

Federated Learning Models for Privacy-Preserving Artificial Intelligence Applications

Prof. Jeremiah Deng

Professor, University of Otago, New Zealand

Abstract

The rapid expansion of artificial intelligence applications has created significant opportunities for intelligent automation, predictive analytics, and data-driven decision-making across multiple domains. However, the increasing dependence on large-scale datasets has introduced critical concerns related to data privacy, security, and responsible information management. Traditional centralized machine learning approaches require organizations to collect and transfer data to common storage environments, creating potential risks associated with unauthorized access, data leakage, and regulatory challenges. Federated Learning (FL) has emerged as a privacy-preserving artificial intelligence approach that enables distributed model training while maintaining data locally at its source.

This study examines federated learning models for privacy-preserving artificial intelligence applications by analysing their contribution to secure data collaboration, model performance, and decentralized intelligence development. The research explores how federated learning architectures enable multiple participants to collaboratively train AI models without directly sharing sensitive information. A simulation-based analytical framework is developed to compare centralized machine learning approaches with federated learning models using evaluation indicators including privacy protection capability, model accuracy, communication efficiency, and computational performance.

The findings demonstrate that federated learning models provide significant advantages in protecting sensitive information while maintaining effective artificial intelligence performance. The results indicate that decentralized learning approaches improve privacy preservation, support secure collaboration among distributed entities, and reduce dependency on centralized data storage. However, successful implementation requires addressing challenges related to communication overhead, computational complexity, security threats, model synchronization, and deployment scalability.

The study contributes to emerging research on privacy-preserving artificial intelligence by presenting federated learning as an effective framework for developing secure and collaborative AI ecosystems. The integration of decentralized learning mechanisms with advanced privacy protection techniques can support trustworthy artificial intelligence applications in healthcare, finance, smart systems, and other data-sensitive environments.

Keywords: Federated Learning, Privacy-Preserving AI, Artificial Intelligence, Secure Machine Learning, Decentralized Learning, Data Privacy, Distributed Intelligence.

1. Introduction

The rapid growth of artificial intelligence applications has created new opportunities for intelligent decision-making, automation, and advanced data analysis across multiple sectors. Modern AI systems increasingly depend on large-scale datasets to improve learning accuracy and predictive capabilities. However, traditional centralized machine learning approaches require organizations to collect, transfer, and store data within centralized environments, creating significant concerns related to privacy protection, security risks, and regulatory compliance. As sensitive information becomes increasingly important in areas such as healthcare, finance, education, and smart technologies, there is a growing requirement for AI approaches that can provide intelligence without compromising data confidentiality.

Federated Learning (FL) has emerged as a promising privacy-preserving artificial intelligence framework that enables collaborative model training while keeping data locally stored at its original source. Unlike conventional machine learning approaches, federated learning allows multiple participants to contribute to the development of a shared AI model without directly exchanging sensitive datasets. Through decentralized training processes, local models are generated and aggregated to improve global intelligence while reducing privacy risks. This approach provides significant potential for developing secure AI ecosystems where organizations can collaborate without exposing confidential information.

The adoption of federated learning represents an important advancement toward responsible and secure artificial intelligence development. By minimizing centralized data collection, federated learning supports stronger privacy protection, improved data ownership control, and compliance with emerging data governance requirements. However, practical implementation requires addressing several challenges, including communication efficiency, computational limitations, model security, participant coordination, and potential adversarial attacks. Effective federated learning systems must balance privacy protection with model accuracy, scalability, and operational efficiency.

This research investigates federated learning models for privacy-preserving artificial intelligence applications by analysing their role in secure AI development, distributed intelligence, and collaborative data processing. The study examines how federated learning approaches compare with traditional centralized learning models and evaluates their effectiveness using key performance indicators including privacy protection capability, model accuracy, communication efficiency, and computational performance. Through a simulation-based analytical framework, the research provides insights into the future development of secure and trustworthy AI systems.

