles, by enabling sophisticated AI-driven applications [1]. However, the increasing reliance on AI and the extensive data collection required for these applications create significant privacy issues [2]. Traditional centralized machine learning approaches, which require aggregating data from multiple sources on a central server, pose a significant risk of data breaches and unauthorized access [3].

Several use cases exist in B5G/6G networks, such as smart cities, smart factories, smart energy grids, smart healthcare, and smart consumer applications [4]. In smart cities, sensors and connected devices manage urban infrastructure, transportation, and public services. Smart factories use industrial Internet of Things (IoT) devices and sensors to improve manufacturing processes, monitor machines, and ensure efficient production. Smart energy grids, smart meters, and grid management systems are used to optimize energy distribution and consumption. In smart healthcare, wearable devices and health monitoring systems track patient health data and provide personalized care. In smart consumer applications, various applications for personal use, such as smart home appliances, wearables, and personal assistants, are used. These use cases can also face specific privacy threats, as shown in Figure 1.

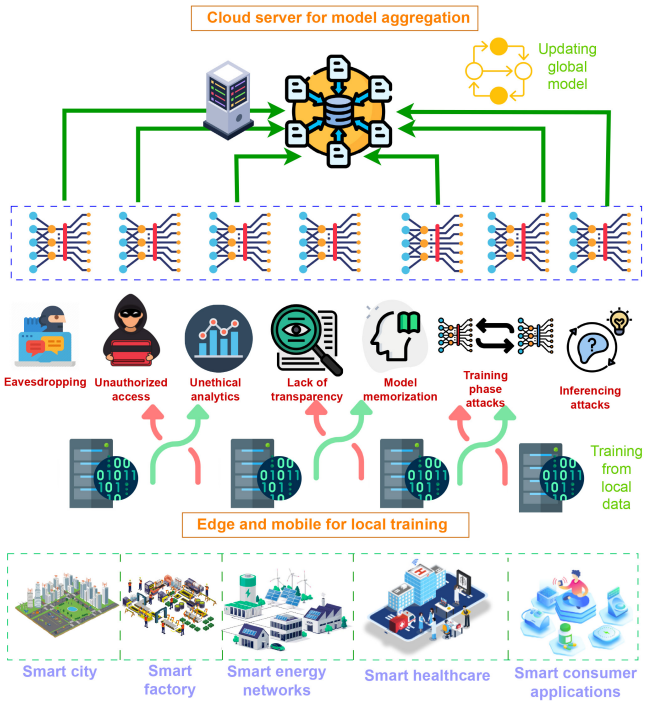

FIGURE 1. Overview of privacy challenges on B5G/6G.

FL effectively solves these privacy challenges as it enables decentralized model training [5]. With FL, the individual devices train a shared model together, keeping their data local and thus minimizing the need to transfer sensitive information. This approach fits well with the privacy requirements of 6G networks, where the sheer volume and data sensitivity require robust privacy mechanisms [6]. By leveraging FL, data remains on local devices, significantly reducing the risk of data breaches compared to traditional centralized methods. This is particularly relevant in 6G networks, which are expected to support many connected devices and handle unprecedented amounts of data [7]. Therefore, the combination of FL and 6G technologies can help maintain data privacy while enabling the deployment of advanced AI applications.

In a typical FL workflow, local devices (e.g., smartphones, IoT devices) train with local data and ensure that the raw data does not leave the device. Model updates are sent from local devices to a central cloud server and aggregated into a global model. Some privacy challenges in FL are: *eavesdropping*, which is unauthorized interception of data transmitted between local devices and the cloud server, which can lead to data leaks [8], *unauthorized access*, the illicit access to sensitive data or model updates by unauthorized persons or entities [9], *unethical analytics*, which is a misuse of data or model outputs for purposes not intended or ethical, such as profiling or targeted advertising without consent [10], *lack of transparency*, i.e., insufficient clarity about how data is used, processed, and shared, leading to a lack of trust among users [11], *model memorization*, i.e., the risk that the global model stores sensitive information from the training data that could be extracted later [12], *training phase attacks*, i.e., attacks that take place during the local training phase, such as poisoning the data to bias the model [13], and *inference phase attacks*, where attempts are made to derive sensitive information from the results of the model, which could jeopardize the privacy of individuals [14].

To overcome these challenges, advanced privacy-preserving techniques must be integrated into FL. Techniques such as Differential Privacy (DP) can add noise to data to obscure individual contributions [15], while Homomorphic Encryption (HE) enables computations on encrypted data without decrypting it [16]. Secure Multiparty Computation (SMC) enables joint computations while keeping the inputs private [17]. In addition, auditability and transparency mechanisms can provide users with clarity on how their data is used, processed, and shared, increasing trust in FL systems [18]. Maintaining privacy at the different layers of 6G networks is also important to ensure comprehensive security and data protection. Robust security measures must be implemented at the device level to prevent unauthorized access and data leakage from user devices. Over The Air (OTA) communication must be secured to protect data integrity during transmission. At the edge AI level, privacy mechanisms should ensure that sensitive information is not exposed during data processing and model training at the network edge. In addition, intelligent network management and orchestration must include FL to protect privacy across the network dynamically. Each layer requires specific strategies and technologies to address the unique privacy challenges and ensure a multi-layered and resilient approach to privacy in 6G networks.

A. MOTIVATION AND CONTRIBUTIONS

The motivation for this paper stems from the increasing demand for privacy in the era of ubiquitous connectivity and AI-driven decision-making, which will be expanded in 6G networks. Despite the numerous surveys on FL-enabled security and privacy for 6G, our survey fills important gaps left by previous works. While many existing surveys focus broadly on FL or specific areas such as IoT or healthcare, this survey provides a focused and comprehensive examination of the unique security and privacy challenges in the context of 6G networks. Having identified the related challenges, we propose ways to integrate additional privacy-enhancing techniques to strengthen the privacy-preserving capabilities of FL in protecting user data while maintaining the performance and scalability required for 6G applications. Our survey also offers an in-depth analysis of how FL can be effectively applied to different layers of 6G networks, including devices, communication channels, edge AI, and network management–an area often overlooked by other surveys. In addition, we adopt a multi-layer privacy preservation approach, diving into strategies for ensuring privacy at different levels of the 6G architecture. This is a crucial advancement, as many existing works do not explore

TABLE 1. Summary of important acronyms.

Acronym	Definition
5G	Fifth Generation
6G	Sixth Generation
AI	Artificial Intelligence
AR	Augmented Reality
B5G	Beyond 5G
BCI	Brain-Computer Interface
CAV	Connected Autonomous Vehicles
CFL	Centralized Federated Learning
CML	Centralized Machine Learning
DDoS	Distributed Denial of Service
DFL	De-centralized Federated Learning
DL	Deep Learning
DoS	Denial of Service
DP	Differential Privacy
FL	Federated Learning
FTL	Federated Transfer Learning
GDPR	General Data Protection Regulation
HE	Homomorphic Encryption
HFL	Hierarchical Federated Learning
HoFL	Horizontal Federated Learning
IID	Independent and Identically Distributed
IoE	Internet of Everything
IoMT	Internet of Medical Things
IoT	Internet of Things
MEC	Multi-access Edge Computing
ML	Machine Learning
mMTC	massive Machine-Type Communication
OTA	Over the Air
QoS	Quality of Service
P2P	Peer-to-Peer
PPML	Privacy Preserved ML
RAN	Radio Access Network
SMC	Secure Multi-Party Computation
TEE	Trusted Execution Environments
UAV	Unmanned Aerial Vehicles
UDN	Ultra-Dense Network
V2X	Vehicle-to-Everything
VFL	Vertical Federated Learning
VLC	Visible Light Communication
VR	Virtual Reality
XAI	Explainable AI
XR	eXtended Reality
ZSM	Zero Touch Network and Service Management

privacy solutions in such a detailed and layered manner. Finally, we offer an in-depth look at lessons learned and future research directions, particularly concerning privacy-preserving mechanisms in 6G and the wider integration of FL. Our contributions can be summarized threefold:

- We provide a comprehensive overview of FL and its role in 6G networks, detailing how FL can leverage the unique features of 6G to enhance privacy and security.
- We discuss use cases and architectural components that highlight the benefits of FL for privacy in 6G. We show how FL ensures data confidentiality and integrity through decentralized data processing and enables secure model training and aggregation in different use cases. We also discuss the implementation frameworks and tools of FL for 6G implementations.
- We address key privacy challenges associated with FL in the context of 6G networks and propose potential solutions to enhance FL's effectiveness in protecting user data. These challenges include model memorization, training phase attacks, inference attacks, eavesdropping, unauthorized access, and unethical analytics. We propose integrating privacy-enhancing techniques such as DP, SMC, HE, and secure aggregation protocols to mitigate these risks. Furthermore, we provide trade-offs of these solutions on 6G and approaches to address them.

Although we have thoroughly covered the existing knowledge and challenges of FL privacy in 6G based on the current state of research, the primary limitation of this survey lies in the early stage of 6G development. The absence of defined 6G architecture, requirements, and real-world deployments limits our ability to provide practical insights or scalability discussions for privacy-preserving FL solutions. Once 6G networks and applications are realized, future work will address these gaps by incorporating real-world examples and system evaluations.

Finally, Table 2 summarizes most important surveys on FL-enabled security and privacy for 6G and shows how our survey differs from them by complementing their limitations.

B. OUTLINE

The rest of the review is organized as follows. Section II provides background information on FL and its role in 6G networks. Section III discusses the application of FL for enhancing privacy in 6G, including specific use cases and architectural considerations. Section IV delves into the key privacy challenges of FL in 6G networks. Section V reviews various privacy-enhancing mechanisms that can be integrated with FL. Section VI explores privacy preservation at different layers of 6G networks. Section VII provides details of 6G use cases from FL. In Section VIII, FL implementation tools and frameworks are available for practical implementations. Section IX summarizes the lessons learned, remaining research questions, and emerging future research directions. Finally, Section X concludes the paper, emphasizing the critical role of FL in ensuring privacy in the next generation of wireless networks.

II. BACKGROUND

We begin this survey by presenting the necessary background information. To this end, this section first explains the background of FL and then its role in 6G networks and related work.

A. FEDERATED LEARNING

Accessibility to large amounts of data has led to an exponential growth in ML technologies and their applications [53], [54]. Conventional ML technologies rely on the availability of the data at a centralized location. This requirement has created a bottleneck for many applications that have difficulties in exchanging end-user data due to concerns of privacy [55], [56]. FL emerges as a robust solution, and this decentralized ML approach ensures that the training data stays at the edge devices while facilitating complex ML models in a collaborative manner [7]. A conceptual illustration of FL is presented in Fig. 2. In an FL setting, each edge device utilizes its local data for training a local

TABLE 2. Summary of important surveys on FL enabled security and privacy for 6G.

	FL for 6G Privacy	FL Privacy Challenges for 6G	Privacy enhancing mechanisms for FL in 6G	Privacy preservation at different 6G Layers	Lessons Learned for FL Privacy in 6G	Future directions analysis for FL Privacy in 6G	Descriptions and Limitations
Yang et al. [19]	L	M	L	H	M	H	FL applications for 6G but limited on privacy challenges and mechanisms specific to 6G.
Porambage et al. [20]	M	M	L	M	M	L	6G security and privacy landscape but lacks deep coverage of FL benefits and specific 6G privacy challenges.
Sirohi et al. [21]	H	H	M	M	M	M	Covers FL vulnerabilities but lacks focus on 6G-specific privacy use cases.
Kazmi et al. [22]	H	H	H	M	H	M	Conceptual techniques and challenges of FL in 6G, but lacks real-world applications.
Nassef et al. [23]	M	M	L	M	M	M	Distributed ML architectures but lacks specific FL privacy enhancements for 6G.
Al-Quraan et al. [24]	H	M	M	M	M	M	Covers FL in wireless edge networks, but limited on privacy-preserving techniques for 6G.
Xu et al. [25]	H	M	M	M	M	M	Focuses on edge learning techniques, lacks privacy aspects for FL in 6G.
Javeed et al. [26]	H	H	M	M	M	M	Theoretical focus on quantum computing and FL, limited real-world 6G applications.
Ferrag et al. [27]	H	H	M	M	M	M	Emerging technologies for edge security, lacks detailed FL implementations for 6G privacy.
Duan et al. [28]	H	H	M	M	M	M	Multi-layer FL architecture for edge computing but does not cover specific 6G privacy issues.
Yin et al. [29]	H	M	H	L	M	M	Comprehensive review of privacy-preserving techniques in FL but lacks focus on 6G scenarios.
Imteaj et al. [30]	M	M	L	M	M	L	Focuses on IoT FL applications, with limited focus on 6G networks.
Aledhari et al. [31]	H	M	H	L	M	M	Covers FL frameworks but less emphasis on 6G privacy challenges.
Sharma et al. [32]	H	M	M	M	M	L	Focus on healthcare FL, limited applicability to other 6G use cases.
Wu et al. [33]	H	M	M	M	M	M	Focuses on edge computing but lacks 6G-specific privacy challenges.
Ghimire et al. [9]	H	M	M	M	M	M	More focus on cybersecurity than privacy-preserving mechanisms specific to 6G.
Zhang et al. [34]	H	M	M	M	M	M	Survey on FL architectures with limited 6G privacy mechanisms.
Issa et al. [35]	M	M	L	M	M	M	Focuses on FL with blockchain for IoT, with less attention to broader 6G privacy concerns.
Gupta et al. [36]	H	M	M	M	M	M	Covers FL algorithms, with limited discussion on 6G privacy issues.
Yu et al. [37]	H	M	M	M	M	M	FL for data analytics, with less focus on 6G-specific privacy challenges.
Nguyen et al. [38]	H	M	M	L	M	M	Comprehensive survey on FL for IoT, covering privacy challenges but less focus on 6G use cases.
Lu et al. [39]	M	M	L	L	M	M	Focus on non-IID data in FL, mostly theoretical, limited discussion on 6G privacy.
Brecko et al. [40]	H	M	M	L	M	M	Survey on FL in edge computing, lacks focus on 6G-specific privacy challenges.
Mothukuri et al. [41]	H	M	H	L	M	M	Comprehensive security and privacy challenges in FL, but lacks detailed 6G implementations.
Kumar et al. [42]	M	M	L	L	M	M	Focuses on adversarial attacks in FL, with limited discussion on privacy in 6G contexts.
Almanifi et al. [43]	M	M	L	L	M	M	Focuses on communication efficiency in FL, limited focus on privacy for 6G.
Nguyen et al. [44]	H	M	M	L	M	M	Survey on FL for smart healthcare systems, limited discussion of 6G-specific privacy.
Zhang et al. [45]	M	M	L	L	M	M	Focuses on FL for transportation systems, with limited 6G privacy-preserving discussions.
Lim et al. [46]	H	M	M	L	M	M	Survey on FL in mobile edge networks, limited focus on privacy techniques specific to 6G.
Chellapandi et al. [47]	M	M	L	L	M	M	Focuses on FL for connected and automated vehicles, with limited coverage on broader 6G privacy.
Boobalan et al. [48]	M	M	L	L	M	M	Fusion of FL and industrial IoT, but lacks attention to 6G-specific privacy issues.
Zhu et al. [49]	M	M	L	L	M	M	Primarily focuses on non-IID data challenges in FL, limited 6G privacy discussion.
Liu et al. [50]	M	M	L	L	M	M	Theoretical focus on federated and meta-learning, with limited coverage of 6G privacy.
Ye et al. [51]	M	M	L	L	M	M	Focus on heterogeneous FL, limited discussion of privacy for 6G.
Khan et al. [52]	H	M	M	L	M	M	Comprehensive survey on FL for IoT, with limited insight into privacy preservation for 6G.
This survey	H	H	H	H	H	H	Comprehensive survey on FL for 6G, addressing privacy challenges, privacy-enhancing mechanisms, and preservation at different 6G layers.

H Explores the field in detail. M Provides some information about the field. L No information or explores the area only briefly.

ML model while updating an FL server that runs a global ML model. It is different from DL as only model updates, such as gradients and model parameters, are shared with the FL server [7] in a manner that ensures the privacy of the end-user data. The FL server aggregates the information from the edge devices to update the weights of its model in an iterative manner [57]. FL enables network operators efficient resource allocation for different services [58], thus is envisioned to play an important role in 6G and other next-generation networks [59].

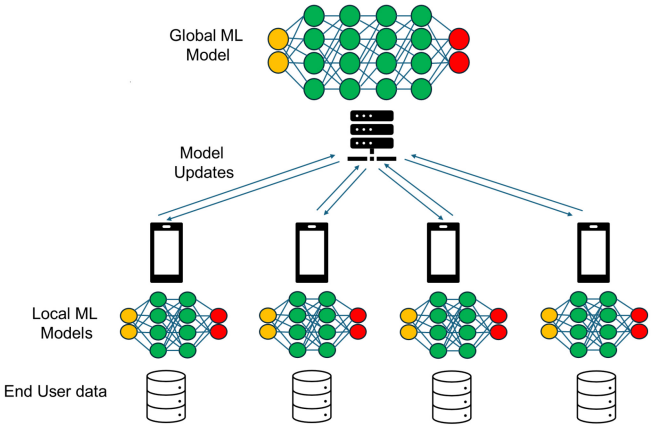

FIGURE 2. A conceptual illustration of FL.

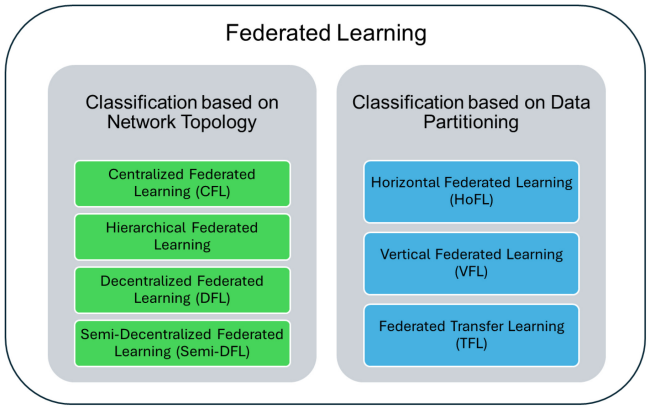

FIGURE 3. Federated learning classifications based on network topology and data partitioning.

FL can be classified based on network topology and data partitioning [38], [55], and it is illustrated in Fig. 3. Under network topology, FL can be classified as Centralized Federated Learning (CFL), Hierarchical FL, Decentralized FL (DFL), and Semi-DFL [52]. In CFL, each client trains its local model independently by using its own user data and transmits the model parameters to the FL server. These parameters are aggregated at the server using a weighted averaging algorithm, e.g., Federated Averaging (FedAvg) [7]. The global model is shared with all clients such that each client has a global model and a local model. Hierarchical FL utilizes several stages of aggregations at the edge servers in a hierarchical manner [60] before the final aggregation is done at the FL server. DFL is significantly different as it omits the requirement of a centralized server for orchestrating the learning process. The clients are nodes in a Peer-to-Peer (P2P) network, such that collaborative model training is possible [61]. Each client performs local model training and shares the model updates with its neighbors. The updates are aggregated at each node to reach a consensus on the global model update. Semi-DFL combines the advantages of hierarchical and decentralized FL [62]. It partitions the clients into several clusters, with a cluster head who is responsible for sub-aggregation in the respective cluster. Once the sub-aggregation is complete, the cluster heads collaborate in a decentralized manner to compute the global model. Again, a centralized server is omitted. This configuration reduces the communication overhead on individual nodes and mitigates the risk of single-point failures.

The classification based on data partitioning is related to how the training data is distributed over the sample and feature spaces. To this end, there are three main classifications, namely Horizontal Federated Learning (HoFL), Vertical Federated Learning (VFL), and Federated Transfer Learning (FTL) [5]. In HoFL, the clients share the same feature space, but they have different data samples. Hence, the same ML model can be used for local training [63]. The FL server aggregates the local updates to compute the global update, which is shared with the clients as the basis for the next iteration of local training. For example, consider a smart city where various data acquisition devices are deployed [19]. These devices share the same feature space, such as weather data and traffic conditions, but they have different sample spaces because of their different locations and the tasks they carry out. VFL, on the other hand, caters to scenarios where the clients possess different subsets of features for the same group of samples [64]. Using a process known as entity alignment, the group of samples common to the clients is collected [65] and used to train a shared model while utilizing encryption for data privacy [66]. For example, consider the Intelligent Transportation Systems (ITS) realm. This setting may consist of various stakeholders with different data, e.g., vehicle manufacturers (data about the vehicles), traffic management authorities (data on road conditions, vehicle traffic, pedestrians), and telecommunication service providers (data on the connectivity of vehicles, drivers, and passengers). The sample space is the same as it is for vehicles/users, but the features are different [67]. These stakeholders can employ VFL to cooperatively train the models to predict traffic congestion, optimize route planning, or enhance the safety and efficiency of autonomous vehicles. This cooperation allows for the harnessing of collective knowledge, enabling more accurate and robust models while ensuring data remains with its original owner, adhering to privacy regulations. Finally, FTL is used in cases where both the feature space and the sample space are different among the clients [68].

B. ROLE OF FL IN 6G NETWORKS

6G networks consist of heterogeneous nodes that align with application scenarios and use cases of the industry verticals. The stringent Quality-of-Service (QoS) constraints in these networks in terms of speed and latency necessitate expensive computational operations to be offloaded towards the edge layer. This, together with the privacy concerns of user data, make FL an ideal candidate for 6G networks that inherently exhibit a distributed nature [69]. The relevance of FL in

TABLE 3. The relevance of FL to the 6G layers and the performance enhancements that can be achieved.

6G Layer	Relevance to FL
Smart Application Layer	FL Enables distributed AI for intelligent 6G applications, e.g., organizational operations, industrial automation, healthcare, and transport logistics.
Network-centric Application Layer	FL enables network-centric applications to facilitate regulatory requirements, ensuring QoS, API management, and resource monitoring and management.
Intelligent Control Layer	FL can be used to control, monitor, and manage network functions, scheduling, monitoring, and secure access.
Intelligent Edge Layer	Hierarchical aggregation of data and model sharing, facilitating cross-silo FL.

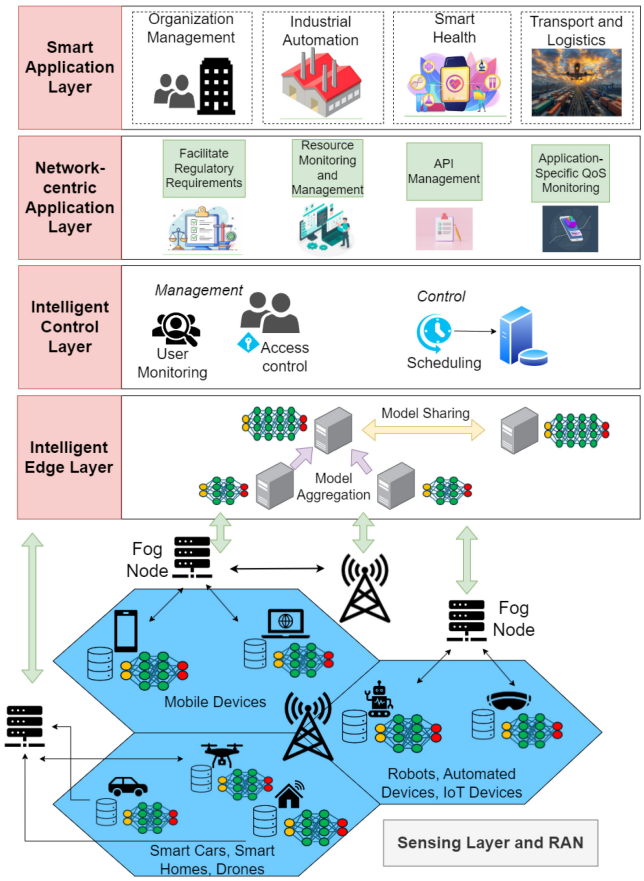

FIGURE 4. Role of FL in 6G networks.

related 6G layers (the Smart Application Layer, the Network-centric Application Layer, the Intelligent Control Layer, and the Intelligent Edge Layer) is presented in TABLE 3. The Radio Access Network (RAN) supports connectivity and data collection through fog nodes, cell site connections, and connected devices, which include mobile phones, sensors, robots, IoT devices, and smart vehicles, as illustrated in Fig. 4.

Moreover, the usage of FL for model training introduces several key advantages in a 6G network [70]. These include privacy, low latency and overheads, and improved scalability. FL inherently preserves privacy as user data remains in its device, mitigating the risk of privacy breaches and unauthorized access in scenarios that involve sensitive data such as mobile traffic [2], [71]. This is crucial in a 6G network where data generation happens at high volumes at end devices. Eliminating the requirement to transmit these large volumes of data reduces latency [72], and hence makes FL an ideal solution for ultra-low latency applications. Devices learn a shared prediction model in parallel and in a collaborative manner with minimum interactions, thus significantly reducing the transmission overheads as model updates are typically much smaller in size compared to raw data [73], [74], [75]. This, in turn, reduces the energy consumption associated with data transmissions as well. Also, model training can be done continuously in a manner that is consistent with application-based timelines, and instantaneous decisions can be made at the end nodes. This will significantly facilitate applications that require real-time response, such as augmented reality, industrial automation, and autonomous driving [46].

