Federated Learning Integration in O-RAN : A Concise Review

Noureen Islam*, Fahad Monir*, M M Mahbubul Syeed*†, Mahady Hasan*†, Mohammad Faisal Uddin*†
*Department of Computer Science & Engineering, Independent University, Bangladesh (IUB)
†RIoT Research Center, Independent University, Bangladesh (IUB)
Email: {i.noureenislamsets*, fahad.monir*, mahbubul.syeed*†, mahady*†, faisal*†}@iub.edu.bd

2023 33rd International Telecommunication Networks and Applications Conference (ITNAC) | 979-8-3503-1713-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/ITNAC59571.2023.10368561

***Abstract*—The rapid growth of the telecommunication industry presents a global challenge in maintaining data security and privacy amid increasing data traffic and diverse applications. Applying Federated Learning (FL) to the upcoming Next Generation Wireless Networks (NextG) or Open Radio Access Network (O-RAN) holds great potential as a solution for addressing these challenges. With this in consideration, our paper explores a secure and privacy-conscious solution, focusing on the potential of FL in upcoming wireless networks or O-RAN. FL's cooperative learning approach ensures data confidentiality, offering significant advancements in security issues associated with growing user numbers, and supports the migration to the NextG. In this paper, the concise review provides valuable insights into O-RAN, FL, and related works, with an emphasis on security and privacy. Additionally, it explores framework utilization and outlines future research directions for integrating FL within O-RAN. This approach aims to offer the readers a quick and clear understanding of FL integration within O-RAN, avoiding the need to navigate through extensive survey papers.**

***Keywords*—Federated Learning (FL), Open Radio Access Network (O-RAN), Wireless Networks, Next Generation (NextG).**

I. Introduction

The expansion of the telecommunications sector with increasing users, data traffic, applications, and device diversity poses a global challenge for ensuring data security and privacy [1]. Handling sensitive customer data and safeguarding data privacy are critical concerns in this telecommunication sector. To tackle these difficulties, the Open Radio Access Network (O-RAN) has surfaced as a strategic approach, offering an open and standardized structure, which incorporates virtualization and network slicing to improve security measures [2]. However, integrating machine learning (ML) into O-RAN presents new challenges like data privacy, latency, and overfitting [3]. To overcome these issues, incorporating Federated Learning (FL) in O-RAN allows telecommunication companies to leverage ML's benefits while maintaining data security [4]. FL offers a decentralized, privacy-preserving approach to model training, enhancing collaboration among servers and edge devices.

Federated Learning revolutionizes collaborative learning by operating in a decentralized manner, ensuring data security and privacy. This technology achieves this by performing model training directly on edge devices without exchanging raw data samples, making it cost-effective with minimal hardware requirements and capable of working offline. O-RAN's open architecture and standardization, combined with FL's privacy-preserving decentralized approach, offer significant advancements in enhancing network security and maintaining user data confidentiality. By incorporating FL within O-RAN, telecommunication companies can leverage machine learning's potential while upholding stringent data protection regulations and ensuring seamless services in the era of rapid technological advancement and data growth.

Moreover, O-RAN Alliance plays a pivotal role in fostering collaborative efforts among telecommunication-based companies and organizations to develop and promote open standards and technologies for 5G/6G networks. By creating secure, modular, efficient, and cost-effective network solutions, O-RAN enables exposure to data and analytics, leading to analytics-driven enhanced solutions, self-adjusting feedback based control systems, and digitization [5]. The openness of O-RAN architecture allows for various vendors to supply network components, enhancing new network architectures and promoting interoperability.

This review paper focuses on exploring the integration of FL within O-RAN architecture, particularly for next-generation networks. It examines FL's potential benefits, with a specific emphasis on enhancing data security and privacy. The paper covers the fundamentals of O-RAN and FL, the implementation of FL, relevant studies employing various integration frameworks, and the challenges faced, along with potential solutions and areas for future research. Our aim was to deliver a succinct and insightful survey paper, furnishing readers with a concise yet thorough understanding of the most recent FL techniques employed in the context of O-RAN.