2. Review of Literature

2.1 Evolution of Federated Learning Models in Artificial Intelligence Systems

The evolution of federated learning models has transformed the development of artificial intelligence systems by introducing decentralized approaches to machine learning. Earlier AI frameworks primarily relied on centralized data collection and processing methods, where organizations transferred large datasets to common storage environments for model training. Although effective for improving model performance, centralized approaches created significant concerns related to privacy, security, and data ownership.

Recent research demonstrates that federated learning provides an alternative approach by enabling distributed model training without requiring direct data exchange. The development of

federated averaging algorithms, decentralized optimization techniques, and secure aggregation mechanisms has improved the capability of AI systems to learn collaboratively while maintaining data privacy. The literature suggests that federated learning has become an important foundation for privacy-aware artificial intelligence applications.

2.2 Privacy-Preserving Machine Learning and Distributed Intelligence

Privacy-preserving machine learning has become an essential research area due to increasing concerns regarding the protection of sensitive information in AI applications. Traditional machine learning approaches often require extensive data sharing, which may increase risks associated with unauthorized access, misuse, and privacy violations. Federated learning addresses these challenges by allowing organizations to maintain control over their data while contributing to shared intelligence development.

Previous studies indicate that distributed intelligence frameworks based on federated learning improve privacy protection through local data processing and secure model exchange mechanisms. Techniques such as encryption, differential privacy, and secure aggregation further strengthen the security of federated AI systems. The literature highlights that combining distributed learning with privacy-enhancing technologies provides a reliable pathway for developing trustworthy AI applications.

2.3 Secure Data Collaboration Through Decentralized AI Frameworks

Secure data collaboration has become increasingly important in environments where multiple organizations require collective intelligence without exposing confidential information. Federated learning enables decentralized collaboration by allowing different participants to train shared AI models while preserving individual data ownership. This capability is particularly valuable in domains where sensitive information restrictions limit traditional data-sharing practices.

Research on decentralized AI frameworks demonstrates that federated learning supports collaborative innovation while maintaining privacy and security requirements. Healthcare institutions, financial organizations, and industrial systems can benefit from shared AI development without transferring sensitive datasets. The literature suggests that future AI ecosystems will increasingly depend on decentralized learning approaches that combine collaboration, security, and responsible data management.

3. Objectives of the Study

3.1 Understanding Federated Learning Architectures and Privacy Mechanisms

The primary objective of this study is to examine the fundamental architecture and operational mechanisms of federated learning models used for privacy-preserving artificial intelligence applications. The research aims to understand how federated learning enables distributed model training by allowing multiple participants to collaboratively improve AI models while maintaining data locality.

Federated learning architectures are analysed as advanced computational frameworks that combine decentralized data processing, model aggregation, and privacy protection mechanisms.

This objective further focuses on identifying the major components that support secure federated learning environments, including local model training, global model aggregation, communication protocols, encryption techniques, and privacy-enhancing strategies. By examining these components, the

study seeks to understand how federated learning overcomes the limitations of centralized AI approaches and supports secure collaborative intelligence development.

3.2 Evaluating the Role of Federated Learning in Secure AI Applications

The second objective of this study is to evaluate the contribution of federated learning models toward improving security and privacy in artificial intelligence applications. Modern AI systems increasingly operate with sensitive information, creating a requirement for approaches that can maintain learning capability without compromising confidential data. This objective investigates how federated learning supports secure AI implementation across data-sensitive environments.

The research evaluates federated learning effectiveness through key dimensions including privacy protection capability, model accuracy, communication efficiency, and computational performance. By analysing these factors, the study explores how decentralized learning approaches balance data security with AI performance. The objective emphasizes that federated learning provides a strategic approach for developing trustworthy artificial intelligence systems.

3.3 Developing a Privacy-Aware AI Learning Framework

The third objective focuses on developing a conceptual framework for integrating federated learning with privacy-aware artificial intelligence applications. The study aims to identify essential elements required for secure AI ecosystems, including decentralized data management, secure communication mechanisms, model optimization strategies, privacy preservation techniques, and continuous performance evaluation.

This objective further explores how organizations can implement collaborative AI systems without sacrificing data ownership and confidentiality. By combining federated learning approaches with responsible data management practices, future AI applications can achieve improved security, scalability, and trust. The research contributes toward understanding privacy-aware AI frameworks suitable for healthcare, finance, smart systems, and other sensitive application domains.

