THE ASIAN BULLETIN OF BIG DATA MANAGEMENT
Vol.4. Issue4 (2024)
https://doi.org/ 10.62019/abbdm.v4i4.277

An insightful Machine Learning based Privacy-Preserving Technique for Federated Learning

Ammar Ahmed*,M. Aetsam Javed, Junaid Nasir Qureshi, Hamayun Khan, Hoor Fatima Yousaf

Chronicle

Article history

Received: Oct 12, 2024
Received in the **revised format:** Oct 29, 2024
Accepted: December 11, 2024
Available online: December 20, 2024

Ammar Ahmed is currently affiliated with Department of Information Technology, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
Email: ammarahmed9917@gmail.com
M. Aetsam Javed is currently affiliated with Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
Email: SU92-PHCSW-F24-023@superior.edu.pk
Junaid Nasir Qureshi is currently affiliated with Department of Computer Science, Bahria University, Lahore Campus, 54000, Pakistan
Email: jnqureshi.bulc@bahria.edu.pk
Hamayun Khan is currently affiliated with Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
Email: hamayun.khan@superior.edu.pk
Hoor Fatima Yousaf is currently affiliated with Department of Computer Science, Bahria University, Lahore Campus, 54000, Pakistan
Email: hoorfatima.bulc@bahria.edu.pk

Corresponding Author*

Abstract

Federated Learning has emerged as a promising paradigm for collaborative machine learning while preserving data privacy. Federated Learning is a technique that enables a large number of users to jointly learn a shared machine learning model, managed by a centralized server while training data remains on user devices. In recent years, along with the blooming of Machine Learning (ML)-based applications and services, ensuring data privacy and security has become a critical obligation. ML-based service providers are not only confronted with difficulties in collecting and managing data across heterogeneous sources but also challenges of complying with rigorous data protection regulations such as the General Data Protection Regulation (GDPR) Federated Learning is very important to reduce data privacy risks. Federated Learning is a scheme in which several consumers work collectively to unravel machine learning problems, with a dominant collector synchronizing the procedure. This paper reviews recent advancements in privacy-preserving techniques for federated learning from a machine-learning perspective. This paper investigates the potential of Federated Learning for privacy-preserving machine learning in domains like healthcare, finance and IOT, where data privacy is paramount. We explore existing techniques to enhance privacy, including differential privacy, secure aggregation, homomorphic encryption, federated learning with encrypted, meta-learning, machine learning, privacy-preserving techniques, blockchain technology, decentralized learning, federated averaging, data privacy, searchable encryption and zero-knowledge proofs. This paper concludes with future research directions to address ongoing challenges & further enhance the effectiveness & scalability of privacy-preserving federated learning.

Keywords: Federated Learning, Privacy-Preserving Techniques, Machine Learning, Collaborative Learning, Data Privacy, Privacy-Preservation, Searchable Encryption, Zero Knowledge Proofs, Differential Privacy, Secure Aggregation, Homomorphic Encryption, Blockchain Technology, Decentralized learning, Federated averaging.

INTRODUCTION

Federated Learning has emerged as a promising paradigm for collaborative model training across decentralized data sources while preserving privacy. Federated Learning is a decentralized machine paradigm where models are trained collaboratively across multiple devices or servers holding Local data. In this paper, we review recent developments in privacy-preserving techniques for federated learning from a machine-learning perspective [1, 2]. We explore methods such as differential privacy, secure multi-party computation (SMPC), homomorphic encryption, and Federated Learning with encrypted data, highlighting their strength and limitations

[3]. By addressing privacy concerns, these techniques pave the way for wider adoption of Federated Learning across diverse domains and applications. Federated Learning preserves user privacy by enabling model training without sharing raw data, in contrast to typical centralized systems. Federated Learning allows global model creation while maintaining data localization through iterative rounds of model distribution, local training, and parameter aggregation. Unlike traditional models, Machine Learning models can continuously with minimal to no intervention. Federated Learning addresses privacy concerns in traditional machine learning by maintaining on-device [4, 5] Federated Learning (FedML) is a distributed machine approach that is developed to provide efficient privacy-preserving machine learning in a distributed environment. Privacy is paramount in federated learning due to its decentralized nature, where models are trained on distributed data sources without centralizing them. This strategy lessens worries about unauthorized access to private data and data privacy violations [6]. Federated Learning protects privacy so that different parties can collaborate without finance and telecommunication. Additionally, maintaining privacy in federated learning builds participant confidence, which promotes wider adoption and collaboration in the federated learning ecosystem. Homomorphic encryption another powerful tool, allows computation on encrypted data, thus ensuring data privacy even during the processing stages. Federated Learning presents several challenges, including communication overhead, heterogeneity in local data, and vulnerabilities to adversarial attacks. The advantages of federated learning include preserving privacy by keeping the data localized on devices [7, 8].

