NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 2, Issue – 1, June 2023
E-ISSN - 2583-7559

Cyber Security Concerns and Mitigation Strategies in Federated Learning: A Comprehensive Review

Param Ahir
Computer/IT Engineering
Gujarat Technological University
Ahmedabad, India
209999913009@gtu.edu.in

Mehul Parikh
Information Technology Department
L. D. College of Engineering
Ahmedabad, India
mehulcparikh@ldce.ac.in

***Abstract*— Federated learning (FL) has emerged as a potential method for training machine learning models on distributed data sources while maintaining data privacy. The distributed nature of FL, on the other hand, creates unique cybersecurity challenges that must be addressed to protect the integrity, confidentiality, and availability of the contributing data and models. This review paper intends to give a thorough examination of the cyber security problems related to federated learning and to investigate various mitigating measures proposed in the literature. The study discusses the possible impact of important vulnerabilities in FL systems, such as adversarial attacks, data poisoning, model inversion, and inference attacks, on privacy and system performance. The study also explores existing solutions and countermeasures proposed to solve these security concerns, such as cryptographic approaches, secure aggregation protocols, differential privacy mechanisms, and model verification methods. This review paper seeks to provide insights for researchers, practitioners, and policymakers on the topic of cyber security in federated learning by synthesising the present state of research and identifying gaps.**

Keywords*— *Federated Learning, Cyber Security, Privacy, Adversarial Attacks, Data Poisoning, Model Inversion, Inference Attacks, Secure Aggregation, Differential Privacy, Cryptographic Techniques, Model Verification

I. INTRODUCTION

Federated learning (FL) has emerged as a transformative paradigm for training machine learning models on distributed data sources while preserving user privacy. In contrast to traditional centralised machine learning approaches [1], FL allows data to remain on local devices or servers, with only model updates shared among participating entities. FL's distributed nature provides numerous benefits, including data privacy preservation, lower communication costs, and increased scalability. However, the use of FL raises new cybersecurity concerns that must be addressed to ensure the integrity, confidentiality, and availability of the participating data and models. The goal of this review paper is to provide a thorough examination of the cyber security concerns associated with federated learning as well as investigate various mitigation strategies proposed in the literature.

The first section of this paper provides an overview of federated learning by explaining its principles and emphasising its benefits and drawbacks. The following section focuses on cybersecurity issues that are unique to federated learning. The following section provides an overview of various mitigation strategies proposed in the literature to address these cybersecurity challenges. This paper also examines the existing frameworks and solutions proposed in the literature, providing a comprehensive overview of cutting-edge approaches to addressing cybersecurity concerns in federated learning. These solutions are analysed and compared based on their effectiveness, efficiency, scalability, and compatibility with various FL settings. Overall, the purpose of this review paper presents the current state of research and identify research gaps related to cyber security in federated learning.

II. BASICS OF FEDERATED LEARNING

Federated Learning (FL) allows models to be trained using decentralised data sources while maintaining data privacy. Unlike traditional centralised approaches, FL enables participating entities to train a global model collaboratively while keeping their data local, addressing concerns about data sharing and data privacy. FL entails a network of devices or servers that work together to train a shared model [2]. FL participants, which can be devices or servers, keep their data and contribute to the training process without sharing raw data with a central authority or other participants. This decentralised approach enables entities to leverage their local data while maintaining control over sensitive information, which is especially important in scenarios where data privacy is critical. Federated learning principles are based on the concepts of decentralisation, local model updates, privacy preservation, and collaboration [3]. Decentralisation emphasises the retention of data on individual devices or servers, and the training process is carried out through local computation and communication. Participants train their models locally using

their respective local data, which is then aggregated to create a global model that incorporates knowledge from all participants. Privacy preservation is a key principle in FL, which is accomplished through techniques such as encryption, secure aggregation protocols [4][5], and differential privacy, which safeguard the confidentiality of participants' data during the training process. In FL, participants voluntarily contribute their computational resources and local expertise to collectively improve the performance of the global model. Federated learning has a wide range of applications, including healthcare, finance, the Internet of Things (IoT) [6], and edge computing [7]. Its principles address data silos, regulatory constraints, and privacy concerns, allowing the benefits of distributed machine learning to be realised in sensitive and privacy-sensitive environments. Federated learning (FL) has distinct advantages over traditional centralised machine learning approaches, but it also introduces new challenges. FL has several advantages that contribute to its appeal and suitability in a variety of situations:

- Data Privacy Preservation: FL addresses privacy concerns and reduces the risk of privacy breaches associated with sharing sensitive data by keeping data local and decentralised.
- Reduced Communication Costs: Because only model updates or gradients are shared among participants, FL reduces the need for large-scale data transmission, resulting in lower communication costs.
- FL's decentralised architecture enables it to handle massive datasets distributed across multiple devices or servers, making it suitable for applications involving a large number of participants or data sources.
- Collaborative Knowledge Sharing: FL encourages participants to contribute their local expertise and computational resources, allowing the network's collective intelligence to improve the performance of the global model.