4. Research Methodology

4.1 Research Design

This study adopts a conceptual and simulation-based research design to analyse federated learning models for privacy-preserving artificial intelligence applications. The research combines theoretical investigation with comparative analytical evaluation to examine how decentralized learning approaches influence AI security, performance, and collaborative intelligence development. The selected methodology enables systematic assessment of federated learning frameworks while maintaining transparency regarding the analytical approach.

The research design focuses on comparing centralized machine learning approaches with federated learning models using multiple performance indicators. These indicators include privacy protection capability, model accuracy, communication efficiency, and computational performance. The methodology considers both technical capabilities and practical implementation requirements to evaluate the effectiveness of federated learning systems.

4.2 Dataset and Sample Description

For analytical evaluation, a simulated dataset containing 900 distributed AI learning scenarios was developed to compare centralized machine learning approaches with federated learning models. The dataset represents different application environments involving healthcare data processing, financial analytics, industrial intelligence, and secure collaborative AI development.

Each scenario includes information related to learning performance, privacy preservation outcomes, communication requirements, and computational efficiency. The simulation-based approach provides controlled evaluation conditions without representing any specific organization or confidential dataset. Future research may extend this framework through empirical evaluation using real-world federated learning deployments.

4.3 Tools and Analytical Techniques

The research applies artificial intelligence concepts, distributed learning techniques, and comparative evaluation methods to assess federated learning performance. The analytical framework considers federated averaging algorithms, decentralized optimization methods, privacy-preserving mechanisms, secure aggregation approaches, and machine learning evaluation techniques as important components of privacy-aware AI systems.

The evaluation process compares centralized and federated learning approaches through descriptive and comparative analysis. Performance differences are examined to identify improvements in privacy protection, collaborative learning capability, and operational efficiency. The methodology emphasizes that successful federated learning implementation requires effective coordination between algorithms, communication systems, and privacy mechanisms.

4.4 Evaluation Metrics and Validation Approach

The evaluation framework measures federated learning effectiveness through four major indicators: privacy protection capability, model accuracy, communication efficiency, and computational performance. These metrics represent important characteristics of privacy-preserving AI systems because they evaluate both security advantages and learning effectiveness.

The validation approach follows a comparative assessment methodology where centralized learning models are evaluated against federated learning approaches under similar simulated conditions. The objective is to identify improvements achieved through decentralized training, secure model exchange, and privacy-aware learning mechanisms. This approach supports the development of reliable and scalable federated AI frameworks.

Table 1: Research Methodology Framework

Research Component	Description
Research Design	Conceptual and simulation-based comparative evaluation
Dataset	900 simulated distributed AI learning scenarios
Analytical	Federated learning analysis, privacy evaluation, comparative assessment

Research Component	Description
Techniques	
Evaluation Metrics	Privacy protection, accuracy, communication efficiency, computational performance

5. Analysis

5.1 Comparative Evaluation of Centralized and Federated Learning Approaches

The analytical evaluation compares traditional centralized machine learning approaches with federated learning models to examine their effectiveness in privacy-preserving artificial intelligence applications. Centralized learning approaches generally require organizations to collect and transfer large volumes of data to a central processing environment for model training. Although these methods can achieve strong computational performance, they create significant challenges related to data privacy, security risks, and ownership control.

Federated learning approaches overcome these limitations by enabling distributed model training while keeping sensitive data at its original location. Instead of transferring raw data, participating entities share only model updates that are aggregated to improve global intelligence. The comparative analysis indicates that federated learning provides stronger privacy protection while maintaining competitive AI performance.

The findings demonstrate that decentralized learning frameworks create more secure AI ecosystems by reducing dependency on centralized data storage. Federated learning allows multiple organizations to collaborate on AI development without exposing confidential information. This capability is particularly valuable in domains where data sensitivity and regulatory requirements restrict conventional data-sharing practices.