However, federated learning is not immune to privacy threats. The exchange of model updates during the training process can still leak sensitive information, necessitating robust privacy presentation strategies. Despite these advancements, the implementation of privacy-preserving techniques in federated learning poses several challenges. Scalability, communication overhead, and the delicate balance between privacy and model accuracy are critical issues that need to be addressed to make these methods viable for real-world application [9, 10].

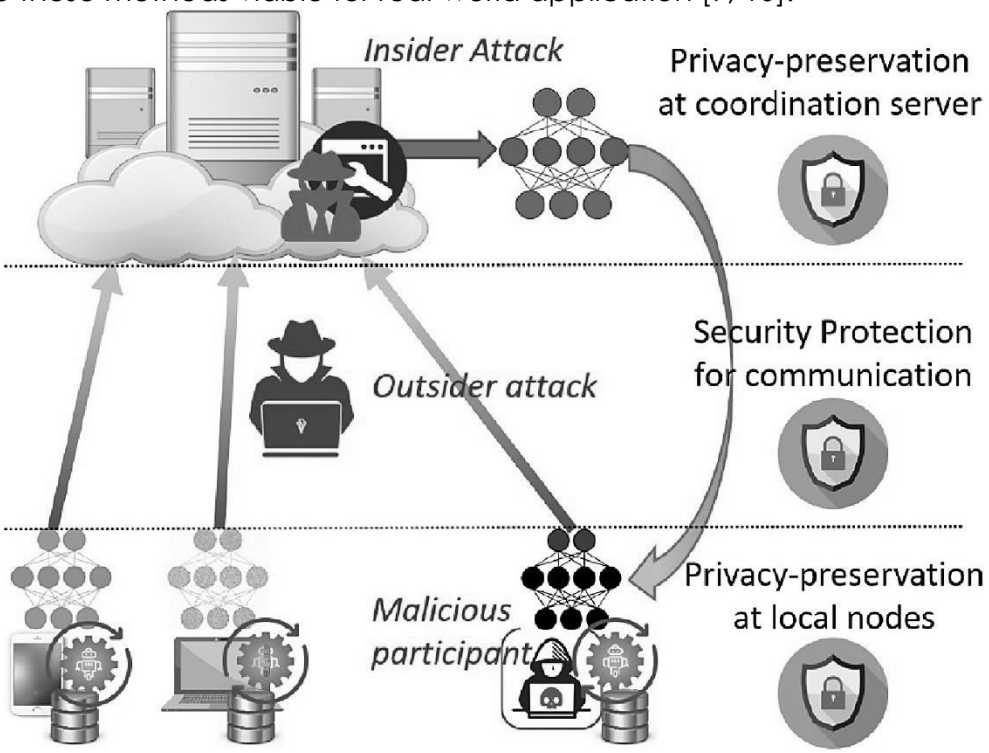

Figure 1: Overview of the Security employed FL framework [11]

The paper also explores emerging trends such as hybrid approaches that combine multiple privacy-preserving techniques to leverage their respective strengths. Additionally, it discusses the application-specific challenges and solutions, highlighting case studies from various industries to illustrate practical implementations [12, 13].

LITERATURE REVIEW

The study proposed a privacy-preserving Federated Learning (FL) framework that integrates bitwise quantization, local differential privacy (LDP), and features hashing to address privacy concerns when training machine learning models on sensitive local data. The approach uses randomized response algorithms and quantizes local model updates to maintain privacy while enabling collaborative model training across edge devices [14]. The paper presents a novel privacy-preserving federated learning solution, PPFL-LQDP that addresses the issue of excessive participation of low-quality data in federated training. By constructing a composite evaluation value for the data, the negative impact of low-quality data on federated training is reduced, while ensuring the privacy and security of participant data through a secure framework [15, 16].

The study offers promising innovations for various fields, including healthcare. Nonetheless, managing substantial volumes of private medical data presents several security and privacy issues. Federated learning presents itself as a viable remedy, allowing machine learning models to be trained without requiring the exchange of raw data. An overview of the literature on federated learning in healthcare is given in this study, with a focus on the technology's uses, difficulties, consequences, and opportunities for improving healthcare analytics and decision-making while protecting patient privacy [17, 18].