II. Fundamentals of FL and O-RAN

A. Open Radio Access Network (O-RAN)

The current cellular communication networking methods rely on closed and proprietary systems provided by a small pool of vendors, limiting transparency and flexibility. To overcome the traditional Radio Access Network (RAN) limitations, various research and standard efforts have proposed O-RAN as the transformative approach for the future of RAN. The O-RAN Alliance focuses on the RAN domain and aims to improve its openness, adaptability, and intelligence [6], [7]. The fundamental concept is to separate hardware from

*Department of Computer Science & Engineering, Independent University, Bangladesh (IUB)

2023 33rd International Telecommunication Networks and Applications Conference (ITNAC)

software and establish accessible interfaces between them. O-RAN implementations consist of software-based, disaggregated and virtualized components - all interconnected via open and standardized interfaces and interoperability through different suppliers. Segregation and virtualization enhance RAN flexibility, making it more adaptable and resilient.

However, the intelligence in the O-RAN concept leverages AI models to automate the radio networks. One of the crucial parts of O-RAN architecture is RAN Intelligent Controller (RIC) and this is where the intelligence resides in the O-RAN concept [8]. As shown in Fig. 1 below, the RIC collects real-time network data and employs AI for quick analysis and decision-making. It continuously monitors and adjusts network performance, resulting in improved performance.

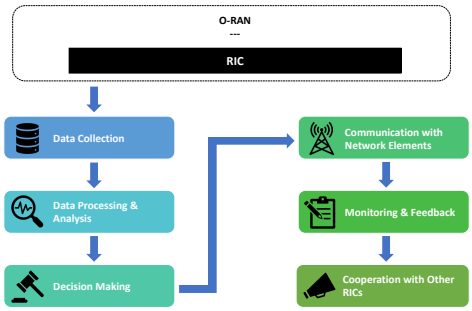

Fig. 1. RIC Working Process in O-RAN for Intelligence Integration

B. Federated Learning (FL)

Federated Learning (FL) represents a form of Distributed Machine Learning that works better than regular ML models in terms of efficiency. To keep data safe, FL uses distributed data and trains models locally [9]. It builds a secure connection using special algorithms like homomorphic encryption, which combines model results without exposing data to a central node for training.

FL treats participants fairly and lets them work independently, ensuring their data stays private. It makes sure that learning and training happen separately to avoid data leaks and protect user privacy. With this system, participants can collaborate to create more accurate global models. Federated Learning has three categories based on how data is shared among participants: horizontal, vertical, and federated transfer learning. These categories help determine which approach is best for different situations.

III. Integration of FL in O-RAN

Federated Learning (FL) seamlessly integrates with Open Radio Access Network (O-RAN) architectures, presenting a powerful method to boost collaborative machine learning in wireless communication systems. O-RAN's structure, which divides the base station into centralized, distributed, and radio units, aligns well with FL's decentralized nature. FL operates by keeping data localized on user devices and enabling collaborative model training without centralizing sensitive information. This decentralized approach ensures data privacy and security, as sensitive data remains on users' devices and is not sent to a central server for training [10].

As shown in Fig. 2 below, FL works by distributing the training process across multiple edge devices or clients, keeping data locally on each device. This approach benefits O-RAN in several ways, including ensuring data privacy, reducing latency, optimizing resource utilization, enabling scalability, and fostering collaborative intelligence within the network. Subfields of distributed machine learning, such as deep learning, reinforcement learning, federated learning and supervised and unsupervised learning, play crucial roles in training models for wireless communication systems [11].

