Ethics and Fair Use Framework for Privacy Preserving Data Sharing

Bita Afsharinia, Anjula Gurtoo, Jyotirmoy Dutta, Minnu Malieckal,

Abstract

Background: The rapid growth in data generation across sectors has intensified the need for privacy-preserving measures that also adhere to ethical standards. However, existing frameworks often fall short in integrating these two aspects effectively, particularly in the context of emerging technologies.

Objective: the study aims to critically evaluate current privacy-preserving technologies and ethical frameworks in data sharing, identifying gaps and proposing a comprehensive, integrated ethical framework.

Methodology: The study utilizes a multi-faceted methodology, starting with detailed literature review focusing on anonymization techniques and ethical principles, including GDPR, DPDPA, and advanced methods including homomorphic encryption and differential privacy. This was followed by a content analysis to systematically analyse data, uncovering recurring themes, gaps, and opportunities.

Results: The literature review highlights significant limitations in current frameworks, especially their adaptability to new technologies and the integration of ethical considerations with technical solutions. Content analysis facilitated the development of a novel framework that bridges these gaps. The proposed framework emphasizes the incorporation of ethical principles such as transparency, consent, and fairness into privacy-preserving technologies, ensuring that data-sharing practices are both secure and ethically sound.

Conclusion: The study underscores the need for a more integrated and dynamic framework that balances privacy protection with data utility while embedding ethical principles into technical solutions. Future research should focus on real-world applications of this framework in complex data-sharing environments to assess its practicality and effectiveness in addressing privacy and ethical challenges. This study contributes to the ongoing evaluation of privacy-preserving frameworks that are adaptable and aligned with contemporary ethical standards, ensuring secure and equitable data-sharing practices.

Keywords: Privacy-preserving technologies; Ethical frameworks; Data sharing; Anonymization, Fairness

Ethics and Fair Use Framework for Privacy Preserving Data Sharing

1. Introduction

Data privacy has become increasingly critical in the digital era, as the surge in data generation across various sectors necessitates stringent measures to safeguard sensitive information. Privacy preservation involves protecting confidential data from unauthorized access (Watson & Jones, 2013), ensuring that machine learning models do not inadvertently expose personal details during training or inference (Rasheed et al., 2022). Techniques such as homomorphic encryption (Jiang et al., 2021), differential privacy (Xu et al., 2023), and federated learning (Yazici et al., 2023), are pivotal in maintain privacy in AI systems and securing data throughout its lifecycle. Recent studies highlight the evolving challenges in privacy-preserving technologies, including the need for dynamic privacy measures that adapt to new threats and technologies (Habbal et al., 2024; Vegesna, 2023).

Ethical considerations in data privacy are essential for upholding individual rights and ensuring control over personal information (Wanbil Lee et al., 2016). Regulations such as the General Data Protection Regulation (GDPR) in the European Union and the Digital Personal Data Protection Act 2023 (DPDPA) in India establish ethical standards for data collection and processing (Aslam & Shyam Kishore, 2024), addressing the need for privacy-preserving measures to mitigate risks and protect public trust (Phillips, 2018). These guidelines are vital for legal compliance and maintaining ethical standards in data management (Groves & Harris-Kojetin, 2017). Further, literature emphasizes the importance of harmonizing global and local regulations to address cross-border data privacy issues and ensure comprehensive protection (Robinson et al., 2015).

Despite advancements in privacy-preserving technologies, significant gaps remain in current frameworks. Techniques aimed at protecting data and context privacy, such as such as k-anonymity (Sweeney, 2002) and l-diversity (Machanavajjhala et al., 2007), differential privacy (Dwork, 2006), face challenges in setting appropriate thresholds and balancing privacy with data utility. Moreover, these technologies often overlook broader ethical issues, such as fairness, transparency, and stakeholder collaboration. This highlights a crucial need for a more comprehensive and context-specific ethical framework that addresses these concerns. Recent critiques argue that current privacy models are insufficient in addressing the ethical implications of big data and AI, calling for frameworks that incorporate ethical reasoning into data privacy practices (Christodoulou & Iordanou, 2021; Wanbil W. Lee et al., 2016; Z. Zhang et al., 2023).

As technology evolves rapidly, new threats and vulnerabilities emerge, affecting data privacy. For instance, advancements in AI and blockchain present unique challenges and opportunities for privacy

management. Furthermore, interdisciplinary perspectives can offer valuable insights into improving privacy practices, highlighting the need for solutions that integrate legal, ethical, and technical considerations. Emerging research underscores the value of interdisciplinary approaches in developing comprehensive privacy solutions that account for technological, ethical and social dimensions (Liu et al., 2023; Raab, 2020). Real-world examples of data breaches underscore the urgency of robust privacy measures.

This paper proposes examining data sharing through the lens of privacy breach risks associated with both the data and its recipient. By qualifying and quantifying these risks, the study aims to establish a consensus on data sharing practices, contributing to the development of evidence-based health benefits. Privacy breaches (Tripathy, 2019), which involve unauthorized access or disclosure of sensitive information, pose significant risks that can be mitigated through robust policies and a comprehensive ethical framework.

Integrating traditional ethical approaches such as autonomy, justice, beneficence, nonmaleficence, and fidelity into privacy frameworks is essential for addressing existing gaps (Richards et al., 2023). While ethical standards are becoming more prevalent, progress in aligning these standards with rapid technological advancements remains slow (Wagner, 2019). Emerging discussions focus on aligning ethical principles with evolving technologies to ensure that privacy frameworks remain relevant and effective (Knijnenburg et al., 2022).

