International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 05 – Sep-Oct 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

Privacy-Preserving Data Sharing in Internet-Based Information Systems

Ali Miri

Professor, Toronto Metropolitan University, Canada

Abstract

The rapid expansion of Internet-based information systems has significantly increased the volume of data exchanged among individuals, organizations, applications, cloud platforms, and interconnected digital services. Although data sharing enables collaboration, personalization, analytics, and efficient service delivery, it also introduces substantial privacy and security risks. Conventional data-sharing mechanisms frequently depend on centralized repositories and extensive access privileges, creating opportunities for unauthorized disclosure, excessive data collection, insider misuse, and secondary use of sensitive information. This paper examines privacy-preserving data sharing as an integrated approach for protecting sensitive information while maintaining the utility and interoperability of Internet-based information systems. The study develops a conceptual framework incorporating data minimization, encryption, access control, anonymization, pseudonymization, privacy-preserving computation, secure authentication, and continuous monitoring. Particular attention is given to privacy-enhancing technologies including differential privacy, secure multiparty computation, homomorphic encryption, federated learning, and blockchain-supported access management. The proposed framework organizes privacy protection across data collection, storage, processing, sharing, and governance stages.

The analysis demonstrates that privacy preservation cannot be achieved effectively through a single security mechanism because different information-sharing scenarios present different privacy requirements and threat conditions. Encryption can protect data during transmission and storage, whereas privacy-preserving computation can reduce exposure during collaborative processing. Differential privacy can reduce disclosure risks from statistical outputs, while decentralized and federated architectures can limit unnecessary data movement. The paper further examines application areas, technical challenges, and future research opportunities related to scalable privacy-preserving information sharing. Key challenges include balancing privacy with data utility, managing computational overhead, supporting interoperability, preventing inference attacks, and maintaining transparency in distributed environments. The study concludes that privacy-preserving data sharing requires a multilayered architecture that integrates technical controls with governance and risk-management mechanisms. Such architectures can enable Internet-based information systems to support secure and responsible data exchange while maintaining trust, usability, and analytical value.

Keywords: Privacy-Preserving Data Sharing, Internet-Based Information Systems, Data Privacy, Encryption, Differential Privacy, Federated Learning, Homomorphic Encryption, Access Control, Cybersecurity, Privacy-Enhancing Technologies.

1. Introduction

Internet-based information systems have transformed the way data is collected, processed, stored, and exchanged. Organizations increasingly depend on interconnected applications, cloud platforms, APIs, online services, and distributed databases to support operational and analytical activities. These systems facilitate rapid information exchange across organizational and geographic boundaries. However, increased connectivity also expands the number of locations where sensitive information can be exposed. Personal, financial, organizational, and behavioral data may pass through multiple systems, creating complex privacy risks that traditional centralized security mechanisms may not adequately address.

Data sharing is essential for many digital services because information often gains greater value when it can be accessed and analyzed by authorized participants. Healthcare collaboration, financial services, online education, e-government, research, and enterprise analytics all depend on controlled data exchange. Nevertheless, unrestricted data sharing can result in unauthorized access, data leakage, profiling, re-identification, and inappropriate secondary use. Consequently, information systems require mechanisms that preserve privacy while allowing legitimate users and applications to obtain sufficient information for their intended purposes.

Traditional security mechanisms such as passwords, firewalls, encryption, and access control remain important but do not fully address privacy risks. Encryption protects information from unauthorized observation while data remains encrypted, but information may need to be decrypted before conventional processing. Access control can restrict who accesses data but may not prevent legitimate recipients from misusing information. Similarly, anonymization can reduce direct identification risks but may remain vulnerable to linkage and inference attacks. These limitations have encouraged the development of privacy-enhancing technologies that protect information throughout different stages of its lifecycle.

Privacy-preserving data sharing therefore requires a multidimensional approach that considers data minimization, identity protection, secure computation, decentralized processing, and governance. Technologies such as differential privacy can limit information leakage from analytical outputs, while homomorphic encryption enables computations over encrypted information. Secure multiparty computation allows multiple parties to jointly compute results without directly revealing their private inputs. Federated learning can support collaborative model development while reducing the need to centralize raw data.