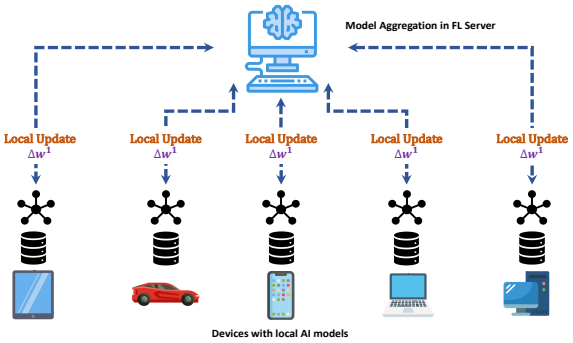

Fig. 2. Implementation Process of Federated Learning

By keeping data localized on devices, FL significantly boosts data privacy. When implementing FL within a slice, it further bolsters privacy protection. Instead of transferring all the data to a central server, models are intelligently allocated within the slices, allowing for instant updates based on slicing requirements. This eliminates the need to communicate with a central controller for decision-making on slicing resources. Moreover, FL aids in predicting potential faults and facilitating proactive repairs, preventing system breakdowns, contributing to a more robust and reliable wireless communication system.

Additionally, disaggregation of RAN promotes interoperability across vendors, enabling flexible cloud-native deployments, enhancing RAN's resilience and adaptability. It enables local data training without centralizing sensitive information, making it ideal for next-gen wireless networks.

Exploring the utilized FL Frameworks in O-RAN. Considering the various scenarios that may arise during the integration of FL with O-RAN, the FL frameworks employed within O-RAN is showcased in Table I, aiming to provide users with a brief overview of this incorporation. The Table I, presented below, outlines the "Objective" category to encompass this range of scenarios. The "Frameworks Used" column shows the employed FL frameworks, and the "Works Done" section describes how these frameworks achieve the objectives.