The study investigates Federated Learning, a burgeoning field aimed at training complex models while preserving data privacy. They recognize the potential benefits of combining data from various sources for model training, but they also stress the significance of safeguarding sensitive data [19]. The study presents recent advancements in privacy-preserving AI techniques applied to biomedicine, aiming to address concerns regarding the privacy of individual participants when training AI models on sensitive data [20].

The study focused on recent years, with the rise of Machine Learning (ML) applications, ensuring data privacy and security has become imperative. Federated Learning (FL), which enables distributed learning without requiring raw data exchange, has come to light as a potential remedy for privacy issues [21, 22]. In this paper, we reiterate the concept of federated learning and propose secure federated learning (SFL), where the ultimate goal is to build trustworthy and safe AI with strong privacy-preserving and IP-right-preserving. We provide a comprehensive overview of existing works, including threats, attacks, and defenses in each phase of SFL from the lifecycle perspective [23].

In this paper, authors present in detail an understanding of Federated Machine Learning, various federated architectures along different privacy-preserving mechanisms. The main goal of this survey work is to highlight the existing privacy techniques and also propose applications of Federated Learning in industries [24]. In addition, in recent years, there has been a lot of work on privacy protection machine learning worthy of attention. Proposed using differential privacy to protect privacy in machine learning, and SMC was used to reduce the noise caused by differential privacy. Federated learning has been widely used in various fields. For example, the Gboard system designed by Google realizes keyboard input prediction while protecting privacy and helping users improve input efficiency [25]. In the medical

field, patients' medical data are sensitive, thus federated learning is very useful. Besides this, natural language processing and recommendation systems are also applicable to federated learning as well [26].

LITERATURE REVIEW

Enhancing The performance of badminton players is influenced by a combination of leadership qualities, cognitive abilities, and fitness parameters. These variables play a critical role in determining both individual and team success in competitive environments. This review examines the existing literature on each of these variables to provide a foundation for their integration into a predictive framework for badminton performance. Leadership qualities significantly impact an athlete's performance and the dynamics of sports teams. Effective leadership enhances decision-making, fosters team cohesion, and promotes motivation under competitive pressure. Smith and Cotterill (2017) highlighted that team captains who exhibit strong leadership traits can positively influence team performance, particularly in strategy-intensive sports like badminton. Leadership also plays a crucial role in enabling athletes to overcome challenges and adapt to dynamic game scenarios (Cotterill, 2013). Cognitive abilities, such as anticipation, decision-making, and reaction time, are pivotal in high-speed sports. Badminton demands rapid processing of visual and spatial information, which affects players' ability to anticipate opponents' moves and respond effectively. Abernethy et al. (2013) found that elite players demonstrate superior cognitive skills compared to novices, emphasizing the importance of these attributes in performance differentiation.

Moreover, cognitive training interventions have shown promise in enhancing these skills, further underscoring their relevance (Farrow & Abernethy, 2015). Fitness parameters are the cornerstone of physical performance in badminton. Agility, endurance, and muscular strength are essential for executing fast-paced movements and maintaining performance throughout matches. Ghosh et al. (2012) emphasized that elite badminton players exhibit superior levels of aerobic capacity and muscular endurance compared to their less successful counterparts. Furthermore, fitness training tailored to the demands of badminton has been shown to improve overall performance, particularly in prolonged competitive settings (Chin et al., 2010). The integration of these variables into predictive models using machine learning is a recent advancement in sports science. Machine learning algorithms can process large datasets and uncover patterns that are not immediately apparent through traditional analysis methods. Hughes and Bartlett (2015) demonstrated the effectiveness of such approaches in identifying key performance indicators in various sports. However, there is limited research that combines leadership, cognitive, and fitness parameters into a single predictive framework, particularly in the context of badminton. This review highlights the importance of addressing the interconnections among leadership, cognitive abilities, and fitness parameters to provide a comprehensive understanding of badminton performance. By leveraging machine learning, the study aims to bridge existing research gaps and offer actionable insights for performance

optimization.

PRIVACY –PRESERVING TECHNIQUES OVERVIEW

Privacy-preserving techniques in federated learning aim to protect sensitive data while enabling collaborative model training across decentralized sources. Diverse methods include homomorphic encryption, secure multi-party computation, federated learning with encrypted data, zero-knowledge proofs, differential privacy, secure aggregation and data masking and perturbation [27].