This paper examines the architecture and analytical foundations of privacy-preserving data sharing in Internet-based information systems. The study develops a conceptual framework integrating privacy-enhancing technologies with access management, encryption, monitoring, and governance. It analyzes major implementation components, application areas, technical challenges, and future research opportunities. The objective is to demonstrate how integrated privacy mechanisms can enable responsible information exchange while maintaining data utility, system interoperability, and user trust.

2. Objectives

2.1 Primary Objective

The primary objective of this study is to examine a comprehensive privacy-preserving framework for secure data sharing in Internet-based information systems. The framework focuses on protecting

Volume 01, Issue 05 – Sep-Oct 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

sensitive information throughout collection, transmission, storage, processing, and sharing while maintaining sufficient data utility for authorized applications and users.

2.2 Development of a Privacy-Preserving Architecture

The first objective is to develop a conceptual architecture integrating encryption, access control, anonymization, pseudonymization, privacy-preserving computation, and monitoring mechanisms. The architecture is designed to distribute privacy protection across multiple system layers rather than relying on a single security mechanism.

2.3 Evaluation of Privacy-Enhancing Technologies

The second objective is to examine major privacy-enhancing technologies used for secure information sharing. The analysis considers differential privacy, homomorphic encryption, secure multiparty computation, federated learning, and decentralized access mechanisms in relation to their privacy benefits, computational requirements, and practical applications.

2.4 Identification of Implementation Challenges

The third objective is to identify challenges associated with privacy-preserving data sharing, including data utility, computational overhead, interoperability, inference attacks, scalability, governance, and transparency. Understanding these challenges is necessary for developing practical and sustainable privacy-aware information systems.

3. Review of Literature

3.1 Foundations of Privacy-Preserving Data Sharing

Privacy-preserving data sharing seeks to enable legitimate information exchange while minimizing the possibility that sensitive information can be disclosed or misused. Early approaches primarily relied on anonymization, aggregation, and access control. Techniques such as k-anonymity, l-diversity, and t-closeness attempted to reduce the possibility of identifying individuals from shared datasets. However, research demonstrated that background knowledge and auxiliary datasets could enable re-identification, motivating stronger formal privacy models.

Differential privacy introduced a mathematical framework for limiting the influence of an individual record on analytical outputs. Rather than attempting to eliminate identifying information completely, differential privacy controls the amount of information that an output can reveal about a particular participant. This approach has become influential in privacy-preserving statistics and machine learning. However, privacy protection must still be balanced against analytical accuracy, particularly when strong privacy parameters are applied to complex or high-dimensional datasets.

3.2 Cryptographic Privacy-Enhancing Technologies

Cryptographic approaches provide mechanisms for protecting information during collaborative processing and exchange. Homomorphic encryption allows specific mathematical operations to be performed on encrypted data, enabling selected computations without directly exposing plaintext information. Secure multiparty computation allows multiple participants to jointly calculate functions while keeping their individual inputs private.

Volume 01, Issue 05 – Sep-Oct 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

These technologies are particularly valuable when participants do not fully trust one another but require collaborative analytics. However, cryptographic privacy mechanisms can introduce substantial computational and communication overhead. Fully homomorphic encryption, for example, may require significantly greater computational resources than conventional processing. Secure multiparty computation can similarly become complex when large numbers of participants or repeated computations are involved. Practical deployment therefore requires careful consideration of performance, scalability, computational infrastructure, and application requirements.

3.3 Distributed and Federated Privacy Models

Distributed privacy-preserving architectures attempt to reduce the need to centralize sensitive information. Federated learning is a prominent example in which machine learning models are trained across multiple data-holding entities while raw datasets remain within local environments. Model updates can be aggregated to produce a shared model. This approach can reduce direct data movement, although model updates may still reveal information if appropriate protection mechanisms are not applied.

Blockchain and decentralized identity technologies have also been explored for privacy-aware information sharing. Distributed ledgers can provide tamper-resistant records of access and transactions, while decentralized identity mechanisms can reduce dependence on centralized identity providers. However, transparency and immutability can introduce privacy concerns when sensitive information or identifying metadata is recorded permanently. Therefore, decentralized systems must be carefully designed to avoid creating new privacy risks.

