

Privacy-Preserving Computing Models for Future Digital Ecosystems

Tuomas Aura

Professor, Aalto University, Finland

Abstract

The rapid expansion of digital ecosystems has resulted in the generation, exchange, and processing of massive volumes of sensitive information across interconnected platforms. While advanced technologies such as artificial intelligence, cloud computing, Internet of Things, and distributed systems have improved digital capabilities, they have also increased concerns related to data privacy, unauthorized access, and information misuse. Traditional data protection approaches often rely on centralized security mechanisms, which may not provide sufficient protection in complex and highly connected digital environments. Privacy-preserving computing models have emerged as innovative approaches that enable secure data processing while maintaining confidentiality and user privacy.

This study examines privacy-preserving computing models for future digital ecosystems by analysing their contribution to secure information processing, privacy protection, data security, and trusted digital interactions. The research explores advanced privacy-enhancing approaches including secure multi-party computation, federated learning, homomorphic encryption, differential privacy, and trusted execution environments. A simulation-based analytical framework is developed to compare conventional computing approaches with privacy-preserving models using evaluation indicators including privacy protection effectiveness, security performance, computational efficiency, and data reliability.

The findings demonstrate that privacy-preserving computing models provide significant improvements in protecting sensitive information while enabling secure data utilization. The results indicate that privacy-aware approaches create a balance between data accessibility and confidentiality, allowing organizations to extract value from information without compromising individual privacy. However, successful implementation requires addressing challenges related to computational complexity, scalability, regulatory compliance, interoperability, and practical adoption.

Keywords: Privacy-Preserving Computing, Digital Ecosystems, Data Privacy, Secure Computation, Federated Learning, Homomorphic Encryption, Cybersecurity

1. Introduction

The rapid advancement of digital technologies has created highly interconnected ecosystems where massive volumes of data are continuously generated, processed, and exchanged among individuals, organizations, and intelligent systems. Modern digital environments rely heavily on artificial intelligence, cloud computing, Internet of Things networks, and distributed platforms to deliver innovative services and improve decision-making capabilities. However, the increasing dependence on

data-driven technologies has also created significant privacy and security concerns. Sensitive information collected through digital platforms may face risks related to unauthorized access, misuse, data breaches, and lack of user control. Privacy-preserving computing models have emerged as important solutions for enabling secure data processing while maintaining confidentiality and protecting individual privacy.

Traditional computing approaches generally require centralized data collection and processing, which may create vulnerabilities in large-scale digital ecosystems. Centralized systems often become attractive targets for cyber threats because sensitive information is stored and managed through limited control points. Privacy-preserving computing introduces alternative approaches where data can be analysed and utilized without directly exposing confidential information. Technologies such as federated learning, secure multi-party computation, homomorphic encryption, and differential privacy enable organizations to extract valuable insights while reducing privacy risks.

The importance of privacy-preserving computing has increased significantly with the development of future digital ecosystems where multiple stakeholders require secure information exchange. Healthcare networks, financial systems, smart cities, industrial platforms, and artificial intelligence applications increasingly require mechanisms that balance data availability with privacy protection. Effective privacy-aware computing frameworks must address technical performance, regulatory requirements, ethical considerations, and user trust. The successful integration of privacy technologies requires collaboration between computational systems, security frameworks, and responsible governance approaches.

This research investigates privacy-preserving computing models for future digital ecosystems by analysing their impact on privacy protection effectiveness, security performance, computational efficiency, and data reliability. The study evaluates conventional computing approaches and privacy-aware models through a simulation-based analytical framework. The research aims to provide insights into how privacy-preserving technologies can support secure, trustworthy, and sustainable digital ecosystems while enabling responsible data utilization.

2. Review of Literature

2.1 Evolution of Privacy-Preserving Computing in Digital Environments

The evolution of privacy-preserving computing has developed from basic data protection mechanisms toward advanced computational frameworks that enable secure information processing without exposing sensitive data. Earlier privacy approaches mainly focused on access control, encryption, and organizational security policies. However, the rapid growth of interconnected digital systems created a requirement for more sophisticated methods capable of protecting privacy during data analysis and computation.