Secure Multi-party Computation (SMPC)-

Secure Multi-party computation (SMPC) is a cryptographic technique that allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. In the context of federated learning, SMPC enables participants to collaborate on model training without revealing their raw data to each other [28]. Differential privacy is a privacy-preserving concept that ensures that the presence or absence of any single data point in a dataset does not significantly affect the outcome of queries or computation. It provides a strong mathematical guarantee of privacy by adding carefully calibrated noise to query responses or statistical computations [29, 30].

Federated Learning with Encrypted Data-

An enhancement of conventional federated learning, Federated Learning with Encrypted Data (FLED) concentrates on protecting privacy by encrypting the data before it leaves the local device. This method guarantees that sensitive data is always safeguarded by enabling model training on encrypted data [30, 31]. Using homomorphic encryption, calculations on encrypted data can be carried out in a way that ensures the outcomes match those of similar calculations done on unencrypted data. Put otherwise, it makes it possible to do operations like addition and multiplication on ciphertexts, or encrypted data, resulting in ciphertexts that, upon decryption, produce the same outcome as if the operations had been carried out on the plaintext, or unencrypted data [32, 33]. Cryptographic techniques known as Zero-Knowledge Proofs (ZKPs) enable one person, known as the prover, to persuade another, known as the verifier, that a given assertion is true while withholding any further information beyond the veracity of the statement. ZKPs can be used in federated learning to protect privacy and maintain the ability to validate model updates [34, 35].

Hybrid Approaches

Hybrid approaches that combine differential privacy with SMPC or homomorphic encryption can provide enhanced privacy guarantees by leveraging the strengths of multiple techniques [36, 37]. Data Masking and perturbation are two key techniques in privacy-preserving data analysis. They aim to obfuscate sensitive information within data while maintaining its usefulness for tasks like model training or statistical analysis [38]. Secure aggregation is a crucial technique in privacy-preserving machine learning that allows multiple parties to combine their data securely while protecting individual privacy [39].

Table 1.
Summary of Privacy-Preserving Techniques for Federated Learning

Techniques	Advantages	Disadvantages	Ref
Secure Multi-party computation (SMPC)	Preserve data privacy without sharing raw data. Supports complex computations	High computational and communication costs.	[40]
Homomorphic Encryption	Preserves data privacy during computation. Supports various operations	High computational overhead, limited operations.	[41]
Federated Learning with Encrypted Data	Protects data privacy during model training. Enables collaboration on sensitive data.	Limited support for complex models, requires specialized encryption schemes.	[42]
Differential Privacy	Strong privacy guarantees, can be applied to various data types.	May reduce data utility, and complex noise calibration.	[43]

Proposed architecture-

Client devices, local model trainers, a central server or aggregator, privacy-preserving methods, model assessment and deployment components, privacy governance and compliance procedures are all part of the suggested architecture for privacy-preserving federated learning [44].

