ITU Journal of Wireless Communications and Cybersecurity

ITU/JWCC

A Survey On Security and Privacy Aspects and Solutions for Federated Learning in Mobile Communication Networks

Şükrü Erdal[1], Ferhat Karakoç[2], and Enver Özdemir[1]

[1] Istanbul Technical University, Informatics Institute, Istanbul, 34469, Turkey
[2] Ericsson Research, Arı Teknokent 2, Istanbul, 34485, Turkey

Abstract: In this study, we delve into cutting-edge solutions for security-centric, privacy-enhanced federated learning, a rapidly evolving area of research that bridges the gap between data privacy and collaborative machine learning. Our analysis offers a comprehensive comparative evaluation of existing methodologies, shedding light on the strengths and limitations of current approaches. By introducing new perspectives, we aim to push the boundaries of secure federated learning, exploring techniques that enhance data protection without compromising learning efficiency. Additionally, we highlight emerging challenges and opportunities in the field, emphasizing the importance of scalable, privacy-preserving mechanisms in decentralized systems. As federated learning continues to gain traction across various sectors such as healthcare, finance, and IoT, our study serves as a foundation for future research, identifying key areas for innovation and improvement. This forward-looking approach ensures that federated learning can continue to evolve as a trustworthy and robust solution for privacy-sensitive applications, addressing both current and future security concerns.

Keywords: Federated learning, privacy, secure aggregation, homomorphic encryption, secure multi-party computation.

Mobil İletişim Ağları Alanında Güvenli ve Mahremiyet Odaklı Federe Öğrenme Üzerine Bir Araştırma

Özet: Bu çalışmada, veri gizliliği ile iş birliğine dayalı makine öğrenimi arasındaki boşluğu dolduran güvenlik odaklı, gizlilik artırılmış federe öğrenme için en son çözümleri ele alıyoruz. Analizimiz, mevcut metodolojilerin kapsamlı bir karşılaştırmalı değerlendirmesini sunarak, mevcut yaklaşımların güçlü ve zayıf yönlerine ışık tutuyor. Yeni bakış açıları sunarak, güvenli federe öğrenmenin sınırlarını zorlamayı ve öğrenme verimliliğinden ödün vermeden veri korumasını artıran teknikleri keşfetmeyi amaçlıyoruz. Ayrıca, merkezi olmayan sistemlerde ölçeklenebilir, mahremiyet odaklı mekanizmaların önemini vurgulayan ortaya çıkan zorluklar ve fırsatlara dikkat çekiyoruz. Federe öğrenme, sağlık hizmetleri, finans ve Nesnelerin Interneti gibi çeşitli sektörlerde hız kazanmaya devam ederken, çalışmamız, yenilik ve gelişim için önemli alanları belirleyerek, gelecekteki araştırmalar için bir temel niteliği taşıyor. Bu ileriye dönük yaklaşım, federe öğrenmenin hem mevcut hem de gelecekteki güvenlik kaygılarını ele alarak, gizliliğe duyarlı uygulamalar için güvenilir ve sağlam bir çözüm olarak gelişmeye devam etmesini sağlıyor.

Anahtar Kelimeler: Federe öğrenme, mahremiyet, güvenli birleştirme, homomorfik şifreleme, çok taraflı güvenli hesaplama.

REVIEW PAPER

Corresponding Author: Şükrü Erdal, erdal21@itu.edu.tr
Reference: Ş. Erdal, F. Karakoç, and E.Özdemir, (2024), “A Survey On Security and Privacy Aspects and Solutions for Federated Learning in Mobile Communication Networks,” *ITU Journ. Wireless Comm. Cyber.*, 1, (1) 29–40.

Submission Date: May, 12, 2024
Acceptance Date: June, 2, 2024
Online Publishing: Sept, 30, 2024

1 INTRODUCTION

Machine Learning (ML) is garnering increased attention due to its promising benefits across a broad spectrum of applications, fulfilling needs such as automated management, optimization, enhanced user experiences, and security automation in IoT and mobile communication use cases. This surge in interest has led to a significant uptick in ML deployment. Given that decisions driven by ML can carry substantial implications, the security of ML systems is paramount. Moreover, considering ML's inherent reliance on vast datasets, which may include sensitive corporate information or personal data, concerns regarding privacy and data security are inevitable. To enhance the precision of ML models, incorporating data from multiple providers—a practice known as collaborative ML—is often preferred. However, the involvement of numerous participants in collaborative ML setups amplifies the risks associated with privacy and security [1]. A notable approach to privacy-conscious collaborative ML is federated learning (FL) [2]. This framework consists of a central server and multiple clients. The server initiates the process by distributing an initial global model to the clients. Subsequently, the clients utilize their private datasets to refine the global model locally. These enhanced models are then transmitted back to the server. Upon receipt, the server aggregates the updates to produce an improved iteration of the global model. This cycle is reiterated until the global model reaches convergence. Nonetheless, the standard implementation of FL falls short in addressing privacy issues, as the model updates relayed from clients to the server may inadvertently disclose sensitive information from the private training datasets of the clients.

The literature abounds with studies aimed at tackling the security (e.g., poisoning attacks) and privacy challenges inherent in collaborative FL [3]. For instance, a prevalent strategy to bolster privacy is the implementation of secure aggregation protocols. These protocols ensure that individual model updates are transmitted to the server in a manner that safeguards the confidentiality of the data. An additional concern pertains to the security of the FL process. Given the multitude of participants within the FL framework, there is a plausible risk that one or more clients may become compromised. Such entities might attempt to engage in malicious activities, including manipulating the global model to serve nefarious objectives—a type of assault known as a poisoning attack [4]. To mitigate such attacks, the server must implement anomaly detection mechanisms to scrutinize model updates from clients. However, if a secure aggregation protocol is in place, the server's ability to inspect individual model updates for poisoning attack detection is hindered due to the encryption. Consequently, the principal challenge lies in achieving both security and privacy concurrently. While the literature presents several solutions that tackle this issue, they often exhibit limitations regarding their practical applicability.

In this paper, we examine the existing privacy and security-enhanced FL solutions, categorize them considering generic approaches used, compare them in terms of their advantages and drawbacks, and analyze their applicability in the industrial IoT (IIoT) domain which is one of the promising domains where the ML is widely used. To be able to analyze the applicability of these privacy and security-enhanced solutions in this domain, we first provide information about the requirements of the application of ML in mobile communication networks, we then conduct a comprehensive survey of existing FL solutions tailored for mobile communication networks. Upon reviewing these FL solutions, we present an overview of generic security and privacy-enhanced FL strategies found in the literature and evaluate their relevance and effectiveness within this specific context. Despite the abundance of surveys on FL, we recognize a gap in the scholarly discourse; to our knowledge, no existing survey thoroughly examines the application and challenges of FL within the mobile communication domain.