While FL has compelling benefits, it also has challenges that must be addressed for successful implementation [8]:

- Communication bottlenecks: In scenarios with a large number of participants or limited communication bandwidth, coordinating the exchange of model updates or gradients among participants can become a bottleneck, reducing training efficiency.
- Heterogeneous Data Sources: FL operates in environments where participants' data distributions and characteristics differ. Handling heterogeneous data sources makes it difficult to achieve model fairness and generalisation performance across all participants.
- Maintaining Model Consistency: Maintaining model consistency across participants is a critical challenge in FL, given differences in computational capacities, network conditions, and data quality.
- Risks to Data Security and Privacy: While FL prioritises data privacy, it also introduces security and privacy risks. Adversarial attacks, such as poisoning or model inversion, can compromise participant privacy or disrupt the learning process.

Understanding FL's benefits and drawbacks is critical for researchers, practitioners, and policymakers to make informed decisions about its use and develop effective solutions.

III. Cyber Security Concerns in Federated Learning

Federated learning (FL) poses unique cybersecurity challenges due to its collaborative nature. In this section, specific cyber security concerns associated with FL and their effect on privacy and system performance are discussed.

A. Adversarial Attacks

Adversarial attacks pose a significant threat to FL systems, jeopardising participant data privacy and integrity as well as the overall model. Poisoning attacks may be attempted by injecting malicious data samples during the training process, resulting in biased models or incorrect predictions. Model inversion attacks seek to extract sensitive information from the trained global model, potentially infringing on participants' privacy. Adversarial attacks can also compromise the model aggregation process or target the communication infrastructure, resulting in manipulated or compromised global models.

B. Breach of Data Privacy

While FL prioritises data privacy, there are potential flaws that could result in data breaches. Malicious entities can infer or reconstruct participants' local data even if it is not directly shared. To infer sensitive training data, inference attacks use information leakage from model updates or gradients. Participants' privacy being violated can have serious consequences, especially in sensitive domains such as healthcare or finance.

C. Risks to Communication and Privacy [9]

To exchange model updates or gradients, FL relies on frequent communication among participants. This communication, however, poses privacy and security risks. Communication channel eavesdropping or interception can expose sensitive information, jeopardising both participant privacy and the confidentiality of model updates. Communication channel bandwidth or latency can also cause delayed or incomplete updates, affecting the overall training process and model performance.

D. Backdoor attacks and model [10]

When malicious participants inject biased or manipulated data into the training process, the global model is influenced to produce the desired results. Backdoor attacks attempt to incorporate hidden patterns or triggers into the model, allowing

attackers to control or manipulate the model's behaviour in specific scenarios. These attacks can have a negative impact on the fairness, robustness, and generalisation performance of FL models.

E. Insider Threats and Data Exfiltration

Insider threats involve participants with authorised access to the FL system who may abuse their privileges or intentionally or unintentionally leak sensitive data. Participants may jeopardise the confidentiality of their local data by sharing it with unauthorised parties or exploiting the trained global model for personal gain. Mitigating insider threats and preventing unintentional data leakage is critical for FL system security and privacy.

Understanding FL cyber security concerns is critical for developing effective countermeasures and mitigating their potential impact. The following section investigates various strategies proposed in the literature to address these concerns and improve FL system security.

IV. Mitigation Strategies

Various mitigation strategies have been proposed in the literature to address cyber security concerns in federated learning (FL). This section discusses key approaches and techniques aimed at improving the security and privacy of FL systems.

A. Cryptographic Methods [11]

In FL, cryptographic techniques are critical for protecting participant data and ensuring secure communication. Homomorphic encryption enables secure model aggregation and computation on encrypted data without revealing the raw information. Secure multiparty computation (MPC) protocols allow participants to collaborate on computations without exposing their inputs, enhancing privacy and preventing information leakage. Differential privacy mechanisms can be used to introduce noise or perturbation into participants' data or model updates, protecting individual privacy while allowing accurate global model training.