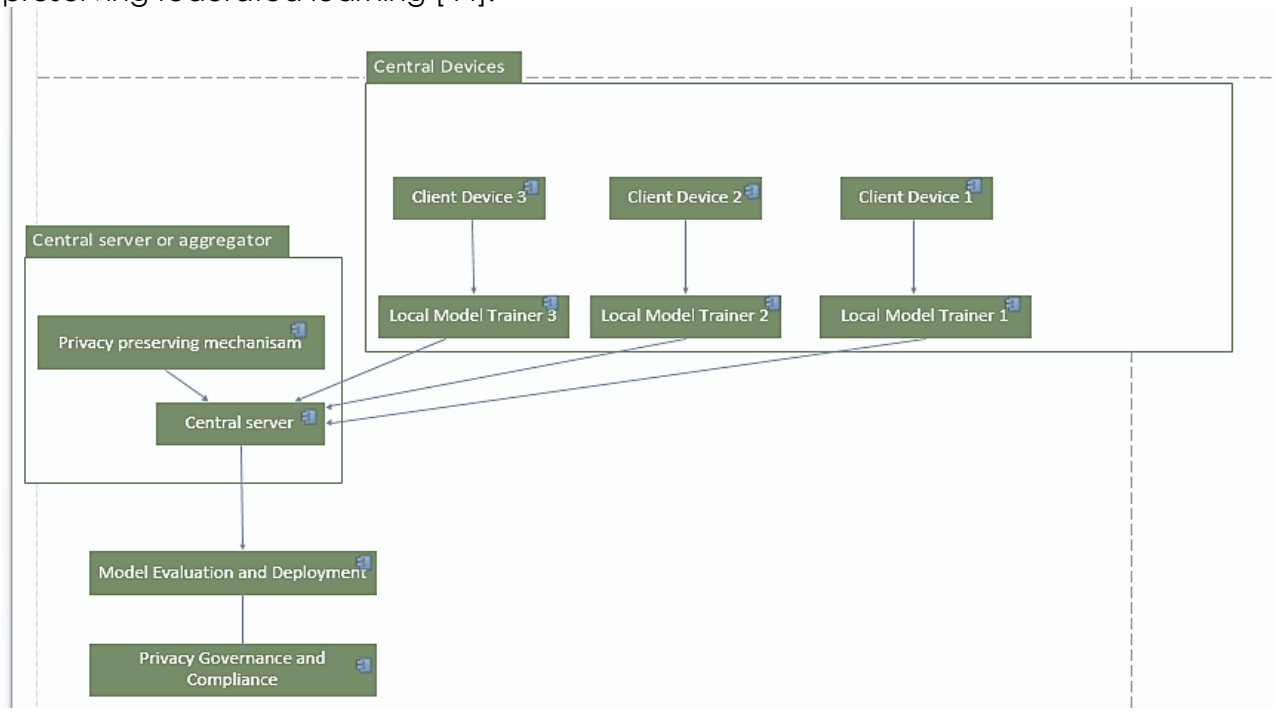

Figure 2.
Architecture for federated learning with a focus on privacy-preserving techniques [45]

Client Devices:

- These are the gadgets-such as cell phones, Internet of Things sensors, or edge devices –where data is first created. Local datasets are stored by them.
- Using its data, each client device oversees training a local device.
- Client devices use methods like federated learning with encrypted data or differential privacy to protect privacy.

Local Model Trainer-

- This part manages the local model's training and is housed within every client device.
- To protect the privacy of the data while training the model, it uses privacy-preserving model.
- Following training, the central server or aggregator receives encrypted model updates (gradients) from the local model trainer.

Central Server or Aggregator-

The central server uses secure aggregation techniques, like secure multi-party computation to protect privacy during aggregation. These techniques enable computations to be done on encrypted data without disclosing individual contributions.

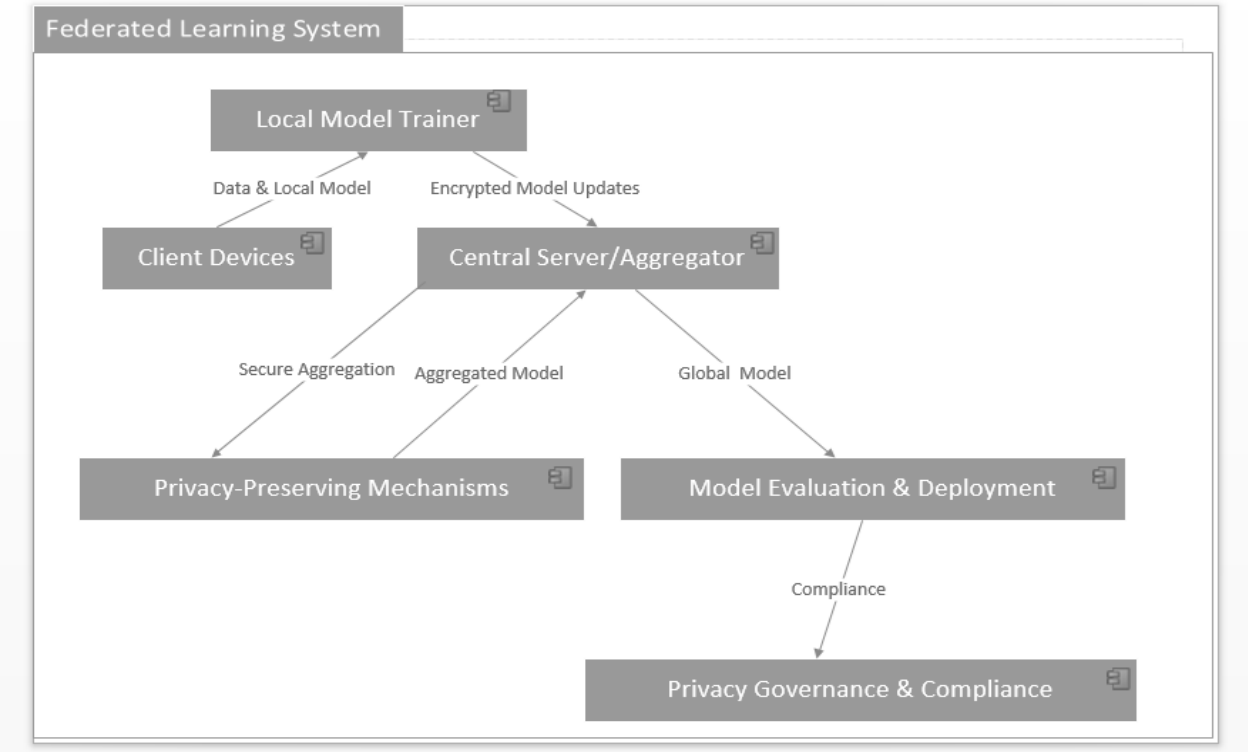

Figure 3.
Components for federated learning with a focus on privacy-preserving techniques [46]