The paper is organized as follows. In Section 2, we mention the existing surveys and highlight our surveys. Section 3 is devoted to domain-specific information and analysis of existing FL solutions applied in this domain. We revisit the generic existing solutions for privacy and security-enhanced FL in the literature in Section 4. We share some identified possible research directions and conclude the paper with Section 5.

2 SURVEYS ON FEDERATED LEARNING

In this section, we commence by aggregating existing surveys that focus on security and privacy in FL. Subsequently, we furnish insights into the surveys that delve into the application of FL in the mobile communication sphere. Lastly, we underscore the unique contributions of our study.

2.1 Security and Privacy in Federated Learning

There have been some survey studies that present the state of the art on security and/or privacy in FL. This subsection gives information about related existing surveys and compares them in Table 1 in terms of covering security aspects ("Security"), privacy aspects ("Privacy"), mitigation solutions "Defense", security and privacy simultaneously ("S&P"), and mobile communication domain ("Mobile Comm").

Soykan et al. [1] presented generic security and privacy attacks not specific to FL but for collaborative ML in general. The work also pointed out generic solutions such as confidential computing, secure multi-party computation, homomorphic encryption, and differential privacy. In 2021, Mothukuri et al. focused on security and privacy issues specific to FL [5]. They first provide an overview and clas-

Table 1 Comparison of the surveys

Survey	Security	Privacy	Defense	S&P	Mobile Comm
Soykan et al. [1]	✓	✓	✓		
Mothukuri et al. [5]	✓	✓	✓		
Blanco-Justicia et al. [6]	✓	✓	✓		
Truong et al. [7]		✓	✓		
Bouacida and Mohapatra [8]	✓		✓		
Mansouri et al. [9]	✓	✓	✓	✓	
Enthoven and Al-Ars [10]		✓	✓		
Lyu et al. [11]	✓	✓	✓		
Mao et al. [12]	✓	✓	✓		
Asad et al. [13]		✓	✓		
Akhtarshenas et al. [14]	✓	✓	✓		
Our survey	✓	✓	✓	✓	✓

sification of FL approaches, and then identify and analyze security and privacy threats in FL settings, mitigation techniques, and trade-off costs, and share information about existing defense mechanisms and possible future directions. Another work presented in 2021 also presents security and privacy challenges in FL and also proposes a solution to enhance privacy by breaking the link between the local model update owners and local models [6]. To achieve unlinkability, they proposed to use peer-to-peer decentralized networks for anonymous communication channels. One existing study looks at the problem from the regulation perspective [7]. Since they focused on privacy regulations, they focused only on privacy aspects in FL, mainly considering privacy requirements from GDPR perspective. They analyze challenges taking the GDPR guidelines into account, which results in the need to use strong cryptographic tools. The study presented by Bouacida and Mohapatra investigated vulnerabilities in FL and performed a systematical classification of the threats in FL [8]. Beyond the research concentrating on security and privacy threats, a select number of surveys extend their scope to encompass solutions for secure and privacy-enhanced FL. The study of Mansouri et al. focused only on secure aggregation protocols which is a widely adapted privacy-enhancing technology to protect privacy in FL [9]. They classified the secure aggregation protocols and presented a comparison of the solutions. Enthoven et al. gave an overview of privacy attacks in FL and surveyed mitigation methods [10]. They also focused on insider attacks while identifying threats, and categorized the threats considering attacker types and capabilities. In a recent survey by Lyu et al., the authors presented an overview of privacy and robustness in FL [11]. Robustness means being able to secure against security attacks. They also identified defense mechanisms against certain types of attacks. They provided helpful guidance for the robust and privacy-enhanced FL. Another survey by Mao et al. discusses security and privacy concerns in FL, mentions some privacy-preserving technologies, and discusses possible future works [12]. Asad et al. examine the challenges related to communication limitations, resource allocation, client selection, and optimization methods in FL [13]. That survey underscores the importance of mitigating communication expenses to enhance the efficiency and scalability of FL. It also outlines future pathways for FL concerning communication costs. Various FL structures are examined in Akhtarshenas et al.'s study by evaluating their efficiency, accuracy, and privacy aspects [14]. The research scrutinizes contributions and findings focusing on security, resource optimization, and FL applications across different domains.

2.2 Surveys on Application of Federated Learning in Mobile Communication

Another type of survey we searched is on the application of FL in mobile communication systems. The survey [15] by Sirohi et al. gives a comprehensive picture of FL and its application in underwater, ground, air, and space environments considering security and privacy challenges. Although it gives detailed and organized information about research around FL, they don't touch the details and comparison of the solutions that try to address the security and privacy aspects in FL simultaneously. Al-Quraan, Mohjazi, et al. [16] focus on potential research directions to extend FL's capabilities into emerging areas such as 5G and 6G wireless communication systems. The specific requirements of 6G communication and the fundamental challenges faced by FL in the context of 6G applications are examined in Liu, Yuan, et al. 's study [17]. To address these challenges, a detailed overview of emerging advanced FL methods is tailored for 6G communications. These methods include communication-efficient FL, secure FL, and effective FL approaches. In a recent survey paper, Rahman et al. [18] discuss the integration of FL into the Information-Centric Networking (ICT) in the IoT domain.

Zuo et al. [19] provide a review of the recent advancements in utilizing blockchain and AI for 6G wireless communications. It thoroughly explores the integration possibilities of blockchain and AI, and motivations for integrating these technologies into 6G wireless communications, followed by discussions on their simultaneous deployment in secure services and IoT smart applications. Specifically, the survey delves into secure services supported by blockchain and AI, such as spectrum management, computation allocation, content caching, and security and privacy services. Overall, the survey aims to comprehensively explore the potential of blockchain and AI technologies in enhancing wireless communications for 6G networks.

Abimannan et al. [20] emphasize the importance of FL and multi-access edge computing (MEC) in air quality monitoring and forecasting, particularly within smart environments and cities. It highlights the increasing interest and emerging trends, as well as the potential benefits and constraints of these technologies enhanced with deep ML. With the integration of new wireless mobile networks (5G and beyond) with MEC, several applications, including air quality monitoring and control, stand to benefit from improved connectivity, faster processing, and enhanced real-time analytics enabled by FL. FL facilitates collaborative model training across edge devices, ensuring data privacy and security while handling heterogeneous data from diverse sources and IoT devices at the network edge. Future research directions include addressing limitations and maximizing the potential of FL and MEC in building effective air quality monitoring and decision-making ecosystems to protect public health.

Khalek et al. [21] investigate the role of ML-driven Cognitive Radio (CR) in various network domains, including IoT, mobile, vehicular, railway, and UAV networks. Across each network category, the paper delved into the motivations behind adopting ML-driven CR and conducted a comprehensive analysis of recent research trends.