4. Methodology

4.1 Research Design

This study uses a conceptual and analytical research design to examine privacy-preserving data sharing in Internet-based information systems. The methodology considers privacy as a lifecycle requirement extending from data collection to final disposal. The proposed framework organizes privacy mechanisms according to data sensitivity, processing requirements, participant trust, and potential disclosure risks. Rather than presenting fabricated experimental results, the study synthesizes technical principles into a structured architecture suitable for future empirical evaluation.

The research approach evaluates privacy-preserving mechanisms according to several dimensions, including confidentiality, disclosure resistance, data utility, computational efficiency, scalability, interoperability, and governance. These dimensions provide a basis for comparing different approaches and determining where particular technologies are most appropriate. The methodology also recognizes that privacy requirements differ across applications, making adaptive and context-aware protection essential for Internet-based information systems.

4.2 Privacy-Preserving Data Sharing Model

The proposed model begins with data classification and sensitivity assessment. Information is categorized according to its privacy requirements and intended use. Data minimization mechanisms then determine which attributes are necessary for a particular transaction or analytical task. Encryption protects information during storage and transmission, while access control restricts availability to

authorized entities. Depending on the processing requirement, anonymization, differential privacy, or cryptographic computation can be applied.

The sharing layer provides controlled interaction among users, applications, organizations, and distributed services. Authentication verifies participating entities, authorization determines permitted operations, and monitoring records relevant security events. Privacy policies define acceptable data uses and retention requirements. A risk-assessment layer continuously evaluates potential disclosure conditions and can modify access privileges or protection mechanisms when threats change.

4.3 Key Methodological Components

The major methodological components of the proposed framework include:

- **Data Classification:** Identification of sensitivity and privacy requirements.
- **Data Minimization:** Limitation of data collection and sharing to necessary attributes.
- **Encryption:** Protection of data during storage and transmission.
- **Access Control:** Restriction of information according to roles, attributes, or policies.
- **Anonymization/Pseudonymization:** Reduction of direct identification risks.
- **Differential Privacy:** Limitation of privacy leakage from analytical outputs.
- **Secure Computation:** Processing sensitive data while minimizing plaintext exposure.
- **Federated Processing:** Keeping raw data within participating local environments.
- **Monitoring:** Detection and recording of unusual access or sharing behavior.
- **Governance:** Enforcement of privacy policies, accountability, retention, and compliance requirements.

The integrated methodology emphasizes layered privacy protection because different mechanisms address different threat conditions. Encryption protects data confidentiality, whereas differential privacy focuses on information leakage from outputs. Secure computation protects data during collaborative processing, while access control regulates who can perform particular operations. Combining these mechanisms enables information systems to maintain privacy across multiple stages of data sharing.

5. Analysis

5.1 Architecture of Privacy-Preserving Data Sharing

A privacy-preserving Internet-based information system requires coordinated protection across data, application, communication, identity, and governance layers. The architecture should prevent unnecessary exposure while allowing legitimate data consumers to obtain required information. The proposed model combines preventive, computational, and monitoring mechanisms to create multiple privacy barriers.

Table 1: Core Components of a Privacy-Preserving Data Sharing Architecture

Component	Privacy Function	Representative Techniques
Data Classification	Determines protection requirements	Sensitivity labeling, risk assessment
Data Minimization	Reduces unnecessary exposure	Attribute reduction, purpose

Volume 01, Issue 05 – Sep-Oct 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

Component	Privacy Function	Representative Techniques
		limitation
Identity Protection	Limits direct identification	Pseudonyms, decentralized identity
Encryption	Protects stored/transmitted information	Symmetric and asymmetric encryption
Access Control	Restricts authorized operations	RBAC, ABAC, policy-based access
Privacy-Preserving Computation	Protects data during processing	Homomorphic encryption, MPC
Statistical Privacy	Limits output disclosure	Differential privacy
Distributed Processing	Reduces centralized data exposure	Federated learning
Monitoring	Detects privacy-related anomalies	Audit logs, behavioral monitoring
Governance	Ensures accountable data use	Policies, retention, compliance controls

Interpretation: Illustrates that privacy preservation is a multilayered process rather than a single technical function. Data minimization reduces the amount of information requiring protection, encryption secures information against unauthorized observation, and access control limits legitimate access. Privacy-preserving computation and statistical privacy address risks that occur during processing and information release. Monitoring and governance provide continuous oversight, enabling organizations to maintain accountability and detect inappropriate data-sharing behavior.