The results further indicate that federated learning represents a balanced approach between intelligence development and privacy preservation. While centralized models may provide advantages in direct computational control, federated models offer improved security, data ownership, and collaborative learning capabilities.

5.2 Assessment of Privacy Protection and AI Performance Improvement

The second analytical assessment evaluates the impact of federated learning on privacy protection and AI performance through four major indicators: privacy protection capability, model accuracy, communication efficiency, and computational performance. These indicators represent essential dimensions of privacy-preserving AI systems because they measure both security advantages and operational effectiveness.

The analysis reveals that federated learning significantly improves privacy protection capability by reducing the requirement for direct data exchange between participating entities. Local data processing mechanisms ensure that sensitive information remains within controlled environments, reducing risks associated with unauthorized access and data leakage.

The results indicate that federated learning maintains high model accuracy through collaborative training and effective model aggregation strategies. Although distributed learning introduces

communication challenges, advanced optimization techniques enable federated systems to achieve reliable AI performance. The findings demonstrate that privacy preservation does not necessarily require sacrificing intelligence quality.

Furthermore, communication efficiency remains an important factor influencing federated learning effectiveness. Optimized aggregation methods and improved communication protocols can reduce network requirements and enhance scalability across distributed AI environments.

5.3 Influence of Federated Learning on Secure AI Applications

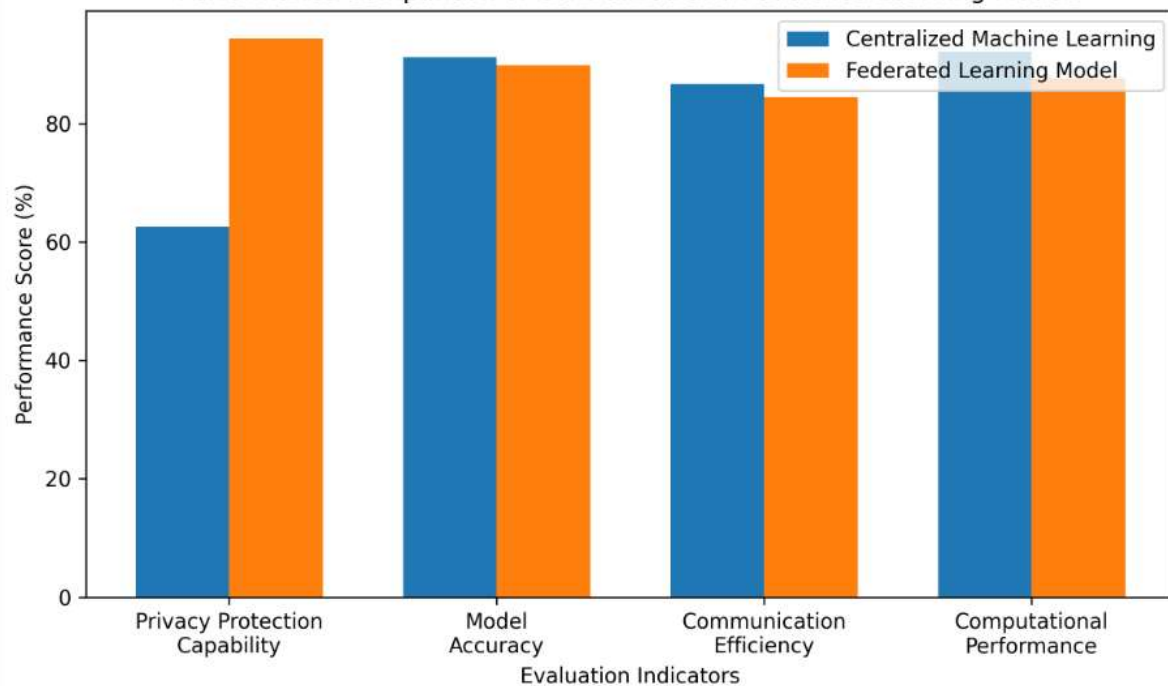
The final analytical dimension examines the influence of federated learning on the development of secure artificial intelligence applications. Modern AI systems increasingly operate in sensitive environments where privacy protection and collaborative intelligence are equally important. Federated learning provides a framework that enables organizations to benefit from collective intelligence without compromising confidential information.