Driss et al. [22] examine FL's role within wireless communication networks. Additionally, it reviews recent contributions utilizing FL to enhance communication and Key Performance Indicators (KPIs) within the protocol stack. Lastly, the paper discusses insights and challenges associated with deploying FL strategies in 5G, 6G, and beyond.

Ferrag et al. 's survey [23] is an expository paper on the state-of-the-art vulnerabilities and defenses in FL for 6G-enabled IoT systems. Also, the paper synthesized existing research on ML security for 6G-IoT, categorizing threats across centralized, federated, and distributed learning modes. Through research and analysis, eight categories of threat models against ML have been identified: backdoor attacks, adversarial examples, combined attacks, poisoning attacks, Sybil attacks, Byzantine attacks, inference attacks, and dropping attacks. Additionally, the survey reviewed current defense methods against vulnerabilities in FL.

I. Bartsiokas et al. 's survey [24] focuses on deploying FL-based approaches within different Physical Layer (PHY) sub-problems in 6G wireless networks. To demonstrate the effectiveness of FL-based schemes in the PHY domain, simulations are conducted to investigate the problem of Relay Node (RN) placement in 6G networks. Two schemes are compared, one employing Centralized Learning (CL) and the other FL.

The complexity of data privacy and confidentiality concerns in 6G Intelligent Networks is highlighted by the presence of diverse data owners and edge devices [25]. Federated Analytics (FA) emerges as a promising distributed computing paradigm to address these challenges, facilitating collaborative value generation from data while ensuring privacy and reducing communication overheads. FA offers significant advantages in managing and securing distributed and heterogeneous data networks within 6G systems. This paper examines FA principles and benefits, proposes an implementation framework tailored for 6G networks, and identifies research challenges and open issues.

Das et al. [26] have provided insights into the deployment of distributed learning over cellular networks, covering design aspects of FL for wireless communications, performance evaluation, and the impact of wireless factors on FL metrics. The article summarizes the advantages and obstacles associated with the utilization of FL schemes. Moreover, it analyzes promising FL-based technologies such as Mobile Edge Computing (MEC), satellite communications, semantic communications, Terahertz (THz) communications, network slicing, and blockchain for 6G-IoT networks. Furthermore, the fundamentals of decentralized Multi-Agent Reinforcement Learning (MARL)-based FL algorithms and operation principles are presented. The article integrates modern concepts into the MARL-enhanced FL framework for wireless networks, including power control mechanisms, interference mitigation, communication mode selection mechanisms, and resource management for handling large state and action spaces in dynamic wireless environments. Lastly, the article discusses potential barriers and outlines further research directions for applying MARL-based FL frameworks in 6G-IoT networks.

In this survey paper, our principal contributions are delineated as follows:

- We concentrate on solutions that concurrently bolster security and privacy within FL.
- A comprehensive comparison of these solutions is conducted using 13 distinct metrics.
- Our focus narrows to the specialized domain of mobile communication networks, where we categorize the proposed FL solutions tailored for this modern era.

- We conclude by pinpointing and deliberating on potential future research directions in this burgeoning field.

3 MOBILE COMMUNICATION AND FEDERATED LEARNING APPLICATION

At a high level, it would be stated that the mobile communication system consists of user equipment (UE), a radio access network (RAN), the core network (CN), a management layer (OAM), exposure layer, roaming interfaces, and business/operation support systems (OSS/BSS). All of these components except the OSS/BSS component are specified by the 3rd Generation Partnership Project (3GPP). Due to the vast and intricate architecture of the system, the implementation of AI/ML for addressing complex optimization challenges facilitates a decrease in operational costs. It ensures the provision of promising services with reduced emissions and the optimized allocation of resources, contributing to a sustainable world and enhancing the user experience.

The extensive integration of AI/ML in mobile communications commenced with the advent of 5G, encompassing not only proprietary solutions but also standardized ones. For instance, the 3GPP has formalized the application of AI/ML within core network management, as delineated in 3GPP TS 23.228, and within the Operation, Administration, and Maintenance (OAM) layer, as specified in 3GPP TS 28.105. In addition to the deployment of AI/ML, the 3GPP has further delineated the use of a collaborative ML approach, known as FL, in Release 18. Also, 3GPP started to study on incorporation of additional AI/ML mechanisms in Release 19, such as vertical FL.

The standardization of 5G systems is nearing completion, and with the advent of Release 20, the groundwork for 6G standardization studies will commence. The foundational elements for the 6G architecture have been identified in Hexa-X European Union research project, and the integration of these enablers is currently being explored in the design of a 6G architecture, as outlined in Hexa-X-II (the follow-up European Union research project of Hexa-X). The fulfillment of 6G use cases—encompassing a connected sustainable world, intelligent autonomous machines, the convergence of physical and cyber worlds, and the Internet of Senses—will necessitate a greater reliance on AI/ML solutions [27]–[29].

3.1 Federated Learning Solutions

In Section 2.2, we have mentioned existing surveys about the utilization of FL in mobile communication. In this subsection, we focus on the existing proposed solutions for usage of FL in mobile communication systems.

In 2020, Liu et al. proposed a framework for secure FL for 5G networks [30]. They focused on the two attacks: poisoning and membership inference attacks. They proposed a blockchain-based solution that prevents malicious actors from joining the FL setup and performing poisoning attacks. To mitigate the privacy concern, they propose local differential privacy. To increase the privacy level of FL usage in the core network, Zhou and Ansari propose the usage of partially homomorphic encryption in the NWDAF (Network Data Analytics Function) FL architecture [31]. They introduce a new entity for the generation and distribution of the keys. Phyu et al. 's study focuses on the RAN side for the use case of traffic forecasting [32]. They address the privacy concerns in the utilization of FL in the multi-slice setting. Hewa et. al. propose to use blockchain to make FL robust in 5G and beyond networks in their study [33]. Khowaja et al. present a comprehensive framework designed to assess the susceptibility of FL to poisoning and inversion attacks within 6G vehicular networks [34]. This analysis underscores the critical need for incorporating robust security and privacy measures in the deployment of FL technologies.

In 2023, Sanon, Reddy, et al. investigate computation on encrypted data technologies via secure multi-party computation for analysis of the network traffic data coming from different companies [35]. In addition to RAN, the core network, and specific vertical domains like vehicular networks, there is burgeoning research within the Open-RAN sector. Notably, one study concentrates on leveraging FL within the Open-RAN architecture to enhance automation capabilities [21].

Wasilewska et al. study the security of FL in the cognitive radio sensing use case [36]. Privacy in FL may especially become important if it is executed among multiple operators. Lan et al.'s study considers this multi-operator setup for the FL execution for performance prediction [37]. Another work that proposes to use block-chain for FL is the study of Moulahi et al. [38], which considers the threat intelligence scenario for cyber-threat detection. The study of Korba et al. [39] also uses FL for attack detection especially to detect zero-day attacks in 5G and beyond V2X networks. The study of Rubina Akter and Kim [40] focuses on the UAV-based beyond 5G networks and considers blockchain for FL.