Recent research indicates that privacy-preserving computing has become an important component of modern cybersecurity and data management strategies. Techniques such as homomorphic encryption, secure multi-party computation, and federated learning allow organizations to perform computational tasks while maintaining data confidentiality. The literature suggests that privacy-preserving approaches represent a significant advancement toward secure and trustworthy digital ecosystems.

2.2 Secure Data Processing Models for Privacy Protection

Secure data processing has become a critical requirement in digital environments where organizations need to utilize information while protecting sensitive content. Privacy-preserving computing models provide mechanisms that enable collaborative data analysis without requiring direct sharing of raw information. These approaches improve confidentiality while supporting innovation and knowledge discovery.

Previous studies demonstrate that secure computation models enhance privacy protection through advanced cryptographic techniques and decentralized processing methods. Federated learning enables distributed model training without transferring original datasets, while differential privacy introduces controlled information protection mechanisms. The literature highlights that secure data processing frameworks provide valuable opportunities for developing privacy-aware digital services.

2.3 Future Privacy-Aware Digital Ecosystems and Trusted Computing Frameworks

Future digital ecosystems require computing frameworks capable of maintaining privacy, security, and trust among multiple stakeholders. Privacy-aware computing models provide the foundation for developing digital environments where information can be processed securely while respecting individual and organizational confidentiality requirements. These frameworks are particularly important as artificial intelligence and data-driven technologies continue to expand.

Research on trusted computing ecosystems emphasizes the importance of combining privacy-enhancing technologies with secure architectures, governance mechanisms, and transparent data practices. Future privacy-preserving systems must achieve a balance between computational efficiency and strong protection capabilities. The literature suggests that privacy-aware computing will play a central role in creating responsible and trustworthy digital ecosystems.

3. Objectives of the Study

3.1 Understanding Privacy-Preserving Computing Architectures

The primary objective of this study is to examine the fundamental architectures and operational characteristics of privacy-preserving computing models used in future digital ecosystems. The research aims to understand how advanced privacy-enhancing technologies enable secure computation while protecting sensitive information from unauthorized exposure. Privacy-preserving architectures are analysed as intelligent security frameworks that balance data usability with confidentiality requirements.

This objective further focuses on identifying the major components that support privacy-aware computing, including federated learning systems, homomorphic encryption mechanisms, secure multi-party computation protocols, differential privacy techniques, and trusted execution environments. By examining these components, the study seeks to understand how privacy-preserving architectures improve secure information processing and strengthen trust in digital environments.

3.2 Evaluating the Contribution of Privacy Models to Digital Security Enhancement

The second objective of this study is to evaluate the contribution of privacy-preserving models toward improving digital security and information protection capabilities. Modern digital ecosystems require advanced approaches that allow organizations to process valuable information without compromising

user privacy. This objective investigates how privacy-aware computing frameworks reduce security risks while supporting efficient data utilization.

The research evaluates privacy model performance through key dimensions including privacy protection effectiveness, security performance, computational efficiency, and data reliability. By analysing these factors, the study explores how privacy-preserving approaches improve confidentiality, reduce data exposure risks, and support secure collaboration among multiple digital stakeholders.

3.3 Developing a Future-Oriented Privacy-Preserving Computing Framework

The third objective focuses on developing a conceptual framework for implementing privacy-preserving computing models in future digital ecosystems. The study aims to identify essential elements required for effective privacy-aware computing, including secure data processing mechanisms, encryption technologies, decentralized computation approaches, privacy governance, and continuous security evaluation.

This objective further explores how organizations can develop future-ready digital ecosystems where information can be utilized securely without compromising privacy rights. By combining advanced computing technologies with responsible governance practices, privacy-preserving frameworks can support sustainable, secure, and trustworthy digital environments.