B. Protocols for Secure Aggregation

Secure aggregation protocols enable participants to aggregate their model updates while maintaining their privacy. During the aggregation process, these protocols ensure that no participant can deduce the individual contributions of others. In FL, techniques such as secure sum, secure averaging, and secure weighted aggregation enable the development of robust and privacy-preserving aggregation schemes.

C. Model Validation and Robustness

It is critical to ensure the integrity and robustness of FL models to mitigate adversarial attacks and maintain reliable performance. Model verification techniques involve evaluating the correctness and trustworthiness of model updates submitted by participants before incorporating them into the global model. Robust optimisation methods can be used to improve the resilience of FL models against poisoning attacks and to mitigate the impact of adversarial data. Adversarial training and defence mechanisms, such as differential privacy-based defences or robust aggregation algorithms, can improve the FL model's robustness to various attacks.

D. Authentication and Access Control for Participants

Robust participant authentication mechanisms should be implemented in FL systems to mitigate insider threats and unauthorised access. Unauthorised participants can be prevented from joining or manipulating the training process by using multi-factor authentication, secure login protocols, and access control mechanisms. Furthermore, secure and accountable participant identification techniques can track and attribute activities to specific participants, improving accountability and discouraging malicious behaviour.

E. System Monitoring and Detection of Anomalies

In FL systems, continuous monitoring and anomaly detection mechanisms can assist in identifying suspicious activities, unusual behaviours, or deviations from expected patterns. Real-time monitoring of model updates, communication channels, and participant activities can help detect potential security breaches or attacks in real-time. To quickly identify and respond to security incidents, anomaly detection algorithms, statistical analysis, and machine learning-based techniques can be used.

F. Data Preprocessing to Protect Privacy

Data pre-processing techniques that protect privacy aim to reduce the privacy risks associated with data sharing in FL. Secure data obfuscation, data perturbation, and privacy-preserving data synthesis are examples of privacy-enhancing technologies that can be used to anonymize or de-identify sensitive data while retaining their utility for model training. These techniques help to protect participant privacy in FL by limiting the exposure of sensitive information.

These mitigation strategies are not mutually exclusive, and a combination of approaches may be required to address FL's cyber security concerns comprehensively. Furthermore, the efficacy and applicability of these strategies may differ depending on the specific FL setting, nature of the data, and threat landscape. FL practitioners can improve the security, privacy, and trustworthiness of FL systems and promote the use of this distributed learning paradigm in sensitive domains by implementing and refining these mitigation strategies.

V. Existing Frameworks

Federated learning (FL) has received a lot of attention in both research and industry, which has resulted in the

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 2, Issue – 1, June 2023
E-ISSN - 2583-7559

development of various frameworks and solutions to help with the implementation and deployment of FL systems. Google's TensorFlow Federated (TFF) framework [12] is one of the most widely used. TFF is a free and open-source framework that includes a programming interface as well as tools for creating and simulating FL systems. It integrates seamlessly with TensorFlow, allowing users to define FL computations while also leveraging the TensorFlow ecosystem. TFF supports federated learning for image classification, natural language processing, and recommendation systems, among other FL scenarios. Another popular solution is PySyft, a Python library built on top of PyTorch [13]. It allows for privacy-preserving machine learning, such as federated learning. PySyft is a higher-level FL API that enables users to define secure multi-party computations, encrypted training, and differential privacy mechanisms. It is intended to work with other deep learning frameworks and supports a wide range of FL architectures and protocols.PySyft Keras is a PySyft [14] extension designed specifically for federated learning by those working with the Keras deep learning library. It has a Keras-like interface for defining FL models and integrates seamlessly with PySyft's privacy-preserving mechanisms. PySyft Keras streamlines FL model implementation by allowing users to leverage existing Keras models and pre-trained weights. Flower, an open-source Python library developed at Imperial College London by Adap, provides a framework for developing FL systems. It supports a wide range of architectures and protocols as well as a flexible and extensible API for defining federated learning tasks. Flower includes features such as automatic model compression, secure aggregation, and dynamic participant selection. Its goal is to make FL more accessible and scalable for use in both research and production settings. Webank, a leading Chinese digital bank, initiated the Federated AI Technology Enabler (FATE) open-source project. FATE provides a comprehensive and adaptable platform for developing secure and private FL systems. Federated XGBoost, Federated GBDT, and Federated Deep Learning are among the FL algorithms available. FATE also supports a variety of privacy safeguards, such as secure multi-party computation (MPC) and differential privacy. OpenMined is a volunteer-led organisation that focuses on privacy-preserving technologies such as federated learning. It provides a library, tool, and educational resource ecosystem to enable secure and privacy-focused machine learning. PySyft is one of OpenMined's core projects, and it emphasises principles like transparency, accountability, and decentralisation in FL. These existing frameworks and solutions provide powerful tools and resources for developers, researchers, and practitioners to implement and evaluate FL systems. Each framework has its own set of advantages and focuses on different aspects of FL, such as integration with deep learning frameworks, privacy protection techniques, or scalability. Specific requirements use cases, and the development team's expertise all influence the framework chosen.