FL also improves the scalability of a network. Firstly, FL stems on decentralized processing which distributes the processing over multiple nodes. This leads to a network that is easily scalable with an increasing number of devices. The system can leverage the computational resources of the new devices to enhance the model training efficiency of the overall network [2]. Secondly, the distributed nature supports managing heterogeneity and geographic distribution of data. In 6G, data is highly heterogeneous due to a diverse set of devices and applications. Thus, data distributions are unlikely to be identical. The local model training in FL facilitates this heterogeneity as models can adapt to the specific characteristics of the local data. Also, personalized models can be used to suit the data diversity among the devices. Heterogeneity can be considered in the data aggregation stage as well by clustering devices with similar data distributions and using weighted or adaptive aggregations according to importance or relevance. Selecting a subset of clients with similar data distributions for each training round can help stabilize the learning process and improve model performance. Moreover, regularization can be used to mitigate the impact of skewed data distributions during training. Incorporating data from varying geographical locations result in more robust and adaptable models that can cater a wide range of scenarios [5]. Finally, FL brings the model to the data, enabling ML in previously inaccessible environments due to legal, privacy, or logistical constraints associated with data protection. This significantly broadens the potential of ML-related applications in the future.

FL aligns well with the communication goals of 6G networks by improving communication efficiency, reducing latency, optimizing network resource usage, and supporting scalable and resilient network architectures. The reduced data transmission from FL alleviates network congestion and increases bandwidth efficiency. The frequency of model

updates can be further adjusted to suit the network congestion similar to adaptive communication scenarios. Local training on the edge devices reduces the need for frequent, high-latency roundtrips to the centralized servers, which allows quicker response times for applications that rely on real-time data [76]. Such applications can be further supported by network slicing by assigning a specific slice optimized for low latency and high reliability. The feature of being able to support massive device connectivity (scalability) ensures efficient utilization of available computational resources. We also note that an FL-based communication network is more resilient and robust as the training process is distributed across multiple devices, avoiding single points of failure. Load balancing is supported, which reduces the risk of bottlenecks and improves the overall network stability. FL can also further enhance the user experience in applications where context-aware and personalized services are required. Thus, by integrating FL, 6G networks can achieve better communication performance and more effective utilization of available resources.

There are some important technical challenges in implementing FL in 6G networks, particularly in terms of hardware requirements and network infrastructure. Firstly, the edge devices need to be complex enough to support FL with sufficient computational power to train models. Training models locally on edge devices consume energy; thus, managing the energy consumption is critical [77]. Some edge devices may even depend on energy harvesting, so the usage of energy-efficient algorithms and hardware is vital in managing the tradeoff between complex and quick computations and energy conservation. Ensuring secure model updates through implementing advanced encryption techniques on resource-constrained devices also poses a significant challenge. The system should also be robust and adaptable to support the device diversity created by a multitude of edge devices with varying computational and storage capabilities, as well as communication interfaces.

The servers should be capable of handling high volumes of data for timely aggregation and updating the centralized models. Efficiently synchronizing updates from a diverse set of edge devices is challenging [78]. Verifying the integrity and authenticity of the model updates from these devices necessitates additional resources at the servers. Servers also require robust version control mechanisms to efficiently and accurately manage the frequent model updates.

There are several technologies that can facilitate FL in 6G networks. These include Multi-Access Edge Computing (MEC), SMC, FedAvg, Network Function Virtualization (NFV), network slicing, Ultra-reliable Low-latency Communication (URLLC), Edge Intelligence Frameworks, and Blockchain Technology [19], [79]. Adaptive protocols like Quick UDP Internet Connections (QUIC) and advanced versions of HTTP/2 that are designed for low-latency communication and efficient data transfer can also support the communication between edge devices and central servers to facilitate FL.

Next, we summarize some noteworthy contributions to using FL in 5G, B5G, and 6G networks. Firstly, we focus on the network topology-based classification of FL. To this end, authors of [70], [80], [81] have studied how CFL is beneficial in B5G and 6G networks. [80] proposes F-BIDS to protect the privacy of existing ML-based cyber-security. They use a centralized federated blending model, and the federated meta-classifier is trained on the meta-data instead of sensitive user data. The authors of [81] studied resource allocation in B5G networks using FL, particularly focusing on dynamic and heterogeneous network environments. In the literature on hierarchical FL, [82] consider hierarchical FL for 5G smart grids by proposing an intrusion detection system, and [83] consider wireless communication networks. The ability to use hierarchical FL to reduce the latency in a cellular network without losing the model accuracy is demonstrated in [84]. The method stems from clustering mobile users in the proximity of edge servers that communicate with a central server for global model aggregation. Similarly, a hierarchical FL-based solution for user assignment and resource allocation is proposed in [85]. The authors highlight the superiority of hierarchical FL over CFL with respect to training, communication overhead, accuracy, and speed.

The authors of [86] propose DFL-based traffic sign recognition in networked vehicles, and DFL for Vehicle-to-Everything (V2X) networks for providing efficient distributed training services is studied in [87]. Furthermore, due to its inherent characteristics, P2P-based communication technologies such as blockchain can be easily incorporated in DFL systems [88]. In this scenario, information on model updates and aggregation can be communicated securely through blockchain ledgers. Furthermore, the performance of semi-DFL in B5G and 6G networks is studied in [89].

With respect to FL classification based on data partitioning, it is shown that Horizontal Federated Learning (HoFL) can utilize high-speed, low-latency communication infrastructure to share model updates between nodes, ensuring timely aggregation and dissemination [90]. Vertical Federated Learning (VFL) can also play a key role in B5G and 6G networks in enabling smart and interconnected systems across various sectors [91]. Federated Transfer Learning (FTL), which expands the possibilities of FL through collaboration, leverages the diversity and richness of data generated from different domains for enhancing the accuracy and robustness of the models [92]. FTL has been proposed as an efficient solution for intrusion detection for 5G IoT in [93].

III. FL FOR 6G PRIVACY

In this section, we discuss these potential applications of FL, including different domains of FL, potential challenges for FL in 6G, and how to enhance the privacy-preserving nature of FL for 6G by integrating other privacy-enhancing techniques. Although the concept of privacy is as old as mankind [94], in recent years, one can observe a modern emergence and discussion of privacy, especially with the

introduction of regulatory approaches such as the European Union's GDPR [95] in 2018. Privacy is generally the assurance that individuals have control or influence over what data about them may be collected and stored and by whom and to whom the information may be shared [96].

With the enhanced communication capabilities and seamless connectivity offered by B5G/6G networks, AI will play a dominant role in individuals' everyday activities, making important decisions based on insights from big data collected from individuals. For these services to function smoothly, AI-driven automation of services will be a mandatory requirement for B5G/6G. For example, the number of attacks on 6G-based services will increase significantly with the enablement of ultra-high communication speeds and the ubiquitous availability of access points and IoT. Therefore, it will not be possible to manually manage the security of these services. Automating the proactive detection and remediation of attacks, therefore, requires AI-driven approaches [97]. However, the requirements for the protection of privacy also apply in the areas of future communication and AI. In the previous example, the AI applied in 6G could be a double-edged sword, as the continuous monitoring of user traffic by these AI models can create a new attack surface for end users and service providers. With advances in the interpretation of big data and advances in AI facilitated by fast communication techniques, the controllability, transparency, and ownership of data from end users, organizations, and states are increasingly being challenged. This issue may become more significant in future B5G/6G network infrastructures as the ability to collect and analyze user data will continue to increase with the support of AI-driven services.

The leakage of unintended information through B5G/6G services can be a critical privacy issue as it directly affects users' rights and control over their data. For example, a smart light connected wirelessly via B5G/6G to a remote server or smart device can increase the energy efficiency of the home. At the same time, however, it can also collect data, e.g., when a user is at home, which rooms are frequently used, and whether there are people in the house. This can then provide insights into the user's habits, preferences, and daily routine [98]. Therefore, the AI-driven 6G applications combined with the expanding IoT layer to sensitive personal data drastically increase the possibility of identifying information about individuals such as their health status, current actions, prediction of decisions, movements, interests, personal beliefs, ideologies, etc. Applications can analyze the data output via sensors, smartphones, and other personal electronic devices with a network connection. Third parties can collect a wide range of signals and extract this information from the individuals/users concerned.

The key privacy requirements that 6G should satisfy come from multiple technological advancements that 6G possess compared to previous network generations. We can list them as follows:

- *AI-based zero-touch automation:* This new progression of network management via AI reduces the delays in establishing communications and the need for human intervention to the network. Zero-touch management promotes distributed ML operations like FL to automatically perform AI model training, collaboration and sharing of models [99]. However, it also creates a major requirement of ensuring the privacy of the models shared over the network. Furthermore, if these shared AI models used in zero-touch management networks consist of vulnerabilities like backdoors or triggers, it will increase the risk of privacy leakage, potentially revealing network patterns or sensitive network-related information such as periodic data or patterns of data usage.
- *Massive connectivity of sensors and smart user devices:* Unlike the previous generations, a surge of new devices like IoT, along with the improvements in the edge AI and lightweight local computation hardware, the upcoming 6G networks will have billions of local devices interconnected wirelessly and collaborating with each other. Thus, privacy requirements are of high importance, considering the relatively less secure communication protocols and encryption mechanisms in these relatively limited resource IoT devices. Furthermore, transmitting data in a more secure manner requires higher computational and energy demand for operations like authentication [100]. Therefore, keeping the data locally for the device without forwarding them to third parties is more favourable for IoT, which is achieved via FL.
- *Location and movement privacy requirements:* In 6G, with the proliferation of billions of new devices and increased localization accuracy, there is a heightened risk of location-based privacy breaches. Highly accurate location tracking could allow adversaries to map individuals' movements or sensitive location data. 6G networks need privacy-preserving ML techniques to train the models containing these location data safely. Furthermore, communication systems like V2X [101] will be further enhanced by the mobility and high bandwidth provided by the 6G networks, facilitating real-time communication among these smart vehicles. Thus, FL can enable training and knowledge sharing among them in a privacy-preserved manner.
- *Privacy in Immersive Applications:* 6G will enable highly immersive applications such as Augmented Reality (AR), virtual reality Virtual Reality (VR), and Extended Reality (XR) beyond the current limitations due to its capability of establishing massive connectivity and ultra-high data rates. These applications will generate vast amounts of sensitive user data, including biometric information, personal behaviour patterns, and interactions within virtual environments. Current research has already investigated numerous privacy vulnerabilities in devices like VR headsets,

such as unrestricted motion, optical and eye-tracking sensors, which could be exploited by an adversary [102]. Protecting this sensitive data from being exposed or misused is a major privacy requirement. Thus, FL can support in enabling privacy-preserved distributed metaverse intelligence.

A. SUPPORT OF FL FOR IMPROVED 6G PRIVACY

FL can improve privacy in 6G communications in several ways. Some of them are summarized in below items:

1) DATA DECENTRALIZATION

In traditional ML, the data for training is collected and stored centrally. In FL, however, the models are trained directly on the devices on which the data is generated (e.g., smartphones, IoT devices), which ensures that the raw data never leaves the device. In 6G networks, where huge amounts of sensitive data are generated and transmitted, the decentralization provided by FL is crucial. By keeping the data local, FL reduces the risk of data breaches and unauthorized access, as there is no central repository for sensitive information to be targeted by attackers. In a 6G-enabled smart healthcare system, for example, patient data remains on wearable devices, maintaining confidentiality while contributing to a global healthcare model [103].

2) MODEL AGGREGATION

FL typically employs secure aggregation protocols where individual model updates (not the raw data) are sent to a central server. These updates are combined to improve the global model. For example, in smart city applications with FL, traffic pattern data can be used to optimize urban mobility without compromising individual commuter privacy [104]. Techniques such as DP can be applied during the aggregation process to add noise to the updates, further obscuring individual data contributions and protecting user privacy [105]. This is particularly important in 6G networks, where the integration of extensive and diverse data sources increases the risk of identifying individuals based on their data patterns.

3) COMMUNICATION EFFICIENCY

To minimize communication overhead, FL often uses techniques to compress model updates before sending them [106]. This not only reduces the required bandwidth but can also include privacy-preserving transformations. This is important in 6G networks as large amounts of data are generated by numerous connected devices.

4) SECURITY

FL updates can be encrypted during transmission, ensuring that even if intercepted, the data remains secure and unintelligible to unauthorized parties [107]. In this respect, the security framework of 6G can be complemented with encrypted FL to address various vulnerabilities, including threats to confidentiality, integrity, and availability. In MEC scenarios of 6G networks [108], for example, where data processing takes place at the edge of the network, i.e., closer to the devices, encrypted data transmission in FL enables collaborative learning on this distributed data while keeping it private. FL can also be used for intrusion and anomaly detection in 6G networks to address privacy concerns and improve security in distributed environments. As 6G brings higher device density, diverse network components and increased real-time data requirements, FL-based intrusion detection offers scalable and secure solutions in areas such as Software Defined Networking (SDN), Industrial Internet of Things (IIoT), Cyber-Physical Systems (CPS) and Vehicular Edge Computing. Each of these areas offers unique challenges and opportunities.

Li et al. [109] presented an efficient FL system for network intrusion detection, focusing on reducing communication cost and improving model accuracy, important considerations for high speed and low latency requirements in 6G networks. Raza et al. [110] extended this idea within SDNs, where FL enables privacy-preserving detection without transmitting sensitive network data. Their model is particularly relevant to 6G due to the inherent programmability and scalability of SDNs, which enable more responsive and adaptive intrusion detection mechanisms. Similarly, Chatzimiltis et al. [111] presented a collaborative SDN-based intrusion detection system tailored for smart grids, an area where the interplay between low-latency 6G communication and high security is crucial to ensure infrastructure resilience. Bhavsar et al. [112] used FL in transportation IoT to facilitate intrusion detection in distributed IoT devices to ensure privacy protection while improving the robustness of transportation networks, an important aspect as 6G increases the number of connected vehicles and devices in smart cities. Huang et al. [113] addressed the specific requirements of CPS and proposed Execution & Evaluation dual network framework, a dual-network FL framework that personalizes intrusion detection based on device characteristics, which aligns well with the need for tailored security in the various application domains of 6G.

Recent advances have further enhanced FL's intrusion detection capabilities by integrating blockchain to secure FL processes through decentralized trust models, which are essential for combating intrusions in highly dynamic and distributed/decentralized environments such as 6G networks. For example, the framework presented in [114] utilizes blockchain to support federated learning for intrusion detection in vehicle edge computing. This approach improves collaboration and anti-tampering protection across distributed vehicles and enables 6G networks to support a secure vehicle ecosystem. In addition, [115] presents a privacy framework that specifically targets jamming attacks and uses FL to jointly detect and mitigate these attacks. This approach is critical for 6G, as maintaining signal integrity is essential for services that require ultra-reliable low-latency communication (URLLC). Authors in [116] build on this by combining FL with explainable AI and blockchain.

This creates a robust intrusion detection system for IoT networks that can ensure both privacy and transparency. Such integration is essential for 6 G's multi-layered security requirements to ensure that the decisions made by the model are understandable and trustworthy for end users. In addition to these frameworks, recent research has explored the intersection of FL with quantum technologies. The paper in [117] proposes a quantum federated learning framework to protect privacy in detecting intrusions into consumer networks. By leveraging the potential of quantum computing for robust encryption, this framework adds an additional layer of security to intrusion detection, addressing the challenges of processing large, sensitive consumer data in 6G networks. Such integration of quantum technologies with FL is critical as it holds promise for overcoming computational and privacy constraints, especially as 6G brings unprecedented amounts of data and diverse devices to the network. The integration of FL with reinforcement learning ([118], [119]) has also been investigated to combat specific attacks such as jamming, which are crucial for secure and reliable 6G communication in wireless sensor networks and open radio access networks.

In summary, the above studies show that FL, supported by blockchain, quantum technologies and advanced AI techniques, provides a flexible, privacy-preserving, and robust framework for addressing the evolving security challenges of 6G. Each domain-specific application illustrates how FL can be adapted to the unique requirements of 6G environments, paving the way for more resilient and responsive security mechanisms in next-generation networks.

5) INTEGRATION OF PRIVACY-PRESERVING MECHANISMS

Homomorphic encryption allows calculations to be performed on encrypted data without decrypting it. In FL, it can be used to enable the central server to aggregate model updates without accessing the underlying data [120]. In the context of 6G, this means that sensitive data from industrial IoT devices can be processed securely, ensuring operational confidentiality. SMC allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. In FL, this can be used to aggregate updates without revealing individual updates to the central server or other parties [121]. As 6G is expected to support a wider range of applications, potentially including more sensitive data, SMC's strong data privacy protection guarantees during the FL process will be crucial in such scenarios.

6) AUDITABILITY AND TRANSPARENCY

FL frameworks often include mechanisms (e.g., blockchain) for auditing data access and use to ensure transparency and traceability regarding the use and sharing of data [18], [122], [123]. This is critical to maintaining user trust in 6G applications where data privacy is paramount. In addition, the users or the owners of the application in an FL setup usually have more control over their data as they can opt in or out of the learning process, decide what data they want to contribute, and have a clearer understanding of how their data will be used [124]. This can build trust and ensure user privacy. Coupled with 6G's low latency and edge computing capabilities in real-time AI applications for smart cities, citizens can decide for themselves whether their anonymized location data or sensor data from their homes will contribute to the training of AI models for city management.

7) ROBUSTNESS AGAINST KNOWN PRIVACY ATTACKS

FL in 6G networks must address a wide array of sophisticated privacy threats to ensure secure and trustworthy communication frameworks. FL can incorporate anonymization techniques to ensure that updates are not linked to specific users, reducing the risk that data can be traced back to an individual. In this regard, a human-centered 6G communication framework equipped with FL can play an important role in such efforts to prevent the frequent disclosure of data and improve users' lives in terms of privacy [125]. Beyond anonymization, FL models can also be designed to be robust against adversarial attacks, such as model poisoning or inference attacks, which further enhances the privacy and security of the data [126]. However, a more thorough investigation of privacy threats is essential for a robust FL framework in 6G. Attacks such as Byzantine attacks, where adversarial participants send misleading model updates, require robust aggregation algorithms that prevent compromised nodes from corrupting the model [127]. Robust aggregation techniques such as Krum and Bulyan are crucial to mitigate the impact of such attacks and ensure that malicious contributions are effectively detected and excluded [128]. The robustness of aggregation algorithms is, therefore, crucial for the security of FL, especially in dense 6G environments where malicious actors can exploit vulnerabilities in model aggregation to skew the model outputs.

Another key threat in 6G FL frameworks is man-in-the-middle attacks on model updates, where an attacker intercepts and alters updates between devices and servers [126], [129]. To ensure the confidentiality and integrity of model updates, secure channels, encryption and continuous verification of model integrity during the update process are required. Techniques such as differential privacy and homomorphic encryption can provide further protection against such attacks and make it more difficult for unauthorized parties to modify or intercept sensitive data in transit.

Fig. 5 provides a high-level overview of how FL techniques can be used to enhance privacy in 6G networks to address these vulnerabilities. By incorporating these strategies, FL can provide a robust framework that maintains improved levels of privacy and security while enabling the benefits of collaborative learning across distributed data sources. We further discuss these privacy-enhancing

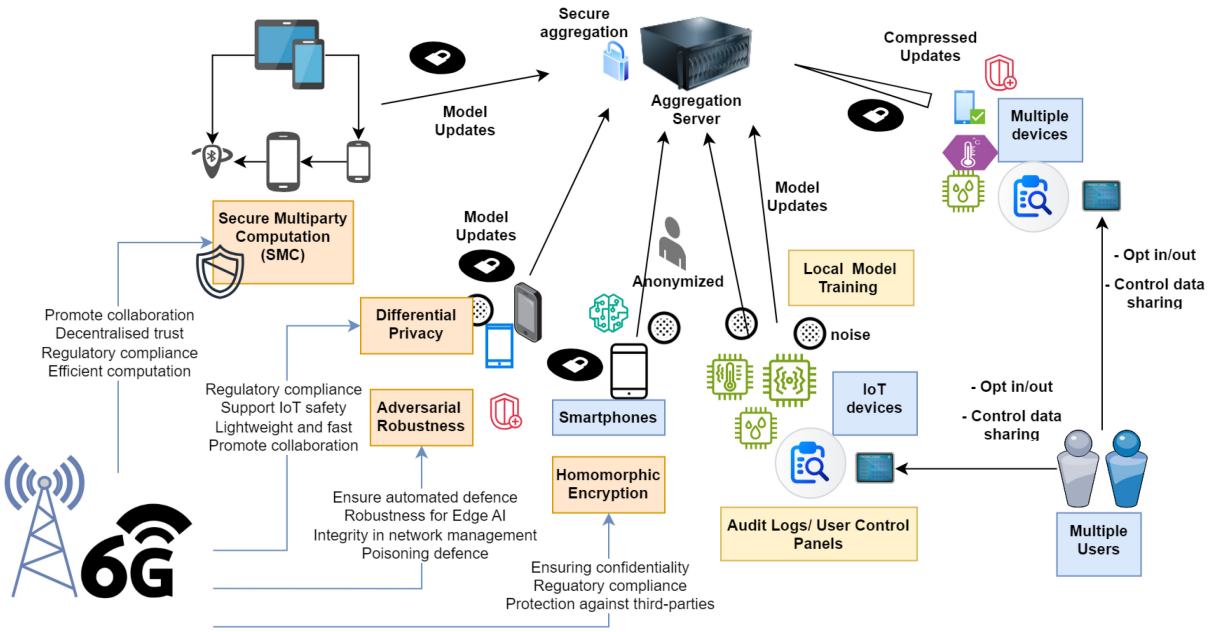

FIGURE 5. FL for enhanced privacy in 6G networks, illustrating the key components and privacy-preserving mechanisms that ensure secure and efficient data processing in a 6G environment.

techniques and their current improvements to be done in Section V.

B. 6G USE CASES WITH IMPROVED PRIVACY THROUGH FL

FL can be used to significantly improve the privacy of 6G networks by enabling the decentralized training of ML models in various 6G use cases. For example, 6G networks can support advanced health monitoring systems with extreme Ultra-Reliable Low-Latency Communication (xURLLC) [130] or real-time holographic communications [131]. *In smart health*, wearable devices can collect health data such as heart rate and blood glucose levels [132]. FL with 6G connectivity enables these devices to collaboratively and rapidly train a large model that can predict health anomalies without sharing the raw data, thereby preserving data confidentiality. This ensures that personal health data is not disclosed or transferred and that patient privacy is protected. 6G's ability to connect numerous devices at high data rates and low latency makes it ideal for smart city applications [133]. *In smart cities*, traffic sensors and connected vehicles can collect data about traffic patterns sent within 6G networks. With the help of FL, these devices can jointly train models to optimize traffic flow and reduce congestion without sharing individual travel data, thus preserving commuters' privacy [134].

6G networks have the potential to revolutionize industrial automation by connecting machines, sensors, and control systems with high reliability and low latency [135]. *In industrial automation*, machines on a production line can use their operating data to train models that predict failures or maintenance needs. With FL, each machine contributes to the model without revealing its data, thus preserving the confidentiality of industrial processes [136]. 6G networks will support autonomous vehicles with high data and ultra-low latency requirements for the safe operation of autonomous vehicles [83]. *In intelligent vehicles*, autonomous cars can collect data on driving behavior and road conditions. FL enables these cars to train models that improve navigation and safety systems while ensuring that individual driving data is not shared to protect user privacy [137].

6G networks will connect a variety of IoT devices in smart homes, from appliances to security systems [138]. FL helps these devices to improve their algorithms locally and ensure data privacy [139]. In *IoT and edge devices*, devices such as smart thermostats and security cameras can use FL to improve their algorithms for energy management and security threat detection. In the field of smart home security, for instance, cameras and sensors can use FL to develop more accurate intrusion detection models by learning locally from the data. This can ensure that personal video recordings and sensor data are not transmitted to central servers and that the privacy of the household is maintained. Each device can process its data locally and only share model updates, so no sensitive household information is exposed. The high bandwidth and low latency of 6G networks can enable these devices can share model updates quickly and efficiently [27].

C. PRIVACY THREATS AND ENHANCEMENTS IN 6G NETWORKS

In 6G networks, the adoption of cutting-edge technologies and architectural changes brings about a new set of privacy challenges, distinct from those seen in earlier generations like

5G. Some of the key features of 6G, such as intelligent surfaces, pervasive AI, massive Machine-Type Communications (mMTC), and the utilization of terahertz (THz) frequencies, present novel vulnerabilities that demand specialized privacy-preserving mechanisms.

One of the most important threats to privacy in 6G comes from Ultra Dense Networks (UDNs). With an unprecedented density of devices, the resulting complex architecture increases the number of potential vulnerabilities. Extensive data exchange in this dense environment increases the risk of data breaches and offers attackers more opportunities to intercept, manipulate or misuse sensitive information. In addition, the use of THz bands in 6G, while beneficial for high data rates and low latency, introduces new risks at the physical layer. These high-frequency signals are more susceptible to eavesdropping, jamming and interference, making it easier for unauthorized parties to access or disrupt communications. Pervasive AI integrated into 6G networks, especially in edge computing environments, poses another significant privacy concern. The role of AI in data collection, processing and decision-making increases vulnerability to sophisticated attacks, such as model inversion and membership inference attacks, where sensitive user data can be derived or extracted from AI models. In addition, 6G networks are expected to integrate multiple communication layers – including satellite, aerial, and terrestrial components – forming space-air-ground networks. The transmission of data across these heterogeneous infrastructures, each with different security protocols, introduces additional vulnerabilities, particularly during the transition between less secure nodes. mMTC in 6G, which is characterized by the connection of billions of IoT devices, further complicates privacy management due to the decentralized nature of these devices. The aggregation of data from such a large number of sources increases the risk of data breaches and unauthorized use. These threats will be intensified by the expected arrival of quantum computers in the 6G era. These could render many of the cryptographic techniques currently used to protect privacy in wireless networks obsolete.