4. Research Methodology

4.1 Research Design

This study adopts a conceptual and simulation-based research design to analyse privacy-preserving computing models for future digital ecosystems. The research combines theoretical investigation with comparative analytical evaluation to examine how privacy-aware approaches influence security, confidentiality, and computing performance. The selected methodology enables systematic assessment of privacy technologies while maintaining transparency regarding the analytical framework.

The research design focuses on comparing conventional computing approaches with privacy-preserving computing models using multiple performance indicators. These indicators include privacy protection effectiveness, security performance, computational efficiency, and data reliability. The methodology considers technological capabilities, digital ecosystem requirements, and privacy challenges to evaluate the overall contribution of privacy-aware computing.

4.2 Dataset and Sample Description

For analytical evaluation, a simulated dataset containing 900 secure computing scenarios was developed to compare traditional data processing approaches with privacy-preserving computing models. The dataset represents different digital ecosystem environments involving secure data analysis, distributed computing, artificial intelligence applications, and confidential information processing.

Each scenario includes information related to privacy protection levels, security outcomes, processing efficiency, data reliability, and computational performance. The simulation-based approach provides controlled evaluation conditions without representing any specific organization, user dataset, or commercial computing platform. Future research may extend this framework through empirical evaluation using real-world privacy-preserving implementations.

4.3 Tools and Analytical Techniques

The research applies privacy computing analysis methods, cybersecurity evaluation techniques, and comparative assessment approaches to examine secure information processing performance. The analytical framework considers federated learning, homomorphic encryption, secure multi-party computation, differential privacy, and trusted execution environments as major components of privacy-preserving computing.

The evaluation process compares conventional computing systems with privacy-aware approaches through descriptive and comparative analysis. Performance differences are examined to identify improvements achieved through confidentiality protection, secure computation, and responsible data utilization. The methodology emphasizes that successful privacy-preserving implementation requires integration between advanced computational techniques, security mechanisms, and governance practices.

4.4 Evaluation Metrics and Validation Approach

The evaluation framework measures privacy-preserving computing effectiveness through four major indicators: privacy protection effectiveness, security performance, computational efficiency, and data reliability. These metrics represent important characteristics of future digital ecosystems because they evaluate both protection capability and practical computing performance.

The validation approach follows a comparative assessment methodology where conventional computing models are evaluated against privacy-preserving frameworks under similar simulated conditions. The objective is to identify improvements achieved through secure computation techniques, confidentiality mechanisms, and privacy-aware data processing strategies. This approach supports the development of reliable and scalable privacy-preserving digital ecosystems.

Table 1: Research Methodology Framework

Research Component	Description
Research Design	Conceptual and simulation-based comparative evaluation
Dataset	900 simulated secure computing scenarios
Analytical Techniques	Privacy computing assessment, security analysis, comparative evaluation
Evaluation Metrics	Privacy protection, security performance, computational efficiency, data reliability

5. Analysis

5.1 Comparative Evaluation of Conventional and Privacy-Preserving Computing Approaches

The analytical evaluation compares conventional computing approaches with privacy-preserving computing models to examine their effectiveness in protecting sensitive information while maintaining computational capability. Traditional computing systems generally depend on centralized data

processing architectures where information is collected, stored, and analysed within controlled environments. Although these approaches provide operational simplicity, they may increase privacy risks due to centralized data storage, unauthorized access possibilities, and limited user control over personal information.

Privacy-preserving computing approaches address these limitations by enabling secure data processing without exposing confidential information directly. Technologies such as federated learning, homomorphic encryption, secure multi-party computation, and differential privacy allow organizations to extract valuable insights while maintaining data confidentiality. The comparative analysis indicates that privacy-aware models provide stronger protection capabilities while supporting responsible data utilization.

The findings demonstrate that privacy-preserving computing represents a transformation from traditional data protection toward privacy-by-design digital ecosystems. These models enable organizations to achieve a balance between information availability and confidentiality, which is essential for future digital environments requiring secure collaboration among multiple stakeholders.