VI. Recent Literature

A. *ShieldFL [15]*

This paper introduces ShieldFL, a privacy-preserving model poisoning defence strategy for Privacy-Preserving Federated Learning (PPFL). The strategy uses two-trapdoor homomorphic encryption, secure cosine similarity, and Byzantine-tolerance aggregation. ShieldFL outperforms existing defence strategies on MNIST, KDDCup99, and Amazon benchmark datasets. It improves model poisoning defence by 30%–80% in IID and non-IID settings. The findings show that ShieldFL improves PPFL system security and robustness.

B. *Cyber-resilient hybrid approach using CNN [16]*

Federated Learning and Convolutional Neural Networks (CNN) are used in this study to forecast short-term wind power generation in Iran. The method emphasises accuracy, generalizability, data independence, and security. CNN extracts region-specific features for nine federated network clients. A generalised global supermodel can forecast wind power in new regions without training data using these features. The approach is tested in various scenarios, including accurate wind power forecasting in Mahshahr, Bojnord, and Lootak with 84%, 85%, and 74% accuracy, respectively. Forecasting models are also tested for data integrity attacks like scaling attacks. Image-processing-based cyber-attack detection is also used. The results show that the proposed wind power forecasting approach works across Iran and is cyber-resilient.

C. *Framework for Evaluating and Mitigating Privacy Leakage Attacks [17]*

This paper addresses Federated Learning (FL) client privacy leakage. FL privacy leakage attacks are evaluated and compared in the study. Formal analysis and experiments show how adversaries can reconstruct private local training data by analysing shared parameter updates. Hyperparameter configurations and attack algorithms affect attack effectiveness and cost. It tests attacks in communication-efficient FL protocols with different gradient compression ratios. The experiments suggest preliminary mitigation strategies and stress the need for a systematic evaluation framework to understand and mitigate FL client privacy leakage threats.

D. *mGAN-AI [18]*

This paper introduces mGAN-AI to analyse and mitigate privacy leakage in federated learning. A multi-task GAN with an auxiliary identification mechanism classifies input samples by category, reality, and client. Client identity discrimination lets the generator recover user-specific private data. The server-side mGAN-AI framework "invisibly" supports federated learning, unlike other methods. The paper discusses

anonymization and introduces a linkability attack to re-identify anonymized updates by associating client representatives. Experimental results show that the proposed methods outperform current methods.

E. ZeKoC [19]

In resource-constrained scenarios, ZeKoC mitigates adversarial attacks in federated learning. The proposed method addresses deep neural network vulnerabilities and distributed federated learning challenges. ZeKoC treats adversarial mitigation as an unsupervised weight clustering problem, letting the server split and merge weight clusters for weight selection and aggregation. ZeKoC outperforms state-of-the-art schemes in mitigating general attacks, especially in non-i.i.d. data settings. This work improves the security and robustness of IoT/CPS-driven smart-world federated learning systems.

F. VCPS data privacy architecture [20]

This article describes a secure and intelligent Vehicular Cyber-Physical Systems (VCPS) data privacy architecture. Dynamic content caching, resource allocation, and data sharing improve service quality and user experience. A privacy-preserving federated learning mechanism with intelligent data transformation and collaborative leakage detection reduces data leakage. Experimental results demonstrate the scheme's accuracy, efficiency, and security in VCPS data privacy. This research improves VCPS security, passenger safety, privacy, and property loss. The proposed architecture and federated learning approach improve data privacy in VCPS, encouraging future deployments of secure and intelligent solutions.