TABLE I
EXPLORING THE UTILIZED FL FRAMEWORKS IN O-RAN

Objective	Frameworks Used	Works Done	Ref.
Anomaly Detection	Normal P2P FL; Clustered P2P FL; Hierarchical P2P FL; Homomorphic P2P FL	The O-RAN architecture employs FL for anomaly detection, ensuring data privacy. It proposes a P2P FL-based mechanism and analyzes four variants for anomaly detection, simulating the models using the UNSW-NB15 dataset.	[12]
Network Automation	Federated learning based model	The proposed model using the ZSM architecture demonstrates the impact of changing training data composition on system accuracy. It aims to be applied in a security analytics framework within the ZSM security architecture.	[13]
Network Security	K Model	A successful poisoning attack with intelligent noise was conducted on the FoolsGold algorithm in FL. A sophisticated defense mechanism was proposed and evaluated, which employed threshold-based clustering to improve the system's resilience. The study demonstrated that the proposed defense mechanism outperforms FoolsGold when subjected to intelligent noise attacks.	[14]
Edge Intelligence	Edge Intelligent Radio Access Network Architecture (EIRA)	EIRA combines artificial intelligence (AI), radio access network (RAN), and edge computing to enhance and enable advanced applications in the field of 6G. It incorporates new intelligence modules and a Markov chain-based RAN Intelligence Control (RIC) scheduling technique to optimize the allocation of intelligence components.	[15]
Network Slicing	Statistical Federated Learning (StFL)-based Analytic engine	The motive of this paper is to attain energy sustainability in 6G networks through architectural and AI-based algorithmic designs, and to introduce a unique statistical federated learning (StFL) based engine for zero-touch massive network slicing. The StFL engine aims to predict slice-level resource utilization while adhering long-term service level agreement (SLA) requirements, leading to improved efficiency and sustainability in network slicing.	[16]
RAN Slicing	Federated Deep Reinforcement Learning (FDRL)	RAN slicing in collaboration through several Mobile Virtual Network Operators (MVNOs) is proposed here. Each MVNO trains a deep reinforcement learning model. Individual models are aggregated and MVNOs are shared. Simulation results demonstrate improved resource allocation, meeting users' Quality of Service (QoS) constraints in terms of delay and data rate.	[17]
Privacy	PrivacyFL simulator	The framework supports both centralized and decentralized Federated Learning (FL) approaches. It integrates privacy and security mechanisms that rely on differential privacy and secure multiparty computation. The framework has been demonstrated to be a scalable and versatile simulator, suitable for testing FL environments.	[18]
Privacy, Utility, and Cost objectives	Multi-Objective Optimization (MOO), Constrained Multi-objective federated learning (CMOFL)	A method called constrained multi-objective federated learning (CMOFL) utilizes multi-objective optimization (MOO) to optimize trustworthy federated learning (TFL) objectives. These algorithms effectively balance privacy, utility, and cost objectives.	[19]
Improved Resource Utilization	Dynamic Multi-Service FL (DMS-FL), Elastic Virtualized FL (EV-FL)	DMS-FL addresses challenges in NextG networks, while EV-FL leverages O-RAN systems with elastic resource provisioning. Both frameworks improve resource utilization and fairness among FL services.	[20]
AI services and Cloud Computing	Digital Twin (DT), Zero Trust Architecture (ZTA)	For the deployment of FL in cloud-edge collaborative architecture, a conceptually layered architecture for a Digital Twin (DT) framework, leveraging AI services and cloud computing has been proposed. This framework also covers the deployment of zero trust architecture (ZTA) as a security foundation for data-driven communication networks.	[21]
Efficient 5G resource utilization, Low Overhead, Resource Allocation, Privacy and Security	Ultra Dense Edge Computing (UDEC)	This framework combines blockchain and AI in 5G UDEC networks. It employs a 2Ts-DRL approach for real-time, low overhead computing offloading choices and resource allocation. The goal is to reduce offloading delay and network resource utilization while ensuring data privacy through federated learning.	[22]
Minimize energy consumption	FedTAR	FedTAR is a task and resource-aware federated learning model in Wireless Computing Power Network (WCPN). It minimizes energy consumption by optimizing computing strategies and collaborative learning among computing nodes. This model adapts neural network depth and collaboration frequency based on task requirements and resource constraints.	[23]
Training Disaggregated Systems	MCORANFed	MCORANFed assists in choosing the local trainers who will participate in each global round of Federated Learning. It also allocates resources to these trainers in a way that reduces the total learning duration and resource expenses.	[24]

IV. Exploring Security and Privacy

In this section, we have examined the preservation of privacy through the incorporation of FL into O-RAN, followed by the categorization of its applications in various contexts.

It is essential to note that the assurance of security and privacy within FL, as it becomes an integral part of O-RAN, holds paramount significance in safeguarding sensitive data and upholding the integrity of the learning process. By keeping data localized on user devices and enabling collaborative model training without sending unstructured data to a centralized server, FL enhances data privacy and mitigates the risk of sensitive information exposure. This decentralized approach ensures that user data remains under the control of individual participants, reducing the potential for data breaches and unauthorized access. Additionally, FL fosters collaboration among diverse vendors and users within the network, promoting cooperative intelligence without compromising data security. Implementing secure communication protocols further fortifies FL's role in enhancing the security of O-RAN, safeguarding against potential malicious attacks and ensuring the integrity of the wireless communication environment. The following section discusses FL's privacy-preserving nature when integrated with O-RAN, categorized by its application in various contexts.

A. Cloud

Data privacy is a significant concern in cloud-based FL [25]. FL's distributed nature and localized data on user devices address data privacy concerns in cloud-based FL. By enabling collaborative model training without centralizing raw data on a central server, FL lessens the possibility of sensitive information exposure and potential data breaches, enhancing data privacy.

B. Unexplainable AI/ML models

Unexplainable AI/ML models in O-RAN can cause unintended repercussions, impacting security, privacy, and causing biased results [26]. To address these issues, adopting explainable AI/ML models becomes crucial. These models provide clear insights into their decision-making, ensuring accountability, building trust, and enhancing security, privacy, and fairness in the system.