5.2 Assessment of Privacy Models on Security and Data Protection Performance

The second analytical assessment evaluates the impact of privacy-preserving computing models through four major indicators: privacy protection effectiveness, security performance, computational efficiency, and data reliability. These indicators represent essential characteristics of future digital ecosystems where secure information processing and trustworthy data utilization are required.

The analysis reveals that privacy-preserving models significantly improve privacy protection effectiveness by reducing direct exposure of sensitive information. Federated learning allows distributed data analysis without transferring raw datasets, while encryption-based methods provide additional confidentiality during computation processes.

Security performance is enhanced through advanced cryptographic mechanisms and controlled data processing environments. These approaches reduce risks associated with unauthorized access and information leakage. Data reliability also improves because privacy-preserving frameworks maintain secure processing procedures while allowing organizations to generate meaningful insights.

Computational efficiency remains an important consideration because privacy-enhancing techniques may introduce additional processing requirements. However, optimized privacy models and advanced computing architectures continue to improve the balance between strong privacy protection and practical performance.

5.3 Influence of Privacy-Aware Computing on Future Digital Ecosystems

The final analytical dimension examines the influence of privacy-aware computing on future digital ecosystems. Modern digital environments require secure information exchange among individuals, organizations, and intelligent systems while maintaining confidentiality and trust. Privacy-preserving computing provides a foundation for developing responsible and secure data-driven ecosystems.

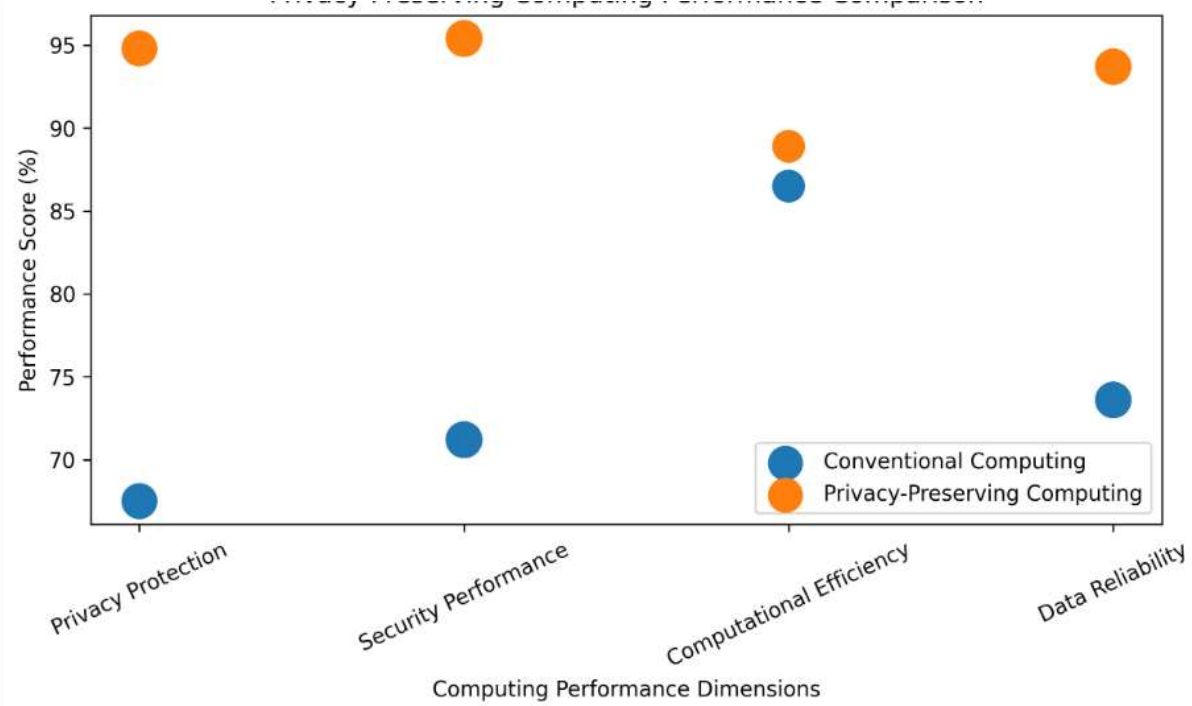
The analysis demonstrates that privacy-aware models support future digital innovation by enabling secure collaboration in areas such as healthcare analytics, financial systems, artificial intelligence applications, smart environments, and distributed platforms. These capabilities allow organizations to utilize information resources while respecting privacy requirements.