Despite these threats to privacy, the advanced features of 6G can be used to enhance privacy protection. For example, several real 6G use cases such as tactile Internet, real-time holographic communications, XR/multi-sensory communication, massive digital twin networks, and remote surgery with haptic feedback introduce new dimensions for privacy enhancement through FL. The tactile Internet in 6G, which supports ultra-low latency and real-time haptic interactions, poses a challenge for privacy. However, FL ensures that sensitive haptic feedback data is processed locally so that personal data remains secure. In real-time holographic communication or telepresence, where large amounts of 3D holographic and motion-capture data are exchanged, FL enables local model updates without the need to exchange raw holographic data, thereby enhancing privacy [134]. XR and multisensory communication require multi-gigabit speeds and ultra- low latency. Here, FL can protect user privacy by keeping the immersive experience data on local devices while still sharing useful insights [140]. Massive digital twin networks collect huge amounts of operational data from multiple sources. FL's decentralized training enables companies to leverage these networks without exposing sensitive operational data to external threats [141]. Remote surgery with haptic feedback benefits from FL by ensuring that highly sensitive surgical data, including both haptic and visual information, remains private while enabling collaborative improvements in surgical procedures [142].

Moreover, pervasive AI can be used for real-time anomaly detection and adaptive privacy policies. By intelligently managing privacy settings based on context, user location and application type, AI can dynamically adjust protections to strengthen privacy. The decentralized architectures supported by 6G, such as blockchain, provide robust and transparent data management that ensures secure storage and traceability of sensitive information and reduces the risk of unauthorized access. Intelligent Reflecting Surfaces (IRS), another key feature of 6G, can improve physical layer security by dynamically controlling the radio environment. This capability helps to mitigate eavesdropping attempts and strengthen the security of communication links. Furthermore, the inclusion of quantum communication technologies, in particular Quantum Key Distribution (QKD), provides an additional layer of security as QKD generates encryption keys that cannot be intercepted or decoded without detection.

Finally, Table 4 summarizes how FL improves privacy in various 6G use cases, leveraging the specific capabilities of 6G networks.

IV. KEY FL PRIVACY CHALLENGES IN 6G NETWORKS

The section explores key privacy challenges in B5G/6G networks. This includes the issues that occur within the training process, communication, and storage of data and models in FL and where these FL issues occur at the 6G architecture.

As 6G networks emerge, they introduce new privacy challenges compared to 5G, especially in the context of FL. These challenges arise from the larger scale of devices, more sensitive and diverse data sources, and the need for real-time processing. Table 5 highlights key privacy challenges in FL for both 5G and 6G networks, illustrating how the complexities grow with the transition to 6G.

Next, we discuss specific issues in the FL lifecycle and how each of these challenges are applicable when performing FL operations in 6G architecture.

A. PRIVACY ISSUES WITHIN THE MODEL TRAINING PROCESS LIFE-CYCLE

Though FL appears to be a promising future for Privacy Preserved ML (PPML) in 6G, there can be potential privacy leakages via FL itself. Fig. 6 provides an overview of how

TABLE 4. 6G use cases and privacy enhancements with federated learning.

Use Cases	6G Capabilities	Data Collected	FL Privacy Enhancements
Tactile Internet	Ultra-low latency, high reliability	Haptic feedback, real-time control signals	FL on edge devices ensures that sensitive haptic data is processed locally, minimizing privacy risks [132]
Real-Time Holographic Communications/Telepresence	Ultra-fast data transmission, high bandwidth	3D holographic data, motion capture data	Local model updates protect the personal holographic data, ensuring that detailed motion and visual data are not shared across networks [134].
XR/Multi-Sensory Communication	Multi-gigabit speeds, ultra-low latency	Multi-sensory data (audio, visual, haptic)	FL enhances privacy by keeping immersive XR experiences on local devices while sharing insights for improvement without compromising user privacy [140].
Massive Digital Twin Networks	Ultra-reliable, massive connections	Digital twin data (sensor, operational data)	FL allows for decentralized training of digital twin models, ensuring sensitive operational data remains protected [141].
Remote Surgery with Haptic Feedback	Ultra-low latency, reliable communication	Haptic and visual data from surgical instruments	Local processing of surgical data ensures that the surgeon's interactions remain private and secure, with FL enabling collaborative improvements [142].
Smart Health	xURLLC, real-time data processing	Heart rate, blood glucose levels, etc.	Local training on devices, data never leaves the device, preserving patient privacy [132]
Smart Cities	High data rates, low latency	Traffic patterns, vehicle data	Joint model training without sharing raw data, optimizing traffic flow while preserving privacy [134]
Industrial Automation	Reliable and low latency connections	Machine operating data	Local model training, preserving confidentiality of industrial processes [136]
Intelligent Vehicles	High data rates, ultra-low latency	Driving behavior, road conditions	Decentralized training to improve navigation and safety, ensuring privacy [137]
IoT and Smart Homes	High bandwidth, low latency	Home appliance data, security camera footage	Local algorithm improvement, preserving household privacy by not transmitting raw data [27]

TABLE 5. Comparison between 5G and 6G FL challenges.

Aspect	5G Networks	6G Networks
Data sensitivity	Data from smartphones, IoT, and wearables; less critical in nature.	More diverse and critical data (e.g., healthcare, autonomous systems, VR, Brain-Computer Interfaces (BCI)
Data ownership and control	Mostly centralized or cloud-based [143]; limited focus on user data ownership	Highly decentralized [143], [144]; greater emphasis on user data control and ownership at the edge
Privacy-preserving techniques	Centralized ML [143] or limited FL with well investigated and mature privacy techniques	Need for more advanced privacy techniques to scale across massively distributed networks
Real-time privacy concerns	FL operates at reasonable latencies [125]; real-time data rarely needed	Real-time applications (e.g., autonomous vehicles) require low-latency FL [125] with strong privacy protection
Cross-border data privacy	Mostly confined to single-domain or local applications	Global, multi-domain applications raise cross-border privacy concerns due to varying regulations
Attack surface expansion	Smaller network; easier to protect against adversarial attacks	Massive attack surface; more devices, more vulnerabilities, need for stronger adversarial defense

the FL process occurs in the B5G/6G architecture, and the vulnerability of the process to privacy threats. We outline the following challenges arising from FL that can impact B5G/6G privacy:

1) MODEL MEMORIZATION

Although data is not directly transmitted from the client, they still have to transmit model parameters trained on each client's private data. Such parameters can consist

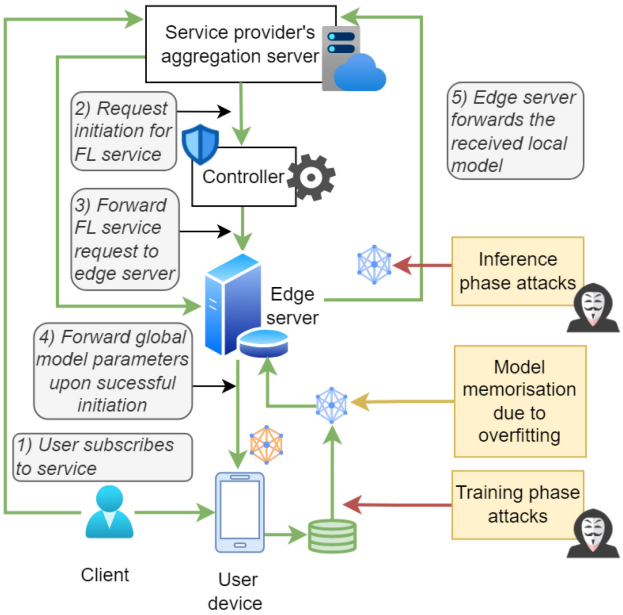

FIGURE 6. Overview of FL services and related privacy issues in FL during the process.

of insights that may be indirectly related to the original data [145], [146], making the models memorize information about the user data. Thus, adversaries can exploit these model parameters to reveal unintended information on data owners. In B5G/6G, when end users communicate models related to private and sensitive information they locally possess, an external party at higher layers could eavesdrop on these model updates to look for potential properties that can reveal the original data.

In 6G networks, the massive scale of data and real-time applications like autonomous vehicles [147] and metaverse [148], [149] heightens the risk of model memorization. It can unintentionally retain sensitive information from the training data. This makes it vulnerable to privacy attacks. Compared to 5G, 6G's increased data diversity and criticality, such as healthcare, BCIs [150] amplify privacy concerns, as more sensitive personal data could be exposed through model leakage across distributed nodes.

Recent research on FL privacy shows that FL is vulnerable to numerous privacy attacks, including reconstruction, model inversion, membership inference, and property inference attacks [41], [145]. These attacks can be categorized into two [151]: training phase attacks and inference phase attacks.

2) TRAINING PHASE ATTACKS

Considering the training phase, we can identify attacks such as backdoor poisoning. Since FL is based on many client devices collaborating together, a malicious client has the potential to inject model updates that are biased towards a certain property, causing backdoors in the aggregated model [152]. Sybil is another attack [151], which seeks to simulate numerous end devices without interfering with the FL protocol. An attacker may also try to eavesdrop on the model updates during transmission to the aggregator by a particular client, even though the adversary does not have access to the client data or the aggregator. All these attacks can mainly happen at the local device layer of B5G/6G. However, during transmission, an attacker can also launch a man-in-the-middle attack such that they can forward malicious data or perform eavesdropping at upper layers.

Gradient leakage attacks are another main attack type [153] that exploits the gradients shared by clients to reconstruct sensitive training data. By analyzing these gradients, attackers may attempt to fully or partially recover the private training data of the clients. In free-rider attacks, malicious clients avoid contributing meaningful data or computation while still benefiting from the collective model, which can be commercially valuable or highly sensitive to user data [154]. Another key concern is model stealing during training, where adversarial clients attempt to steal the ownership of the client models, their contributions and watermarks [155].

In 6G, the large-scale, decentralized nature of networks with massive IoT devices, edge computing, and critical applications such as healthcare and autonomous systems increases the risk of training phase attacks. Compared to 5G, 6G's reliance on distributed FL models across a broader and more diverse range of devices means attackers have more entry points to inject malicious data or manipulate models. The increased heterogeneity of data sources in 6G also complicates detection, making such attacks more challenging to mitigate than in the relatively centralized 5G networks.

3) INFERENCE PHASE ATTACKS

Inference phase attacks involve inferring attributes of the training data through trained model parameters. Examples of inference attacks include membership inference, model inversion, and property inference attacks [145]. Here, the attacker captures model parameters through different means, such as eavesdropping and compromising the client or the aggregator. The attacker then attempts to infer information on the training data of the captured victim's model through its predictions. For this, the attackers may create their own dataset containing the required infer properties. The differences in the output of the victim's model on target properties can reveal information about the training data. To identify these differences, the attacker feeds this data to another ML model called the attack model, which is designed by the attacker and it attempts to reveal the private information of the victim's target dataset. These attacks can occur at the service aggregator or at intermediate B5G/6G layers if eavesdroppers can illicitly obtain local client models.

Additionally, evasion [156] of defense mechanisms in FL is a growing concern. Here, attackers may exploit the advanced connectivity and adaptive capabilities of 6G to evade security measures that aim to protect the model. With 6G's support for enhanced edge computing and real-time data processing, attackers can craft more precise and frequent

attack queries and data at a rapid rate, increasing the risk of bypassing the safeguards.

The richer context and more critical nature of the data in 6G make property inference attacks more trivial and threatening, as attackers can extract private attributes beyond the intended model output, making privacy harder to protect compared to 5G.

B. PRIVACY THREATS IN COMMUNICATION AND STORAGE

Future B5G/6G networks can face numerous privacy issues with increased interactions among devices, ease of entering as third-party services, and sharing of user data for applications based on classical centralized approaches followed in AI model training. We outline the following challenges that could occur in such a setup:

1) DATA EAVESDROPPING

Eavesdropping of client data during generation, storage, and transmission in B5G/6G can be considered a significant privacy issue if the data consists of attributes or properties that are linked to a natural person's Personally Identifiable Information (PII) [157]. Furthermore, even if it is not linked with individuals, it could still raise a critical privacy issue if it consists of sensitive non-personal data [158], [159] related to a legal entity like an organization. Therefore, direct transmission of big data via B5G/6G networks can pose a significant threat to adversaries with respect to all layers. The adversaries can be both insiders or outsiders, who tend to eavesdrop via means such as side-channel attacks [160] for exploiting weaknesses in the encryption process [161]. If FL is implemented, even if an attacker eavesdrops on the model during the transmission or on the server side, the information that can be obtained is relatively limited compared to the actual data. If coupled with a privacy preservation technique described in Section V, revealing private information from FL models will be practically difficult for an attacker.

The highly decentralized architecture and reliance on edge computing in 6G increase the risk of opening gateways to possible attacks like data poisoning or inference. While 5G already faces eavesdropping risks, 6G's expansion in device connectivity and network complexity amplifies this issue, making secure encryption and privacy-preserving protocols essential to prevent unauthorized access to sensitive data as it travels across the network.

2) UNAUTHORIZED ACCESS

An adversary can also actively attempt to gain access to the ML training process at different layers of 6G. The client layer would be the easiest to access due to vulnerabilities of the end user devices and social engineering [162]. However, the privacy leakage will mainly be limited to the owner of that particular device. The issue would get more critical if the upper layers, where millions or even billions of devices are connected and are accessed. In such a case, a high risk exists for information leakage by observing the patterns of model sharing, and the susceptibility exists for an attacker to inject malicious models or backdoors into the aggregation process. As solutions, many secure aggregation techniques like pair-wise masking and homomorphic encryption-based aggregation for FL exist [163], which are further discussed in Section V.

In 6G networks, unauthorized access risks increase due to the expanded attack surface with the decentralized, edge-based FL systems. Unlike 5G's more centralized controls, 6G's distributed architecture makes unified security approaches more difficult, exposing vulnerabilities in access control.

3) UNETHICAL ANALYTICS AND DATA MISUSE

Even the outsider attacks are avoided by security and privacy measures in the B5G/6G network during transmission; in the context of centralized ML, end-user data collected and stored by third parties can potentially misuse them by performing analytics [164]. Furthermore, these third parties can sell the data to other entities without the permission of the original data generator, whose intentions could be malicious. FL, by default, can avoid a majority of such situations as there is no data transfer between the data generator and a third-party service provider. This will also support the mitigation of the ambiguity and legal disputes on claiming the ownership of data [165], where end users will get the exclusive right to their data. However, the model behaviors and evolution of the models can still be monitored by the third-party aggregators by observing the continuous changes in the model parameters from a unique client if plain FL is used [166]. Moreover, by monitoring other properties in the network like communication latency, IP addresses, FL global cycle time, and quality of the model updates, an aggregator and its third-party service provider may be able to identify the information such as type and computational capacity of the client device, approximate location and the quality of data used for training.

While 5G networks are more centralized, making it easier to monitor and regulate data use, 6G's distributed architecture enables service providers to potentially analyze FL models without clear user consent. The increase in edge AI-based analytics and sensitive data collection in 6G amplifies this risk, making stricter privacy controls and transparency measures more essential than in the relatively controlled 5G environment.

4) LACK OF STANDARDIZATION AND TRANSPARENCY

In B5G/6G, end-user environments such as IoT can pose a relatively higher vulnerability of getting exploited by attackers due to reasons such as less frequent device updates, dense availability, less stringent privacy preservation mechanisms, and lack of standardization in resource-constrained devices [167], [168], [169]. The privacy guarantees on data provided by the organizations or services can also vary depending on the region, where no unified minimum protection standards are defined. Furthermore, even when

data is transmitted to third-party services, they may not fully disclose the applications that user data is used in. This makes it difficult for a general user to trust service providers. With FL, such problems can generally be mitigated. FL can provide a unified mechanism for privacy-preserved distributed model training since many different types of ML models can be aggregated together. Then, data storage at the local devices is the only requirement that needs to be strengthened. Yet, FL itself can have multiple approaches for architectural designs as described in Section II, where the privacy-preserving techniques applied for one approach may not be suited for another. For instance, algorithms available for robust aggregation in a centralized FL may not be fully applicable in a P2P FL scenario. This is because an adversary can craft malicious updates to evade such defenses as the attacker knows the defense strategy of robust aggregation in the P2P FL scenario due to the requirement of sharing of aggregation protocol across all clients. However, new standards for FL for critical applications are continuously being proposed [170], and they can provide even better privacy protection in the future.

While 5G has established protocols and frameworks, 6G's rapidly evolving decentralized architecture and diverse applications can have diverse data handling, privacy, and security approaches. This can lead to inconsistencies in how FL models are managed and increases the potential for opaque practices, such as unethical data use or exploitation. Without standardized guidelines, it becomes difficult to ensure transparency in model training and data analytics, leading to a higher risk of privacy violations than in 5G, where regulatory structures are more established.

C. WHERE DO THE FL ISSUES OCCUR IN THE 6G ARCHITECTURE?

There are many current discussions in the relevant literature about the privacy of B5G/6G. The survey in [157] provides a general overview of privacy concerns, problems, and possible solutions in B5G/6G networks. They consider that privacy issues arise in multiple layers of a 6G vision architecture proposed in [171]: 1) Smart sensor layer, which includes AI-driven IoT sensor devices and the edge AI; 2) Data mining and analytics layer, on which operations such as storage, knowledge discovery, and data filtering are performed, 3) Smart control layer, which performs management and orchestration, and 4) Smart application layer, on which 6G applications and related third-party services are operated.

Fig. 7 shows an overview of the main FL-based components operating at each layer and the associated privacy challenges. This multi-layered architecture for an FL system within a 6G network highlights the various components, processes, and associated privacy and security challenges.

Considering the top level, which is *the smart application layer*, AI applications are used in various fields such as industrial automation, smart health, and transportation. It should also define interfacing among multiple application-level components and should establish proper communication among them. This layer focuses on regulations, requirements, and communication interfaces. It contains templates for AI models that adhere to the specific business requirements and regulations. At this level, some challenges are unethical consumer analytics with the misuse of consumer data for unethical analytics, lack of transparency with insufficient transparency in data processing and handling, and lower standards for privacy and security by implementing privacy and security standards that are below the optimal level.

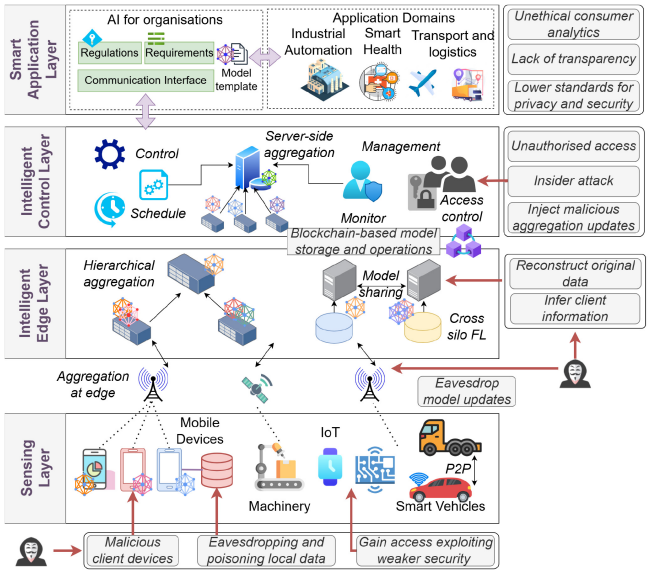

FIGURE 7. Overview of usage of FL over 6G vision layered architecture and potential privacy challenges.

Below the smart application layer, *the Intelligent Control Layer* handles server-side aggregation, model management, and monitoring using the blockchain for secure operations. This layer also includes access control to prevent unauthorized data access and insider attacks. In this layer, control and scheduling interact with server-side aggregation to manage the AI models. Access control ensures that only authorized personnel can access the data and models. It oversees the activities of the entire FL process. Blockchain-based model storage acts as a secure storage, and decentralized FL operations can also be performed using blockchain technology and are located between the intelligent control and edge layers. Potential security and privacy challenges at this level include unauthorized access to sensitive data, insider attacks initiated by authorized personnel within the organization, and the injection of malicious aggregation updates that introduce false updates into the aggregation process.

The Intelligent Edge Layer focuses on hierarchical and edge-level data aggregation, with mechanisms for model sharing across different silos while highlighting risks like eavesdropping and data reconstruction. Potential security and privacy challenges in this layer include eavesdrop model updates where unauthorized interception of model updates occur, reconstruction of original data where inferring or

TABLE 6. Privacy issues and its impact on B5G/6G architectural layers.

Privacy Issue	Impact			
	SL	*EL*	*CL*	*AL*
Data eavesdropping	H	H	H	H
Unauthorized access	H	H	H	H
Unethical analytics and data misuse	L	M	H	H
Lack of standardization and transparency	H	M	H	H
Model memorization	H	H	M	M
Training phase attacks	H	H	H	L
Inference phase attacks	L	H	H	H

SL - Sensing Layer, EL -Edge Layer, CL - Control Layer, AL - Application Layer

L Low Impact M Medium Impact H High Impact

reconstruction of original data from aggregated information is enabled, and client information inference to determine sensitive client information through analysis.

At the base, *the Sensing Layer* includes mobile devices, IoT, and smart vehicles that collect and preliminarily aggregate data, facing challenges such as malicious devices, data poisoning, and security vulnerabilities. Potential security and privacy challenges at this level include malicious client devices that are at risk of intentionally corrupting data, eavesdropping, and poisoning local data through unauthorized access and malicious data manipulation, and exploiting weaker security measures to gain access to systems with weaker security measures. In terms of data flow and interactions, data flow begins in the sensing layer, where devices collect and possibly aggregate data. This data is then sent to the intelligent edge layer for further aggregation and initial sharing of models. The aggregated data and models are forwarded to the intelligent control layer for centralized control, scheduling, and monitoring. Finally, the smart application layer uses this data and models for various applications, adhering to regulations and requirements. Table 6 provides some key overlapping threats and attacks across multiple layers of 6G. This 6G architecture highlights the importance of securing each layer to protect the overall integrity and privacy of the FL process in a 6G network. Each layer interacts to ensure efficient data processing and AI model application while addressing specific security threats and maintaining privacy through measures such as blockchain storage and stringent access controls.

V. PRIVACY ENHANCING MECHANISMS FOR FL IN 6G

Privacy-enhancing mechanisms refer to a broad class of technologies designed to safeguard various dimensions of privacy, including data confidentiality, user anonymity, and data integrity. Several privacy-preserving mechanisms have been proposed in the recent literature, e.g., [17], [41], [105], [172], [173], to enhance the resilience of FL against privacy attacks. These solutions mainly include DP, SMC, model masking and cryptographic techniques such as HE. They focus on different aspects of privacy, such as keeping data confidential, ensuring users remain anonymous, and making sure that the data being processed is accurate. For example, HE helps maintain data confidentiality by

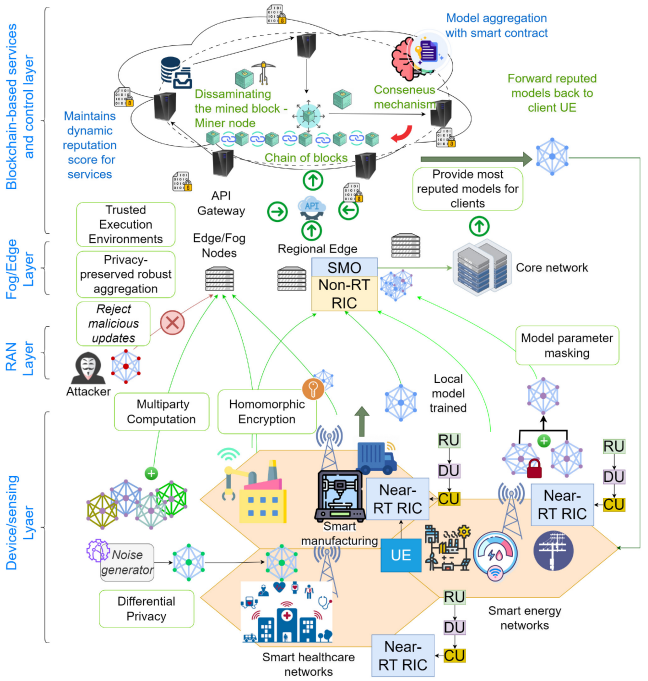

FIGURE 8. Possible privacy-enhancing solutions to mitigate privacy-related threats in FL.

allowing computations to be performed on encrypted data without ever revealing the original information. SMC keeps data confidential and ensures user anonymity, as it enables collaboration without exposing individual data inputs. DP focuses on protecting user identities by adding random noise to data, preventing personal details from being uncovered in aggregated results. Model masking further safeguards data by ensuring that sensitive information does not leak during machine learning model training.

Additionally, technologies such as Blockchain contribute to maintaining data integrity and security by offering a decentralized and tamper-resistant approach to storing data, which ensures that information remains intact and unaltered across a distributed network. These privacy-enhancing mechanisms are essential for addressing the unique challenges posed by the decentralized and data-heavy nature of 6G environments. Fig. 8 provides an overview of the potential privacy issues and their applicability over different layers in the 6G architecture. Next, we further discuss each of these solutions in detail.