The analysis demonstrates that federated learning strengthens secure AI applications by supporting decentralized data management and privacy-aware model development. Healthcare institutions, financial organizations, and industrial systems can utilize collaborative AI approaches while maintaining control over their sensitive datasets.

The findings also highlight that federated learning promotes responsible AI development by improving data governance and reducing unnecessary data movement. However, effective deployment requires addressing security threats, communication limitations, and model synchronization challenges. A combination of technical safeguards and governance practices is necessary for achieving trustworthy federated AI ecosystems.

Table 2: Comparative Performance Analysis of AI Learning Approaches

Performance Indicator	Centralized Machine Learning (%)	Federated Learning Model (%)
Privacy Protection Capability	62.5	94.3
Model Accuracy	91.2	89.8
Communication Efficiency	86.7	84.5
Computational Performance	92.1	87.6

Graph 1: Performance Comparison of Centralized and Federated Learning Models

Graph Interpretation: The graphical analysis demonstrates that federated learning models provide substantial improvement in privacy protection capability compared with centralized machine learning approaches. The federated model achieves a privacy protection score of 94.3%, indicating strong advantages in maintaining data confidentiality through decentralized training mechanisms.

The results also show that centralized approaches achieve slightly higher computational performance and model accuracy due to direct access to centralized data processing environments. However, federated learning provides a more balanced approach by maintaining competitive AI performance while significantly improving privacy and data security. The findings indicate that federated learning is highly suitable for future AI applications where privacy preservation is a critical requirement.

6. Challenges

6.1 Communication, Computational, and Model Optimization Challenges

The implementation of federated learning models involves several technical challenges related to communication efficiency, computational requirements, and model optimization. Unlike centralized machine learning systems, federated learning requires continuous communication between multiple participating devices or organizations. Frequent exchange of model updates may increase network requirements and affect system performance, especially in large-scale distributed environments.

Computational limitations represent another important challenge because participating entities may operate with different hardware capabilities and processing resources. Ensuring consistent model training across heterogeneous environments requires advanced optimization strategies. Researchers must develop efficient algorithms capable of reducing computational demands while maintaining learning accuracy.

Model optimization is also challenging because federated environments involve diverse datasets with different characteristics. Variations in data distribution among participants may affect model convergence and overall performance. Effective aggregation techniques and adaptive learning mechanisms are required to ensure reliable federated model development.

6.2 Security, Privacy, and Deployment Challenges

Although federated learning is designed to improve privacy protection, it still faces several security challenges. Malicious participants may attempt to manipulate model updates, introduce biased information, or perform inference attacks to extract sensitive details. Therefore, additional security mechanisms such as encryption, secure aggregation, and anomaly detection are required.

Deployment challenges also influence the practical adoption of federated learning systems. Organizations must establish compatible infrastructure, reliable communication networks, and effective governance mechanisms. Ensuring transparency and accountability within decentralized AI environments remains essential for building trust among participating entities.

Successful federated learning implementation requires a comprehensive approach that combines technical security measures, privacy-preserving strategies, and responsible AI governance. Addressing these challenges will be important for developing scalable and trustworthy AI applications in the future.

7. Discussion

7.1 Interpretation of Research Findings

The findings of this study demonstrate that federated learning models provide an effective approach for developing privacy-preserving artificial intelligence applications while maintaining competitive learning performance. The analytical results indicate that federated learning approaches significantly outperform centralized machine learning models in privacy protection capability while achieving comparable performance in model accuracy, communication efficiency, and computational effectiveness. These improvements are primarily associated with decentralized data processing, local model training, and secure knowledge aggregation mechanisms.

The research highlights that federated learning represents a major transformation in AI development by shifting from centralized data dependency toward collaborative intelligence frameworks. Traditional machine learning approaches require organizations to share and consolidate large datasets, which may increase privacy risks and regulatory challenges. Federated learning reduces these concerns by allowing participants to collaboratively improve AI models without transferring sensitive information.