5.2 Privacy-Enhancing Technologies and Applications

Different privacy-enhancing technologies address different information-sharing requirements. Differential privacy is particularly suitable for statistical analysis, while homomorphic encryption can support selected computations over encrypted datasets. Secure multiparty computation is useful when multiple parties need collaborative results without revealing private inputs. Federated learning is appropriate when distributed participants need to develop shared models while retaining local datasets.

International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 05 – Sep-Oct 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

Table 2: Privacy-Enhancing Technologies for Internet-Based Information Sharing

Technology	Primary Privacy Mechanism	Suitable Application
Differential Privacy	Limits information leakage from outputs	Statistical analytics
Homomorphic Encryption	Enables computation on encrypted data	Secure cloud analytics
Secure Multiparty Computation	Joint computation without direct input disclosure	Collaborative analytics
Federated Learning	Keeps raw data distributed	Collaborative machine learning
Anonymization	Removes or transforms identifiers	Dataset sharing
Pseudonymization	Replaces direct identifiers	Identity-aware data exchange
Attribute-Based Access Control	Restricts access using policies	Enterprise information systems
Blockchain-Based Access Management	Provides distributed transaction records	Decentralized data sharing
Trusted Execution Environments	Protects processing environments	Secure cloud computation

Interpretation: Shows that privacy-enhancing technologies have different strengths and limitations. No single mechanism is sufficient for every Internet-based information-sharing scenario. For example, differential privacy can protect analytical outputs but does not directly secure stored data. Encryption provides strong confidentiality but may not address inference from legitimate outputs. Consequently, practical systems should select and combine technologies according to data sensitivity, computation requirements, trust relationships, and privacy risks.

5.3 Factors Affecting Privacy and Data Utility

The effectiveness of privacy-preserving data sharing depends on the relationship between privacy protection and data utility. Strong privacy mechanisms may reduce the precision or usefulness of shared information, while weak protection can increase disclosure risks. Differential privacy illustrates this trade-off because stronger privacy guarantees may require greater perturbation of analytical outputs.

Similarly, encryption-based computation can preserve data confidentiality but may introduce processing delays. System architecture also affects privacy performance. Centralized models can simplify management but create attractive targets for attackers, whereas distributed approaches can reduce centralized exposure but introduce coordination and consistency challenges.

Volume 01, Issue 05 – Sep-Oct 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

Interoperability is another important factor because Internet-based information systems commonly integrate heterogeneous platforms, APIs, databases, and identity mechanisms. Privacy policies must therefore operate consistently across technological boundaries.

6. Discussion

6.1 Privacy-Preserving Data Sharing as a Multilayered Strategy

Privacy protection should be treated as a system-wide architectural principle rather than an isolated security feature. Data minimization, encryption, access control, identity protection, secure computation, and monitoring address different stages of the information lifecycle. A multilayered strategy reduces dependence on any individual mechanism and provides greater resilience against different forms of privacy attacks.

Such an approach is particularly relevant to Internet-based information systems because data frequently crosses organizational and technical boundaries. A secure sharing framework must therefore maintain protection even when information moves between cloud services, enterprise applications, external partners, and distributed computing environments. Policy-driven architectures can help organizations apply consistent privacy requirements across these environments.

6.2 Balancing Privacy and Data Utility

A fundamental challenge in privacy-preserving systems is maintaining useful information while limiting disclosure. Excessive anonymization or perturbation can reduce the analytical value of datasets, while insufficient protection may expose sensitive information. Privacy-preserving mechanisms must therefore be selected according to the intended analytical purpose and acceptable risk level.

Adaptive privacy models can provide a more balanced solution. Instead of applying identical protection to all information, systems can dynamically adjust mechanisms based on data sensitivity, user authorization, analytical requirements, and threat conditions. Such approaches can support efficient information sharing while maintaining appropriate privacy guarantees. Machine learning may further assist in estimating privacy risk and selecting suitable protection levels.

6.3 Trust, Governance, and Accountability

Technical mechanisms alone cannot guarantee responsible data sharing. Organizations also require privacy governance, clear data-use policies, accountability structures, retention controls, and auditing procedures. Users and participating organizations need confidence that information will be used only for authorized purposes. Transparent privacy policies can improve trust and clarify how data is collected, processed, and shared.