C. Communication Security

FL encounter communication security challenges, including Distributed Denial of Service (DDoS) and that can impact model uploads and downloads [27]. To mitigate these threats, encryption, secure protocols, and traffic analysis detection must be employed to safeguard data transmission.

Moreover, FL is vulnerable to Evasion and poisoning attacks, posing risks to ML models [28], [29]. To counter these, defenses like model poisoning detection and Federated Byzantine Fault Tolerance (FBFT) can be employed for improved security and data integrity.

D. Blockchain

For blockchain industry, FL offers to secure data sharing architecture, allowing multiple parties to share data securely while maintaining privacy [30]. In the context of blockchain, the combination of O-RAN and FL can enhance data privacy and security in decentralized networks, ensuring that the user data remains under the control of individual participants, thus, reducing the potential for data breaches and unauthorized access.

E. Edge Computing

Extensive data analysis and automation in 6G applications involving edge server deployment raise privacy concerns [31]. By leveraging FL's collaborative learning capabilities, edge devices can perform local model training and processing, minimizing the need to transmit raw data to centralized servers. This decentralized approach ensures that sensitive information remains localized, thereby reducing the risk of data exposure during transmission and enhancing data security. O-RAN and FL together offer an effective strategy to address privacy issues in edge computing scenarios.

F. AI & IoT

For AI and IoT applications, O-RAN and FL can be leveraged to achieve privacy-preserving analytics. In AI systems, FL allows multiple devices to collaborate on model training without sharing raw data, ensuring data privacy. In IoT environments, where devices collect vast amounts of sensitive data, FL's decentralized approach helps protect user privacy by keeping data local and reducing the reliance on centralized servers.

G. Disaggregated O-RAN

The distributed nature of O-RAN components introduces new attack surfaces and shared environments [2]. However, O-RAN's architecture and interfaces enable FL frameworks and the network infrastructure to work together effectively to train and infer models across a wide area. This integration enables improved data privacy, decreased latency, and more accurate models [32]. By using advanced encryption, secure protocols, and privacy-preserving techniques, FL in O-RAN can unlock its potential, mitigate threats, and establish user trust in collaborative learning.

Overall, the combination of O-RAN and FL benefits these applications in terms of security and privacy by enabling decentralized data processing, collaborative model training, and reduced data transmission to centralized servers.

V. Challenges faced and Solutions

The incorporation of Open Radio Access Network (O-RAN) in Federated Learning (FL) presents both challenges and opportunities. Considering this, Table II outlines the challenges that have arisen with their potential solutions, depending on different situations.