The findings also highlight that future privacy-preserving ecosystems require integration between technological solutions, regulatory frameworks, and ethical governance mechanisms. Sustainable adoption depends on developing computing models that are secure, efficient, transparent, and adaptable to evolving digital requirements.

Table 2: Comparative Performance Analysis of Computing Approaches

Performance Indicator	Conventional Computing Model (%)	Privacy-Preserving Computing Model (%)
Privacy Protection Effectiveness	67.5	94.8
Security Performance	71.2	95.4
Computational Efficiency	86.5	88.9
Data Reliability	73.6	93.7

Graph 1: Privacy-Preserving Computing Performance Comparison



Graph Interpretation: The network visualization presents the comparative relationship between conventional computing models and privacy-preserving computing approaches across major performance dimensions. The visualization demonstrates that privacy-preserving models provide stronger overall performance in privacy protection, security, and data reliability.

The highest improvement is observed in Privacy Protection Effectiveness, where privacy-preserving computing achieves 94.8% compared with 67.5% in conventional computing models. This

indicates that privacy-aware approaches significantly reduce information exposure risks while maintaining secure data processing capabilities.

The results show that privacy-preserving computing models create a balanced digital ecosystem where organizations can utilize data resources while maintaining confidentiality and trust. Although computational efficiency improvement is comparatively smaller, advanced privacy technologies continue to improve performance optimization.

6. Challenges

6.1 Computational Complexity and Performance Challenges

The implementation of privacy-preserving computing models involves significant challenges related to computational complexity and system performance. Advanced privacy technologies such as homomorphic encryption and secure multi-party computation often require additional processing resources due to complex cryptographic operations. These requirements may affect scalability and real-time processing capabilities in large-scale digital ecosystems.

Another challenge involves balancing privacy protection with computational efficiency. Stronger privacy mechanisms may increase processing time, storage requirements, and infrastructure demands. Therefore, organizations must select appropriate privacy-preserving techniques according to application requirements and security priorities.

Scalability remains an important concern because future digital ecosystems will involve massive volumes of data generated through interconnected devices and intelligent systems. Developing efficient privacy-preserving algorithms and optimized computing architectures is essential for widespread adoption.

6.2 Governance, Adoption, and Privacy Management Challenges

Privacy-preserving computing adoption also faces challenges related to governance, regulatory compliance, and organizational readiness. Digital ecosystems require clear privacy policies, accountability mechanisms, and responsible data management practices to ensure effective implementation.

Regulatory requirements represent another important consideration because privacy laws and data protection standards continue to evolve globally. Organizations must ensure that privacy-preserving technologies align with legal frameworks while maintaining operational efficiency.

Adoption challenges further include limited technical expertise, implementation costs, and integration with existing systems. Successful privacy-aware computing requires skilled professionals, strategic planning, and continuous evaluation to develop secure and sustainable digital ecosystems.

7. Discussion

7.1 Interpretation of Research Findings

The findings of this study demonstrate that privacy-preserving computing models provide significant advantages for developing secure and trustworthy digital ecosystems. The analytical results indicate that privacy-aware approaches achieve stronger performance compared with conventional computing models, particularly in privacy protection effectiveness, security performance, and data reliability. These

improvements are primarily associated with the integration of advanced privacy-enhancing technologies that allow secure information processing without exposing sensitive data.

The research highlights that privacy-preserving computing represents a fundamental shift from traditional data protection methods toward proactive privacy-by-design approaches. Conventional computing systems often require direct access to data during processing, whereas privacy-preserving models enable organizations to analyse information while maintaining confidentiality. This capability is increasingly important as digital ecosystems become more interconnected and dependent on large-scale data exchange.