Accountability mechanisms are especially important in distributed systems involving multiple data controllers and processors. Audit logs, policy enforcement, and continuous monitoring can help identify inappropriate access and support investigations. Future privacy-aware systems should therefore integrate technical protection with governance mechanisms to create comprehensive accountability throughout the information lifecycle.

7. Challenges

Privacy-preserving data sharing faces a major challenge in balancing privacy guarantees with computational efficiency and data utility. Advanced technologies such as homomorphic encryption and secure multiparty computation can provide strong privacy protection but may require substantial processing and communication resources. Organizations with large datasets or real-time applications may therefore experience performance limitations. Designing lightweight privacy mechanisms that maintain strong protection remains an important technical challenge.

Another challenge involves inference and re-identification attacks. Removing direct identifiers does not necessarily guarantee privacy because attackers can combine available information with external datasets to infer sensitive characteristics. Behavioral and transactional data can also reveal information indirectly. Privacy-preserving systems must therefore consider linkage attacks, membership inference, attribute inference, and other forms of indirect disclosure when evaluating protection effectiveness.

Interoperability and governance further complicate implementation. Internet-based systems commonly use different databases, APIs, identity frameworks, security protocols, and privacy policies. Ensuring consistent privacy protection across these heterogeneous environments can be difficult. In addition, distributed data-sharing arrangements require clear responsibility for data ownership, processing, retention, and incident response. Effective privacy preservation therefore requires both technical integration and organizational governance.

8. Future Research

Future research should investigate intelligent privacy-preserving architectures capable of dynamically selecting protection mechanisms according to context. Machine learning can support privacy-risk prediction, adaptive access control, and automated identification of sensitive data. Such systems could evaluate data sensitivity, user trust, processing purpose, and threat conditions before determining whether encryption, differential privacy, federated processing, or another mechanism should be applied.

Another promising direction is the integration of privacy-enhancing technologies with distributed artificial intelligence. Federated learning combined with differential privacy and secure aggregation can provide stronger protection for collaborative machine learning. Research should also examine efficient cryptographic computation for resource-constrained environments. Lightweight protocols will be particularly important for large-scale Internet applications, edge computing, and systems requiring near-real-time information processing.

Future research should additionally focus on explainable privacy management and interoperable privacy policies. Users and organizations need understandable explanations of how privacy decisions are generated and why particular information-sharing restrictions are applied. Standardized policy frameworks could facilitate consistent privacy management across cloud platforms, APIs, enterprise systems, and distributed services. Combining explainability, automation, interoperability, and strong technical protection could establish more trustworthy foundations for next-generation Internet-based information systems.

9. Conclusion

Privacy-preserving data sharing has become an essential requirement as Internet-based information systems increasingly connect users, organizations, applications, cloud platforms, and distributed services. Although data sharing provides substantial operational and analytical benefits, uncontrolled information exchange can create risks involving unauthorized access, re-identification, inference, profiling, and secondary use. This study examined a multilayered conceptual framework that integrates data minimization, encryption, access control, identity protection, privacy-preserving computation, distributed processing, monitoring, and governance to address these risks throughout the data lifecycle. The analysis demonstrates that privacy-enhancing technologies provide complementary rather than interchangeable capabilities.

Differential privacy can reduce disclosure from analytical outputs, homomorphic encryption can support computation over encrypted information, secure multiparty computation can facilitate collaborative processing, and federated learning can reduce the need to centralize raw datasets. However, each approach introduces different trade-offs involving computational cost, scalability, interoperability, and data utility. Therefore, privacy-preserving information systems should select and combine technologies according to application requirements, data sensitivity, trust relationships, and threat conditions.

Future Internet-based information systems should move toward adaptive, decentralized, and policy-driven privacy architectures. Intelligent risk assessment, privacy-preserving machine learning, secure aggregation, efficient cryptographic protocols, explainable privacy management, and interoperable governance mechanisms can strengthen responsible data sharing. Privacy should ultimately be treated as an architectural and operational requirement rather than an additional security feature applied after system development. By integrating privacy-enhancing technologies with access management, continuous monitoring, and accountable governance, organizations can support secure information exchange while preserving user trust, system utility, and long-term sustainability.