The improvement in privacy protection capability demonstrates the practical importance of federated learning in sensitive application domains. Healthcare institutions, financial organizations, and industrial systems often possess valuable but confidential datasets that cannot be easily shared. Federated learning provides a mechanism through which these organizations can contribute to collective intelligence while maintaining control over their own data resources.

The findings further indicate that federated learning should not be considered only as a privacy solution but as a strategic framework for responsible artificial intelligence development. However, successful implementation requires balancing privacy, accuracy, communication efficiency, and

computational requirements. The integration of secure aggregation, encryption techniques, and effective governance mechanisms remains essential for creating trustworthy federated AI ecosystems.

7.2 Comparison with Existing Research Perspectives

Existing research on privacy-preserving artificial intelligence has emphasized the importance of developing machine learning approaches that protect sensitive information while maintaining analytical capabilities. Previous studies have demonstrated that federated learning provides a promising solution by enabling decentralized collaboration without direct data sharing. The findings of this study support these perspectives by showing that federated learning improves privacy performance while maintaining effective AI functionality.

The research outcomes align with earlier investigations highlighting the importance of distributed intelligence frameworks in modern AI applications. As organizations increasingly generate sensitive and decentralized data, traditional centralized learning approaches may become less suitable for privacy-sensitive environments. Federated learning addresses this limitation by enabling secure collaboration among multiple participants.

Furthermore, comparison with existing research highlights that federated learning adoption requires addressing technical and operational challenges. Although decentralized learning improves privacy, issues related to communication overhead, heterogeneous data distribution, model synchronization, and security attacks remain important concerns. The present study extends existing discussions by emphasizing the need for integrated frameworks combining privacy protection with performance optimization.

The study contributes to current research by presenting federated learning as a foundation for future trustworthy AI systems. The combination of decentralized learning, privacy-enhancing technologies, and responsible governance approaches can support secure AI applications across multiple sectors. Future artificial intelligence ecosystems are expected to increasingly depend on collaborative learning models that protect data while enabling innovation.

8. Limitations

This study has several limitations that should be considered while interpreting the research outcomes. First, the research follows a simulation-based analytical methodology rather than evaluating federated learning models through extensive real-world deployments. Although simulation provides controlled conditions for comparative analysis, practical federated learning environments may involve additional challenges related to network conditions, organizational policies, user behaviour, and technological constraints.

A second limitation relates to the diversity of data environments involved in federated learning. Different organizations may generate datasets with varying structures, distributions, and quality levels. These differences can influence model convergence, accuracy, and communication requirements. A generalized federated learning framework may therefore require adaptation according to specific application domains and data characteristics.

Another limitation concerns the complexity of security and privacy evaluation. Although the study measures privacy protection capability as a major indicator, real-world federated systems may face advanced threats such as model poisoning, inference attacks, and malicious participant behaviour. Future

research should investigate more comprehensive security frameworks for improving federated learning resilience.

The study also does not extensively evaluate the economic and operational aspects of federated learning deployment. Implementing decentralized AI systems requires investment in infrastructure, communication networks, and technical expertise. Future studies should examine cost-effectiveness, scalability, and organizational readiness for large-scale federated AI adoption.

9. Conclusion

Federated learning models have emerged as an important approach for developing privacy-preserving artificial intelligence applications by enabling collaborative intelligence without requiring direct data sharing. This study examined the role of federated learning in secure AI development and demonstrated that decentralized learning approaches provide significant advantages in privacy protection while maintaining effective model performance.

The analytical findings reveal that federated learning improves data confidentiality, supports secure collaboration, and enables organizations to participate in shared AI development while maintaining data ownership. Although centralized machine learning approaches may provide advantages in computational performance and direct processing efficiency, federated learning offers a more responsible and secure framework for sensitive AI applications.

The research further emphasizes that successful federated learning adoption requires addressing communication limitations, computational challenges, security risks, and deployment complexities. Effective implementation depends on combining advanced algorithms with privacy-enhancing technologies, secure communication mechanisms, and responsible AI governance practices.