TABLE II
CHALLENGES FACED AND SOLUTIONS

Scenario	Challenge(s)	Solution(s)
Dropped participants	Mobile devices in FL may go offline or drop out due to connectivity or energy limitations, significantly impact the FL system's performance in terms of accuracy and convergence speed [33].	Algorithms for participant selection and resource allocation to address training bottleneck and resource heterogeneity [34], [35] are proposed. To reduce dropouts, initiatives such as offering participants an incentive-based free dedicated connection (e.g., cellular) can be implemented.
Unlabeled data	The server faces difficulties in recognizing individuals who possess appropriate data for training the model [36].	Allowing mobile devices to generate their own labeled data by learning from each other can be helpful. Recent study has additionally investigated the application of techniques inspired by semi-supervised learning [37].
Ethical Issues in AI	Machines learn differently from humans and lack ethical considerations since they can strictly follow their training and cannot deviate from logic like humans.	The "Ethics by Design" [38] approach incorporates ethical considerations into the early stages of AI system design.
Security	Evasion attacks occur which tries to bypass ML models during inference. Poisoning attacks affect the training stage of a machine learning system, causing the model to learn inaccurately [28], [29]. Communication security issues like Distributed Denial-of-Service (DDoS) and jamming attacks [27], [29] lead to errors in model uploads/downloads followed by degraded performance.	Applying adversarial machine learning, moving target defense, and various protection methods like input validation, robust learning, adversarial training, defensive distillation, differential privacy, and homomorphic encryption can bolster AI system resilience. Employing anti-jamming techniques like frequency hopping [39] further enhances security.
Privacy	The extensive data analysis capabilities of AI and the increasing need for automation in future networks poses privacy concerns. Users can no longer predict how external systems deal with their data [40] as 6G networks collect massive amounts of user information from billions of electronic devices. Insecure IoT devices, such as low-powered sensors, pose a risk of data theft when they share personal data to AI systems. Model inversion attacks on machine learning (ML) can be used to retrieve training data, potentially leading to privacy violations [28].	Edge-based FL to maintain data closer to the user. Homomorphic encryption, which allows performing mathematical operations by not decrypting data. Differential privacy techniques introduce random noise to the training data and prevent private information disclosure towards learning models.
Use of AI for Attacking 6G	AI can analyze large volumes of data across to identify patterns and vulnerabilities in the network. AI has the potential to detect and exploit vulnerabilities, such as identifying vulnerable IoT devices, transforming them into bots, and releasing DDoS attacks on critical nodes.	Moving target defense techniques introduce network dynamicity [41], weakening AI-enabled attackers' learning process. However, according to [42], quantum machine learning can be utilized .

VI. CONCLUSION

This paper presents a concise review of the integration of Federated Learning (FL) in Open Radio Access Network (O-RAN) architectures. It explores the potential of FL in NextG networks, emphasizing data security and privacy. The summary provides an overview of O-RAN and FL, detailing the implementation process of FL. Identification of relevant research and applications utilizing various frameworks for collaborating FL into O-RAN is presented here. Furthermore, the review investigates the challenges encountered in this collaborative effort and proposes potential solutions, while also identifying areas for future research. As future work, the use-age of AI in the new developed wireless technologies continue to pique the interest in the research community.

VII. FUTURE WORK

According to our studies, the incorporation of AI into wireless technology holds significant promise for future research and innovation. Keeping this in mind, some of the future works are discussed below in this section accordingly.

In the concept of Edge Intelligence and Caching, FL can enable intelligent caching decisions at the network edge by training models on local cache hit or miss patterns. By integrating FL into O-RAN, caching algorithms can be enhanced to adapt to dynamic content popularity, user behavior, and network conditions - resulting in improved content delivery and reduced latency.

Simultaneously, Multi-Modal Federated Learning extends FL to support multiple modalities of data, like audio and video, and sensor data collected by O-RAN devices. By combining different data types, models can be trained to extract richer insights, enabling advanced use cases like video-based traffic analysis, or environmental monitoring and etc..

However, Adaptive Network Intelligence can be used in future to explore the use of FL to develop adaptive network intelligence algorithms that can dynamically adjust network parameters and configurations based on real-time data from distributed O-RAN nodes. This can lead to self-optimizing networks that continuously adapt to changing conditions and user demands.

Further studies on learning convergences can also be focused in future. Since FL involves distributed optimization, the convergence of FL, which refers to the minimization of global model weights during aggregation, is not guaranteed in all cases.

As we progress, it is essential to maintain adaptability and embrace emerging challenges and opportunities within this dynamic field.

REFERENCES

[1] X. Lin and N. Lee, *Introduction to 5G and Beyond*. Cham: Springer, 2021.

[2] M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, "Open ran security: Challenges and opportunities," *Journal of Network and Computer Applications*, vol. 214, p. 103621, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804523000401

[3] M. Chen *et al.*, "Distributed learning in wireless networks: Recent progress and future challenges," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 12, pp. 3579–3605, Dec 2021.