Sharma et al. consider the localization for mass-beamforming beyond the 5G use case for the application of privacy-enhanced FL [41]. Rajabzadeh and Outtagarts focus on the core network NWDAF architecture [42]. Li et al. propose a framework based on blockchain to increase the trustworthiness level of FL in the Internet of Vehicles use case [43]. As mentioned before, one of the main benefits of AI/ML in mobile communication is the automation aspect. Saad et al. investigate how to secure the FL against poisoning attacks in the context of zero-touch beyond 5G communication systems [44].

The study of Zhang et al. takes the cell-free massive-MIMO use case and works on privacy aspects in the usage of FL in that use case [45]. In a recent study by Ayepah-Mensah et al., resource allocation and trading for network slicing is taken as a use case and blockchain usage for FL is investigated [46]. The study by Sanon, Lipps, et al. analyzes the effect of precision loss due to the usage of homomorphic encryption in a 5G wireless network traffic prediction use case [47]. The utilization of federated split learning was studied by Jiang et al. for the satellite-terrestrial integrated networks [48]. In most of the studies, FL is considered in the centralized setting where the setup consists of a central server and FL clients, but there are other approaches that do not need a centralized server. The study covers that aspect and proposes to use blockchaing [49]. I. A. Bartsiokas et al.'s study takes the multicellular next-generation network topologies into account and proposes to use FL for resource allocation use case [50].

RIS-based communication for collaborative computing in a swarm of drones setup is considered by Rahbari et al. [51] and they proposed the usage of FL for computation offloading. Danish Javeed, n.d. investigates Quantum-Empowered FL for 6G Wireless Networks for IoT Security and discusses the concepts, challenges, and future directions[52].

The study by Taghia et al. works on Congruent Learning in Self-regulated FL for the 6G system [53]. Reliability aspects of FL in the mmWave networks were investigated in [54], [55].

4 EXISTING GENERIC SOLUTIONS FOR SECURITY AND PRIVACY IN FEDERATED LEARNING

Before presenting details about existing solutions that resolve the security and privacy requirements simultaneously, we first present the metrics that we use in the comparison of these solutions in Table 2 and then compare the existing solutions in Table 3.

ELSA [57] proposes a solution for both security and privacy by utilizing secure multi-party computation and two non-colluding servers. To detect anomalies in the local model updates it uses the Norm Bounding approach. The solution works in the malicious adversary model but requires that at least one of the servers should be semi-honest to meet the assumption that the servers should not collude, i.e., unless both of them are infected and compromised, the privacy of peers is guaranteed. ELSA paper compares ELSA with six other custom (state-of-the-art FL) solutions and it is claimed that considering the comparison ELSA is accepted as superior to all of them. The paper also shares the cloud infrastructure details for the performance experiments, source codes, programming language, and libraries which enables the researchers to experiment with the scenarios. Although it addresses security and privacy, it doesn't meet the fairness expectations. The solution only guarantees malicious privacy and leaves the exploration of malicious security (privacy with correctness) for future work. Efficiently achieving malicious security seems quite challenging given that standard techniques aren't compelling for a large number of parties in the system.

Co-utility presented in [58] utilizes multi-hop communication topology and reputation-based approach to address security (e.g., such as Byzantine and Poisoning attacks) and privacy aspects simultaneously. They also claim that their solution is performance-efficient. The incentiveness approach is used to separate good and malicious participants. They compare their solution with the Homomorphic Encryption and Differential Privacy based ones. Despite presented tables and graphs that depict the solution's results, no source codes or test infrastructure info are shared.

Rofl [59] works in the single server model which is a more realistic scenario in most of the use cases, but they have to use zero-knowledge proofs to allow the server to validate that the clients' inputs, without violating privacy. Because of the usage of ZK proofs, the performance results of the solution are not good compared to the two-server-based solutions.

The Byzantine-Resilient Secure FL on Low-Bandwidth Networks proposal introduced in [60] also focuses on both security and privacy. Similar to ELSA they utilize secret sharing and distance nom bounds but the difference in that paper is that they don't need two or more servers but the clients secretly share their local model updates with each other and the security attack detection is performed on these shares.

Ensuring Integrity For Federated Learning (EIFFeL) in [61] is another recent work on security and privacy in FL. They formalize the problem of having privacy and integrity simultaneously in FL and propose a new solution. That solution validates the updates and removes them from the aggregation result, without allowing the server access to the updates. Similar to the Rofl, they don't require two non-colluding serves but need to utilize zero-knowledge proofs which reduces the performance of the solution.

SAFEFL introduced in [62] also focuses on privacy and poisoning attacks. They utilize secure multi-party computation to be able to address both the security and privacy aspects simultaneously.

DP-BREM addresses the privacy challenges by using differential privacy and secure aggregation and makes the FL process robust against Byzantine poisoning attacks by introducing the concept of client momentum which means taking averages of model updates of different rounds [63].

Flamingo [64] is based on a single-server solution that uses secure aggregation for privacy aspects. The clients encrypt the inputs by a masking operation and a small group of clients decrypts and communicates with the server. It also supports client drop-outs.

zPROBE [65] prefers to use high break point rank-based

Table 2 Metrics for comparison of security&privacy solutions

Metric	Acronym	Definition
Single server	SS	The solution does not require more than one server in the protocol
Multiple server	MS	The solution requires more than one server where at least one of the servers is semi-honest (i.e., all the servers cannot collude)
Semi-honest server	SHS	The solution is secure against the server that follows the protocol steps for the computation of the aggregation result
Malicious server	MCS	The solution is secure against the server that may not follow the protocol steps for the computation of the aggregation result
Aggregation integrity	AI	The solution ensures that the aggregation result is not altered by the server after the computation of the aggregation result.
Input privacy	IP	The solution does not leak information about the input of clients to the server(s)
Client drop-outs	CDO	The solution is robust against the client drop-outs (i.e., the secure aggregation can be computed even if some of the clients drops-out)
Input integrity	II	The solution ensures that the inputs of the clients are in a pre-defined input range
Semi-honest clients	SHC	The solution is secure against the client who follows the protocol steps after starting the protocol by providing their inputs
Malicious clients	MCC	The solution is secure against the clients who may not follow the protocol steps after starting the protocol by providing their inputs
Star topology	ST	The clients only need to communicate with the server
P2P topology	P2PT	The clients need to communicate with each other in addition to the server
Scalable	S	The solution computation and communication are linear both in the number of clients

Table 3 Comparison of security&privacy solutions

Solution	SS	MS	SHS	MCS	AI	IP	CDO	II	SHC	MCC	ST	P2PT	S
ELSA		✓	✓		✓	✓	✓	✓		✓		✓	✓
Co-utility	✓		✓			✓	✓	✓		✓		✓	✓
Rofl	✓		✓			✓	✓	✓		✓	✓		✓
Byzantine-Resilient	✓		✓			✓		✓	✓			✓	✓
EIFFeL	✓			✓	✓	✓	✓	✓		✓	✓		✓
SAFEFL		✓		✓	✓	✓	✓	✓		✓	✓		✓
DP-BREM	✓		✓			✓		✓	✓			✓	✓
Flamingo	✓			✓		✓	✓	✓		✓	✓		✓
zPROBE	✓		✓			✓		✓		✓	✓		✓
Prio		✓	✓			✓		✓		✓	✓		✓
Karakoç et al. [56]	✓		✓			✓	✓	✓		✓		✓	✓

statistics on aggregated model updates instead of medians. They also utilize zero-knowledge protocols. With these approaches, they propose a solution that is secure against Byzantine type of attacks while still preserving privacy.