A. DIFFERENTIAL PRIVACY

The notion of DP is based on giving plausible deniability to the participants, generally by adding random noise to their inputs [174]. FL can, therefore, apply DP-based techniques to guarantee privacy for its users, even if the model updates are captured by an adversary since the models trained via techniques like Differentially Private Stochastic Gradient Descent (DP-SGD) [175] can minimize the leakage of data through DP-based noise.

The (ϵ-δ) DP is formally defined through the following inequality [176]:

$$Pr[M(x) \in S] \leq e^{\epsilon} Pr\big[M(y) \in S\big] + \delta, \tag{1}$$

where the randomised algorithm M gives ϵ-DP if datasets x and y differing on at most one element $\forall S \subset Range(M)$. The value ϵ is called the privacy budget, and δ is the probability of privacy leakage, which is a constant. However, the work in [177] shows that the model accuracy may get reduced with noise through DP. The authors in [178] apply Local Differential Privacy (LDP) to provide privacy guarantees for FL model parameter updates and a collaborative training approach for utility-aware perturbations to prevent uncontrolled noise. They also mention that the LDP mechanism can protect FL from inference attacks.

In the context of B5G/6G, DP can be applied at the device layer, where end users can introduce a controlled noise via DP-based aggregation. This step is relatively simple and has lesser computational complexity as noise is randomly generated and added to the model or data. Furthermore, no additional communication overhead can be expected as the structure and architecture of the model parameters will remain the same. It could support various user devices in future networks since the algorithms and noise bounds are well-defined and implemented as DP-based wrappers [179]. However, the issue of reduction of model accuracy comes as a significant trade-off for DP [180], [181], as it limits the utility of the FL models.

B. SECURE MULTI-PARTY COMPUTATION

SMC enhances privacy in FL by enabling multiple participants to jointly compute aggregated model updates without revealing individual data. It divides the model parameters into secret shares among participating devices [173]. Each device holds a share of the model and collaborates through secure protocols to perform computations on its share. These computations, such as addition and multiplication, are executed without disclosing the actual model parameters. Only the final aggregated result is obtained, ensuring individual contributions remain confidential throughout the process. B5G/6G services can adopt SMC so that malicious aggregators cannot isolate any targeted client. This helps mitigate several privacy-related issues in B5G/6G with FL, including privacy leakage via model memorization since the end server will only get the aggregated models. Thus, it will also mitigate the possibility of inference phase attacks and build trust among end users to contribute more to the FL-based services in B5G/6G. In FL, SMC can be efficiently implemented using a technique such as secret sharing, such as Shamir's Secret Sharing scheme [182], [183]. In this setup, each participant splits their secret (e.g., model update or gradient) into multiple shares. Let s_i represent the secret from participant i, and let N denote the total number of participants. Each secret is divided into N shares, where a share for the client j can be presented as S_i^j. Hence, the original secret is the total of $s = S_i^1 + S_i^2 + \cdots + S_i^N$.

In FL, when each participant has received their shares, they send them to a trusted aggregator or a subset of devices, which securely sums the shares to reconstruct the global model update. The total sum of all secrets s_i is calculated by summing the shares from all clients as:

$$S = \sum_{i=1}^{N} s_i = \sum_{i=1}^{N} \left(S_i^1 + S_i^2 + \cdots + S_i^N \right) \tag{2}$$

Therefore, the final result S is the aggregated value of all participants' contributions, and privacy is preserved, as no individual can learn another participant's full secret. This method enables privacy-preserving aggregation in FL over 6G networks, as 6G provides the required communication capacity to split the shares and establish rapid communication.

SMC can also be combined with other approaches like DP. Authors in [184] use a hybrid approach of using both SMC and DP, where they attempt to reduce the utility loss from DP by providing lower noise quantity through SMC. Importantly, SMC ensures that privacy protection doesn't compromise model utility [185], as the final aggregated model can remain accurate. Therefore, SMC is a powerful technique that effectively safeguards privacy in 6G by enabling collaborative model training without exposing sensitive data. However, it also comes with tradeoffs, including heightened communication overhead [185], which should be carefully considered in designing privacy-conscious FL systems.

C. MODEL MASKING

Another approach for preserving privacy in FL model updates is by using a mask on top of the original model update, which gets canceled upon aggregation. For example, work in [186] uses a self-canceling zero-mean uniform noise mask on the model parameters during client model training, which gets canceled over local epochs. This helps mitigate privacy leakage if an adversary accesses the local models during the training phase. Further, the noise is added during model transmission, where individual clients' noise additions will be mitigated over many client contributions. Work presented in [187] provides a dual-masking framework to prevent model inversion and model poisoning attacks by partially updating model weights with masks for two layers. Additive pairwise masking is another approach where two trustworthy clients agree on a random mask, which gets canceled out when aggregated at the server [188]. This makes any malicious or curious server unable to learn about the individual clients. Since the computation overhead for calculating masks is relatively low, B5G services could utilize this technique in applications where lightweight computations are possible, such as IoT edge and resource-constrained user devices. However, if the mask is known by the attacker, the model will be recoverable. Thus, it should be kept private and secure.

D. HOMOMORPHIC ENCRYPTION

HE offers a compelling application within the context of FL for the evolution into B5G/6G networks. Allowing computable functions on encrypted data enables secure model aggregation without exposing the model parameters [189]. This approach ensures robust privacy guarantees while maintaining model utility. In HE, each client encrypts their local model update before sending it to the central server, ensuring that their raw data is never exposed. Let s_i represent the secret, such as the model update or gradient from client i, and let N be the total number of clients. Suppose the encryption operation from the client i is $Enc(s_i)$. HE allows the server to perform aggregation without decryption as:

$$Enc(S) = Enc(s_1) + Enc(s_2) + \cdots + Enc(S_N) \quad (3)$$

Here, the aggregator cannot learn the individual model updates. It can only decrypt the encrypted version of the global model S via a decryption function as $S = Dec(Enc(s))$. Therefore, it makes the individual updates confidential.

The work in [190] proposes a framework for FL using a partially HE scheme and shows that accuracy deviation with the mechanism is less than 1%. Despite these benefits, this technique comes with trade-offs. The authors show that increasing key lengths also increases the time taken for aggregation. Thus, the computational cost and complexity associated with HE can be significant [190], [191], especially for resource-constrained IoT devices in the dynamic and data-intensive environments of B5G/6G networks. Furthermore, HE prevents any inspection of client models, thus, requiring all the clients to be trustworthy. Therefore, they may be of limited use when there are untrustworthy clients performing model poisoning [192]. However, in cases where FL is done at higher layers in the B5G/6G architecture, where the parties involved are resourceful (e.g., cross-silo FL among multiple organizations), this approach can provide strong protection against privacy leakages.

E. BLOCKCHAIN-BASED MECHANISM IN FL

Blockchain can be incorporated in developing privacy-preserved model sharing [193] through a tamper-proof ledger to improve transparency. FL architectures such as P2P FL can incorporate blockchain with techniques such as SMC to make scalable and fault-tolerant defenses against attacks through consensus mechanisms [193], [194]. It can also provide incentive mechanisms for honest clients for their trustworthiness and encourage them to high-quality model updates [71]. However, issues such as latency [195] and computational costs [196] for mining and validation are seen as trade-offs when integrating blockchain.

When considering privacy-preserving FL for IoT and edge computing with blockchain, work in [71] focuses on blockchain-based privacy-preserving FL for IoT devices ensuring secure model updates. Authors in [88] introduce a decentralized privacy-preserving framework using blockchain and FL in fog computing, while [197] proposes a privacy-preserving framework using FL and blockchain for IoT healthcare data. Additionally, [198] discusses integrating FL and blockchain for privacy protection in IoT, [199] proposes a multi-layered security FL platform for IoT using blockchain, [200] focuses on blockchain-enabled FL for privacy-preserving deep learning in industrial IoT systems and [201] discusses the use of blockchain and FL in healthcare IoT systems for privacy and fraud prevention. For privacy-preserving FL in vehicular networks using blockchain, [202] proposes a blockchain-based FL scheme for privacy in the Internet of Vehicles (IoV), [203] proposes a blockchain solution for privacy-preserving FL in IoV, ensuring secure updates. Reference [204] provides a comprehensive survey on blockchain and FL integration in vehicular IoT networks, [205] discusses a blockchain-based privacy-preserving FL system for detecting cyber threats in intelligent transportation systems and [206] proposes "ShareChain," a blockchain-enabled model for secure patient data sharing using FL in healthcare.

For blockchain-enabled privacy-preserving FL in healthcare, authors in [207] focuses on blockchain-enabled FL for privacy in healthcare systems. For privacy-preserving and verifiable FL using blockchain, authors in [208] present a blockchain-based, privacy-preserving, and verifiable FL method, a verifiable blockchain-based FL approach is proposed in [209], ensuring secure model updates. Authors in [210] introduce a Byzantine-robust, privacy-preserving FL system using blockchain, and the paper in [211] discusses a blockchain-based reputation-aware FL system for enhancing trust. For blockchain-enabled FL with decentralized learning, the paper in [212] proposes a blockchain-based FL model for privacy-preserving traffic flow prediction, authors in [213] integrate blockchain and FL for privacy-preserving mobile crowdsensing, the paper in [214] presents a blockchain-enabled FL design for privacy preservation in decentralized environments, authors in [215] introduce a privacy-preserving blockchain-enabled FL model for B5G-driven edge computing, the paper in [216] proposes a privacy-preserving blockchain-based FL system for large-scale decentralized machine learning and the paper in [217] proposes "Artificial Identification," a novel privacy framework for FL based on blockchain. Finally, opportunities and challenges in FL and blockchain integration are highlighted in [38] to explore the overlap of FL and blockchain in edge computing and discuss challenges and opportunities.

F. OTHER POSSIBLE PRIVACY ENHANCING SOLUTIONS

Other notable mechanisms for FL include solutions such as:

- Federated knowledge distillation - transferring knowledge from a fully trained model to an alternative model [218]. This can prevent the sharing of original model parameters; instead, knowledge is shared through the alternative model [41]. However, the reduction in efficacy or the loss of knowledge is a problem to be addressed, and designing effective transfer models is another challenging concern [219].

TABLE 7. Summary of main privacy preserving techniques in FL, their methodology and limitations.

Privacy Mechanism	Methodology	Advantages	Limitations
Differential privacy	Add plausible deniability for the data to carry actual details of data owners [225]. Use perturbation-based techniques on data or models during the FL process by adding noise.	Prevents local model overfitting [226]. Provides a guarantee with quantifiable privacy level with noise addition to maintaining trust in the service [226]. B5G/6G network transmission can itself induce noise without additional computation for Over the Air FL [227].	Reduction of model utility due to the impact of noise [180], [181]. The original model is unable to be recovered due to the addition of perturbations.
Multiparty computation	Split the model to secret components [173] and share among multiple parties to jointly compute aggregation function. Use a chain of clients to partially aggregate model [17].	Does not cost accuracy/utility drop in the aggregated model for service providers [185]. Original models can be recovered when needed.	High local computation and communication overhead that increases network traffic among clients can affect users' QoS [185].
Homomorphic encryption	Perform computable functions on encrypted data [189]. Encrypted models can be aggregated without knowing the original model parameters.	Strong privacy guarantee due to encryption of model parameters. No disruption to the overall model utility; beneficial for 6G service providers [190], [191].	High complexity and computation cost in operations [191]. Larger ciphertext requiring high memory capability and high transmission cost [191]. Bounded user count and the inability to perform HE on multikey encrypted data [189], [191].
Federated knowledge distillation	Transfer knowledge from a fully trained model to a small model [222].	Mitigate inference and data reconstruction attacks as original model information is not directly sent.	Loss of knowledge from the original model and difficulty of designing effective transfer models [219].
Robust aggregation	Detection of malicious client updates during the aggregation process [222].	Filter out anomalous clients, such as backdoor poisoned models, before aggregation.	Erroneously classify benign client updates as malicious and eliminate honest updates. Difficulty in distinguishing malicious clients from non-IID clients [223].
Blockchain-based mechanisms	Blockchain can be integrated as a tamper-proof ledger [193]. Decentralized P2P FL uses Blockchain to aggregate models with a consensus mechanism [193], [194]	Provides practically tamper-proof operations and storage for models and transactions among clients. Incentive mechanisms to the clients for participation and trustworthiness [71].	Can introduce latency in transaction confirmation in real-time collaboration among clients [195], which can affect user application QoS. Depending on the consensus, the computational costs for mining and validation could be high [196].
Trusted execution environments	Model parameters are hidden from adversaries during aggregation running on trusted server environments [224]	Opt out of the possibility of an outsider inferring from clients during aggregation. The service provider will be fully responsible for the privacy of client models.	Does not consider the reliability and trustworthiness of client models.

- Robust aggregation - robust aggregation techniques can play a pivotal role in addressing critical privacy concerns such as backdoor poisoning [220], [221] in the training phase of FL for B5G/6G. Robust aggregation methods incorporate mechanisms to detect and filter out anomalous or adversarial contributions [222], ensuring that the collaborative learning process remains resilient against privacy breaches, thereby safeguarding the global model's integrity of the service provider. An issue that may be concerning is the possibility of filtering out honest updates mistakenly categorized as malicious, thus losing the possibility of aggregating important contributions. Especially for non-IID clients, FL robust algorithms can struggle to detect poisoners from honest clients [223].
- Trusted Execution Environments (TEE) - TEE can be incorporated in local model training and on servers for secure aggregation, such that model parameters are hidden from adversaries [224]. This method helps mitigate inference by an external attacker on clients or the aggregator. However, TEE assumes the availability of honest clients for aggregation while the aggregator properly uses TEE to establish secure communication with the clients. This may only be applicable to limited trusted entities.

TABLE 8. Privacy solutions and their applicability in addressing the issues in FL.

Privacy Issue	Addressed privacy issues						
	SMC	*DP*	*HE*	*KD*	*RA*	*BC*	*TEE*
Eavesdropping	✓	✓	✓	✓			
Unauthorized access						✓	✓
Unethical analytics	✓	✓	✓	✓			
Lack of standardization		✓				✓	✓
Model memorization	✓	✓		✓			
Training phase attacks					✓	✓	
Inference phase attacks	✓	✓	✓	✓			✓

KD - Knowledge Distillation, RA - Robust Aggregation, BC - Blockchain

A summary comparison of these discussed privacy solutions is given in Table 7, including their advantages and limitations. Furthermore, Table 8 provides the applicability of each solution to ameliorate the issues in FL. In addition, Figure 8 presents information on where the solutions are best suited to be implemented at the 6G vision architectural layers.

All these solutions have strengths and limitations. The trade-offs may be evaluated, especially when applied to resource-constrained B5G/6G IoT environments, considering

the utility and practicality of implementing the solutions with limited resources.

G. PERFORMANCE TRADE-OFFS OF PRIVACY ENHANCEMENT MECHANISMS

Individual privacy mechanisms have their unique trade-offs when practically implementing them. However, these issues will impact the underlying 6G network performance as well. Following problems can be identified with privacy-preservation techniques on large-scale FL implementations, which would affect the model training life-cycle of FL and put a stress on the 6G network:

1) COMMUNICATION OVERHEAD

One of the major trade-offs against the implementation of privacy-enhancing mechanisms in FL within the context of 6G is that techniques such as SMC require heavy exchange of data, with many steps of encryption and decryption involved [228], [229]. This significantly inflates the communication overhead. Furthermore, when DP adds noise into model updates, it makes the FL system run more iterations to achieve the same level of accuracy without privacy. This increased traffic can further strain the resources of the 6G network, especially in scaling up to millions of IoT devices. While 6G will come with ultra-high data rates and low latency, privacy mechanisms indeed challenge the efficiency of FL by consuming more bandwidth and causing possible delays, hindering the real-time decision-making process in applications sensitive to latency, for instance, driving autonomously or monitoring healthcare remotely.

2) MODEL UTILITY DEGRADATION

Several privacy-enhancing mechanisms in FL often lead to a decrease in model accuracy. DP adds random noise to model updates to obfuscate individual data contributions, reducing the likelihood of re-identification and introducing inaccuracies in the learning process. For 6G networks, which will process data from a diverse range of devices, such as IoT sensors and edge devices, this loss in accuracy could have significant consequences, particularly for applications that require high precision, such as predictive maintenance in smart factories or personalized healthcare systems. The challenge is to balance the degree of privacy protection with an acceptable level of accuracy, as overly stringent privacy measures may render models less effective in practice, undermining the potential of 6G to enable AI-driven automation. In [230], the accuracy of FL models is heavily penalized with the Gaussian DP, where the accuracy of the aggregated models without DP reaches over 90%, while when using DP, it does not converge the models, and the overall accuracy remains less than 10%. Figure 9 provides the overall accuracy differences over 10 FL iterations as presented in [230]. It shows that the model does not tend to converge if high DP is applied. However, without any DP, it can converge well. Furthermore, the time taken to run the local epochs with DP is significantly high compared to a scenario with no privacy.

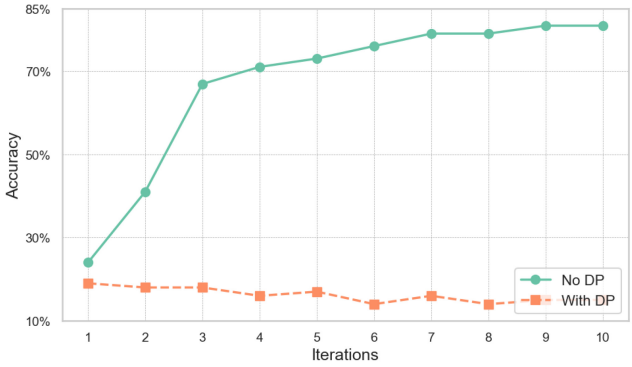

FIGURE 9. No privacy vs. with DP over FL training [230].

3) ENERGY CONSUMPTION

Energy consumption is a significant concern in FL as the iterative process of local model training and frequent communication of model updates between numerous edge devices and central servers can lead to substantial energy usage [77]. This issue is intensified in 6G environments, where resource-constrained devices like IoT sensors and mobile devices are prevalent, making energy efficiency critical for prolonged operation. With millions and billions of devices, a small percentage of increased energy consumption will heavily impact the global energy demand and could potentially impact the environment and cause a heavy increase in costs for organizations and states. Moreover, the incorporation of privacy-preserving techniques such as DP and HE increases the demand for computation [228], [231], further elevating energy consumption on edge devices. Addressing these challenges requires the development of energy-efficient FL algorithms, optimized communication protocols, and energy-aware scheduling strategies to minimize energy expenditure without compromising learning performance or privacy in 6G networks.

4) COMPUTATION COMPLEXITY

Privacy-preserving mechanisms like HE and SMC introduce substantial computational complexity [228], [231]. These techniques are computationally expensive because they require additional cryptographic operations, which can significantly slow down the training process, especially when deployed on resource-constrained edge devices. As 6G moves towards edge computing and distributed intelligence, FL will rely heavily on devices with limited computational power, such as IoT sensors or smartphones. Implementing privacy mechanisms in such devices could reduce the overall system's efficiency and scalability. Moreover, since 6G is expected to handle vast amounts of data in real-time, the added computational burden might compromise the network's ability to manage time-sensitive tasks like traffic control or industrial automation.

5) SCALABILITY ISSUES

The scalability of FL in 6G networks is challenged by privacy mechanisms, particularly when deployed in large networks with thousands or millions of devices. Techniques such as HE and SMC become less efficient as the number of participants grows due to the need for increased cryptographic operations and more complex secure communication rounds. Moreover, computation costs on robust aggregation algorithms that inspect each model update can drastically increase over larger number of clients [221]. As 6G aims to support massive device connectivity, especially in the context of IoT and edge computing, scalability is a crucial factor. Implementing privacy mechanisms across such vast networks without compromising performance will be difficult. The increased computational and communication overhead may limit the capacity of FL systems to scale while maintaining strong privacy guarantees, which could reduce the effectiveness of large-scale AI-driven applications.

6) IMPACT ON INTERPRETABILITY

Implementing privacy-preserving techniques such as DP, HE, and SMC in FL for 6G networks can significantly impact model interpretability and explainability due to the added complexity of privacy preservation. These techniques often introduce additional obfuscation to safeguard user data, which can obscure the internal workings of ML models. For example, as we discussed, DP adds noise to model updates or outputs to prevent the leakage of individual data points, potentially it makes harder to understand how individual and specific features influence the model's predictions, which can lead to difficulties in understanding the model behaviours and justify its outputs [232]. HE and SMC enable computations on encrypted data without revealing the underlying inputs, limiting access to intermediate computations that are often used for interpretability analyses. Moreover, the decentralized nature of FL means that training data remains on local devices, reducing transparency and making it challenging to perform traditional interpretability methods that rely on direct access to data and model parameters. This impact on interpretability underscores the need for developing new techniques and tools that can provide insights into model behavior without compromising privacy.

7) IMPACT ON FL ROBUST DEFENSES

Integrating privacy-preserving techniques into FL for 6G networks introduces significant challenges to implementing robust defenses against adversarial attacks. While these techniques enhance user privacy by obscuring or encrypting data and model updates, they can also hinder the detection of malicious activities like model poisoning or backdoor attacks. For instance, DP adds noise to model updates to protect individual data, which can diminish the effectiveness of anomaly detection methods that rely on precise gradient information to identify corrupt updates, making it difficult to differentiate between honest or adversarial clients. Furthermore, techniques like DP are vulnerable to model poisoning attacks, as these DP functions are easy access to perform mutations in the model [233]. This makes the attacks more stealthy and difficult to be detected by robust algorithms. Moreover, HE and SMC encrypt computations and communications, limiting the aggregation server's ability to inspect individual model updates for irregularities. This encryption prevents the application of traditional robust defense mechanisms that require access to raw gradients or parameters to function correctly. As a result, the use of DP, HE, and SMC in FL necessitates the development of novel defense strategies that can operate under these privacy constraints, ensuring that FL systems remain secure against adversarial threats while upholding the stringent privacy requirements of 6G networks.

Table 9 provides a summary of the discussed performance trade-offs and the potential solutions that can be applied to mitigate them.

VI. PRIVACY PRESERVATION AT DIFFERENT 6G LAYERS

When equipped with proper privacy-enhancing mechanisms, FL can be a powerful distributed PPML for future networks. The following subsections discuss privacy benefits when using FL for B5G/6G-related applications and services at each 6G vision architecture layer.

A. PRIVACY PRESERVATION AT THE B5G/6G DEVICES

FL can provide a significant advantage for local client devices for maintaining the privacy of private and sensitive data, giving users more control. FL can also be used over many end-user devices, mobile phones, wearables, sensor equipment, and IIoT-based equipment, which provides more possibility for addressing privacy issues for a wide range of user bases across numerous applications that require ML. It promotes data localization, where massive data generated from B5G/6G devices will remain at the individual devices. In many jurisdictions, data protection regulations are becoming more stringent for end devices such as IoT [234]. FL can help organizations comply with these regulations by minimizing the need to collect, store, and transmit sensitive data from the devices they provide the service to. It inherently reduces raw data sharing, thus reducing the overhead of computationally expensive encryption techniques. However, as the device layer can be considered highly vulnerable to attacks, it is important to implement privacy-enhancing techniques at the devices. Local DP [235] added at the device level can further increase the privacy of local models shared by the clients. Furthermore, lightweight encryption techniques [236] and increased security measures at user-level access can be employed to minimize the risks of privacy leakages.