Privacy-Preserving Mechanisms-

- Differential privacy Module
- Secure Aggregation Module

- Homomorphic Encryption Module

Model Evaluation and Deployment-

- Following aggregation, the global model can be used for inference tasks and its performance assessed.
- To ensure data confidentiality, privacy-preserving measures might be used again when evaluating and deploying the model.

Privacy Governance and Compliance-

- This part of the architecture includes the mechanisms to manage data access rights, obtain user consent, audit privacy-preserving processes to ensure compliance with legal and ethical requirements, and ensure that privacy-regulations and standards are followed throughout the federated learning process.

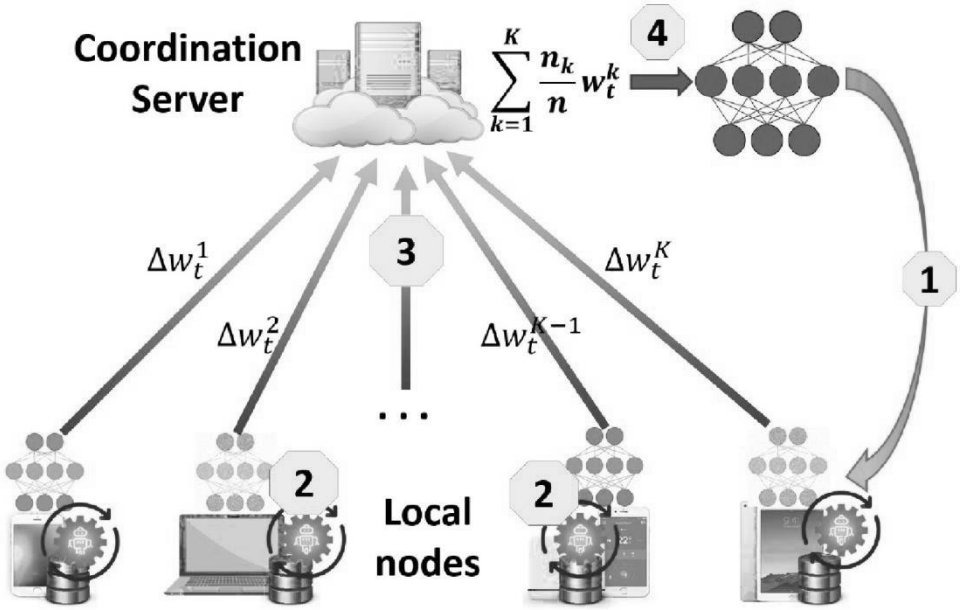

Figure 4.
Workflow cycle in FL framework [47]

Table 2.
Summary of Privacy-Preserving Techniques for Federated Learning

Techniques	Advantages	Disadvantages	Ref
Zero-knowledge Proofs	Provides cryptographic proofs without data disclosure. Supports privacy-preserving authentication.	High computational complexity, limited applications.	[48]
Secure Aggregation	Improves data security and compliance with privacy regulations.	Choosing the appropriate protocol for specific needs.	[49]
Data Masking and perturbation	Complies with regulations: Supports adherence to data	Not foolproof: Sophisticated attackers might still	[50]

	privacy regulations like GDPR and HIPAA.	be able to deanonymize data.	
Hybrid Approaches	Enhanced privacy protection; Flexible in application.	Complexity in implementation; May involve high overhead.	[50]