Prio [66] is also another that requires more than one server and has the assumption that at least one of the servers is semi-honest. They use secret sharing and secret-shared non-interactive proofs in their solution.

Another multi-hop communication-based solution was presented by Karakoç et al. [56]. To prevent malicious activities of the clients because of this anonymity, they propose to use partially blind signatures.

5 DISCUSSIONS AND CONCLUSION

While there has been progress in integrating ML into practical applications, there is still work to be done in order to improve security and privacy in these applications. Simultaneously addressing security and privacy in ML creates new potential for innovation as well as obstacles. Existing solutions frequently have drawbacks, such as the requirement for expensive and intricate cryptographic processes, dependence on numerous non-colluding servers, or dependence on peer-to-peer network topologies for communication. There are particular disadvantages associated with each of these strategies that may prevent their broad use and efficacy. Domain-specific research has investigated the use and application of ML with improvements to security and privacy; on the other hand, there is a significant lack of information in the literature about FL systems that simultaneously handle these issues. The distinct needs of different industries, like mobile communications, call for customized solutions that guarantee privacy and security. One area of research that shows promise is the use of FL in the telco industry. Examining use cases that require privacy and security at the same time may provide insightful information and innovative solutions. Depending on the particular use case, security and privacy needs can differ greatly, emphasising the necessity for adaptable and flexible solutions. Research ought to take into account the application of safe and privacy-enhanced ML in other sectors, in addition to telecommunications. Future research could examine how these specifications vary in various contexts and how FL can be modified to satisfy these changing requirements. All things considered, the way forward entails not only tackling the technical obstacles related to secure and privacy-enhanced ML but also comprehending the wider ramifications for many industries. In order to provide reliable solutions that can be successfully applied in practical applications, cooperation between academic institutions and businesses will be essential. The goal of future research should be to close the gaps that now exist and provide thorough frameworks that meet the various needs of various disciplines.

In conclusion, even though ML has made great progress in being incorporated into real-world applications, there is still more work to be done to create completely safe and private ML systems. It is particularly exciting to investigate FL as a way to accomplish these objectives simultaneously, especially in niche industries like telecoms. Future studies must tackle the distinct problems that different use cases provide in order to guarantee that the solutions are practical and flexible. We can open new possibilities and protect the integrity and privacy of data in ever more technical ways by pushing the limits of ML.

ACKNOWLEDGEMENTS

This work was supported by the Scientific and Technological Research Council of Turkey (TUBITAK) through the 1515 Frontier Research and Development Laboratories Support Program under Project 5169902.

REFERENCES

[1] E. U. Soykan, L. Karaçay, F. Karakoç, and E. Tomur, “A survey and guideline on privacy enhancing technologies for collaborative machine learning,” *IEEE Access*, vol. 10, pp. 97 495–97 519, 2022. DOI: 10.1109/ACCESS.2022.3204037. [Online]. Available: https://doi.org/10.1109/ACCESS.2022.3204037.

[2] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, “Communication-efficient learning of deep networks from decentralized data,” in *Artificial intelligence and statistics*, PMLR, 2017, pp. 1273–1282.

[3] P. Kairouz, H. B. McMahan, B. Avent, *et al.*, “Advances and open problems in federated learning,” *Foundations and trends® in machine learning*, vol. 14, no. 1–2, pp. 1–210, 2021.

[4] D. Cao, S. Chang, Z. Lin, G. Liu, and D. Sun, “Understanding distributed poisoning attack in federated learning,” in *2019 IEEE 25th international conference on parallel and distributed systems (ICPADS)*, IEEE, 2019, pp. 233–239.

[5] 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, 2021. DOI: 10.1016/J.FUTURE.2020.10.007. [Online]. Available: https://doi.org/10.1016/j.future.2020.10.007.

[6] A. Blanco-Justicia, J. Domingo-Ferrer, S. Martínez, D. Sánchez, A. Flanagan, and K. E. Tan, “Achieving security and privacy in federated learning systems: Survey, research challenges and future directions,” *Eng. Appl. Artif. Intell.*, vol. 106, p. 104 468, 2021. DOI: 10.1016/J.ENGAPPAI.2021.104468. [Online].

Available: https://doi.org/10.1016/j.engappai.2021.104468.

[7] N. B. Truong, K. Sun, S. Wang, F. Guitton, and Y. Guo, “Privacy preservation in federated learning: An insightful survey from the GDPR perspective,” *Comput. Secur.*, vol. 110, p. 102 402, 2021. DOI: 10.1016/J.COSE.2021.102402. [Online]. Available: https://doi.org/10.1016/j.cose.2021.102402.

[8] N. Bouacida and P. Mohapatra, “Vulnerabilities in federated learning,” *IEEE Access*, vol. 9, pp. 63 229–63 249, 2021. DOI: 10.1109/ACCESS.2021.3075203. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3075203.

[9] M. Mansouri, M. Önen, W. B. Jaballah, and M. Conti, “SoK: Secure aggregation based on cryptographic schemes for federated learning,” *Proc. Priv. Enhancing Technol.*, vol. 2023, no. 1, pp. 140–157, 2023. DOI: 10.56553/POPETS-2023-0009. [Online]. Available: https://doi.org/10.56553/popets-2023-0009.

[10] D. Enthoven and Z. Al-Ars, “An overview of federated deep learning privacy attacks and defensive strategies,” *CoRR*, vol. abs/2004.04676, 2020. arXiv: 2004.04676. [Online]. Available: https://arxiv.org/abs/2004.04676.

[11] L. Lyu, H. Yu, X. Ma, *et al.*, “Privacy and robustness in federated learning: Attacks and defenses,” *CoRR*, vol. abs/2012.06337, 2020. arXiv: 2012.06337. [Online]. Available: https://arxiv.org/abs/2012.06337.