B. OVER THE AIR FL FOR NETWORK PRIVACY

OTA FL performs aggregation by signal superposition of wireless multiple-access channels [227]. The work in [237] presents an OTA FL with anonymized devices for transmission. Here, the devices can simultaneously and efficiently

TABLE 9. Performance trade-offs of privacy enhancement mechanisms and possible solutions

Trade-off	Description	Impact on 6G Networks	Possible Solutions
Communication Overhead: Increased bandwidth and delay	Techniques like SMC require heavy data exchange with multiple encryption/decryption steps [228], [229], significantly inflating communication overhead. DP requires additional iterations due to noise and increasing traffic.	High bandwidth usage and potential delays could hinder real-time decision-making in latency-sensitive applications, such as autonomous driving and remote healthcare monitoring.	1. Use lightweight cryptographic methods (e.g., partial homomorphic encryption). 2. Optimize data compression and aggregation techniques to reduce data volume. 3. Prioritize privacy settings dynamically based on network congestion.
Model Utility Degradation: Reduced Accuracy	Privacy mechanisms such as DP add noise to model updates, reducing accuracy and affecting tasks requiring high precision [230].	Impacts the effectiveness of AI-driven automation in 6G, with potentially drastic accuracy reductions (e.g., Gaussian DP penalties accuracy significantly).	1. Implement adaptively adjusted privacy levels based on the required accuracy. 2. Use of masking and privacy-by-aggregation as alternative methods. 3. Use post-processing correction methods to refine model outputs.
Energy Consumption: Increased Power Usage	Energy consumption in FL are high due to iterative local training and frequent communication; privacy mechanisms like DP and HE increase computational demands [77], [228], [231].	Significantly increases energy usage in 6G networks, affecting the battery life of devices and raising operational costs, which can hinder large-scale FL deployment and sustainability efforts.	1. Employ energy-efficient cryptographic algorithms. 2. Utilize edge caching and efficient scheduling to reduce redundant computations.
Computation Complexity: Slower Processing & Scalability	Privacy-preserving techniques like HE and SMC are computationally intensive [228], [231], requiring significant cryptographic operations, slowing training, especially on resource-limited devices like IoT sensors.	Edge devices may face reduced efficiency, impacting the network's ability to handle time-sensitive tasks (e.g., traffic control, industrial automation).	1. Select the privacy-enhancing techniques by evaluating the resource availability in the network infrastructure. 2. Offload computation to more capable nearby devices or edge servers when possible. 3. Develop specialized hardware accelerators for lightweight cryptographic functions.
Scalability Issues: Limited System Expansion	Privacy techniques face efficiency issues in large-scale networks due to increased cryptographic operations. Robust aggregation algorithms become computationally expensive with more clients [221].	Compromises the capacity of 6G FL systems to scale efficiently, challenging large-scale AI applications.	1. Use decentralized aggregation models to distribute workload evenly. 2. Apply hierarchical FL models to group and manage data updates. 3. Implement adaptive privacy policies based on network size and client capabilities.
Impact on Interpretability: Reduced Explainability	Privacy techniques like DP, HE, and SMC add complexity and obfuscation to FL models, reducing interpretability and explainability [231].	Limits transparency of AI models in 6G, affecting trust and adoption in critical applications that require XAI, necessitating new tools for insight without compromising privacy.	1. Integrate explainable AI methods within privacy-preserving frameworks. 2. Design interpretable models that inherently support explainability without compromising privacy.
Impact on Robust Defences: Reduced Defense performance	Privacy-preserving techniques like DP, HE, and SMC in FL hinder the detection of adversarial attacks by obscuring data, making it difficult to identify malicious activities such as model poisoning [233].	Compromises the security and reliability of AI services in 6G networks as adversarial threats become harder to detect, necessitating new defense strategies compatible with privacy measures.	1. Develop adaptive, robust defense mechanisms compatible with privacy constraints. 2. Incorporate approaches to differentiate malicious clients by considering the model output behavior. 3. Integration of approaches for detecting minority groups and attributions with non-IID data distributions.

transmit the uncoded model updates using the available spectrum. Here, uncoded refers to the transmission of models without considering error-correction codes in case of noise disruptions in the channel. In the uncoded transmission of FL implementation, the induced channel noise added to the original updates can be used directly as an advantage by considering it as a free privacy-inducing mechanism [238]. To measure the noise level in a differentially private manner, the authors in [238] use signal-to-noise ratio (SNR) to maintain an acceptable level of learning performance. We will further discuss differential privacy in Section V. Adding quantifiable noise naturally through this mechanism can reduce any extra computation costs for manually applying noise via differential privacy algorithms. Therefore, OTA FL

TABLE 10. Summary of related work for privacy of FL and its applicability on 6G

Ref.	Key Contributions	Privacy Issues	Solutions	Applicability for 6G			
				Device Layer	RAN and Edge	Control Layer	Application Layer
[161]	This work evaluates the Man-in-the-Middle attacks on Bluetooth-based client devices.	✓		✓	✓		
[163]	Provides an assessment of privacy preserving techniques on FL, including DP, HE, blockchain and SMC.	✓	✓	✓	✓	✓	
[167]	Investigates on privacy issues in IoT and proposes countermeasures against privacy threats, including authentication control, intrusion detection and privacy-by-design for IoT.	✓	✓	✓		✓	
[145]	Provides a taxonomy of privacy threats in FL systems, including data privacy attacks like inference, model inversion and reconstruction attacks, and model performance-based threats like poisoning.	✓	✓	✓	✓		
[41]	Discusses privacy issues in FL and potential solutions, including adversarial training, DP, SMC and hybrid techniques, and costs of implementing privacy solutions.	✓	✓	✓	✓		✓
[152]	Addition of backdoor-based poisoning attacks on FL.	✓					
[174]	Uses Local DP to defend against privacy attacks on FL.		✓	✓			
[175]	Discusses the use of the DP-SGD algorithm during the training of the ML models to gradually apply controlled noise over local iterations.		✓	✓			
[173]	Develops an SMC-based aggregation against gradient leakage in FL systems.	✓	✓	✓	✓		
[186]	Provides an application of self-canceling noise masks for local iterations and global rounds in FL to defend against inference and deep leakage attacks.	✓	✓	✓	✓		
[189]	Discusses different homomorphic encryption schemes and their technical implementations for secure communication and aggregation without exposing original model information.		✓	✓	✓		
[218]	Uses federated model distillation to transfer knowledge from a fully trained model to an alternative model to hide original model parameters from third parties.		✓	✓	✓		✓
[221]	Provides an explainable robust aggregation framework for FL against data poisoning attacks and privacy threats from poisoning-based inference attacks.	✓	✓	✓	✓		✓
[194]	Uses blockchain to develop a P2P FL system that performs multi-party ML and defends against privacy attacks.	✓	✓	✓	✓	✓	
[224]	Develops a PPFL framework using TEE for both client and server-side privacy preservation and protection from privacy-related attacks.	✓	✓	✓	✓		

can be considered an attractive privacy-preserving strategy for wireless 6G networks when aggregating FL models over the network.

C. PRIVACY PRESERVATION AT THE B5G/6G EDGE AI

Limiting data exposure [239], [240] to external parties is a possible way of mitigating unintentional privacy leakages. One of the strategies to implement this in 6G is by bringing AI closer to the IoT edge [241], [242], where data and decisions are shared within the closer proximity of the data owners or the end users. This can be referred to as *edge AI* [243], [244]. With this approach, it will be easier to manage data privacy since they will be shared within a limited scope. Future B5G/6G networks are expected to include edge AI as a key enabler for greatly improved QoS and low latency communication [245], [246]. However, if centralized client-server-based ML is considered to train edge AI models, data from IoT sensors and user devices may still be transmitted to the edge server, which can lead to privacy leakages. Therefore, the question of achieving ML model training while keeping data private needs to be answered.

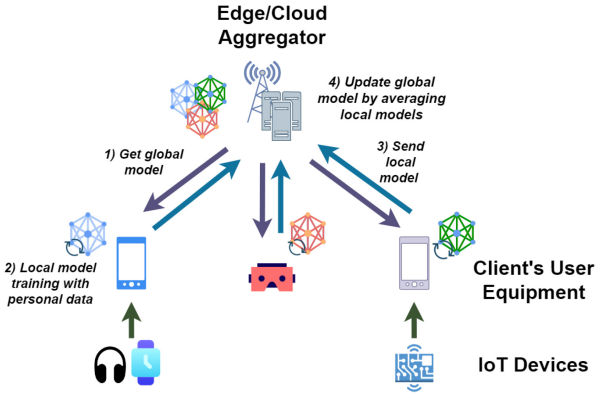

FIGURE 10. Aggregator and client-based FL system with IoT.

To address this question, FL is emerging as a PPML solution [7], which can be implemented at the edge. It aims to provide high-quality ML models while maintaining data privacy. Since data used in FL does not need to be moved from its original source, and the ML models are trained locally near the data source and aggregated remotely to create a global model, data privacy is protected with safety within the user premises. Thus, multiple IoT devices can act as workers to communicate with the edge server aggregator without sharing actual datasets [38]. Many recent works show the feasibility of FL to be implemented at the IoT edge as a privacy-preserved edge AI technique [46], [73], [247], [248]. A typical FL system with IoT clients at the edge and an aggregator is shown in Fig. 10.

Here, the aggregator can be either an edge or a remote cloud server. It can also have hierarchical model updates, where models will be aggregated at multiple levels of edge and cloud [85]. FL is designed to protect the privacy of individuals who contribute to the training process. Thus, 6G can utilize this distributed ML technique at the edge of AI to fulfill the requirements of ML-associated service functionalities while preserving privacy.

D. ENHANCING PRIVACY WITH FL-DRIVEN INTELLIGENT NETWORK MANAGEMENT AND ORCHESTRATION

The privacy of AI-driven network management tasks can be enhanced using FL. When managing multiple services, it may be necessary to make automated decisions based on the properties of services. Exposing them directly to the management layer can create a risk of leaking sensitive and private business data from these services since these management and control components can get compromised, be honest but curious, or malicious. This can create a lack of trust among service providers in the upper layer to share such information directly. In such cases, FL can be provided as a solution by facilitating distributed model training without sharing private data. For example, the work in [59] uses FL for predicting network slice performances where models trained on service-oriented privacy-sensitive Key Performance Indicator (KPI) are shared by slice managers without directly exposing KPIs to the slice orchestrator. Another requirement in achieving zero-touch network management is to automate the detection of any malicious entities in the networks. For this, ML models that can detect anomalies in network traffic may be required; however, they could contain sensitive information if the individuals or devices who consume these services can be traced. Therefore, FL can provide an alternative approach by allowing privacy-preserved local training of such detection and defense models based on individual data [99], [249].

E. PRESERVING PRIVACY FOR 6G ASSOCIATED SERVICE APPLICATIONS WITH FL

Many applications serving as B5G/6G-based services can use FL to manage their internal data and collaborate among multiple services. For example, vertical FL can facilitate joint training of ML models based on data with fewer overlapping features. This may resemble a scenario where multiple services are provided by different applications for the same consumer base. It could be beneficial for applications like Metaverse, where numerous services should collaborate at high speeds to maintain better QoS and provide a seamless experience to users. FL done by a distinct set of clients is also termed as cross-silo FL [250]. One feature that could arise in cross-silo FL is the relatively small number of collaborators compared with cross-device FL, which can be millions of devices. Therefore, proper privacy mechanisms are an essential requirement for the models that organizations contribute to the FL process. Another key issue emerging here is the central server, where no party involved in sharing the models can no longer trust the other collaborators unless the services are provided by the same organization. In such cases, many approaches are available that perform decentralized aggregations, and blockchain is often used for transparency and decentralized control. Examples include the work in [251], which employs an FL framework for multiple organizations with decentralized aggregation and blockchain for verification and reward based on the quality of model updates.

VII. FEDERATED LEARNING PRIVACY IMPLEMENTATION IN 6G USE CASES

Integrating FL Privacy mechanisms such as DP, HE, and SMC techniques in 6G networks addresses key privacy challenges. This section outlines three specific use cases demonstrating how these technologies can be applied in 6G networks.

A. FEDERATED LEARNING FOR REAL-TIME CROWD SENSING IN 6G-ENABLED ULTRA-DENSE ENVIRONMENTS

In ultra-dense environments, 6G's high bandwidth and low latency support FL for real-time crowd sensing [252]. Devices train models locally on sensed data, sending only encrypted model updates to an edge server, avoiding raw data sharing. This distributed learning approach reduces the

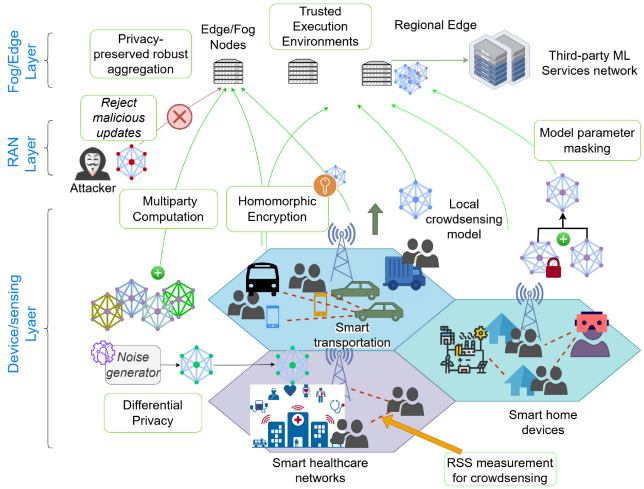

FIGURE 11. Crowdsensing among multiple domains and securely sharing the FL models.

risk of privacy breaches and minimizes the network load, as raw data transfer is replaced by periodic model updates. The edge servers can aggregate these updates from numerous devices, building a global model that reflects crowd insights without compromising individual privacy [253]. Scenarios like crowd density estimation, environmental monitoring, or public safety alerts can be developed via this FL-enabled approach.

Figure 11 provides an overview of the mobile crowdsensing-based FL in a 6G network. Multiple domains with highly dense networking environments like urban smart vehicle traffic, public offices or private home complexes can utilize FL to collect signal data like Received Signal Strength (RSS) locally and train FL models without exposing exact information about the signal sources. Moreover, DP can be applied to device model updates, adding noise to prevent re-identification. HE secures model updates in transit, enabling aggregation without decryption and ensuring robust crowd analytics and privacy.

1) IMPLEMENTATION CHALLENGES

Implementing FL with added privacy-enhancing mechanisms like DP and HE in a real-time crowd-sensing environment presents several challenges. Due to the limited processing power of many user devices, especially smartphones, applying DP and HE may significantly increase computational demands and latency, potentially impacting the real-time responsiveness required for crowd management. HE's intensive computations can slow down edge-device interactions, particularly in ultra-dense settings where many devices simultaneously transmit model updates, increasing congestion at the edge server. Additionally, the noise introduced by DP can reduce the accuracy of crowd predictions, making it difficult to achieve high-quality insights. Maintaining synchronized encryption standards across devices complicates seamless data aggregation at the edge. Moreover, the differences in hardware and mobile devices in such

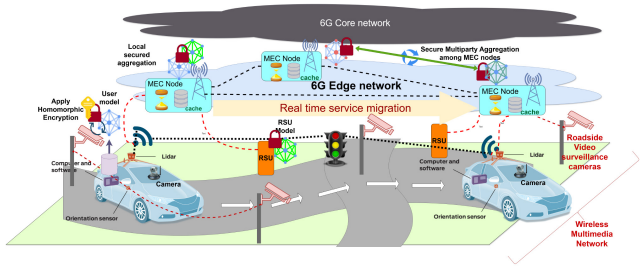

FIGURE 12. FL-based secure and private model sharing of vehicles and RSUs with MEC.

diverse environments can make it further difficult to enable a unified approach of encryption standards and processing capabilities, which further complicates data aggregation, limiting the scalability and responsiveness in real environments.

2) STRATEGIES TO ADDRESS CHALLENGES

To address these challenges, optimized encryption protocols specifically designed for mobile devices can be employed to reduce processing load. Offloading some computations to nearby 6G-enabled edge nodes can help mitigate latency, as these nodes can handle more intensive data processing. Adaptive privacy mechanisms could also be implemented, adjusting the level of DP noise based on crowd density and ensuring the right balance between data accuracy and privacy. Utilizing specialized hardware, like mobile-optimized encryption accelerators, could also help in processing encrypted updates faster.

B. FEDERATED LEARNING FOR 6G-ENABLED REAL-TIME AUTONOMOUS VEHICLE AND TRAFFIC MANAGEMENT

The ultra-low latency of 6G networks enables real-time management of autonomous vehicles and traffic systems using FL to create adaptive AI models [252]. In this scenario, autonomous vehicles, roadside units (RSUs), and mobile edge computing (MEC) nodes collaborate to train local models on traffic and sensor data [254], sending only encrypted model updates to a central model without transferring raw data. This decentralized learning process allows for real-time traffic predictions and collision avoidance strategies while ensuring data privacy.

As shown in Fig. 12, MEC nodes and RSUs support Federated Learning by aggregating model updates from autonomous vehicles and other roadside sensors, such as LiDAR and video surveillance cameras. These updates are encrypted using HE, allowing MEC nodes to aggregate data without accessing unencrypted information. SMC ensures that model updates from different sources (e.g., vehicles and RSUs) are aggregated privately, maintaining the confidentiality of each data source. This collaborative approach in 6G networks allows for efficient, privacy-preserving real-time traffic and vehicle management.

1) IMPLEMENTATION CHALLENGES

Implementing FL with HE and SMC in autonomous vehicle and traffic management raises significant challenges, primarily due to the ultra-low latency requirements essential for safety-critical applications. The computational overhead of HE can delay data processing, especially on devices with limited resources like RSUs. Additionally, SMC requires secure and synchronized data communication between multiple parties, which can be challenging in high-speed, mobile environments with fluctuating network quality. Ensuring data integrity and security during transmission over open network channels adds another layer of complexity.

2) STRATEGIES TO ADDRESS CHALLENGES

To mitigate these challenges, leveraging the dedicated infrastructure of 6G networks, such as MEC nodes located near RSUs and autonomous vehicles, can reduce latency by offloading complex computations to powerful edge nodes. Hardware accelerators, including GPUs and specialized encryption chips in MEC nodes, can enhance the processing speed of HE and SMC. Implementing adaptive encryption, where only essential or sensitive data is fully encrypted, may also balance processing load and data security. Continuous synchronization protocols across 6G-connected devices will ensure the secure and efficient aggregation of model updates in real-time.

C. FEDERATED LEARNING FOR INTELLIGENT TRAFFIC MANAGEMENT IN 6G-ENABLED OPEN RADIO ACCESS NETWORKS

Open Radio Access Networks (ORAN) leverage the flexibility of 6G to support scalable and efficient network management. In this scenario, FL is used to develop intelligent traffic management models across distributed ORAN nodes. Each ORAN node, such as base stations and edge computing units, trains a local model on network traffic data, adjusting parameters for load balancing, congestion control, and resource allocation. These local models then send encrypted updates to a central controller for aggregation, enabling a global model without needing access to raw data from individual ORAN nodes.

As shown in Fig. 13, MEC nodes within ORAN collect and aggregate model updates using privacy-preserving methods. HE can be applied to these updates, allowing the MEC nodes to perform computations on encrypted data without decrypting it. SMC further enhances privacy by ensuring that updates from various ORAN nodes can be aggregated securely, preventing any single entity from gaining full access to the underlying data. This approach enables the development of adaptive, real-time traffic management models that respect user privacy and network security.

1) IMPLEMENTATION CHALLENGES

Implementing FL in ORAN with HE and SMC faces several challenges, primarily due to the need for ultra-low latency in handling real-time traffic data. HE is computationally intensive, which can delay traffic management responses if not optimized for edge devices. Additionally, maintaining synchronization across multiple ORAN nodes that operate independently in diverse geographic locations can be difficult. Furthermore, SMC requires reliable and secure communication channels, which can be challenging in ORAN environments with potentially fluctuating connectivity.

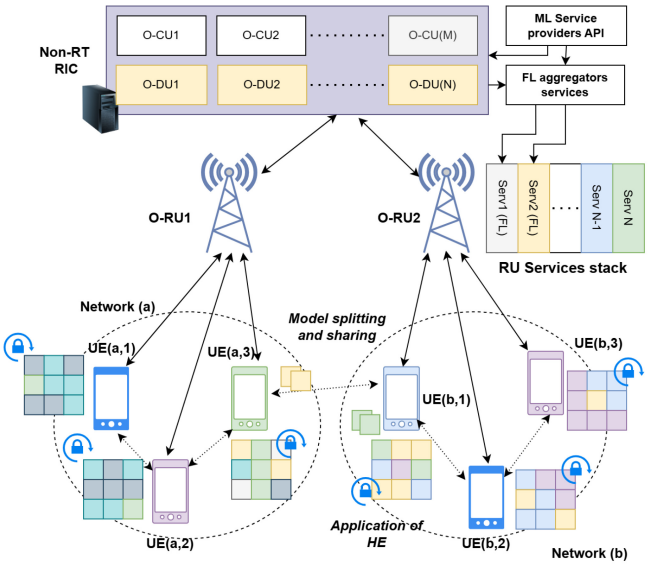

FIGURE 13. ORAN-based FL services and model aggregation over the network.

2) STRATEGIES TO ADDRESS CHALLENGES

To address these challenges, using hardware accelerators like GPUs and FPGAs in MEC nodes can speed up HE operations, ensuring that data remains encrypted without compromising processing time. Hybrid encryption schemes, where only high-priority data is fully encrypted, can also reduce computational load. For synchronization, adaptive aggregation protocols across ORAN nodes can help maintain model consistency and allow for seamless integration of model updates. Establishing robust, high-speed communication links in the 6G infrastructure further supports the secure and timely aggregation of data, ensuring that ORAN-based traffic management models remain responsive and effective.

VIII. FEDERATED LEARNING IMPLEMENTATION TOOLS FOR 6G NETWORKS

The integration of FL into 6G networks requires advanced tools that support large-scale distributed learning with robust security, scalability and efficiency. Several open-source frameworks have been developed to address the unique challenges of FL, including privacy preservation, high bandwidth, low latency, and adaptability to complex network architectures in 6G. Among these tools, *Flower* [255], *PySyft* [256], *TensorFlow Federated (TFF)* [257], *FATE* (Federated AI Technology Enabler) [258] and *NEBULA* [259] are known

for their contributions to FL. Each of these frameworks has specific advantages and limitations, depending on the use case and environment. Below, we compare and analyze these tools based on their core features, strengths and suitability for 6G network applications.

A. FLOWER (FL OPEN RESEARCH FRAMEWORK)

Flower is a highly flexible, open-source framework specifically designed for scalable and secure FL. With its focus on extensibility, Flower supports experimentation with different aggregation methods, privacy mechanisms, and client-server architectures.

- *Capabilities:* Flower is language agnostic and supports integration with popular machine learning libraries such as TensorFlow and PyTorch, which can enable easy customization across different devices and platforms in a 6G environment. It offers robust support for multi-device scenarios and scales efficiently across a large number of clients.
- *Security Features:* Flower does not natively include privacy-preserving features but is highly customizable and allows researchers to incorporate differential privacy, homomorphic encryption or secure aggregation methods.
- *Suitability for 6G:* Flower's scalable architecture is ideal for the massive device density expected at 6G. However, additional configurations are required to meet the specific 6G privacy and security requirements.

B. PYSYFT

PySyft, developed by OpenMined, is an FL framework based on PyTorch. It focuses primarily on privacy-preserving techniques such as secure multi-party computation SMC, DP and HE.

- *Capabilities:* PySyft offers comprehensive support for privacy-preserving computations, making it highly secure. It integrates seamlessly with PyTorch and allows developers to leverage PyTorch's machine-learning capabilities while ensuring secure data handling.
- *Security Features:* PySyft is characterized by its extensive built-in privacy tools, including SMC and differential privacy, which are essential for 6G's data security and privacy requirements.
- *Suitability for 6G:* PySyft's strengths lie in secure computation, but its lack of cross-platform compatibility and limited scalability make it less suitable for real-time, high-bandwidth applications across extensive 6G networks.

C. TENSORFLOW FEDERATED

TFF is an open-source FL framework from Google that builds directly on TensorFlow. TFF supports machine learning on decentralized data and focuses on cross-device and cross-silo federated learning.

- *Capabilities:* TFF is tightly integrated with TensorFlow and provides robust support for implementing federated learning algorithms in Python. It provides simulation capabilities to test FL applications in a controlled environment.
- *Security Features:* Although TFF supports basic privacy protection measures, such as differential privacy, it requires external libraries to implement advanced privacy protection techniques, such as homomorphic encryption and secure aggregation.
- *Suitability for 6G:* TFF is advantageous because of its high-quality machine-learning capabilities and simulation tools, which are useful in testing federated algorithms for 6G. However, the scalability and privacy features of TFF need to be improved to meet the requirements of a fully decentralized, large-scale 6G deployment.

D. FATE

FATE is a production-grade FL platform developed by Webank that provides comprehensive support for federated learning in various domains. It is designed to enable secure federated AI systems and is widely used in finance, healthcare and the IoT.

- *Capabilities:* FATE contains integrated modules for machine learning, data management and secure data exchange, making it ideal for enterprise-level applications. It supports both vertical and horizontal federated learning and enables flexible partitioning of data between nodes.
- *Security Features:* FATE supports privacy-preserving techniques such as SMC and federated encryption protocols. Its robustness in privacy protection makes it particularly suitable for highly regulated environments.
- *Suitability for 6G:* FATE's architecture is highly adaptable for secure and large-scale deployments and is, therefore, well suited for the multi-layered requirements of data transmission in 6G. However, its complexity may require additional optimizations for the real-time applications expected in 6G.

E. NEBULA (A PLATFORM FOR DECENTRALIZED FEDERATED LEARNING)

NEBULA is an open-source platform dedicated to decentralized, federated learning and aims to enable secure and efficient model training across distributed nodes without a central server. NEBULA can be used to meet the privacy and security requirements that are critical for large-scale 6G applications since it is designed to be flexible and scalable.

- *Capabilities:* NEBULA uses a decentralized architecture that enables seamless model training across different devices, making it ideal for the heterogeneous environments of 6G. NEBULA supports blockchain-based model validation, ensuring transparency and traceability while enabling secure cross-device computation for multiple parties.

TABLE 11. Comparison of federated learning tools for 6G networks.

Feature	Flower [255]	PySyft [256]	TensorFlow Federated [257]	FATE [258]	NEBULA [259]
Integration	TensorFlow, PyTorch	PyTorch	TensorFlow	Flexible across platforms	Decentralized platform
Security	Limited (extensible)	Strong (SMC, DP)	Moderate (DP)	Strong (SMC, encryption)	High (blockchain, decentralized verification)
Scalability	High	Moderate	Moderate	High	High (decentralized architecture)
Ease of Use	High	Moderate	High	Moderate	Moderate
Use Cases in 6G	IoT, Edge Computing	Secure IoT	Testing, Simulation	Financial IoT, Regulated Sectors	IoT, Smart Cities, Industrial IoT

- *Security Features:* NEBULA includes participant anonymity, decentralized aggregation and model validation via the blockchain. This improves data protection by reducing dependence on central servers and ensuring that model updates remain verifiable and tamper-resistant.
- *Suitability for 6G:* NEBULA's decentralized structure fits well with the distributed, high-density 6G networks. It is particularly suitable for IoT, smart city applications and other use cases that require robust data privacy and security across different and potentially untrusted nodes.