G. TiFL [21]

TiFL introduces a tier-based architecture to address resource and data heterogeneity in Federated Learning (FL) systems. TiFL mitigates the impact on training time and model accuracy by selecting clients from the same tier during training rounds. Additionally, TiFL incorporates an adaptive tier selection approach to handle non-IID data and resource heterogeneity. Experimental evaluation demonstrates superior performance compared to conventional FL methods. TiFL shows promise for enhancing FL in real-world scenarios, enabling more effective and efficient collaborative learning in heterogeneous environments.

VII. Open Challenges and Future Directions

Despite advances and promising results in federated learning (FL), several open challenges remain, and there are a variety of future research and development directions. Addressing these issues will improve FL systems' security, privacy, efficiency, and scalability. The following are some of the most important open challenges and future directions:

A. Techniques for Preserving Privacy

Developing more robust and efficient privacy-preserving techniques is an important area for future research. Enhancing the effectiveness of differential privacy mechanisms, experimenting with advanced cryptographic methods, and investigating novel approaches such as homomorphic encryption and secure multiparty computation can all help to strengthen FL's privacy guarantees.

B. Adversarial Robustness

Adversarial attacks can be devastating to FL systems. Developing strong defences against poisoning attacks, model inversion attacks, and backdoor attacks is critical. Exploring techniques such as adversarial training, robust aggregation algorithms, and secure model verification can improve FL models' resilience and robustness to various attacks.

C. Communication Overhead Reduction

Reducing communication overhead in Florida is an ongoing challenge. It is critical to develop efficient communication protocols and compression techniques for transmitting model updates while maintaining privacy. Exploring the use of edge computing, federated learning over heterogeneous networks, and adaptive communication strategies can aid in reducing communication bottlenecks and improving FL efficiency overall.

D. Heterogeneity and Scalability

FL systems must be scalable in order to accommodate a large number of participants and diverse data sources. Developing techniques for dealing with heterogeneous data distributions, varying computational capabilities, and resource-constrained devices is critical. Investigating distributed learning algorithms, adaptive participant selection methods, and efficient aggregation schemes can help FL overcome scalability and heterogeneity issues.

E. Considerations for Regulatory and Legal Frameworks

FL systems operate within a variety of regulatory and legal frameworks. It is critical to address the issues of data ownership, data governance, and compliance with privacy regulations. FL adoption can be facilitated by researching and developing mechanisms to ensure accountability, transparency, and compliance in healthcare, finance, and government domains.

F. Standardisation and Benchmarking

In order to compare and benchmark different FL approaches, standard evaluation metrics, datasets, and benchmarks must be established. Creating representative benchmark datasets and developing standardised evaluation protocols will improve the reproducibility and comparability of research results in Florida.

G. *Real-World Deployments*

Practical challenges such as network heterogeneity, unreliable or intermittent connections, and limited computational resources must be addressed to expand FL deployment in real-world settings. Investigating deployment strategies, adaptive learning algorithms, and fault tolerance mechanisms can help FL be implemented effectively in a variety of environments.

Collaboration between researchers, practitioners, policymakers, and domain experts from various disciplines is essential for effectively addressing Florida's complex challenges. Interdisciplinary collaboration and knowledge sharing can lead to innovative solutions, informed policy frameworks, and practical FL deployments in a variety of domains. Addressing these open challenges and exploring the above-mentioned future directions will pave the way for FL's widespread adoption and application. Continued research, collaboration, and innovation in these areas will help to advance the state-of-the-art in FL and realise its potential for secure and privacy-preserving distributed machine learning. Conclusion

Federated Learning (FL) presents unique cybersecurity challenges, such as adversarial attacks, data privacy breaches, and communication risks. Researchers have proposed strategies including cryptographic methods, secure aggregation protocols, model validation, authentication, system monitoring, and data pre-processing. Further exploration is needed in privacy-preserving techniques, adversarial robustness, scalability, heterogeneity, standardization, and real-world deployments. Sustained research and interdisciplinary collaboration are crucial. FL holds promise in addressing privacy and scalability issues in machine learning, but cybersecurity concerns must be addressed. Embracing future directions and advancing privacy-preserving techniques can revolutionize collaborative and privacy-preserving machine learning. The secure adoption of FL relies on privacy measures and standardized evaluation metrics.

REFERENCES

[1] Majeed, I. A., Kaushik, S., Bardhan, A., Tadi, V. S. K., Min, H. K., Kumaraguru, K., & Muni, R. D. (2022). Comparative assessment of federated and centralized machine learning. arXiv preprint arXiv:2202.01529.