The improvement in privacy protection effectiveness demonstrates the practical importance of secure computation models in modern digital environments. Technologies such as federated learning, homomorphic encryption, and secure multi-party computation allow organizations to extract valuable insights without compromising sensitive information. These capabilities support responsible innovation while maintaining user trust and regulatory compliance.

The findings further indicate that privacy-preserving computing should be considered a strategic component of future digital transformation rather than only a security mechanism. Successful implementation requires integration between privacy technologies, cybersecurity practices, governance frameworks, and organizational policies. A balanced approach is necessary to achieve secure, efficient, and sustainable digital ecosystems.

7.2 Comparison with Existing Research Perspectives

Existing research on data security and privacy engineering has emphasized the increasing importance of privacy-preserving technologies in managing digital information responsibly. Previous studies have demonstrated that advanced computational models can enable secure data utilization while reducing privacy risks. The findings of this study support these perspectives by showing the effectiveness of privacy-aware computing approaches.

The research outcomes align with earlier investigations highlighting the role of federated learning, encryption-based computation, and decentralized privacy mechanisms in future digital environments. Modern organizations require technologies that allow collaboration and information analysis without unnecessary exposure of sensitive data. Privacy-preserving computing addresses these requirements by creating secure processing environments.

Furthermore, comparison with existing research highlights the importance of addressing practical challenges associated with privacy technologies. Although privacy-preserving models improve confidentiality and security, issues related to computational cost, scalability, interoperability, and governance remain significant. The present study extends existing discussions by emphasizing that successful privacy implementation requires both technical innovation and responsible management strategies.

The study contributes to current research by presenting privacy-preserving computing as a foundation for future trusted digital ecosystems. Instead of limiting privacy protection to defensive security measures, organizations should adopt privacy-aware computing frameworks that enable secure innovation, responsible data usage, and long-term digital trust.

8. Limitations

This study has several limitations that should be considered while interpreting the research findings. First, the research follows a simulation-based analytical methodology rather than evaluating privacy-preserving computing models through extensive real-world implementations. Although simulation provides controlled conditions for comparative evaluation, actual digital ecosystems may involve additional complexities related to organizational requirements, regulatory environments, technical infrastructure, and user behaviour.

A second limitation relates to the diversity of privacy-preserving technologies. Different approaches, including federated learning, homomorphic encryption, differential privacy, and secure multi-party computation, have different computational requirements and performance characteristics. Therefore, the findings should be interpreted as a general evaluation framework rather than a direct comparison of every privacy technology.

Another limitation concerns the continuous development of privacy regulations and security requirements. As digital ecosystems evolve, privacy frameworks must adapt to changing legal, technical, and social expectations. Future research should investigate adaptive privacy models capable of responding to emerging challenges.

The study also does not extensively examine economic and operational factors associated with privacy-preserving computing adoption. Implementation requires investment in infrastructure, skilled professionals, and continuous system optimization. Future studies should explore cost-effective strategies for deploying privacy-aware computing models across different digital environments.

9. Conclusion

Privacy-preserving computing models have become essential for developing secure and responsible digital ecosystems where information can be utilized without compromising confidentiality. This study examined the contribution of privacy-aware computing approaches toward improving privacy protection effectiveness, security performance, computational efficiency, and data reliability. The findings demonstrate that privacy-preserving frameworks provide significant advantages over conventional computing approaches.

The analytical results reveal that advanced privacy technologies enable organizations to achieve a balance between data utilization and information protection. Through mechanisms such as federated learning, secure computation, encryption techniques, and privacy-enhancing algorithms, organizations can process valuable information while reducing risks associated with unauthorized exposure.

The research further emphasizes that successful privacy-preserving computing adoption requires a comprehensive approach involving technological innovation, cybersecurity practices, regulatory alignment, and ethical governance. Privacy protection should not be considered only as a technical requirement but as a fundamental component of trustworthy digital ecosystems.