[4] S. Niknam, H. S. Dhillon, and J. H. Reed, "Federated learning for wireless communications: Motivation, opportunities, and challenges," *IEEE Communications Magazine*, vol. 58, no. 6, pp. 46–51, June 2020.

[5] M. Polese, R. Jana, V. Kounev, K. Zhang, S. Deb, and M. Zorzi, "Machine learning at the edge: A data-driven architecture with applications to 5g cellular networks," *IEEE Transactions on Mobile Computing*, vol. 20, no. 12, pp. 3367–3382, Dec 2021.

[6] S.-Y. Lien and et al., "Federated deep reinforcement learning for user access control in open radio access networks," in *Proceedings of the ICC*, 2021.

[7] Shuh, "Toward an ai-enabled o-ran-based and sdn/nfv-driven 5g and iot network era," *Network and Communication Technologies*, vol. 6, no. 1, 2021.

[8] M. Dryjański, L. Kułacz, and A. Kliks, "Toward modular and flexible open ran implementations in 6g networks: Traffic steering use case and o-ran xapps," *Sensors*, vol. 21, no. 24, p. 8173, Dec 2021. [Online]. Available: http://dx.doi.org/10.3390/s21248173

[9] TianLi, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50–60, 2020.

[10] S. Wenting and et al., "A survey distributed machine learning for 5g and beyond," *Computer Networks*, vol. 207, 2022.

[11] A. K. M. and et al., "Machine learning techniques for 5g and beyond," *IEEE Access*, vol. 9, 2021.

[12] D. Attanayaka, P. Porambage, M. Liyanage, and M. Ylianttila, "Peer-to-peer federated learning based anomaly detection for open radio access networks," in *IEEE International Conference on Communications (ICC)*, June 2023.

[13] 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 *2022 Joint European Conference on Networks and Communications and 6G Summit (EuCNC/6G Summit)*, 2022, pp. 345–350.

[14] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "Robust and resilient federated learning for securing future networks," in *2022 Joint European Conference on Networks and Communications and 6G Summit (EuCNC/6G Summit)*, 2022, pp. 351–356.

[15] Y. Liu, Q. Wang, H. Liu, J. Zong, and F. Yang, "Edge intelligence-based ran architecture for 6g internet of things," *Dynamic Modelling and Optimization for Intelligent IoT Networks*, 2022. [Online]. Available: https://www.hindawi.com/journals/ddns/2022/4955498/

[16] H. Chergui, L. Blanco, L. A. Garrido, K. Ramantas, S. Kukliński, A. Ksentini, and C. Verikoukis, "Zero-touch ai-driven distributed management for energy-efficient 6g massive network slicing," *IEEE Network*, vol. 35, no. 6, pp. 43–49, 2021.

[17] T. Afaf and et al., "Federated deep reinforcement learning for open ran slicing in 6g networks," *IEEE Communications Magazine*, 2022.

[18] P.-B. Anton and L. Kagal, "Privacyfl: A simulator for privacy-preserving and secure federated learning," in *Proceedings of the 29th ACM International Conference on Information and Knowledge Management*, 2023, p. 3085.

[19] G. Hanlin and et al., "Optimizing privacy utility and efficiency in constrained multi-objective federated learning," *arXiv preprint arXiv*, 2023.

[20] P. Abdisarabshali, N. Accurso, F. Malandra, W. Su, and S. Hosseinalipour, "Synergies between federated learning and o-ran: Towards an elastic virtualized architecture for multiple distributed machine learning services," 2023.

[21] J. Jagannath, K. Ramezanpour, and A. Jagannath, "Digital twin virtualization with machine learning for iot and beyond 5g networks: Research directions for security and optimal control," in *Proceedings of the 2022 ACM Workshop on Wireless Security and Machine Learning*, ser. WiseML '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 81–86. [Online]. Available: https://doi.org/10.1145/3522783.3529519

[22] S. Yu, X. Chen, Z. Zhou, X. Gong, and D. Wu, "When deep reinforcement learning meets federated learning: Intelligent multitimescale resource management for multiaccess edge computing in 5g ultradense network," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2238–2251, 2021.