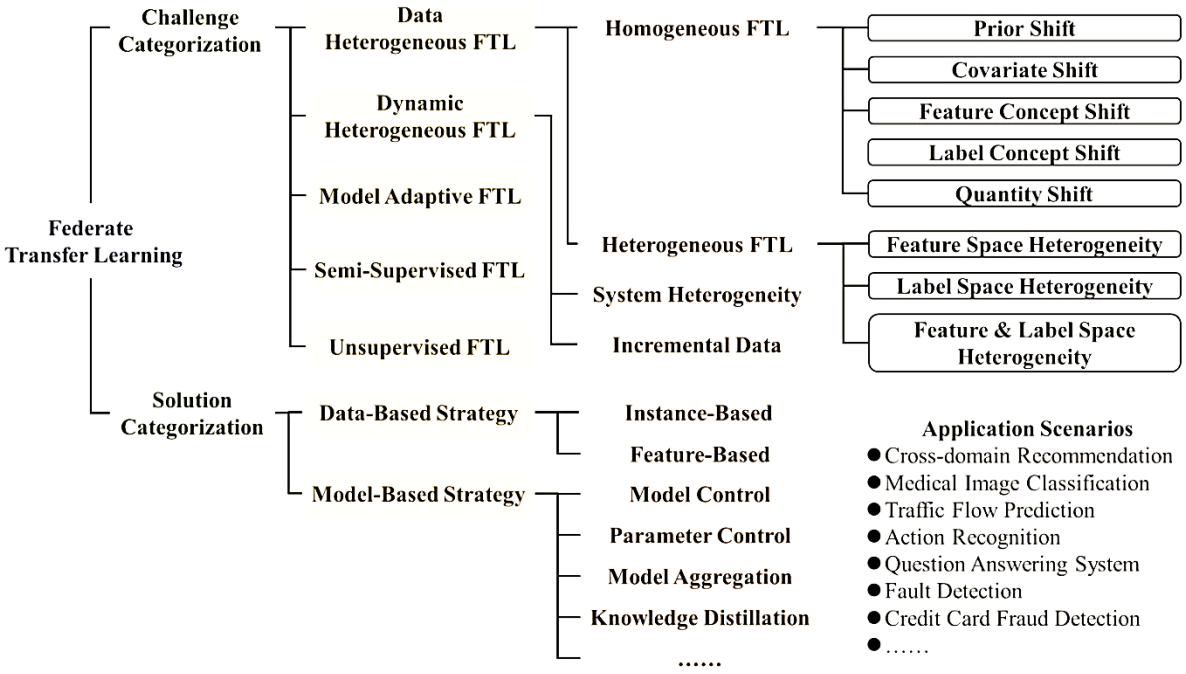

Figure 5.
Workflow cycle in FL Challenges & Solution [51]

Hybrid HE with Secure Aggregation:

Combining homomorphic encryption with secure aggregation protocols to protect individual client updates while ensuring only aggregated values are shared.

Secret Sharing Schemes:

Techniques like Shamir's secret sharing and additive secret sharing are now being optimized for federated learning environments, allowing model parameters to be shared across multiple parties securely. This approach has become more popular, where the server aggregates encrypted client updates without learning any of the individual updates. Federated Averaging (FedAvg) is enhanced to include privacy-preserving methods like secure aggregation, gradient clipping, and quantization. This ensures that aggregated gradients cannot expose sensitive information. Combining SMPC and TEEs to further improves the privacy guarantees by offloading part of the computation to a trusted environment while ensuring that no single party learns the complete update.

CONCLUSION

In conclusion, this paper has provided a comprehensive overview of recent advancements in privacy-preserving techniques for federated learning from a machine learning perspective. By categorizing and analyzing state-of-the-art approaches, we have gained insights into the strengths, limitations, and potential applications of these techniques. Federated learning holds great promise for

collaborative machine learning while safeguarding data privacy, and addressing concerns associated with centralized data processing. However, several challenges remain, including scalability issues, performance overhead, and robustness concerns. Addressing these challenges requires further research and innovation in the development of efficient and secure privacy-preserving mechanisms. Additionally, ensuring regulatory compliance and building trust among stakeholders are crucial aspects that need to be considered in the deployment of federated learning systems. Looking ahead, future research directions should focus on enhancing the effectiveness and scalability of privacy-preserving federated learning techniques. This includes exploring novel algorithms, improving communication efficiency, and addressing emerging threats and vulnerabilities. By addressing these challenges, we can unlock the full potential of federated learning for collaborative machine-learning applications across various domains while upholding the highest standards of data privacy and security.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the supervisors and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author participated equally to the creation of this work.
Conflicts of Interests: The author declares that there is no conflict of interest related to this study. All research activities, data collection, and analysis were conducted with full transparency and impartiality. No financial or personal relationships that could influence the research outcomes exist. The findings and conclusions presented in this work are solely based on the data collected and the academic analysis carried out throughout the study.
Consent to Participate: Yes
Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

[1] R. Gosselin, L. Vieu, F. Loukil, and A. Benoit, "Privacy and Security in Federated Learning: A Survey," Appl. Sci., vol.12, no. 19, pp. 1–15, 2022, doi: 10.3390/app1219990

[2] T. Alam and R. Gupta, "Federated Learning and Its Role in the Privacy Preservation of IoT Devices," Futur. Internet, vol.14, no. 9, pp. 1–22, 2022, doi: 10.3390/fi14090246.