F. COMPARISON SUMMARY

Each of these tools offers unique advantages for implementing FL in 6G networks as shown in Table 11. Flower is ideal for scalable environments with high device density, while PySyft excels at privacy-sensitive use cases. TensorFlow Federated provides an accessible environment for experimenting with FL models, and FATE is great for regulated applications that require robust privacy protection. NEBULA, with its blockchain-based, decentralized structure, is especially suited for privacy-focused and decentralized applications in 6G, such as IoT and smart city implementations. To meet 6G-specific requirements, these tools may need to be improved, especially in terms of real-time processing, ultra-low latency, and cross-layer privacy that matches the capabilities of 6G networks.

IX. LESSONS LEARNED AND FUTURE RESEARCH DIRECTIONS

In this section, we present the lessons learned from this survey and the emerging directions in this area of research.

A. FL FOR 6G PRIVACY

1) LESSONS LEARNED

Implementing FL in 6G networks can help gain several important insights. First, FL significantly improves data privacy by ensuring that sensitive data remains localized on devices, reducing the risk of data breaches and unauthorized access during transmission. This approach fits well with the high-security requirements of 6G applications in various sectors, such as healthcare, smart cities, and industrial automation. Secondly, integrating FL with other privacy-preserving techniques, such as blockchain and differential privacy, can further enhance security and create a layered defense against potential threats. Another key insight is the importance of secure and efficient communication protocols. The high data rates and low latency of 6G networks are essential for the timely and reliable aggregation of model updates so that AI-driven applications can work seamlessly and effectively. However, the deployment of FL in 6G may also bring some challenges, such as malicious 6G client devices, much faster access exploiting weak security, requiring robust access control mechanisms to prevent insider attacks, and AI-native infrastructure, which may bring the risk of attacks such as model poisoning or the injection of malicious aggregation updates by malicious entities. Finally, FL's adaptability as a versatile solution for different application areas has the potential for privacy protection in various 6G scenarios, from smart homes to autonomous vehicles.

2) REMAINING RESEARCH QUESTIONS

Despite the progress made, some research issues still need to be addressed in order to fully utilize FL for 6G privacy. These critical questions are as follows:

- How can we minimize bandwidth usage while maintaining model accuracy and timely updates, especially considering the huge number of connected devices in a 6G network?
- Can FL maintain its efficiency and security at large-scale, when millions of devices are involved in the learning process?
- How can we integrate quantum computing or advanced cryptographic methods to improve the security and performance of FL?
- What frameworks and guidelines are needed to ensure that the use of FL complies with global privacy standards and ethical considerations?

3) EMERGING AND FUTURE RESEARCH DIRECTIONS

To address the challenges in FL research, several techniques can be applied. Model pruning, gradient compression, and edge-based aggregation are some of the techniques that can

reduce bandwidth utilization by minimizing communication overheads. Hence, timely updates are guaranteed with the highest model accuracy. Hierarchical FL and adaptive sampling can ensure efficiency at large scales, while security can be enhanced using blockchain, among other decentralized methods. This integration of quantum computing with advanced cryptographic techniques, such as QKD and adversary-filtered HE, can further enhance the security of FL without performance compromise. Compliance with global privacy standards is needed through frameworks that include standardized privacy-preserving techniques like enhanced DP with utility trade-offs addressed, together with standardized ethical guidelines addressing issues such as data ownership and fairness across multiple jurisdictions. Methods can be scaled efficiently for FL in the complex landscape of 6G networks.

Future research on FL for 6G networks for privacy should focus on several promising directions. One area is the improvement of privacy-preserving techniques natively built into the FL process. Advancements in HE or SMC can provide additional layers of security and enable secure collaborative learning in 6G networks. Another direction is the development of lightweight FL algorithms specifically designed for resource-constrained IoT devices in 6G networks. These algorithms should strike a balance between computational efficiency and high privacy standards. Exploring hybrid FL models that combine centralized and decentralized approaches could also bring significant benefits and optimize both privacy and performance. In addition, the application of AI-driven anomaly detection systems can play a critical role in identifying and mitigating potential privacy threats in real time. The integration of FL with edge computing paradigms in 6G networks with demanding requirements is another crucial area of research that could improve processing capabilities and further reduce latency. Finally, interdisciplinary research involving data science/engineering, cybersecurity, and standardization/regulatory frameworks is essential to address the wider implications of privacy-preserving FL deployment in 6G networks and ensure that technological progress is aligned with societal needs and ethical standards.

B. KEY FL PRIVACY CHALLENGES IN 6G NETWORKS

1) LESSONS LEARNED

The privacy of B5G/6G-based services can be enhanced with the support of FL over all the vision layers of the 6G architecture. However, several privacy issues can be raised from FL itself due to the ML model's memorization nature and the attacks that occur with it. Many solutions for addressing these issues in FL are available and can address certain aspects. However, trade-offs exist in each of these solutions, which should be carefully assessed based on the expectation of the level of privacy, available resources, architectural layer, and the use case requirements.

Specifically, ML attacks such as inference and reconstruction attacks are notable concerns due to the model's memorization. During the training process, these attacks can occur, exposing sensitive data that the model has unintentionally memorized. Additionally, attacks can occur due to weaknesses in communication and model storage. These include threats from unauthorized access, analytics by third-party service providers, or exploitation of the lack of transparency in FL frameworks and standardizations.

Moreover, these threats can span across different layers in the 6G network. More vulnerabilities in the training process are likely to occur in the edge and sensing layers due to their proximity to data sources and the potential for direct data interception. Conversely, issues such as access control and data management would be more prevalent in the control and application layers, where higher-level data processing and decision-making occur.

Thus, ensuring robust privacy in 6G-based services using FL requires a comprehensive approach that addresses the unique challenges at each layer of the architecture. This includes implementing secure communication protocols, enhancing transparency and standardization in FL frameworks, and applying tailored privacy-preserving techniques that balance the trade-offs between privacy, resource availability, and functional requirements.

2) REMAINING RESEARCH QUESTIONS

The ongoing evolution of B5G/6G architecture, coupled with issues such as vulnerabilities, privacy threats and attacks, gives rise to the following research questions that need to be addressed:

- What are the architectural updates for the 6G and FL learning process that could potentially enhance the existing privacy protection and guarantees for FL?
- What new threat scenarios could emerge from architectural updates upon design and development?
- How can defense strategies and attack detection approaches be updated to properly test the impact of these threats?

3) EMERGING AND FUTURE RESEARCH DIRECTIONS

To address the research questions, novel architectural updates in 6G FL, such as Distributed Ledger Technologys (DLTs), federated analytics, and federated transfer learning, can be used to enhance privacy by securing model updates and reducing data sharing. Defense strategies must evolve to include decentralized trust management, quantum-resistant cryptography, AI-driven model verification, and game-theoretic defenses that dynamically adapt to emerging attack vectors. Such approaches can support to security of both data privacy and the integrity of FL systems in 6G.

Further research can thus be conducted to explore novel defense strategies that effectively balance these trade-offs while ensuring guaranteed privacy bounds. These strategies can be tailored to specific layers of the B5G/6G architecture, considering resource availability, the number of connected components, and the desired levels of privacy. Considering threat identification, new threat models should be developed,

and adversarial testing should be done on the models. Novel approaches for adversarial testing should be explored, such as the addition of perturbations to the models to evaluate the impact of attacks and assess the model's sensitivity to certain parameters or data types. This can help identify potential AI model biases and vulnerabilities. Furthermore, these testing methodologies can provide insights into the robustness of the models under various adversarial conditions, enabling the development of more resilient FL frameworks. Moreover, research should also focus on successfully quantifying the threats using metrics beyond the conventional ones, such as attack success rates and accuracy impact. This includes developing new metrics that can provide a more comprehensive understanding of the threats, considering factors like data leakage, privacy loss, and long-term effects on model performance. By adopting a broader set of evaluation criteria, researchers can gain deeper insights into the efficacy of defense mechanisms and the overall security capabilities of FL systems in B5G/6G networks.

C. PRIVACY ENHANCING MECHANISMS FOR FL IN 6G

1) LESSONS LEARNED

When considering privacy-enhancing mechanisms for FL in 6G networks, a common observation is the emergence of trade-offs when attempting to achieve privacy. For instance, popular perturbation-based techniques such as DP or noise addition often result in a trade-off with the overall utility of the model. This is inevitable in most cases because the noise added to protect privacy causes the model parameters to deliberately "forget" parts of their learning, thereby reducing model accuracy and effectiveness. Techniques like HE can preserve the original model configurations in an encrypted form, thus maintaining the integrity of the model parameters. However, these techniques require high computational and communication bandwidths to transfer the encrypted model parameters, which can be a significant drawback in resource-constrained environments. Similarly, SMC techniques, while providing robust privacy guarantees, can also increase the communication overhead in the network, potentially leading to delays and inefficiencies.

In addition to these primary techniques, several other emerging methods are gaining traction. Techniques such as knowledge distillation, robust aggregation, blockchained FL, and TEE offer promising solutions for mitigating privacy leakage and poisoning attacks. However, these techniques also come with their own set of trade-offs and limitations. For example, knowledge distillation and robust aggregation may introduce additional computation overhead, while TEE often relies on a trusted entity or infrastructure, which can be a potential single point of failure or a bottleneck. Therefore, while these emerging techniques offer innovative approaches to enhancing privacy in FL, their implementation requires careful consideration of the specific use case requirements, resource availability, and potential limitations. Therefore, a thorough understanding of these trade-offs and the specific needs of the application is essential for selecting and implementing the most suitable privacy-enhancing mechanisms.

2) REMAINING RESEARCH QUESTIONS

Regarding the FL defenses and their identified trade-offs, we raise the following research questions that are significant to be addressed:

- How can trade-offs between privacy and utility be quantified effectively while aiming to optimize privacy gains in FL implementations within 6G networks?
- What key criteria should guide the selection of one or multiple defense strategies for FL in various 6G network scenarios?
- How can multiple privacy-enhancing techniques be effectively combined to create a holistic defense mechanism for FL, and what frameworks or models can be developed to facilitate this integration?
- What approaches can be developed to ensure transparency and standardization in FL defenses over networks, particularly considering end-user privacy policies and practices?

3) EMERGING AND FUTURE RESEARCH DIRECTIONS

In the case of FL for 6G, privacy-utility trade-offs could be measured through privacy-utility curves and multi-objective optimization balancing privacy and model performance [260]. Choosing defense strategies depends on data sensitivity, threat level, network topology, resource limitations, and defense layers that are specifically designed for the intended use case. An integrated defense approach is based on the possible incorporation of an array of privacy protection techniques into a framework of discrete and layered structures with a flexible architecture that can be fitted to the requirements of various domains of the network. Compliance with transparency and standardization stipulates open architecture, privacy protection, and aggregate standards, increasing the users' confidence in FL augmentation.

Future research in enhancing privacy for FL in 6G networks can explore several directions to mitigate the trade-offs. One approach is to develop improved versions of perturbation techniques that apply selective perturbations only to the most privacy-sensitive regions of the model. This can minimize the overall impact on the model's utility. Incorporating Explainable AI (XAI)-based approaches can be supportive in this context, as XAI can identify critical decision-making processes within the model, detect the use of privacy-related attributes in decisions, and analyze the impact of privacy mechanisms on model performance. Additionally, there is a requirement for improved lightweight algorithms that can reduce the computational and communication overhead associated with techniques like HE and SMC. These algorithms should incorporate network capacity-related metrics to optimize resource use without compromising the overall quality of service for other applications. By focusing on these areas, future research can

develop more efficient, effective, and context-aware privacy-enhancing mechanisms for FL in 6G networks.

D. PRIVACY PRESERVATION AT DIFFERENT 6G LAYERS

1) LESSONS LEARNED

FL can be effectively used with appropriate defense mechanisms at different architectural layers in a 6G network to enhance privacy preservation at each layer. The main applications of FL can be observed at the sensing and RAN layers, where FL-based use cases can be executed directly on client devices that are closely connected to end-user applications. Techniques such as OTA FL can be used in wireless networks such as 6G to leverage the potential of signal superposition, thereby reducing the computational requirements in FL aggregation. This approach improves privacy by localizing the data and optimizes resource utilization, making it suitable for the resource-constrained environments typical of the sensing and RAN layers.

FL can typically act as a final or intermediate aggregator at the edge layer, or it can forward the models to upper layers depending on specific requirements. This layer is crucial in balancing computational load and ensuring efficient model updates. Utility-driven intelligent applications, such as intrusion detection systems, can be trained via FL at the upper layers, benefiting from the aggregated data from multiple sources while maintaining user privacy. However, these upper layers mainly function as service providers or perform orchestration, management, and regulatory operations for end-user-based applications. By decentralizing data processing and ensuring that sensitive data remains at the edge or client level, FL, coupled with robust privacy-preserving techniques, can provide a scalable and secure solution across the diverse layers of the 6G architecture.

2) REMAINING RESEARCH QUESTIONS

Based on the application of FL across 6G network architecture based on its current limitations in the discussions, we can consider the following research questions to be addressed:

- What architectural designs can unify FL pipelines spanning multiple layers of the 6G network to ensure seamless integration and efficiency?
- How can different architectures, such as hierarchical FL, P2P FL, or hybrid architectural designs, be effectively incorporated into various 6G architectural layers to enhance privacy and performance?
- How much transparency should be allowed at each 6G layer regarding the model aggregation and sharing process to balance security, privacy, and operational efficiency?
- What mechanisms can be developed to optimize the FL training process dynamically across different 6G layers, considering resource availability and network performance parameters?

3) EMERGING AND FUTURE RESEARCH DIRECTIONS

In the architectural design unifying FL pipelines across 6G layers, multi-tier systems have several advantages, such as the edge layer implementing local aggregation and core layers handling global integration. Hierarchical FL offers better performance and privacy by clustering devices and doing local aggregation; P2P FL will be suitable for decentralized systems. The selective transparency managed through role-based access control ensures that privacy is at lower layers and trust is possible at higher layers. Adaptive resource management and reinforcement learning can dynamically adjust the FL training processes regarding network performance and resource availability so that their efficiency and scalability are ensured in 6G.

Future research on privacy preservation for FL within 6G networks should address the deployment of defenses across different architectural layers. It is important to recognize that protection measures using the FL algorithm in the upper layers may not be appropriate for the lower layers. For example, the noise level at the edge layer, where a relatively small number of models are aggregated, must be carefully calibrated. In contrast, many thousands or more FL models are processed at the control layer. In the latter case, adding more noise might not significantly affect performance due to the large amount of aggregated data. Therefore, investigating optimal strategies for applying protective measures in overlapping FL pipelines is an important area for future work. In addition, the need for standardization and regulatory approaches to FL must be addressed at various levels. Establishing clear guidelines and regulatory frameworks will ensure consistent and secure implementation of FL, facilitate interoperability and increase trust in these advanced networks. Research should also focus on developing dynamic defense mechanisms that can adapt to network conditions and resource availability in real-time to ensure robust privacy protection while achieving better performance.

E. OTHER FUTURE RESEARCH DIRECTIONS

Regarding the other potential future research directions for FL, several aspects can be summarized. The advantages of quantum computers are well known when compared to classical computers; thus, integration of quantum computing and FL is an interesting research direction [261]. In [262], the advantages of faster training for FL are clearly highlighted. However, the integration of these technologies is deemed to be challenging due to the distributed nature of FL [263]. Also, there is a bottleneck in terms of financial feasibility as quantum computing is expensive [264]. In addition, the evolution of quantum computing may affect privacy and security in networks that resort to classical cryptographic algorithms [265]. Thus, network service providers should use complex cryptographic algorithms, which in turn will demand more processing power and increase the latency in the network. 6G application security is deemed to be expensive in this regard.

Green computing focuses on managing computing and its associated technologies while giving prominence to the environment and the carbon footprint [266]. FL is an enabler of green computing as it makes ML more sustainable and energy efficient. By utilizing FL, the training energy can be reduced significantly [267], and the training loss can be reduced given a limited energy budget [268]. The improvement in energy efficiency leads to reduced energy consumption and carbon emissions, contributing to an eco-friendly approach to ML. From the security and privacy perspective, it is necessary to consider these environmental constraints simultaneously when designing novel cryptographic algorithms, as the complexity of these algorithms may require more energy, ultimately creating a conflict with green computing ambitions. Overall, priority should be given to communication-efficient FL [121].

XAI is an emerging technology that ensures trustworthy AI. It facilitates the reasoning of AI models trained with FL, which were conventionally considered uninterpretable models. The ability to gain insights on the model is useful for detecting possible security and privacy threats on the AI models, e.g., intrusion detection [269], poisoning detection with post-hoc Shapley value explainers [270]. However, with increasing levels of explainability, XAI is deemed to impact the privacy of the end users as well, which creates a trade-off. For example, a clear security threat is created if an adversarial server has the ability to access the model parameters and the XAI metrics, which may allow the adversary to gain insights such as the user data distribution and properties of existing data. This affects the privacy of clients and makes the system vulnerable to attacks like model inversion and membership inference [271], [272]. Fine-tuning these trade-offs is a potential future direction on FL-XAI [273].

There are some important technical challenges in implementing FL in 6G networks, particularly in terms of hardware requirements and network infrastructure, and it is another key future research direction. To this end, the energy efficiency of the edge devices through energy-efficient algorithms and hardware, advanced encryption techniques on resource-constrained devices, robust and adaptable FL networks, synchronization of updates from edge devices, verification of the integrity and authenticity of the model updates, robust version control mechanisms, are some interesting sub-topics. The research focus will also extend to novel technologies and protocols that can further facilitate FL.

Finally, it is challenging to make exact technological predictions as 6G rapidly evolves and requires ongoing updates to reflect new architectures and use cases. Industry-specific practical challenges, such as privacy-preserving FL in healthcare, industrial IoT, and autonomous vehicles, may need to be explored once 6G applications in these sectors are more defined. Additionally, the absence of defined 6G architecture, requirements, and real-world deployments limits the ability to provide practical insights or scalability discussions for privacy-preserving FL solutions. When 6G networks and real-world applications become available, research should focus on incorporating practical data and scalability assessments. Addressing these gaps will ensure more accurate and applicable findings in privacy and security for FL in 6G environments.

X. CONCLUSION

This paper investigated the application of FL in future 6G networks to perform privacy-enhanced distributed machine learning. Key issues in such FL-based implementations were examined, highlighting the numerous trade-offs associated with current solutions. The application of these solutions must be carefully designed, considering the different layers within the 6G architecture on which FL systems are implemented. Future research directions include improving existing approaches and developing novel techniques to quantify, monitor, and explain the quality of the FL process and its defense mechanisms. In addition, strengthening standardization and regulatory approaches is essential for the widespread deployment of FL in 6G networks. These advances will ensure robust, secure, and efficient FL implementations and pave the way for their full integration into next-generation 6G networks.

REFERENCES

[1] 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.
[2] P. Kairouz et al., "Advances and open problems in federated learning," *Found. Trends Mach. Learn.*, vol. 14, nos. 1–2, pp. 1–210, 2021.
[3] M. Alazab, R. M. S. Priya, M. Parimala, P. K. R. Maddikunta, T. R. Gadekallu, and Q.-V. Pham, "Federated learning for cybersecurity: Concepts, challenges, and future directions," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3501–3509, May 2022.
[4] The Next G Alliance. "6G roadmap for vertical industries." 2023. [Online]. Available: https://nextgalliance.org/white_papers/6g-roadmap-vertical-industries/
[5] 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, 2019.
[6] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50–60, May 2020.
[7] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. Artif. Intell. Stat.*, 2017, pp. 1273–1282.
[8] C. Xu and G. Neglia, "What else is leaked when eavesdropping federated learning?" in *Proc. CCS Workshop Privacy Preserving Mach. Learn. (PPML)*, 2021, p. 12.
[9] B. Ghimire and D. B. Rawat, "Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8229–8249, Jun. 2022.
[10] J. Passerat-Palmbach et al., "Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, 2020, pp. 550–555.
[11] M. Y. Topaloglu, E. M. Morrell, S. Rajendran, and U. Topaloglu, "In the pursuit of privacy: The promises and predicaments of federated learning in healthcare," *Front. Artif. Intell.*, vol. 4, Oct. 2021, Art. no. 746497.
[12] O. Marfoq, G. Neglia, R. Vidal, and L. Kameni, "Personalized federated learning through local memorization," in *Proc. Int. Conf. Mach. Learn.*, 2022, pp. 15070–15092.

[13] P. Liu, X. Xu, and W. Wang, "Threats, attacks and defenses to federated learning: issues, taxonomy and perspectives," *Cybersecurity*, vol. 5, no. 1, p. 4, 2022.

[14] X. Luo, Y. Wu, X. Xiao, and B. C. Ooi, "Feature inference attack on model predictions in vertical federated learning," in *Proc. IEEE 37th Int. Conf. Data Eng. (ICDE)*, 2021, pp. 181–192.

[15] A. E. Ouadrhiri and A. Abdelhadi, "Differential privacy for deep and federated learning: A survey," *IEEE Access*, vol. 10, pp. 22359–22380, 2022.

[16] C. Zhang, S. Li, J. Xia, W. Wang, F. Yan, and Y. Liu, "BatchCrypt: Efficient homomorphic encryption for cross-silo federated learning," in *Proc. USENIX Annu. Techn. Conf. (USENIX ATC)*, 2020, pp. 493–506.

[17] Y. Li, Y. Zhou, A. Jolfaei, D. Yu, G. Xu, and X. Zheng, "Privacy-preserving federated learning framework based on chained secure multiparty computing," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6178–6186, Apr. 2021.

[18] S. K. Lo et al., "Toward trustworthy Ai: Blockchain-based architecture design for accountability and fairness of federated learning systems," *IEEE Internet Things J.*, vol. 10, no. 4, pp. 3276–3284, Feb. 2023.

[19] Z. Yang, M. Chen, K.-K. Wong, H. V. Poor, and S. Cui, "Federated learning for 6G: Applications, challenges, and opportunities," *Engineering*, vol. 8, pp. 33–41, Jan. 2022.

[20] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021.

[21] D. Sirohi, N. Kumar, P. S. Rana, S. Tanwar, R. Iqbal, and M. Hijjii, "Federated learning for 6G-enabled secure communication systems: A comprehensive survey," *Artif. Intell. Rev.*, vol. 56, pp. 11297–11389, Mar. 2023.

[22] 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.

[23] O. Nassef, W. Sun, H. Purmehdi, M. Tatipamula, and T. Mahmoodi, "A survey: Distributed machine learning for 5G and beyond," *Comput. Netw.*, vol. 207, 2022, Art. no. 108820.

[24] M. Al-Quraan et al., "Edge-native intelligence for 6G communications driven by federated learning: A survey of trends and challenges," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 7, no. 3, pp. 957–979, Jun. 2023.

[25] W. Xu, Z. Yang, D. W. K. Ng, M. Levorato, Y. C. Eldar, and M. Debbah, "Edge learning for B5G networks with distributed signal processing: Semantic communication, edge computing, and wireless sensing," *IEEE J. Sel. Topics Signal Process.*, vol. 17, no. 1, pp. 9–39, Jan. 2023.

[26] D. Javeed, M. S. Saeed, I. Ahmad, M. Adil, P. Kumar, and A. N. Islam, "Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions," *Future Gener. Comput. Syst.*, vol. 160, pp. 577–597, Nov. 2024.

[27] M. A. Ferrag et al., "Edge learning for 6G-enabled Internet of Things: A comprehensive survey of vulnerabilities, datasets, and defenses," 2023, *arXiv:2306.10309*.

[28] Q. Duan, J. Huang, S. Hu, R. Deng, Z. Lu, and S. Yu, "Combining federated learning and edge computing toward ubiquitous intelligence in 6G network: Challenges, recent advances, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 4, pp. 2892–2950, 4th Quart., 2023.

[29] X. Yin, Y. Zhu, and J. Hu, "A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions," *ACM Comput. Surveys*, vol. 54, no. 6, pp. 1–36, 2021.

[30] A. Imteaj, U. Thakker, S. Wang, J. Li, and M. H. Amini, "A survey on federated learning for resource-constrained IoT devices," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 1–24, Jan. 2022.

[31] M. Aledhari, R. Razzak, R. M. Parizi, and F. Saeed, "Federated learning: A survey on enabling technologies, protocols, and applications," *IEEE Access*, vol. 8, pp. 140699–140725, 2020.

[32] S. Sharma and K. Guleria, "A comprehensive review on federated learning based models for healthcare applications," *Artif. Intell. Med.*, vol. 146, Dec. 2023, Art. no. 102691.

[33] J. Wu, F. Dong, H. Leung, Z. Zhu, J. Zhou, and S. Drew, "Topology-aware federated learning in edge computing: A comprehensive survey," *ACM Comput. Surveys*, vol. 56, no. 10, pp. 1–41, 2024.

[34] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, "A survey on federated learning," *Knowl.-Based Syst.*, vol. 216, Mar. 2021, Art. no. 106775.

[35] W. Issa, N. Moustafa, B. Turnbull, N. Sohrabi, and Z. Tari, "Blockchain-based federated learning for securing Internet of Things: A comprehensive survey," *ACM Comput. Surveys*, vol. 55, no. 9, pp. 1–43, 2023.

[36] R. Gupta and T. Alam, "Survey on federated-learning approaches in distributed environment," *Wireless Pers. Commun.*, vol. 125, no. 2, pp. 1631–1652, 2022.

[37] B. Yu, W. Mao, Y. Lv, C. Zhang, and Y. Xie, "A survey on federated learning in data mining," *Interdiscipl. Rev. Data Min. Knowl. Disc.*, vol. 12, no. 1, 2022, Art. no. e1443.