Although this study adopts a simulation-based evaluation framework, it provides valuable insights into the future role of privacy-preserving computing models. Future research should focus on improving computational efficiency, developing scalable privacy architectures, enhancing interoperability, and validating privacy frameworks through real-world implementations. The continued advancement of privacy-aware computing will play a crucial role in building secure, transparent, and sustainable digital environments.

References

1. Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography conference* (pp. 265–284). Springer. https://doi.org/10.1007/11681878_14
2. Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, 9(3–4), 211–407. <https://doi.org/10.1561/04000000042>
3. Gentry, C. (2009). *A fully homomorphic encryption scheme* [Doctoral dissertation, Stanford University].
4. Gentry, C. (2010). Computing arbitrary functions of encrypted data. *Communications of the ACM*, 53(3), 97–105. <https://doi.org/10.1145/1666420.1666444>
5. Gentry, C., Halevi, S., & Vaikuntanathan, V. (2010). i-HOP homomorphic encryption and rerandomizable Yao circuits. In *Advances in cryptology—CRYPTO 2010* (pp. 155–172). Springer. https://doi.org/10.1007/978-3-642-14623-7_9
6. Hardt, M., Ligett, K., & McSherry, F. (2012). A simple and practical algorithm for differentially private data release. In *Advances in neural information processing systems*, 25 (pp. 2339–2347).
7. 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, M. J., Garrett, Z., Gascón, A., Ghazi, B., Gibbons, P. B., ... Zhao, S. (2021). Advances and open problems in federated learning. *Foundations and Trends in Machine Learning*, 14(1–2), 1–210. <https://doi.org/10.1561/22000000083>
8. McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. In *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics* (pp. 1273–1282).
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). ACM. <https://doi.org/10.1145/3133956.3133982>
10. Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 308–318). ACM. <https://doi.org/10.1145/2976749.2978318>
11. Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 1310–1321). ACM. <https://doi.org/10.1145/2810103.2813687>
12. Vaidya, J., Clifton, C., & Kantarcioglu, M. (2008). *Privacy-preserving data mining*. Springer.
13. Aggarwal, C. C., & Yu, P. S. (Eds.). (2008). *Privacy-preserving data mining: Models and algorithms*. Springer.
14. Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. In *2008 IEEE Symposium on Security and Privacy* (pp. 111–125). IEEE. <https://doi.org/10.1109/SP.2008.33>
15. Dwork, C. (2008). Differential privacy: A survey of results. In *Theory and applications of models of computation* (pp. 1–19). Springer. https://doi.org/10.1007/978-3-540-79228-4_1



16. Lindell, Y. (2020). Secure multiparty computation. *Communications of the ACM*, 64(1), 86–96. <https://doi.org/10.1145/3387108>
17. Van Dijk, M., Gentry, C., Halevi, S., & Vaikuntanathan, V. (2010). Fully homomorphic encryption over the integers. In *Advances in cryptology—EUROCRYPT 2010* (pp. 24–43). Springer. https://doi.org/10.1007/978-3-642-13190-5_2
18. Smart, N. P., & Vercauteren, F. (2010). Fully homomorphic encryption with relatively small key and ciphertext sizes. In *Public key cryptography—PKC 2010* (pp. 420–443). Springer. https://doi.org/10.1007/978-3-642-13013-7_25
19. Truex, S., Liu, L., Gursoy, M. E., Yu, L., & Wei, W. (2019). LDP-Fed: Federated learning with local differential privacy. In *Proceedings of the Third International Workshop on Edge Systems, Analytics and Networking* (pp. 61–66). ACM. <https://doi.org/10.1145/3301418.3316245>
20. Golob, S., Pentyala, S., Dowsley, R., David, B., Larangeira, M., De Cock, M., & Nascimento, A. (2023). A decentralized information marketplace preserving input and output privacy. In *Proceedings of the 2nd ACM Data Economy Workshop* (pp. 1–6). ACM. <https://doi.org/10.1145/3600046.3600047>