[12] J. Mao, C. Cao, L. Wang, J. Ye, and W. Zhong, “Research on the security technology of federated learning privacy preserving,” *Journal of Physics: Conference Series*, vol. 1757, no. 1, p. 012 192, Jan. 2021. DOI: 10.1088/1742-6596/1757/1/012192. [Online]. Available: https://dx.doi.org/10.1088/1742-6596/1757/1/012192.

[13] M. Asad, S. Shaukat, D. Hu, *et al.*, “Limitations and future aspects of communication costs in federated learning: A survey,” *Sensors*, vol. 23, no. 17, p. 7358, 2023. DOI: 10.3390/S23177358. [Online]. Available: https://doi.org/10.3390/s23177358.

[14] A. Akhtarshenas, M. A. Vahedifar, N. Ayoobi, B. Maham, T. Alizadeh, and S. Ebrahimi, “Federated learning: A cutting-edge survey of the latest advancements and applications,” *CoRR*, vol. abs/2310.05269, 2023. DOI: 10.48550/ARXIV.2310.05269. arXiv: 2310.05269. [Online]. Available: https://doi.org/10.48550/arXiv.2310.05269.

[15] D. Sirohi, N. Kumar, P. S. Rana, S. Tanwar, R. Iqbal, and M. Hijji, “Federated learning for 6G-enabled secure communication systems: A comprehensive survey,” *Artif. Intell. Rev.*, vol. 56, no. 10, pp. 11 297–11 389, 2023. DOI: 10.1007/S10462-023-10417-3. [Online]. Available: https://doi.org/10.1007/s10462-023-10417-3.

[16] M. Al-Quraan, L. S. Mohjazi, L. Bariah, *et al.*, “Edge-native intelligence for 6G communications driven by federated learning: A survey of trends and challenges,” *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 7, no. 3, pp. 957–979, 2023. DOI: 10.1109/TETCI.2023.3251404. [Online]. Available: https://doi.org/10.1109/TETCI.2023.3251404.

[17] Y. Liu, X. Yuan, Z. Xiong, J. Kang, X. Wang, and D. Niyato, “Federated learning for 6G communications: Challenges, methods, and future directions,” *CoRR*, vol. abs/2006.02931, 2020. arXiv: 2006.02931. [Online]. Available: https://arxiv.org/abs/2006.02931.

[18] A. Rahman, K. Hasan, D. Kundu, *et al.*, “On the ICN-IoT with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives,” *Future Gener. Comput. Syst.*, vol. 138, pp. 61–88, 2023. DOI: 10.1016/J.FUTURE.2022.08.004. [Online]. Available: https://doi.org/10.1016/j.future.2022.08.004.

[19] Y. Zuo, J. Guo, N. Gao, Y. Zhu, S. Jin, and X. Li, “A survey of blockchain and artificial intelligence for 6G wireless communications,” *IEEE Commun. Surv. Tutorials*, vol. 25, no. 4, pp. 2494–2528, 2023. DOI: 10.1109/COMST.2023.3315374. [Online]. Available: https://doi.org/10.1109/COMST.2023.3315374.

[20] S. Abimannan, E.-S. M. El-Alfy, S. Hussain, *et al.*, “Towards federated learning and multi-access edge computing for air quality monitoring: Literature review and assessment,” *Sustainability*, vol. 15, no. 18, 2023, ISSN: 2071-1050. DOI: 10.3390/su151813951. [Online]. Available: https://www.mdpi.com/2071-1050/15/18/13951.

[21] N. A. Khalek, D. H. Tashman, and W. Hamouda, “Advances in machine learning-driven cognitive radio for wireless networks: A survey,” *IEEE Communications Surveys Tutorials*, pp. 1–1, 2023. DOI: 10.1109/COMST.2023.3345796.

[22] M. B. Driss, E. Sabir, H. Elbiaze, and W. Saad, “Federated learning for 6G: Paradigms, taxonomy, recent advances and insights,” *CoRR*, vol. abs/2312.04688, 2023. DOI: 10.48550/ARXIV.2312.04688. arXiv: 2312.04688. [Online]. Available: https://doi.org/10.48550/arXiv.2312.04688.

[23] M. A. Ferrag, O. Friha, B. Kantarci, *et al.*, “Edge learning for 6G-enabled internet of things: A comprehensive survey of vulnerabilities, datasets, and defenses,” *IEEE Commun. Surv. Tutorials*, vol. 25, no. 4, pp. 2654–2713, 2023. DOI: 10.1109/COMST.2023.3317242. [Online]. Available: https://doi.org/10.1109/COMST.2023.3317242.

[24] I. Bartsiokas, P. Gkonis, A. Papazafeiropoulos, D. Kaklamani, and I. Venieris, “Federated learning for 6G hetnets’ physical layer optimization: Perspectives, trends, and challenges federated learning for 6G hetnets’ physical layer optimization,” in Jul. 2024, p. 1–28, ISBN: 9781668473665. DOI: 10.4018/978-1-6684-7366-5.ch070.

[25] J. M. P. Ullauri, X. Zhang, A. Bravalheri, Y. Wu, R. Nejabati, and D. Simeonidou, “Federated analytics for 6G networks: Applications, challenges, and opportunities,” *CoRR*, vol. abs/2401.03878, 2024. DOI: 10.48550/ARXIV.2401.03878. arXiv: 2401.03878. [Online]. Available: https://doi.org/10.48550/arXiv.2401.03878.

[26] S. K. Das, R. Mudi, M. S. Rahman, and A. O. Fapojuwo, “Distributed learning for 6G–IoT networks: A comprehensive survey,” *Authorea Preprints*, 2023.

[27] L. S. Mohjazi, B. Selim, M. Tatipamula, and M. A. Imran, “The journey towards 6G: A digital and societal revolution in the making,” *CoRR*, vol. abs/2306.00832, 2023. DOI: 10.48550/ARXIV.2306.00832. arXiv: 2306.00832. [Online]. Available: https://doi.org/10.48550/arXiv.2306.00832.

[28] C. Anitha, B. Balakiruthiga, S. Angayarkanni, P. P. Selvi, and L. S. Kumar, “Recent developments, application cases, and lingering issues on the path to a 6G IoT,” in *2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE)*, IEEE, 2023, pp. 1–10.

[29] S. Polymeni, S. Plastras, D. N. Skoutas, G. Kormentzas, and C. Skianis, “The impact of 6G-IoT technologies on the development of agriculture 5.0: A review,” *Electronics*, vol. 12, no. 12, 2023, ISSN: 2079-9292. DOI: 10.3390/electronics12122651. [Online]. Available: https://www.mdpi.com/2079-9292/12/12/2651.

[30] Y. Liu, J. Peng, J. Kang, A. M. Iliyasu, D. Niyato, and A. A. A. El-Latif, “A secure federated learning framework for 5G networks,” *CoRR*, vol. abs/2005.05752, 2020. arXiv: 2005.05752. [Online]. Available: https://arxiv.org/abs/2005.05752.