[38] D. C. Nguyen et al., "Federated learning meets blockchain in edge computing: Opportunities and challenges," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12806–12825, Aug. 2021.

[39] Z. Lu, H. Pan, Y. Dai, X. Si, and Y. Zhang, "Federated learning with non-IID data: A survey," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 19188–19209, Jun. 2024.

[40] A. Brecko, E. Kajati, J. Koziorek, and I. Zolotova, "Federated learning for edge computing: A survey," *Appl. Sci.*, vol. 12, no. 18, p. 9124, 2022.

[41] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A survey on security and privacy of federated learning," *Future Gener. Comput. Syst.*, vol. 115, pp. 619–640, Feb. 2021.

[42] K. N. Kumar, C. K. Mohan, and L. R. Cenkeramaddi, "The impact of adversarial attacks on federated learning: A survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 46, no. 5, pp. 2672–2691, May 2024.

[43] O. R. A. Almanifi, C.-O. Chow, M.-L. Tham, J. H. Chuah, and J. Kanesan, "Communication and computation efficiency in federated learning: A survey," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100742.

[44] D. C. Nguyen et al., "Federated learning for smart healthcare: A survey," *ACM Comput. Surveys*, vol. 55, no. 3, pp. 1–37, 2022.

[45] R. Zhang, J. Mao, H. Wang, B. Li, X. Cheng, and L. Yang, "A survey on federated learning in intelligent transportation systems," *IEEE Trans. Intell. Veh.*, early access, Aug. 20, 2024, doi: 10.1109/TIV.2024.3446319.

[46] W. Y. B. Lim et al., "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 2031–2063, 3rd Quart., 2020.

[47] V. P. Chellapandi, L. Yuan, S. H. Zak, and Z. Wang, "Federated learning for connected and automated vehicles: A survey of existing approaches and challenges," *IEEE Trans. Intell. Veh.*, vol. 9, no. 1, pp. 119–137, Jan. 2024.

[48] P. Boobalan et al., "Fusion of federated learning and Industrial Internet of Things: A survey," *Comput. Netw.*, vol. 212, Jul. 2022, Art. no. 109048.

[49] H. Zhu, J. Xu, S. Liu, and Y. Jin, "Federated learning on non-IID data: A survey," *Neurocomputing*, vol. 465, pp. 371–390, Nov. 2021.

[50] X. Liu, Y. Deng, A. Nallanathan, and M. Bennis, "Federated learning and meta learning: Approaches, applications, and directions," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 1, pp. 571–618, 1st Quart., 2024.

[51] M. Ye, X. Fang, B. Du, P. C. Yuen, and D. Tao, "Heterogeneous federated learning: State-of-the-art and research challenges," *ACM Comput. Surveys*, vol. 56, no. 3, pp. 1–44, 2023.

[52] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, "Federated learning for Internet of Things: Recent advances, taxonomy, and open challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1759–1799, 3rd Quart., 2021.

[53] O. Aouedi, "Machine learning-enabled network traffic analysis," Ph.D. dissertation, Dept. Comput. Sci., Nantes Université, Nantes, France, 2022.

[54] O. Aouedi, K. Piamrat, and B. Parrein, "Intelligent traffic management in next-generation networks," *Future Internet*, vol. 14, no. 2, p. 44, 2022.

[55] Q. Li et al., "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.

[56] O. Aouedi and K. Piamrat, "SURFS: Sustainable intrusion detection with hierarchical federated spiking neural networks," in *Proc. ICC*, 2024, pp. 2173–2178.

[57] J. Liu et al., "From distributed machine learning to federated learning: A survey," *Knowl. Inf. Syst.*, vol. 64, no. 4, pp. 885–917, 2022.

[58] S. Wijethilaka and M. Liyanage, "A federated learning approach for improving security in network slicing," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2022, pp. 915–920.

[59] B. Brik and A. Ksentini, "On predicting service-oriented network slices performances in 5G: A federated learning approach," in *Proc. IEEE 45th Conf. Local Comput. Netw. (LCN)*, 2020, pp. 164–171.

[60] L. Liu, J. Zhang, S. Song, and K. B. Letaief, "Client-edge-cloud hierarchical federated learning," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2020, pp. 1–6.

[61] E. T. M. Beltrán et al., "Decentralized federated learning: Fundamentals, state-of-the-art, frameworks, trends, and challenges," 2022, *arXiv:2211.08413*.

[62] Y. Sun, J. Shao, Y. Mao, J. H. Wang, and J. Zhang, "Semi-decentralized federated edge learning for fast convergence on non-IID data," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2022, pp. 1898–1903.

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

[64] Y. Cui et al., "A survey on contribution evaluation in vertical federated learning," 2024, *arXiv:2405.02364*.

[65] Y. Liu et al., "Vertical federated learning," 2022, *arXiv:2211.12814*.

[66] Y. Wu, S. Cai, X. Xiao, G. Chen, and B. C. Ooi, "Privacy preserving vertical federated learning for tree-based models," 2020, *arXiv:2008.06170*.

[67] S. Zhang et al., "Federated learning in intelligent transportation systems: Recent applications and open problems," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 5, pp. 3259–3285, May 2024.

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

[69] Z. Yang, M. Chen, W. Saad, M. Shikh-Bahaei, H. V. Poor, and S. Cui, "Federated learning in 6G mobile wireless networks," in *6G Mobile Wireless Networks*. Heidelberg, Germany: Springer, 2021, pp. 359–378.

[70] Y. Xiao, G. Shi, and M. Krunz, "Towards ubiquitous Ai in 6G with federated learning," 2020, *arXiv:2004.13563*.

[71] Y. Zhao et al., "Privacy-preserving blockchain-based federated learning for IoT devices," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1817–1829, Feb. 2021.

[72] S. Samarakoon, M. Bennis, W. Saad, and M. Debbah, "Federated learning for ultra-reliable low-latency V2V communications," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2018, pp. 1–7.

[73] 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.

[74] O. Aouedi, K. Piamrat, G. Muller, and K. Singh, "Federated semisupervised learning for attack detection in Industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 286–295, Jan. 2023.

[75] J. Mu, Y. Cui, W. Ouyang, Z. Yang, W. Yuan, and X. Jing, "Federated learning in 6G non-terrestrial network for IoT services: From the perspective of perceptive mobile network," *IEEE Netw.*, vol. 38, no. 4, pp. 72–79, Jul. 2024.

[76] J. He, S. Guo, M. Li, and Y. Zhu, "AceFL: Federated learning accelerating in 6G-enabled mobile edge computing networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 3, pp. 1364–1375, May/Jun. 2023.

[77] B. Luo, X. Li, S. Wang, J. Huang, and L. Tassiulas, "Cost-effective federated learning design," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, 2021, pp. 1–10.

[78] Z. Qu et al., "Partial synchronization to accelerate federated learning over relay-assisted edge networks," *IEEE Trans. Mobile Comput.*, vol. 21, no. 12, pp. 4502–4516, Dec. 2022.

[79] H. Chergui et al., "Zero-touch AI-driven distributed management for energy-efficient 6G massive network slicing," *IEEE Netw.*, vol. 35, no. 6, pp. 43–49, Nov./Dec. 2021.

[80] O. Aouedi and K. Piamrat, "F-BIDS: Federated-blending based intrusion detection system," *Pervasive Mobile Comput.*, vol. 89, Feb. 2023, Art. no. 101750.

[81] S. Niknam, H. S. Dhillon, and J. H. Reed, "Federated learning for wireless communications: Motivation, opportunities, and challenges," *IEEE Wireless Commun. Mag.*, vol. 58, no. 6, pp. 46–51, Jun. 2020.

[82] X. Sun et al., "A hierarchical federated learning-based intrusion detection system for 5G smart grids," *Electronics*, vol. 11, no. 16, p. 2627, 2022.

[83] T. V. Nguyen, N. D. Ho, H. T. Hoang, C. D. Do, and K.-S. Wong, "Toward efficient hierarchical federated learning design over multi-hop wireless communications networks," *IEEE Access*, vol. 10, pp. 111910–111922, 2022.

[84] M. S. H. Abad, E. Ozfatura, D. Gunduz, and O. Ercetin, "Hierarchical federated learning across heterogeneous cellular networks," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, 2020, pp. 8866–8870.

[85] A. A. Abdellatif et al., "Communication-efficient hierarchical federated learning for IoT heterogeneous systems with imbalanced data," *Future Gener. Comput. Syst.*, vol. 128, pp. 406–419, Mar. 2022.

[86] K. Xie et al., "Efficient federated learning with spike neural networks for traffic sign recognition," *IEEE Trans. Veh. Technol.*, vol. 71, no. 9, pp. 9980–9992, Sep. 2022.

[87] L. Barbieri, S. Savazzi, M. Brambilla, and M. Nicoli, "Decentralized federated learning for extended sensing in 6G connected vehicles," *Veh. Commun.*, vol. 33, Jan. 2022, Art. no. 100396.

[88] Y. Qu et al., "Decentralized privacy using blockchain-enabled federated learning in fog computing," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5171–5183, Jun. 2020.

[89] B. Xu, H. Zhao, H. Cao, S. Garg, G. Kaddoum, and M. M. Hassan, "Edge aggregation placement for semi-decentralized federated learning in Industrial Internet of Things," *Future Gener. Comput. Syst.*, vol. 150, pp. 160–170, Jan. 2024.

[90] V. K. Quy, D. C. Nguyen, D. Van Anh, and N. M. Quy, "Federated learning for green and sustainable 6G IIoT applications," *Internet Things*, vol. 25, Apr. 2024, Art. no. 101061.

[91] Z. Zhang, G. Zhu, and S. Cui, "Low-latency cooperative spectrum sensing via truncated vertical federated learning," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2022, pp. 1858–1863.

[92] C. Ju, D. Gao, R. Mane, B. Tan, Y. Liu, and C. Guan, "Federated transfer learning for eeg signal classification," in *Proc. 42nd Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, 2020, pp. 3040–3045.

[93] Y. Fan, Y. Li, M. Zhan, H. Cui, and Y. Zhang, "IoTDefender: A federated transfer learning intrusion detection framework for 5G IoT," in *Proc. IEEE 14th Int. Conf. Big Data Sci. Eng. (BigDataSE)*, 2020, pp. 88–95.

[94] J. Holvast, "27—History of privacy," in *The History of Information Security*, K. D. Leeuw and J. Bergstra, Eds. Amsterdam, The Netherlands: Elsevier, 2007, pp. 737–769. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780444516084500286

[95] H. Li, L. Yu, and W. He, "The impact of GDPR on global technology development," *J. Global Inf. Technol. Manag.*, vol. 22, no. 1, pp. 1–6, 2019.

[96] W. Stallings and M. P. Tahiliani, *Cryptography and Network Security: Principles and Practice*. Upper Saddle River, NJ, USA: Prentice Hall, 2014.

[97] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "AI and 6G security: Opportunities and challenges," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, 2021, pp. 616–621.

[98] M. Ylianttila et al., "6G white paper: Research challenges for trust, security and privacy," 2020, *arXiv:2004.11665*.

[99] S. Jayasinghe, Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "Federated learning based anomaly detection as an enabler for securing network and service management automation in beyond 5G networks," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, 2022, pp. 345–350.

[100] K. Ramezanpour, J. Jagannath, and A. Jagannath, "Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective," *Comput. Netw.*, vol. 221, Feb. 2023, Art. no. 109515.

[101] M. Noor-A-Rahim et al., "6G for Vehicle-to-Everything (V2X) communications: Enabling technologies, challenges, and opportunities," *Proc. IEEE*, vol. 110, no. 6, pp. 712–734, Jun. 2022.

[102] T. Ni, "Sensor security in virtual reality: Exploration and mitigation," in *Proc. 22nd Annu. Int. Conf. Mobile Syst. Appl. Services*, 2024, pp. 758–759.

[103] A. P. Kalapaaking, V. Stephanie, I. Khalil, M. Atiquzzaman, X. Yi, and M. Almashor, "SMPC-based federated learning for 6G-enabled Internet of Medical Things," *IEEE Netw.*, vol. 36, no. 4, pp. 182–189, Jul./Aug. 2022.

[104] Y. Djenouri, T. P. Michalak, and J. C.-W. Lin, "Federated deep learning for smart city edge-based applications," *Future Gener. Comput. Syst.*, vol. 147, pp. 350–359, Oct. 2023.

[105] K. Wei et al., "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3454–3469, 2020.

[106] K. T. Putra et al., "Federated compressed learning edge computing framework with ensuring data privacy for PM2.5 prediction in smart city sensing applications," *Sensors*, vol. 21, no. 13, p. 4586, 2021.

[107] N. M. Hijazi, M. Aloqaily, M. Guizani, B. Ouni, and F. Karray, "Secure federated learning with fully homomorphic encryption for IoT communications," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 4289–4300, Feb. 2024.

[108] M. Kim, I. Oh, K. Yim, M. Sahlabadi, and Z. Shukur, "Security of 6G enabled vehicle-to-everything communication in emerging federated learning and blockchain technologies," *IEEE Access*, vol. 12, pp. 33972–34001, 2023.

[109] J. Li, X. Tong, J. Liu, and L. Cheng, "An efficient federated learning system for network intrusion detection," *IEEE Syst. J.*, vol. 17, no. 2, pp. 2455–2464, Jun. 2023.

[110] M. Raza, M. J. Saeed, M. B. Riaz, and M. A. Sattar, "Federated learning for privacy preserving intrusion detection in software defined networks," *IEEE Access*, vol. 12, pp. 69551–69567, 2024.

[111] S. Chatzimiltis, M. Shojafar, M. B. Mashhadi, and R. Tafazolli, "A collaborative software defined network-based smart grid intrusion detection system," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 700–711, 2024.

[112] M. H. Bhavsar, Y. B. Bekele, K. Roy, J. C. Kelly, and D. Limbrick, "FL-IDS: Federated learning-based intrusion detection system using edge devices for transportation IoT," *IEEE Access*, vol. 12, pp. 52215–52226, 2024.

[113] X. Huang, J. Liu, Y. Lai, B. Mao, and H. Lyu, "EEFED: Personalized federated learning of execution&evaluation dual network for CPS intrusion detection," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 41–56, 2022.

[114] Z. A. E. Houda, H. Moudoud, B. Brik, and L. Khoukhi, "Blockchain-enabled federated learning for enhanced collaborative intrusion detection in vehicular edge computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 7, pp. 7661–7672, Jul. 2024.

[115] Z. A. E. Houda, D. Naboulsi, and G. Kaddoum, "A privacy-preserving collaborative jamming attacks detection framework using federated learning," *IEEE Internet Things J.*, vol. 11, no. 7, pp. 12153–12164, Apr. 2024.

[116] Z. A. E. Houda, H. Moudoud, B. Brik, and L. Khoukhi, "Securing federated learning through blockchain and explainable Ai for robust intrusion detection in IoT networks," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, 2023, pp. 1–6.

[117] Z. A. E. Houda, H. Moudoud, B. Brik, and M. Adil, "A privacy-preserving framework for efficient network intrusion detection in consumer network using quantum federated learning," *IEEE Trans. Consum. Electron.*, early access, Sep. 12, 2024, doi: 10.1109/TCE.2024.3458985.

[118] H. Moudoud, Z. A. E. Houda, and B. Brik, "Advancing security and trust in WSNs: A federated multi-agent deep reinforcement learning approach," *IEEE Trans. Consum. Electron.*, early access, Aug. 7, 2024, doi: 10.1109/TCE.2024.3440178.

[119] Z. A. E. Houda, H. Moudoud, and B. Brik, "Federated deep reinforcement learning for efficient jamming attack mitigation in O-RAN," *IEEE Trans. Veh. Technol.*, vol. 73, no. 7, pp. 9334–9343, Jul. 2024.

[120] C. Zhou and N. Ansari, "Securing federated learning enabled NWDAF architecture with partial homomorphic encryption," *IEEE Netw. Lett.*, vol. 5, no. 4, pp. 299–303, Dec. 2023.

[121] K. Kishor, "Communication-efficient federated learning," in *Federated Learning for IoT Applications*. Heidelberg, Germany: Springer, 2022, pp. 135–156.

[122] 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.*, to be published.

[123] S. K. Lo et al., "Blockchain-based trustworthy federated learning architecture," 2021, *arXiv:2108.06912*.

[124] G. Damaskinos, R. Guerraoui, A.-M. Kermarrec, V. Nitu, R. Patra, and F. Taiani, "FLEET: Online federated learning via staleness awareness and performance prediction," *ACM Trans. Intell. Syst. Technol.*, vol. 13, no. 5, pp. 1–30, 2022.

[125] G. Liu, X. Ma, Y. Yang, C. Wang, and J. Liu, "Federated unlearning," 2020, *arXiv:2012.13891*.

[126] B. D. Son et al., "Adversarial attacks and defenses in 6G network-assisted IoT systems," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 19168–19187, Jun. 2024.

[127] Z. Luan, W. Li, M. Liu, and B. Chen, "Robust federated learning: Maximum correntropy aggregation against Byzantine attacks," *IEEE Trans. Neural Netw. Learn. Syst.*, early access, Apr. 23, 2024, doi: 10.1109/TNNLS.2024.3383294.

[128] K. Pillutla, S. M. Kakade, and Z. Harchaoui, "Robust aggregation function in federated learning," in *Proc. Int. Conf. Inf. Knowl. Syst.*, 2023, pp. 168–175.

[129] H. Sedjelmaci, N. Kaaniche, A. Boudguiga, and N. Ansari, "Secure attack detection framework for hierarchical 6G-enabled Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 73, no. 2, pp. 2633–2642, Feb. 2024.

[130] M. A. Khoshkholghi, T. Mahmoodi, S. Pal, S. Chopra, M. Tendulkar, and S. Sarka, "XURLLC in 6G with meshed RAN," *ITU J. Future Evol. Technol.*, vol. 3, no. 3, pp. 612–622, 2022.

[131] H. Yu, T. Taleb, K. Samdanis, and J. Song, "Toward supporting holographic services over deterministic 6G integrated terrestrial and non-terrestrial networks," *IEEE Netw.*, vol. 38, no. 1, pp. 262–271, Jan. 2023.

[132] A. Kumar, R. Jain, M. Gupta, and S. M. Islam, *6G-Enabled IoT and AI for Smart Healthcare: Challenges, Impact, and Analysis*. Hoboken, NJ, USA: CRC Press, 2023.

[133] A. Al Amin, J. Hong, V.-H. Bui, and W. Su, "Emerging 6G/B6G wireless communication for the power infrastructure in smart cities: Innovations, challenges, and future perspectives," *Algorithms*, vol. 16, no. 10, p. 474, 2023.

[134] M. Murroni et al., "6G—Enabling the new smart city: A survey," *Sensors*, vol. 23, no. 17, p. 7528, 2023.

[135] S. R. Pokhrel, "Learning from data streams for automation and orchestration of 6G Industrial IoT: Toward a semantic communication framework," *Neural Comput. Appl.*, vol. 34, no. 18, pp. 15197–15206, 2022.

[136] A. Moubayed, A. Shami, and A. Al-Dulaimi, "On end-to-end intelligent automation of 6G networks," *Future Internet*, vol. 14, no. 6, p. 165, 2022.

[137] L. U. Khan, Y. K. Tun, M. Alsenwi, M. Imran, Z. Han, and C. S. Hong, "A dispersed federated learning framework for 6G-enabled autonomous driving cars," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 6, pp. 5656–5667, Nov./Dec. 2024.

[138] 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.

[139] S. K. Das, R. Mudi, M. S. Rahman, and A. O. Fapojuwo. "Distributed learning for 6G—IoT networks: A comprehensive survey." 2023. [Online]. Available: https://www.authorea.com/users/685107/articles/680237-distributed-learning-for-6g-iot-networks-a-comprehensive-survey

[140] M. Alkaeed, A. Qayyum, and J. Qadir, "Privacy preservation in artificial intelligence and extended reality (AI-XR) metaverses: A survey," *J. Netw. Comput. Appl.*, vol. 231, Nov. 2024, Art. no. 103989.

[141] A. Rizwan, R. Ahmad, A. N. Khan, R. Xu, and D. H. Kim, "Intelligent digital twin for federated learning in AIoT networks," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100698.

[142] S. Chaudjary, R. Kakkar, R. Gupta, S. Tanwar, S. Agrawal, and R. Sharma, "Blockchain and federated learning-based security solutions for telesurgery system: A comprehensive review," *Turkish J. Elect. Eng. Comput. Sci.*, vol. 30, no. 7, pp. 2446–2488, 2022.

[143] X. Qiao, Y. Huang, S. Dustdar, and J. Chen, "6G vision: An AI-driven decentralized network and service architecture," *IEEE Internet Comput.*, vol. 24, no. 4, pp. 33–40, Jul./Aug. 2020.

[144] M. A. Hossain, A. R. Hossain, and N. Ansari, "AI in 6G: Energy-efficient distributed machine learning for multilayer heterogeneous networks," *IEEE Netw.*, vol. 36, no. 6, pp. 84–91, Nov./Dec. 2022.

[145] M. S. Jere, T. Farnan, and F. Koushanfar, "A taxonomy of attacks on federated learning," *IEEE Security Privacy*, vol. 19, no. 2, pp. 20–28, Mar./Apr. 2021.

[146] L. Li, Y. Fan, M. Tse, and K.-Y. Lin, "A review of applications in federated learning," *Comput. Ind. Eng.*, vol. 149, Nov. 2020, Art. no. 106854.

[147] X. Zhou, W. Liang, J. She, Z. Yan, I. Kevin, and K. I.-K. Wang, "Two-layer federated learning with heterogeneous model aggregation for 6G supported Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5308–5317, Jun. 2021.

[148] L. Chang et al., "6G-enabled edge AI for metaverse: Challenges, methods, and future research directions," *J. Commun. Inf. Netw.*, vol. 7, no. 2, pp. 107–121, 2022.

[149] C. Sandeepa, S. Wang, and M. Liyanage, "Privacy of the metaverse: Current issues, AI attacks, and possible solutions," in *Proc. IEEE Int. Conf. Metaverse Comput. Netw. Appl. (MetaCom)*, 2023, pp. 234–241.

[150] H. Hu et al., "A survey on brain–computer interface-inspired communications: Opportunities and challenges," *IEEE Commun. Surveys Tuts.*, early access, May 6, 2024, doi: 10.1109/COMST.2024.3396847.

[151] T. Alam and R. Gupta, "Federated learning and its role in the privacy preservation of IoT devices," *Future Internet*, vol. 14, no. 9, p. 246, 2022.

[152] E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin, and V. Shmatikov, "How to backdoor federated learning," in *Proc. Int. Conf. Artif. Intell. Stat.*, 2020, pp. 2938–2948.

[153] L. Zhu, Z. Liu, and S. Han, "Deep leakage from gradients," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 32, 2019, pp. 17–31.

[154] Y. Fraboni, R. Vidal, and M. Lorenzi, "Free-rider attacks on model aggregation in federated learning," in *Proc. Int. Conf. Artif. Intell. Stat.*, 2021, pp. 1846–1854.

[155] X. Zhang, S. Lin, C. Chen, and X. Chen, "MODA: Model ownership deprivation attack in asynchronous federated learning," *IEEE Trans. Depend. Secure Comput.*, vol. 21, no. 4, pp. 4220–4235, Jul./Aug. 2024.

[156] T. Kim, S. Singh, N. Madaan, and C. Joe-Wong, "Characterizing internal evasion attacks in federated learning," in *Proc. Int. Conf. Artif. Intell. Stat.*, 2023, pp. 907–921.

[157] C. Sandeepa, B. Siniarski, N. Kourtellis, S. Wang, and M. Liyanage, "A survey on privacy for B5G/6G: New privacy challenges, and research directions," *J. Ind. Inf. Integr.*, vol. 30, Nov. 2022, Art. no. 100405.

[158] M. Finck and F. Pallas, "They who must not be identified—Distinguishing personal from non-personal data under the GDPR," *Int. Data Privacy Law*, vol. 10, no. 1, pp. 11–36, 2020.

[159] C. Sandeepa, B. Siniarski, N. Kourtellis, S. Wang, and M. Liyanage, "A survey on privacy of personal and non-personal data in B5G/6G networks," *ACM Comput. Surveys*, vol. 56, no. 10, pp. 1–37, 2024.

[160] M. Devi and A. Majumder, "Side-channel attack in Internet of Things: A survey," in *Proc. Appl. Internet Things (ICCCIOT)*, 2021, pp. 213–222.

[161] S. Pallavi and V. A. Narayanan, "An overview of practical attacks on BLE based IoT devices and their security," in *Proc. 5th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, 2019, pp. 694–698.

[162] Z. Wang, L. Sun, and H. Zhu, "Defining social engineering in cybersecurity," *IEEE Access*, vol. 8, pp. 85094–85115, 2020.

[163] Z. Liu, J. Guo, W. Yang, J. Fan, K.-Y. Lam, and J. Zhao, "Privacy-preserving aggregation in federated learning: A survey," *IEEE Trans. Big Data*, early access, Jul. 15, 2022, doi: 10.1109/TBDATA.2022.3190835.

[164] S. Latif, A. Qayyum, M. Usama, J. Qadir, A. Zwitter, and M. Shahzad, "Caveat emptor: The risks of using big data for human development," *IEEE Technol. Soc. Mag.*, vol. 38, no. 3, pp. 82–90, Sep. 2019.