[2] AbdulRahman, S., Tout, H., Ould-Slimane, H., Mourad, A., Talhi, C., & Guizani, M. (2020). A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. IEEE Internet of Things Journal, 8(7), 5476-5497.

[3] Bonawitz, K., Kairouz, P., McMahan, B., & Ramage, D. (2021). Federated Learning and Privacy: Building privacy-preserving systems for machine learning and data science on decentralized data. Queue, 19(5), 87-114.

[4] Hosseini, E., & Khisti, A. (2021, December). Secure aggregation in federated learning via multiparty homomorphic encryption. In 2021 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.

[5] Zhang, C., Li, S., Xia, J., Wang, W., Yan, F., & Liu, Y. (2020, April). Batchcrypt: Efficient homomorphic encryption for cross-silo federated learning. In Proceedings of the 2020 USENIX Annual Technical Conference (USENIX ATC 2020).

[6] Khan, L. U., Saad, W., Han, Z., Hossain, E., & Hong, C. S. (2021). Federated learning for internet of things: Recent advances, taxonomy, and open challenges. IEEE Communications Surveys & Tutorials, 23(3), 1759-1799.

[7] Abreha, H. G., Hayajneh, M., & Serhani, M. A. (2022). Federated learning in edge computing: a systematic survey. Sensors, 22(2), 450.

[8] Jere, M. S., Farnan, T., & Koushanfar, F. (2020). A taxonomy of attacks on federated learning. IEEE Security & Privacy, 19(2), 20-28.

[9] Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. Future Generation Computer Systems, 115, 619-640.

[10] Bagdasaryan, E., Veit, A., Hua, Y., Estrin, D., & Shmatikov, V. (2020, June). How to backdoor federated learning. In International Conference on Artificial Intelligence and Statistics (pp. 2938-2948). PMLR.

[11] Zhang, S., Li, Z., Chen, Q., Zheng, W., Leng, J., & Guo, M. (2021, August). Dubhe: Towards data unbiasedness with homomorphic encryption in federated learning client selection. In 50th International Conference on Parallel Processing (pp. 1-10).

[12] Sun, Z., Kairouz, P., Suresh, A. T., & McMahan, H. B. (2019). Can you really backdoor federated learning?. arXiv preprint arXiv:1911.07963.

[13] Imambi, S., Prakash, K. B., & Kanagachidambaresan, G. R. (2021). PyTorch. Programming with TensorFlow: Solution for Edge Computing Applications, 87-104.

[14] Ziller, A., Trask, A., Lopardo, A., Szymkow, B., Wagner, B., Bluemke, E., ... & Kaissis, G. (2021). Pysyft: A library for easy federated learning. Federated Learning Systems: Towards Next-Generation AI, 111-139.

[15] Z. Ma, J. Ma, Y. Miao, Y. Li and R. H. Deng, "ShieldFL: Mitigating Model Poisoning Attacks in Privacy-Preserving Federated Learning," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1639-1654, 2022, doi: 10.1109/TIFS.2022.3169918.

[16] Moayyed, H., Moradzadeh, A., Mohammadi-Ivatloo, B., Aguiar, A. P., & Ghorbani, R. (2022). A Cyber-Secure generalized supermodel for wind power forecasting based on deep federated learning and image processing. Energy Conversion and Management, 267, 115852.

[17] Wei, W. et al. (2020). A Framework for Evaluating Client Privacy Leakages in Federated Learning. In: Chen, L., Li, N., Liang, K., Schneider, S. (eds) Computer Security – ESORICS 2020. ESORICS 2020. Lecture Notes in Computer Science(), vol 12308. Springer, Cham. https://doi.org/10.1007/978-3-030-58951-6_27

[18] M. Song et al., "Analyzing User-Level Privacy Attack Against Federated Learning," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 10, pp. 2430-2444, Oct. 2020, doi: 10.1109/JSAC.2020.3000372.

[19] Z. Chen, P. Tian, W. Liao and W. Yu, "Zero Knowledge Clustering Based Adversarial Mitigation in Heterogeneous Federated Learning," in IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1070-1083, 1 April-June 2021, doi: 10.1109/TNSE.2020.3002796.

[20] Y. Lu, X. Huang, Y. Dai, S. Maharjan and Y. Zhang, "Federated Learning for Data Privacy Preservation in Vehicular Cyber-Physical Systems," in IEEE Network, vol. 34, no. 3, pp. 50-56, May/June 2020, doi: 10.1109/MNET.011.1900317.