[31] 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, 2023. DOI: 10.1109/LNET.2023.3294497. [Online]. Available: https://doi.org/10.1109/LNET.2023.3294497.

[32] H. P. Phyu, R. Stanica, and D. Naboulsi, “Multi-slice privacy-aware traffic forecasting at RAN level: A scalable federated-learning approach,” *IEEE Trans. Netw. Serv. Manag.*, vol. 20, no. 4, pp. 5038–5052, 2023. DOI: 10.1109/TNSM.2023.3267725. [Online]. Available: https://doi.org/10.1109/TNSM.2023.3267725.

[33] T. Hewa, P. Porambage, M. Liyanage, and M. Ylianttila, “Towards attack resistant federated learning with blockchain in 5G and beyond networks,” in *2023 Joint European Conference on Networks and Communications & 6G Summit, EuCNC/6G Summit 2023, Gothenburg, Sweden, June 6-9, 2023*, Jun. 2023.

[34] S. A. Khowaja, P. Khuwaja, K. Dev, and A. Antonopoulos, “SPIN: Simulated poisoning and inversion network for federated learning-based 6G vehicular networks,” in *IEEE International Conference on Communications, ICC 2023, Rome, Italy, May 28 - June 1, 2023*, IEEE, 2023, pp. 6205–6210. DOI: 10.1109/ICC45041.2023.10279339. [Online]. Available: https://doi.org/10.1109/ICC45041.2023.10279339.

[35] S. P. Sanon, R. Reddy, C. Lipps, and H. D. Schotten, “Secure federated learning: An evaluation of homomorphic encrypted network traffic prediction,” in *20th IEEE Consumer Communications & Networking Conference, CCNC 2023, Las Vegas, NV, USA, January 8-11, 2023*, IEEE, 2023, pp. 1–6. DOI: 10.1109/CCNC51644.2023.10060116. [Online]. Available: https://doi.org/10.1109/CCNC51644.2023.10060116.

[36] M. Wasilewska, H. Bogucka, and H. V. Poor, “Secure federated learning for cognitive radio sensing,” *CoRR*, vol. abs/2304.06519, 2023. DOI: 10.48550/ARXIV.2304.06519. arXiv: 2304.06519. [Online]. Available: https://doi.org/10.48550/arXiv.2304.06519.

[37] X. Lan, J. Taghia, F. Moradi, *et al.*, “Federated learning for performance prediction in multi-operator environments,” *ITU Journal on Future and Evolving Technologies*, vol. 4, pp. 166–177, Mar. 2023. DOI: 10.52953/PFYZ9165.

[38] T. Moulahi, R. Jabbar, A. Alabdulatif, *et al.*, “Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security,” *Expert Syst. J. Knowl. Eng.*, vol. 40,

no. 5, 2023. DOI: 10.1111/EXSY.13103. [Online]. Available: https://doi.org/10.1111/exsy.13103.

[39] A. A. Korba, A. Boualouache, B. Brik, R. Rahal, Y. Ghamri-Doudane, and S. M. Senouci, "Federated learning for zero-day attack detection in 5G and beyond V2X networks," in *IEEE International Conference on Communications, ICC 2023, Rome, Italy, May 28 - June 1, 2023*, IEEE, 2023, pp. 1137–1142. DOI: 10.1109/ICC45041.2023.10279368. [Online]. Available: https://doi.org/10.1109/ICC45041.2023.10279368.

[40] A. Z. Rubina Akter and D.-S. Kim, "UAV-based B5G networks: Blockchain and federated learning technology," 2023.

[41] D. Sharma, A. Kumar, and R. B. Battula, "Fedbeam: Federated learning based privacy preserved localization for mass-beamforming in 5GB," in *International Conference on Information Networking, ICOIN 2023, Bangkok, Thailand, January 11-14, 2023*, IEEE, 2023, pp. 616–621. DOI: 10.1109/ICOIN56518.2023.10048980. [Online]. Available: https://doi.org/10.1109/ICOIN56518.2023.10048980.

[42] P. Rajabzadeh and A. Outtagarts, "Federated learning for distributed NWDAF architecture," in *26th Conference on Innovation in Clouds, Internet and Networks, ICIN 2023, Paris, France, March 6-9, 2023*, pp. 24–26. DOI: 10.1109/ICIN56760.2023.10073493. [Online]. Available: https://doi.org/10.1109/ICIN56760.2023.10073493.

[43] A. Li, X. Chang, J. Ma, S. Sun, and Y. Yu, "VTFL: A blockchain based vehicular trustworthy federated learning framework," in *2023 IEEE 6th Information Technology,Networking,Electronic and Automation Control Conference (ITNEC)*, vol. 6, 2023, pp. 1002–1006. DOI: 10.1109/ITNEC56291.2023.10082698.

[44] S. B. Saad, B. Brik, and A. Ksentini, "Toward securing federated learning against poisoning attacks in zero touch B5G networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 20, no. 2, pp. 1612–1624, 2023. DOI: 10.1109/TNSM.2023.3278838. [Online]. Available: https://doi.org/10.1109/TNSM.2023.3278838.

[45] J. Zhang, J. Zhang, D. W. K. Ng, and B. Ai, "Federated learning-based cell-free massive MIMO system for privacy-preserving," *IEEE Trans. Wirel. Commun.*, vol. 22, no. 7, pp. 4449–4460, 2023. DOI: 10.1109/TWC.2022.3225812. [Online]. Available: https://doi.org/10.1109/TWC.2022.3225812.

[46] D. Ayepah-Mensah, G. Sun, G. O. Boateng, S. Anokye, and G. Liu, "Blockchain-enabled federated learning-based resource allocation and trading for network slicing in 5G," *IEEE/ACM Trans. Netw.*, vol. 32, no. 1, pp. 654–669, 2024. DOI: 10.1109/TNET.2023.3297390. [Online]. Available: https://doi.org/10.1109/TNET.2023.3297390.

[47] S. P. Sanon, C. Lipps, and H. D. Schotten, "Fully homomorphic encryption: Precision loss in wireless mobile communication," in *2023 Joint European Conference on Networks and Communications & 6G Summit, EuCNC/6G Summit 2023, Gothenburg, Sweden, June 6-9, 2023*, IEEE, 2023, pp. 466–471. DOI: 10.1109/EUCNC/6GSUMMIT58263.2023.10188286. [Online]. Available: https://doi.org/10.1109/EuCNC/6GSummit58263.2023.10188286.

[48] W. Jiang, H. Han, Y. Zhang, and J. Mu, "Federated split learning for sequential data in satellite-terrestrial integrated networks," *Inf. Fusion*, vol. 103, p. 102 141, 2024. DOI: 10.1016/J.INFFUS.2023.102141. [Online]. Available: https://doi.org/10.1016/j.inffus.2023.102141.