[165] M. Janssen, P. Brous, E. Estevez, L. S. Barbosa, and T. Janowski, "Data governance: Organizing data for trustworthy artificial intelligence," *Govt. Inf. Quart.*, vol. 37, no. 3, 2020, Art. no. 101493.

[166] C. Sandeepa, B. Siniarski, S. Wang, and M. Liyanage, "FL-TIA: Novel time inference attacks on federated learning," in *Proc. IEEE 22nd Int. Conf. Trust Security Privacy Comput. Commun. (TrustCom)*, 2023, pp. 173–180.

[167] M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A survey on privacy and security of Internet of Things," *Comput. Sci. Rev.*, vol. 38, Nov. 2020, Art. no. 100312.

[168] A. K. R. Nadikattu, "IoT and the issue of data privacy," *Int. J. Innov. Eng. Res. Technol.*, vol. 5, no. 10, pp. 23–26, 2018.

[169] M. Seliem, K. Elgazzar, and K. Khalil, "Towards privacy preserving IoT environments: A survey," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–15, Nov. 2018.

[170] A. Alamleh et al., "Federated learning for IoMT applications: A standardization and benchmarking framework of intrusion detection systems," *IEEE J. Biomed. Health Informat.*, vol. 27, no. 2, pp. 878–887, Feb. 2023.

[171] H. Yang, A. Alphones, Z. Xiong, D. Niyato, J. Zhao, and K. Wu, "Artificial-intelligence-enabled intelligent 6G networks," *IEEE Netw.*, vol. 34, no. 6, pp. 272–280, Nov./Dec. 2020.

[172] N. Rodríguez-Barroso, D. Jiménez-López, M. V. Luzón, F. Herrera, and E. Martínez-Cámara, "Survey on federated learning threats: Concepts, taxonomy on attacks and defences, experimental study and challenges," *Inf. Fusion*, vol. 90, pp. 148–173, Feb. 2023.

[173] C. Zhang, S. Ekanut, L. Zhen, and Z. Li, "Augmented multi-party computation against gradient leakage in federated learning," *IEEE Trans. Big Data*, vol. 10, no. 6, pp. 742–751, Dec. 2024.

[174] B. Bebensee, "Local differential privacy: A tutorial," 2019, *arXiv:1907.11908*.

[175] M. Abadi et al., "Deep learning with differential privacy," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 308–318.

[176] C. Dwork et al., "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, nos. 3–4, pp. 211–407, 2014.

[177] E. Bagdasaryan, O. Poursaeed, and V. Shmatikov, "Differential privacy has disparate impact on model accuracy," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 32, 2019, pp. 1–10.

[178] S. Truex, L. Liu, K.-H. Chow, M. E. Gursoy, and W. Wei, "LDP-FED: Federated learning with local differential privacy," in *Proc. 3rd ACM Int. Workshop Edge Syst. Anal. Netw.*, 2020, pp. 61–66.

[179] A. Yousefpour et al., "OPACUS: User-friendly differential privacy library in pyTorch," 2021, *arXiv:2109.12298*.

[180] R. Hu, Y. Guo, H. Li, Q. Pei, and Y. Gong, "Personalized federated learning with differential privacy," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9530–9539, Oct. 2020.

[181] H. Hu, Z. Salcic, L. Sun, G. Dobbie, and X. Zhang, "Source inference attacks in federated learning," in *Proc. IEEE Int. Conf. Data Min. (ICDM)*, 2021, pp. 1102–1107.

[182] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[183] H. F. Khojir, D. Alhadidi, S. Rouhani, and N. Mohammed, "FedShare: Secure aggregation based on additive secret sharing in federated learning," in *Proc. 27th Int. Database Eng. Appl. Symp.*, 2023, pp. 25–33.

[184] S. Truex et al., "A hybrid approach to privacy-preserving federated learning," in *Proc. 12th ACM Workshop Artif. Intell. Security*, 2019, pp. 1–11.

[185] E. Sotthiwat, L. Zhen, Z. Li, and C. Zhang, "Partially encrypted multi-party computation for federated learning," in *Proc. IEEE/ACM 21st Int. Symp. Cluster Cloud Internet Comput. (CCGrid)*, 2021, pp. 828–835.

[186] C. Sandeepa, B. Siniarski, S. Wang, and M. Liyanage, "REC-DEF: A recommendation-based defence mechanism for privacy preservation in federated learning systems," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 2716–2728, Feb. 2024.

[187] T.-C. Chiu, W.-C. Lin, A.-C. Pang, and L.-C. Cheng, "Dual-masking framework against two-sided model attacks in federated learning," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2021, pp. 1–6.

[188] I. Ergun, H. U. Sami, and B. Guler, "Sparsified secure aggregation for privacy-preserving federated learning," 2021, *arXiv:2112.12872*.

[189] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Comput. Surveys*, vol. 51, no. 4, pp. 1–35, 2018.

[190] H. Fang and Q. Qian, "Privacy preserving machine learning with homomorphic encryption and federated learning," *Future Internet*, vol. 13, no. 4, p. 94, 2021.

[191] G. Peralta, R. G. Cid-Fuentes, J. Bilbao, and P. M. Crespo, "Homomorphic encryption and network coding in IoT architectures: Advantages and future challenges," *Electronics*, vol. 8, no. 8, p. 827, 2019.

[192] Z. Ma, J. Ma, Y. Miao, Y. Li, and R. H. Deng, "ShieldFL: Mitigating model poisoning attacks in privacy-preserving federated learning," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 1639–1654, 2022.

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

[194] M. Shayan, C. Fung, C. J. M. Yoon, and I. Beschastnikh, "Biscotti: A blockchain system for private and secure federated learning," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 7, pp. 1513–1525, Jul. 2021.

[195] Z. Yang, Y. Shi, Y. Zhou, Z. Wang, and K. Yang, "Trustworthy federated learning via blockchain," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 92–109, Jan. 2023.

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

[197] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon, "A framework for privacy-preservation of IoT healthcare data using federated learning and blockchain technology," *Future Gener. Comput. Syst.*, vol. 129, pp. 380–388, Apr. 2022.

[198] M. Al Asqah and T. Moulahi, "Federated learning and blockchain integration for privacy protection in the Internet of Things: Challenges and solutions," *Future Internet*, vol. 15, no. 6, p. 203, 2023.

[199] Z. Mahmood and V. Jusas, "Blockchain-enabled: Multi-layered security federated learning platform for preserving data privacy," *Electronics*, vol. 11, no. 10, p. 1624, 2022.

[200] D. Hamouda, M. A. Ferrag, N. Benhamida, and H. Seridi, "PPSS: A privacy-preserving secure framework using blockchain-enabled federated deep learning for Industrial IoTs," *Pervasive Mobile Comput.*, vol. 88, Jan. 2023, Art. no. 101738.

[201] A. Lakhan et al., "Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare," *IEEE Sensors J. Biomed. Health Informat.*, vol. 27, no. 2, pp. 664–672, Feb. 2023.

[202] N. Wang et al., "A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles," *Digit. Commun. Netw.*, vol. 10, no. 1, pp. 126–134, 2022.

[203] B. Ghimire and D. B. Rawat, "Secure, privacy preserving, and verifiable federating learning using blockchain for Internet of Vehicles," *IEEE Consum. Electron. Mag.*, vol. 11, no. 6, pp. 67–74, Nov. 2022.

[204] A. R. Javed et al., "Integration of blockchain technology and federated learning in vehicular (IoT) networks: A comprehensive survey," *Sensors*, vol. 22, no. 12, p. 4394, 2022.

[205] T. Moulahi et al., "Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security," *Exp. Syst.*, vol. 40, no. 5, 2023, Art. no. e13103.

[206] L. Javed, A. Anjum, B. M. Yakubu, M. Iqbal, S. A. Moqurrab, and G. Srivastava, "ShareChain: Blockchain-enabled model for sharing patient data using federated learning and differential privacy," *Exp. Syst.*, vol. 40, no. 5, 2023, Art. no. e13131.

[207] Z. A. E. Houda, A. S. Hafid, L. Khoukhi, and B. Brik, "When collaborative federated learning meets blockchain to preserve privacy in healthcare," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 5, pp. 2455–2465, Sep./Oct. 2023.

[208] C. Fang, Y. Guo, J. Ma, H. Xie, and Y. Wang, "A privacy-preserving and verifiable federated learning method based on blockchain," *Comput. Commun.*, vol. 186, pp. 1–11, Mar. 2022.

[209] I. Ullah, X. Deng, X. Pei, P. Jiang, and H. Mushtaq, "A verifiable and privacy-preserving blockchain-based federated learning approach," *Peer-to-Peer Netw. Appl.*, vol. 16, no. 5, pp. 2256–2270, 2023.

[210] Y. Miao et al., "Privacy-preserving Byzantine-robust federated learning via blockchain systems," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 2848–2861, 2022.

[211] M. H. Ur Rehman, K. Salah, E. Damiani, and D. Svetinovic, "Towards blockchain-based reputation-aware federated learning," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, 2020, pp. 183–188.

[212] Y. Qi, M. S. Hossain, J. Nie, and X. Li, "Privacy-preserving blockchain-based federated learning for traffic flow prediction," *Future Gener. Comput. Syst.*, vol. 117, pp. 328–337, Apr. 2021.

[213] Q. Hu, Z. Wang, M. Xu, and X. Cheng, "Blockchain and federated edge learning for privacy-preserving mobile crowdsensing," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 12000–12011, Jun. 2023.

[214] M. Qi et al., "A blockchain-enabled federated learning model for privacy preservation: System design," in *Proc. 26th Aust. Conf. Inf. Security Privacy (ACISP)*, 2021, pp. 473–489.

[215] Y. Wan, Y. Qu, L. Gao, and Y. Xiang, "Privacy-preserving blockchain-enabled federated learning for B5G-driven edge computing," *Comput. Netw.*, vol. 204, Feb. 2022, Art. no. 108671.

[216] K. M. Sameera et al., "Privacy-preserving in blockchain-based federated learning systems," *Comput. Commun.*, vol. 222, pp. 38–67, Jun. 2024.

[217] L. Ouyang et al., "Artificial identification: A novel privacy framework for federated learning based on blockchain," *IEEE Trans. Comput. Soc. Syst.*, vol. 10, no. 6, pp. 3576–3585, Dec. 2023.

[218] D. Li and J. Wang, "FedMD: Heterogenous federated learning via model distillation," 2019, *arXiv:1910.03581*.

[219] J. Gou, B. Yu, S. J. Maybank, and D. Tao, "Knowledge distillation: A survey," *Int. J. Comput. Vis.*, vol. 129, pp. 1789–1819, Mar. 2021.

[220] C. Xie, M. Chen, P.-Y. Chen, and B. Li, "CRFL: Certifiably robust federated learning against backdoor attacks," in *Proc. Int. Conf. Mach. Learn.*, 2021, pp. 11372–11382.

[221] C. Sandeepa, B. Siniarski, S. Wang, and M. Liyanage, "SHERPA: Explainable robust algorithms for privacy-preserved federated learning in future networks to defend against data poisoning attacks," in *Proc. IEEE Symp. Security Privacy (SP)*, 2024, pp. 201–204.

[222] M. Benmalek, M. A. Benrekia, and Y. Challal, "Security of federated learning: Attacks, defensive mechanisms, and challenges," *Revue des Sciences et Technologies de l'Information-Série RIA: Revue d'Intelligence Artificielle*, vol. 36, no. 1, pp. 49–59, 2022.

[223] Y. Li, A. S. Sani, D. Yuan, and W. Bao, "Enhancing federated learning robustness through clustering non-IID features," in *Proc. Asian Conf. Comput. Vis.*, 2022, pp. 41–55.

[224] F. Mo, H. Haddadi, K. Katevas, E. Marin, D. Perino, and N. Kourtellis, "PPFL: Privacy-preserving federated learning with trusted execution environments," in *Proc. 19th Annu. Int. Conf. Mobile Syst. Appl. Services*, 2021, pp. 94–108.

[225] G. Cormode, S. Jha, T. Kulkarni, N. Li, D. Srivastava, and T. Wang, "Privacy at scale: Local differential privacy in practice," in *Proc. Int. Conf. Manag. Data*, 2018, pp. 1655–1658.

[226] T. Zhu, D. Ye, W. Wang, W. Zhou, and S. Y. Philip, "More than privacy: Applying differential privacy in key areas of artificial intelligence," *IEEE Trans. Knowl. Data Eng.*, vol. 34, no. 6, pp. 2824–2843, Jun. 2022.

[227] K. Yang, T. Jiang, Y. Shi, and Z. Ding, "Federated learning via over-the-air computation," *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 2022–2035, Mar. 2020.

[228] R. Kanagavelu et al., "Two-phase multi-party computation enabled privacy-preserving federated learning," in *Proc. 20th IEEE/ACM Int. Symp. Clust. Cloud Internet Comput. (CCGRID)*, 2020, pp. 410–419.

[229] R. Kanagavelu et al., "CE-Fed: Communication efficient multi-party computation enabled federated learning," *Array*, vol. 15, Sep. 2022, Art. no. 100207.

[230] C. Sandeepa, T. Senevirathna, B. Siniarski, S. Wang, and M. Liyanage, "Navigating explainable privacy in federated learning," in *Proc. IFIP Netw. Conf. (IFIP Netw.)*, 2024, pp. 763–768.

[231] 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.*, vol. 10, no. 5, pp. 2864–2880, Sep./Oct. 2023.

[232] N. Patel, R. Shokri, and Y. Zick, "Model explanations with differential privacy," in *Proc. ACM Conf. Fairness Accountability Transp.*, 2022, pp. 1895–1904.

[233] M. T. Hossain, S. Islam, S. Badsha, and H. Shen, "DeSMP: Differential privacy-exploited stealthy model poisoning attacks in federated learning," in *Proc. IEEE 17th Int. Conf. Mobility Sens. Netw. (MSN)*, 2021, pp. 167–174.

[234] J. Seo, K. Kim, M. Park, M. Park, and K. Lee, "An analysis of economic impact on IoT industry under GDPR," *Mobile Inf. Syst.*, vol. 2018, pp. 1–6, Dec. 2018.

[235] Y. Zhao et al., "Local differential privacy-based federated learning for Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8836–8853, Jun. 2021.
[236] P. Zhao, Z. Cao, J. Jiang, and F. Gao, "Practical private aggregation in federated learning against inference attack," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 318–329, Jan. 2023.
[237] B. Hasırcıoğlu and D. Gündüz, "Private wireless federated learning with anonymous over-the-air computation," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, 2021, pp. 5195–5199.
[238] D. Liu and O. Simeone, "Privacy for free: Wireless federated learning via uncoded transmission with adaptive power control," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 1, pp. 170–185, Jan. 2021.
[239] A. Goldsteen, G. Ezov, R. Shmelkin, M. Moffie, and A. Farkash, "Data minimization for GDPR compliance in machine learning models," *AI Ethics*, vol. 2, pp. 477–491, Sep. 2021.
[240] A. J. Biega, P. Potash, H. Daumé, F. Diaz, and M. Finck, "Operationalizing the legal principle of data minimization for personalization," in *Proc. 43rd Int. ACM SIGIR Conf. Res. Develop. Inf.*, 2020, pp. 399–408.
[241] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016.
[242] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, "Edge intelligence: Paving the last mile of artificial intelligence with edge computing," *Proc. IEEE*, vol. 107, no. 8, pp. 1738–1762, Aug. 2019.
[243] M. S. Murshed, C. Murphy, D. Hou, N. Khan, G. Ananthanarayanan, and F. Hussain, "Machine learning at the network edge: A survey," *ACM Comput. Surveys*, vol. 54, no. 8, pp. 1–37, 2021.
[244] H. H. Kumar, V. Karthik, and M. K. Nair, "Federated *k*-means clustering: A novel edge Ai based approach for privacy preservation," in *Proc. IEEE Int. Conf. Cloud Comput. Emerg. Markets (CCEM)*, 2020, pp. 52–56.
[245] Y. Zhang, "Mobile edge computing for beyond 5G/6G," in *Mobile Edge Computing*. Cham, Switzerland: Springer, 2022, pp. 37–45.
[246] A. Dogra, R. K. Jha, and S. Jain, "A survey on beyond 5G network with the advent of 6G: Architecture and emerging technologies," *IEEE Access*, vol. 9, pp. 67512–67547, 2020.
[247] T. Zhang, C. He, T. Ma, L. Gao, M. Ma, and S. Avestimehr, "Federated learning for Internet of Things," in *Proc. 19th ACM Conf. Embedded Netw. Sensor Syst.*, 2021, pp. 413–419.
[248] Q. Wu, K. He, and X. Chen, "Personalized federated learning for intelligent IoT applications: A cloud-edge based framework," *IEEE Open J. Comput. Soc.*, vol. 1, pp. 35–44, 2020.
[249] F. Naeem, M. Ali, and G. Kaddoum, "Federated-learning-empowered semi-supervised active learning framework for intrusion detection in ZSM," *IEEE Commun. Mag.*, vol. 61, no. 2, pp. 88–94, Feb. 2023.
[250] C. Huang, J. Huang, and X. Liu, "Cross-silo federated learning: Challenges and opportunities," 2022, *arXiv:2206.12949*.
[251] T. Ranathunga, A. McGibney, S. Rea, and S. Bharti, "Blockchain-based decentralized model aggregation for cross-silo federated learning in industry 4.0," *IEEE Internet Things J.*, vol. 10, no. 5, pp. 4449–4461, Mar. 2023.
[252] C. De Alwis, Q.-V. Pham, and M. Liyanage, *6G Frontiers: Towards Future Wireless Systems*. Hoboken, NJ, USA: Wiley, 2022.
[253] Y. Wang, Z. Su, N. Zhang, and A. Benslimane, "Learning in the air: Secure federated learning for UAV-assisted crowdsensing," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1055–1069, Apr./Jun. 2021.
[254] A. M. Elbir, B. Soner, S. Çöleri, D. Gündüz, and M. Bennis, "Federated learning in vehicular networks," in *Proc. IEEE Int. Mediterr. Conf. Commun. Netw. (MeditCom)*, 2022, pp. 72–77.
[255] D. J. Beutel et al., "Flower: A friendly federated learning research framework," 2020, *arXiv:2007.14390*.
[256] A. Ziller et al., "Pysyft: A library for easy federated learning," in *Federated Learning Systems: Towards Next-Generation AI*. Cham, Switzerland: Springer, pp. 111–139, 2021.
[257] Google. "TensorFlow federated: Machine learning on decentralized data." Accessed: Oct. 10, 2024. [Online]. Available: https://www.tensorflow.org/federated
[258] Federated AI Technology Enabler (FATE). "An industrial grade federated learning framework," Accessed: Oct. 10, 2024. [Online]. Available: https://github.com/FederatedAI/FATE
[259] University of Murcia Federated Learning Research Group. "NEBULA: A platform for decentralized federated learning." 2024. [Online]. Available: https://federatedlearning.inf.um.es/
[260] Z. Hu, K. Shaloudegi, G. Zhang, and Y. Yu, "Federated learning meets multi-objective optimization," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 4, pp. 2039–2051, Jul./Aug. 2022.
[261] S. B. Ramezani, A. Sommers, H. K. Manchukonda, S. Rahimi, and A. Amirlatifi, "Machine learning algorithms in quantum computing: A survey," in *Proc. IEEE Int. Joint Conf. Neural Netw. (IJCNN)*, 2020, pp. 1–8.
[262] S. Y.-C. Chen and S. Yoo, "Federated quantum machine learning," *Entropy*, vol. 23, no. 4, p. 460, 2021.
[263] H. T. Larasati, M. Firdaus, and H. Kim, "Quantum federated learning: Remarks and challenges," in *Proc. IEEE 9th Int. Conf. Cyber Security Cloud Comput. (CSCloud) IEEE 8th Int. Conf. Edge Comput. Scalable Cloud (EdgeCom)*, 2022, pp. 1–5.
[264] Q. Xia and Q. Li, "QuantumFED: A federated learning framework for collaborative quantum training," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2021, pp. 1–6.
[265] C. Easttom, "Quantum computing and cryptography," in *Modern Cryptography: Applied Mathematics for Encryption and Information Security*. Cham, Switzerland: Springer, 2022, pp. 397–407.
[266] R. R. Harmon and N. Auseklis, "Sustainable it services: Assessing the impact of green computing practices," in *Proc. IEEE Int. Conf. Manag. Eng. Technol. (PICMET)*, 2009, pp. 1707–1717.
[267] Q. Zeng, Y. Du, K. Huang, and K. K. Leung, "Energy-efficient radio resource allocation for federated edge learning," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, 2020, pp. 1–6.
[268] S. Wang et al., "Adaptive federated learning in resource constrained edge computing systems," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 6, pp. 1205–1221, Jun. 2019.
[269] T. T. Huong et al., "Federated learning-based explainable anomaly detection for industrial control systems," *IEEE Access*, vol. 10, pp. 53854–53872, 2022.
[270] A. Manna, H. Kasyap, and S. Tripathy, "MOAT: Model agnostic defense against targeted poisoning attacks in federated learning," in *Proc. 23rd Int. Conf. Inf. Commun. Security (ICICS)*, 2021, pp. 38–55.
[271] X. Zhao, W. Zhang, X. Xiao, and B. Lim, "Exploiting explanations for model inversion attacks," in *Proc. IEEE/CVF Int. Conf. Comput. Vis.*, 2021, pp. 682–692.
[272] A. Kuppa and N.-A. Le-Khac, "Adversarial XAI methods in cybersecurity," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4924–4938, 2021.
[273] J. L. C. Bárcena et al., "Fed-XAI: Federated learning of explainable artificial intelligence models," in *Proc. 3rd Italian Workshop Explain. Artif. Intell. (XAI.it)*, 2022, pp. 104–117.

CHAMARA SANDEEPA (Student Member, IEEE) received the bachelor's degree in electrical and information engineering from the University of Ruhuna, Sri Lanka, in 2020. He is currently pursuing the Ph.D. degree with the School of Computer Science, University College Dublin, Ireland. He is also a member of the Network Softwarization and Security Labs, UCD, a Contributing Researcher in the EU ROBUST-6G Project and a Research Engineer of the EU H2020 SPATIAL Project. He is currently working in the field of privacy aspects of Federated Learning, with a focus on privacy vulnerabilities and attacks targeting Federated Learning clients and potential defenses against the threats. During his undergraduate period and later work, he actively contributed to research and published in multiple IEEE conferences and journals. He has professional experience in software engineering and working experience in the fields of Open RAN, IoT, and explainable AI.

ENGIN ZEYDAN (Senior Member, IEEE) received the Ph.D. degree from the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ, USA, in 2011. He is a Senior Researcher with the Services as Networks Research Unit, Centre Tecnològic de Telecomunicacions de Catalunya, Barcelona, Spain. He was the Project Coordinator of the European Union H2020 MonB5G Project from 2021 to 2023. His research interests are in the areas of telecommunications, data engineering/science, and network security.

THARAKA SAMARASINGHE (Senior Member, IEEE) was born in Colombo, Sri Lanka. He received the B.Sc. degree in engineering from the Department of Electronic and Telecommunication Engineering, University of Moratuwa, Sri Lanka, in 2008, and the Ph.D. degree from the Department of Electrical and Electronic Engineering, University of Melbourne, Australia, in 2012. He was a Postdoctoral Research Fellow with the Department of Electrical and Computer Systems Engineering, Monash University, Australia, from 2012 to 2014. He has been with the Department of Electronic and Telecommunication Engineering, University of Moratuwa since January 2015, where he is a Senior Lecturer. He has also served as an Honorary Fellow with the Department of Electrical and Electronic Engineering, University of Melbourne from 2016 to 2023 and a Postdoctoral Research Fellow with the School of Engineering, RMIT University, Australia, from 2022 to 2023. His research interests are in communications theory, information theory, and wireless networks. He received the award for the most outstanding undergraduate upon graduation from the University of Moratuwa.

MADHUSANKA LIYANAGE (Senior Member, IEEE) received the Doctor of Technology degree in communication engineering from the University of Oulu, Oulu, Finland, in 2016. He is an Associate Professor/Ad Astra Fellow and the Director of Graduate Research with the School of Computer Science, University College Dublin, Ireland. He leads the Network Softwarization and Security Labs, UCD. He is also acting as a Docent/Adjunct Professor with the Center for Wireless Communications, University of Oulu, and a Honorary Adjunct Professor with the University of Ruhuna, Sri Lanka, and the University of Sri Jayawardhanepura, Sri Lanka. He also received the prestigious Marie Skłodowska-Curie Actions Individual Fellowship and the Government of Ireland Postdoctoral Fellowship from 2018 to 2020. His research interests are 5G/6G, blockchain, network security, artificial intelligence (AI), explainable AI, federated learning, network slicing, Internet of Things, and multiaccess edge computing. In 2020, he received the "2020 IEEE ComSoc Outstanding Young Researcher" Award from IEEE ComSoc EMEA. Also, he was awarded an Irish Research Council (IRC) Research Ally Prize as part of the IRC Researcher of the Year 2021 Awards for his positive impact as a Supervisor. In 2022, he received "The 2022 Tom Brazil Excellence in Research Award" from the SFI CONNECT Center. In 2021, 2022, 2023, and 2024, he was ranked among the World's Top 2% Scientists (2020, 2021, 2022, and 2023) in the List that Elsevier BV, Stanford University, USA, prepared. For more information, see www.madhusanka.com.