[23] W. Sun, Z. Li, Q. Wang, and Y. Zhang, "Fedtar: Task and resource-aware federated learning for wireless computing power networks," *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 4257–4270, 2023.

[24] A. K. Singh and K. K. Nguyen, "Mcoranfed: Communication efficient federated learning in open ran," in *2022 14th IFIP Wireless and Mobile Networking Conference (WMNC)*, 2022, pp. 15–22.

[25] T. Ngo, D. C. Nguyen, P. N. Pathirana, L. A. Corben, M. Horne, and D. J. Szmulewicz, "Blockchained federated learning for privacy and security preservation: Practical example of diagnosing cerebellar ataxia," *IEEE Xplore*, Jul. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9871371

[26] Amy Zwarico S.J. and et al., "The o-ran alliance security task group tackles security challenges on all o-ran interfaces and components," 2020.

[27] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, 2006.

[28] Y. Sun, J. Liu, J. Wang, Y. Cao, and N. Kato, "When machine learning meets privacy in 6g: A survey," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 4, pp. 2694–2724, 2020.

[29] O-RAN Policy Coalition, "Open-ran security in 5g," Online, 2021. [Online]. Available: https://www.openranpolicy.org/wp-content/uploads/2021/04/Open-RAN-Security-in-5G-4.29.21.pdf

[30] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, 2020.

[31] B. Mao, J. Liu, Y. Wu, and N. Kato, "Security and privacy on 6g network edge: A survey," *IEEE Communications Surveys and Tutorials*, pp. 1–1, 2023.

[32] D. Wypior, M. Klinkowski, and I. Michalski, "Open ran—radio access network evolution, benefits and market trends," *Applied Sciences*, vol. 12, no. 1, p. 408, 2022.

[33] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and et al., "Communication-efficient learning of deep networks from decentralized data," *arXiv preprint arXiv:1602.05629*, 2016.

[34] T. Nishio and R. Yonetani, "Client selection for federated learning with heterogeneous resources in mobile edge," *arXiv preprint arXiv:1804.08333*, 2018.

[35] N. Yoshida, T. Nishio, M. Morikura, K. Yamamoto, and R. Yonetani, "Hybrid-fl: Cooperative learning mechanism using non-iid data in wireless networks," *arXiv preprint arXiv:1905.07210*, 2019.

[36] Z. Gu, H. Jamjoom, D. Su, H. Huang, J. Zhang, T. Ma, D. Pendarakis, and I. Molloy, "Reaching data confidentiality and model accountability on the caltrain," in *Proceedings of the International Conference on Dependable Systems and Networks*, 2019, pp. 336–348.

[37] A. Albaseer, B. S. Ciftler, M. Abdallah, and A. Al-Fuqaha, "Exploiting unlabeled data in smart cities using federated learning," *arXiv preprint arXiv:2001.04030*, 2020.

[38] M. d'Aquin, P. Troullinou, N. E. O'Connor, A. Cullen, G. Faller, and L. Holden, "Towards an 'ethics by design' methodology for ai research projects," in *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, 2018, pp. 54–59.

[39] M. Strasser, C. Popper, S. Capkun, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *IEEE Symposium on Security and Privacy*, 2008, pp. 64–78.

[40] H. Fang, X. Wang, and S. Tomasin, "Machine learning for intelligent authentication in 5g and beyond wireless networks," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 55–61, 2019.

[41] J.-H. Cho, D. P. Sharma, H. Alavizadeh, S. Yoon, N. Ben-Asher, T. J. Moore, D. S. Kim, H. Lim, and F. F. Nelson, "Toward proactive, adaptive defense: A survey on moving target defense," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 709–745, 2020.

[42] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning," *Nature*, vol. 549, no. 7671, pp. 195–202, 2017.