[3] A. Jawale, P. Warole, S. Bhandare, K. Bhat, and R. Chandre, "Jeevn-Net: Brain Tumor Segmentation using Cascaded U-Net & Overall Survival Prediction," Int. Res. J. Eng. Technol., pp. 56–62, 2020.

[4] B. Nagy et al., "Privacy-preserving Federated Learning and its application to natural language processing," Knowledge-Based Syst., vol. 268, p. 110475, 2023, doi: 10.1016/j.knosys.2023.110475.

[5] L. Campanile, S. Marrone, F. Marulli, and L. Verde, "Challenges and Trends in Federated Learning for Well-being andHealthcare," Procedia Comput. Sci., vol. 207, no. Kes, pp. 1144–1153, 2022, doi: 10.1016/j.procs.2022.09.170.

[6] [A. Velez-Estevez, P. Ducange, I. J. Perez, and M. J. Cobo, "Conceptual structure of federated learning research field,"Procedia Comput. Sci., vol. 214, no. C, pp. 1374–1381, 2022, doi: 10.1016/j.procs.2022.11.319.

[7] R. Torkzadehmahani et al., "Privacy-Preserving Arti fi cial Intelligence Techniques in

Biomedicine," pp. 12–27, 2022.
[8] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023
[9] M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019
[10] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.
[11] U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023
[12] Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",sss Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019
[13] H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023
[14] Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.
[15] S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024
[16] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018
[17] Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024
[18] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020
[19] Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.
[20] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024
[21] Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024
[22] Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical

Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

[23] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

[24] Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

[25] Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

[26] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[27] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

[28] Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

[29] Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

[30] Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

[31] Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

[32] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

[33] Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

[34] Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

[35] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

[36] Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

[37] Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (AI) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power IoT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

[38] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for

Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

[39] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[40] Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

[41] Abdullah, M., Khan, H., Shafqat, A., Daniyal, M., Bilal, M., & Anas, M. (2024). Internet of Things (IoT's) in Agriculture: Unexplored Opportunities in Cross–Platform. Spectrum of engineering sciences, 2(4), 57-84.

[42] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[43] A. Guerra-Manzanares, L. Julian Lechuga Lopez, M. Maniatakos, and F. E. Shamout, "ICLR 2023 Workshop onTrustworthy Machine Learning for Healthcare PRIVACY-PRESERVING MACHINE LEARNING FORHEALTHCARE: OPEN CHALLENGES AND FUTURE PER-SPECTIVES," pp. 1–13, 2023.

[44] S. R. Kurupathi and W. Maass, "Survey on Federated Learning Towards Privacy Preserving AI," pp. 235–253, 2020, doi:10.5121/csit.2020.101120.

[45] H. Chen, H. Wang, Q. Long, D. Jin, and Y. Li, "Advancements in Federated Learning: Models, Methods, and Privacy," J.ACM, vol. 1, no. 1, 2023, [Online]. Available: http://arxiv.org/abs/2302.11466.

[46] Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

[47] S. K. M. et al., "Privacy-Preserving in Blockchain-based Federated Learning Systems," pp. 1–44, 2024, [Online].Available: http://arxiv.org/abs/2401.03552.

[48] J. Zhang, H. Zhu, F. Wang, J. Zhao, Q. Xu, and H. Li, "Security and Privacy Threats to Federated Learning: Issues,Methods, and Challenges," Secur. Commun. Networks, vol. 2022, 2022, doi: 10.1155/2022/2886795.

[49] W. Si and C. Liu, "Privacy Preservation Learning with Deep Cooperative Method for Multimedia Data Analysis," Secur.Commun. Networks, vol. 2022, no. Iid, 2022, doi: 10.1155/2022/8449987.

[50] Q. Yang et al., "Federated Learning with Privacy-preserving and Model IP-right-protection," Mach. Intell. Res., vol. 20,no. 1, pp. 19–37, 2023, doi: 10.1007/s11633-022-1343-2.

[51] G. A. Kaissis, M. R. Makowski, D. Rückert, and R. F. Braren, "Secure, privacy-preserving and federated machine learningin medical imaging," Nat. Mach. Intell., vol. 2, no. 6, pp. 305–311, 2020, doi: 10.1038/s42256-020-0186-