References

1. Conde, D. J. S., Kämpf, N. L., Rößler-von Saß, D., Schurig, T., & Kliewer, N. (2024). Privacy-preserving data sharing: A systematic review and future research directions. *European Conference on Information Systems (ECIS)*.
2. Tang, Y. J., & Chi, P. W. (2024). Theseus data synthesis approach: A privacy-preserving online data sharing service. *IEEE Access, 12*, 141130–141143. https://doi.org/10.1109/ACCESS.2024.3467373
3. Liu, L., & Han, M. (2024). Data sharing and exchanging with incentive and optimization: A survey. *Discover Data, 2*, 2.
4. Li, B., Yang, J., Wang, Y., Huang, X., Ren, J., & Wang, L. (2023). A blockchain-based privacy-preserving data sharing scheme with security-enhanced access control. *2023 International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. https://doi.org/10.1109/CSCWD57460.2023.10152751
5. Jiang, S., Cao, J., Wu, H., Chen, K., & Liu, X. (2023). Privacy-preserving and efficient data sharing for blockchain-based intelligent transportation systems. *Information Sciences, 635*, 72–85. https://doi.org/10.1016/j.ins.2023.03.121

6. PD2S: A privacy-preserving differentiated data sharing scheme based on blockchain and federated learning. (2023). *IEEE Internet of Things Journal, 10*(24), 21489–21501. https://doi.org/10.1109/JIOT.2023.3295763
7. *PRIDN: A privacy preserving data sharing on Named Data Networking*. (2024). *IEEE Transactions on Information Forensics and Security, 19*, 677–692. https://doi.org/10.1109/TIFS.2023.3327660
8. Ma, X., Wang, C., & Chen, X. (2021). Trusted data sharing with flexible access control based on blockchain. *Computer Standards & Interfaces, 77*, 103543. https://doi.org/10.1016/j.csi.2021.103543
9. Piao, C., Hao, Y., Yan, J., & Jiang, X. (2021). Privacy preserving in blockchain-based government data sharing: A Service-On-Chain (SOC) approach. *Information Processing & Management, 58*(5), 102651. https://doi.org/10.1016/j.ipm.2021.102651
10. *Privacy-preserving data sharing scheme with FL via MPC in financial permissioned blockchain*. (2021). *IEEE International Conference on Communications (ICC)*. https://doi.org/10.1109/ICC42927.2021.9500868
11. Huang, H., Zhu, P., & Xiao, F. (2020). A blockchain-based scheme for privacy-preserving and secure sharing of medical data. *Computers & Security, 99*, 102010. https://doi.org/10.1016/j.cose.2020.102010
12. Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., & Ni, W. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers & Security, 88*, 101653. https://doi.org/10.1016/j.cose.2019.101653
13. Puri, V., Sachdeva, S., & Kaur, P. (2019). Privacy preserving publication of relational and transaction data: Survey on the anonymization of patient data. *Computer Science Review, 32*, 45–61. https://doi.org/10.1016/j.cosrev.2019.02.001
14. Fung, B. C. M., Wang, K., Chen, R., & Yu, P. S. (2010). Privacy-preserving data publishing: A survey of recent developments. *ACM Computing Surveys, 42*(4), Article 14. https://doi.org/10.1145/1749603.1749605
15. Chen, B. C., Kifer, D., LeFevre, K., & Machanavajjhala, A. (2009). Privacy-preserving data publishing. *Foundations and Trends in Databases, 2*(1–2), 1–167. https://doi.org/10.1561/1900000008
16. Aggarwal, C. C., & Yu, P. S. (2008). A general survey of privacy-preserving data mining models and algorithms. In *Privacy-Preserving Data Mining: Models and Algorithms*, 11–52. Springer.
17. Machanavajjhala, A., Kifer, D., Gehrke, J., & Venkitasubramaniam, M. (2007). ℓ-diversity: Privacy beyond k-anonymity. *ACM Transactions on Knowledge Discovery from Data, 1*(1), Article 1217302. https://doi.org/10.1145/1217299.1217302
18. Li, N., Li, T., & Venkatasubramanian, S. (2007). t-Closeness: Privacy beyond k-anonymity and l-diversity. *2007 IEEE International Conference on Data Engineering*, 106–115. https://doi.org/10.1109/ICDE.2007.367856
19. Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography Conference (TCC 2006)*, 265–284. Springer. https://doi.org/10.1007/11681878_14