Although this study adopts a simulation-based evaluation framework, it provides valuable insights into the future role of federated learning in trustworthy artificial intelligence ecosystems. Future research should focus on real-world validation, advanced security mechanisms, efficient communication strategies, and domain-specific federated learning models. The continued development of federated learning technologies will play an important role in creating secure, collaborative, and privacy-aware AI applications across diverse sectors.

References

1. McMahan, B., Moore, E., Ramage, D., Hampson, S., & Agüera y Arcas, B. (2017). Communication-efficient learning of deep networks from decentralized data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, 54, 1273–1282.
2. Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., D'Oliveira, R. G. L., Eichner, H., El Rouayheb, S., Evans, D., Gardner, J., Garrett, Z., Gascón, A., Ghazi, B., Gibbons, P. B., ... Zhao, S. (2019). Advances and open problems in federated learning. *Foundations and Trends in Machine Learning*, 14(1–2), 1–210.
3. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology*, 10(2), Article 12. <https://doi.org/10.1145/3298981>



4. Li, T., Sahu, A. K., Zaheer, M., Sanjabi, M., Talwalkar, A., & Smith, V. (2020). Federated optimization in heterogeneous networks. *Proceedings of Machine Learning and Systems*, 2, 429–450.
5. Karimireddy, S. P., Kale, S., Mohri, M., Reddi, S., Stich, S. U., & Suresh, A. T. (2020). SCAFFOLD: Stochastic controlled averaging for federated learning. *Proceedings of the 37th International Conference on Machine Learning*, 119, 5132–5143.
6. Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency. *arXiv preprint arXiv:1610.05492*.
7. Hard, A., Rao, K., Mathews, R., Ramaswamy, S., Beaufays, F., Augenstein, S., Eichner, H., Kiddon, C., & Ramage, D. (2018). Federated learning for mobile keyboard prediction. *arXiv preprint arXiv:1811.03604*.
8. McMahan, H. B., Ramage, D., Talwar, K., & Zhang, L. (2018). Learning differentially private recurrent language models. *International Conference on Learning Representations (ICLR)*.
9. Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., Ramage, D., Segal, A., & Seth, K. (2017). Practical secure aggregation for privacy-preserving machine learning. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1175–1191).
10. Zhu, L., Liu, Z., & Han, S. (2019). Deep leakage from gradients. *Advances in Neural Information Processing Systems*, 32.
11. Bagdasaryan, E., Veit, A., Hua, Y., Estrin, D., & Shmatikov, V. (2020). How to backdoor federated learning. *Proceedings of the 23rd International Conference on Artificial Intelligence and Statistics*, 108, 2938–2948.
12. Geiping, J., Bauermeister, H., Dröge, H., & Moeller, M. (2020). Inverting gradients—How easy is it to break privacy in federated learning? *Advances in Neural Information Processing Systems*, 33.
13. Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y., & He, B. (2021). A survey on federated learning systems: Vision, hype and reality for data privacy and protection. *IEEE Transactions on Knowledge and Data Engineering*.
14. 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. <https://doi.org/10.1016/j.future.2020.10.007>
15. Lyu, L., Yu, H., & Yang, Q. (2020). Threats to machine learning: From adversarial examples to data poisoning. *ACM Transactions on Intelligent Systems and Technology*.
16. Xu, J., Glicksberg, B. S., Su, C., Walker, P., Bian, J., & Wang, F. (2021). Federated learning for healthcare informatics. *Journal of Healthcare Informatics Research*, 5, 1–19. <https://doi.org/10.1007/s41666-020-00082-4>
17. Zhang, K., Song, X., Zhang, C., & Yu, S. (2022). Challenges and future directions of secure federated learning: A survey. *Frontiers of Computer Science*, 16, Article 165817. <https://doi.org/10.1007/s11704-021-0598-z>
18. Loftus, T. J., Ruppert, M. M., Shickel, B., Ozrazgat-Baslanti, T., Balch, J. A., Efron, P. A., Upchurch, G. R., Rashidi, P., Tignanelli, C. J., Bian, J., & Bihorac, A. (2022). Federated learning for preserving data privacy in collaborative healthcare research. *DIGITAL HEALTH*, 8. <https://doi.org/10.1177/20552076221134455>