[49] F. Wilhelmi, L. Giupponi, and P. Dini, "Blockchain-enabled Server-less Federated Learning," *CoRR*, vol. abs/2112.07938, 2021. arXiv: 2112.07938. [Online]. Available: https://arxiv.org/abs/2112.07938.

[50] I. A. Bartsiokas, P. K. Gkonis, D. I. Kaklamani, and I. S. Venieris, "A federated learning-based resource allocation scheme for relaying-assisted communications in multicellular next generation network topologies," *Electronics*, vol. 13, no. 2, 2024, ISSN: 2079-9292. DOI: 10.3390/electronics13020390. [Online]. Available: https://www.mdpi.com/2079-9292/13/2/390.

[51] D. Rahbari, M. M. Alam, Y. L. Moullec, and M. Jenihhin, "Applying RIS-based communication for collaborative computing in a swarm of drones," *IEEE Access*, vol. 11, pp. 70 093–70 109, 2023. DOI: 10.1109/ACCESS.2023.3293737. [Online]. Available: https://doi.org/10.1109/ACCESS.2023.3293737.

[52] D. Javeed, M. Saeed, I. Ahmad, M. Adil, P. Kumar, and N. Islam, "Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions," *Future Generation Computer Systems*, Jun. 2024. DOI: 10.1016/j.future.2024.06.023.

[53] J. Taghia, F. Moradi, H. Larsson, *et al.*, "Congruent learning for self-regulated federated learning in 6G," *IEEE Transactions on Machine Learning in Communications and Networking*, vol. 2, pp. 129–149, 2024. DOI: 10.1109/TMLCN.2023.3347680.

[54] M. Al-Quraan, A. Zoha, A. Centeno, *et al.*, "Enhancing reliability in federated mmwave networks: A practical and scalable solution using radar-aided dynamic blockage recognition," *CoRR*, vol. abs/2307.06834, 2023. DOI: 10.48550/ARXIV.2307.06834. arXiv: 2307.06834. [Online]. Available: https://doi.org/10.48550/arXiv.2307.06834.

[55] M. Al-Quraan, A. Centeno, A. Zoha, M. A. Imran, and L. S. Mohjazi, "Federated learning for reliable mmwave systems: Vision-aided dynamic blockages prediction," in *IEEE Wireless Communications and Networking Conference, WCNC 2023, Glasgow, UK, March 26-29, 2023*, IEEE, 2023, pp. 1–6. DOI: 10.1109/WCNC55385.2023.10118675. [Online]. Available: https://doi.org/10.1109/WCNC55385.2023.10118675.

[56] F. Karakoç, L. Karaçay, P. Ç. D. Cnudde, U. Gülen, R. Fuladi, and E. U. Soykan, "A security-friendly privacy-preserving solution for federated learning," *Comput. Commun.*, vol. 207, pp. 27–35, 2023. DOI: 10.1016/j.comcom.2023.05.004. [Online]. Available: https://doi.org/10.1016/j.comcom.2023.05.004.

[57] M. Rathee, C. Shen, S. Wagh, and R. A. Popa, "ELSA: Secure aggregation for federated learning with malicious actors," *IACR Cryptol. ePrint Arch.*, p. 1695, 2022. [Online]. Available: https://eprint.iacr.org/2022/1695.

[58] J. Domingo-Ferrer, A. Blanco-Justicia, J. A. Manjón, and D. Sánchez, "Secure and privacy-preserving federated learning via co-utility," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3988–4000, 2022. DOI: 10.1109/JIOT.2021.3102155. [Online]. Available: https://doi.org/10.1109/JIOT.2021.3102155.

[59] H. Lycklama, L. Burkhalter, A. Viand, N. Küchler, and A. Hithnawi, "Rofl: Robustness of secure federated learning," in *44th IEEE Symposium on Security and Privacy, SP 2023, San Francisco, CA, USA, May 21-25, 2023*, IEEE, 2023, pp. 453–476. DOI: 10.1109/SP46215.2023.10179400. [Online]. Available: https://doi.org/10.1109/SP46215.2023.10179400.

[60] H. Masuda, K. Kita, Y. Koizumi, J. Takemasa, and T. Hasegawa, "Byzantine-resilient secure federated learning on low-bandwidth networks," *IEEE Access*, vol. 11, pp. 51 754–51 766, 2023. DOI: 10.1109/ACCESS.2023.3277858.

[61] A. R. Chowdhury, C. Guo, S. Jha, and L. van der Maaten, "EIFFeL: Ensuring integrity for federated learning," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022*, pp. 2535–2549. DOI: 10.1145/3548606.3560611. [Online]. Available: https://doi.org/10.1145/3548606.3560611.

[62] T. Gehlhar, F. Marx, T. Schneider, A. Suresh, T. Wehrle, and H. Yalame, "SafeFL: MPC-friendly framework for private and robust federated learning," in *2023 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, May 25, 2023*, IEEE, 2023, pp. 69–76. DOI: 10.1109/SPW59333.2023.00012. [Online]. Available: https://doi.org/10.1109/SPW59333.2023.00012.

[63] X. Gu, M. Li, and L. Xiong, "DP-BREM: Differentially-private and byzantine-robust federated learning with client momentum," *CoRR*, vol. abs/2306.12608, 2023. DOI: 10.48550/ARXIV.2306.12608. arXiv: 2306.12608. [Online]. Available: https://doi.org/10.48550/arXiv.2306.12608.

[64] Y. Ma, J. Woods, S. Angel, A. Polychroniadou, and T. Rabin, "Flamingo: Multi-round single-server secure aggregation with applications to private federated learning," in *44th IEEE Symposium on Security and Privacy, SP 2023, San Francisco, CA, USA, May 21-25, 2023*, IEEE, 2023, pp. 477–496. DOI: 10.1109/SP46215.2023.10179434. [Online]. Available: https://doi.org/10.1109/SP46215.2023.10179434.

[65] Z. Ghodsi, M. Javaheripi, N. Sheybani, X. Zhang, K. Huang, and F. Koushanfar, "zPROBE: Zero peek robustness checks for federated learning," in *IEEE/CVF International Conference on Computer Vision, ICCV 2023, Paris, France, October 1-6, 2023*, IEEE, 2023, pp. 4837–4847. DOI: 10.1109/ICCV51070.2023.00448. [Online]. Available: https://doi.org/10.1109/ICCV51070.2023.00448.

[66] H. Corrigan-Gibbs and D. Boneh, "Prio: Private, robust, and scalable computation of aggregate statistics," *CoRR*, vol. abs/1703.06255, 2017. arXiv: 1703.06255. [Online]. Available: http://arxiv.org/abs/1703.06255.