The current study contributes to the literature in three keyways. First, it identifies gaps in existing privacy-preserving techniques by critically analysing their limitations, such as difficulties in setting appropriate thresholds and balancing privacy protection with data utility. The aim is to highlight these shortcomings and recommend improvements to make privacy-preserving methods more robust and applicable. Second, it proposes a comprehensive framework for ethical data sharing that integrates ethical principles with privacy-preserving practices. This framework is designed to address the complexities of data sharing by considering key ethical dimensions, including fairness, transparency, and user consent, thereby enhancing the ethical management of data across various contexts. Third, it underscores the need for a comprehensive approach to ethical and fair use in data management. This approach advocates for a context-specific framework that extends beyond traditional privacy measures to incorporate ethical considerations, ensuring theta data sharing is secure, equitable, and respectful of individual rights. By addressing these areas, the paper seeks to advance the development of a more ethical and effective framework for data sharing, thereby contributing to the broader field of data privacy and management.

The paper is organized into five sections: First, related works review privacy-preserving techniques and ethical data management frameworks. Second, methods detail the development of the proposed framework. Third, results present findings and identify gaps in current frameworks. Fourth, the discussion explores implications and suggests improvements. Finally, the conclusion summarizes contributions and future research directions.

2. Methods

To achieve the objective of proposing a comprehensive framework for ethical data sharing, this paper employs a multi-faceted methodology, including a thorough literature review and content analysis.

The first step is a comprehensive review of literature on privacy-preserving data sharing, focusing on anonymization techniques, evaluation methods, and ethical principles. It assesses the effectiveness and limitations of current frameworks and explores guidelines like the Belmont Report and recent advancements such as homomorphic encryption and differential privacy, identifying gaps and areas for improvement in ethical data management.

2.1 Literature Review: Data Privacy Ethics and Privacy-Preserving Data Sharing

The exponential growth in data generation across various sectors underscores the critical need for robust data privacy measures. Addressing this need involves both ethical considerations and advanced privacy-preserving techniques to manage and protect sensitive information effectively.

2.1.1 Ethical Considerations in Data Privacy

Ethical considerations play a crucial role in evaluating data privacy frameworks, particularly in ensuring vendor practices align with principles that safeguard personal data. Frameworks such as the GDPR and the DPDPA emphasize core values like transparency, consent, and fairness (GDPR.EU, 2024; Pop, 2023). However, these frameworks often fall short in addressing the ethical implications of emerging technologies, such as AI and big data, and the complex integration of vendor practices (Medium, 2023).

Floridi and Taddeo (2016) argue for aligning technological advancements with societal values (L. Floridi & Taddeo, 2016), while Brey, (2012) advocates for Value-Sensitive Design (VSD) in technology development (Brey, 2012). Despite their comprehensive, existing frameworks struggle to adapt to the dynamic nature of technology and ethical dilemmas it presents. There is a notable gap in

developing guidelines that account for these evolving concerns and establishing robust ethical standards for new technological contexts.

2.1.2 Existing Ethical Frameworks

Several established ethical frameworks guide data sharing practices. The Belmont Report outlines principles such as respect for persons, beneficence, and justice, relevant to data sharing (Belmont Report, 1979). Similarly, the OECD Privacy Guidelines focus on limiting data collection, ensuring data accuracy, and providing access to data (OECD, 2023). While these frameworks provide a solid foundation, they face significant challenges in integrating emerging technologies, managing cross-border data sharing, and adopting to dynamic threats (L. Floridi & Taddeo, 2016; Vegesna, 2023).

The need for these frameworks to evolve is critical, as they must now consider the ethical implications of vendor practices and the complexities of global data flows. Enhancing these frameworks requires a dynamic and adaptive approach, integrating vendor practices, harmonizing cross-border standards, and engaging stakeholders to ensure ethically aligned data sharing.

2.1.3 Privacy-Preserving Data Sharing

Privacy-preserving data sharing techniques aim to balance privacy with effective data utilization. Techniques such as de-identification and anonymization are crucial in protecting sensitive information (Mishra, 2024). However, these techniques primarily focus on technical solutions, often overlooking the ethical considerations that should guide their application. For instance, while these methods protect privacy, they may also reduce data utility or inadvertently introduce biases.

Recent innovations, such as blockchain-based privacy solutions for AI (Hai & Liu, 2022), highlight the need for a multifaceted approach that integrates ethical principles with technical advancements. There is a critical need to develop a framework that not only advances these technical solutions but also embeds ethical considerations, ensuring responsible and balanced data sharing practices.

2.1.4 Privacy-Preserving Techniques

Key privacy-preserving techniques, such as homomorphic encryption and federated learning, play a vital role in protecting data throughout its lifecycle. Homomorphic encryption allows computations on encrypted data without decryption, preserving privacy during data processing (Jiang et al., 2021). Differential privacy introduces noise to data queries, preventing the identification of individuals

while still allowing useful data analysis (Dwork, 2006). Federated learning decentralized model training, reducing the risk of data breaches by keeping data local (Yazici et al., 2023).

However, while these techniques are advanced, they often fail to address the ethical implications of their implication, particularly concerning fairness and data utility. Current methods primarily focus on the technical aspects of privacy (Habbal et al., 2024; Vegesna, 2023), neglecting the broader ethical considerations that must be integrated to ensure balanced and fair data sharing practices. To bridge this gap, the proposed framework should advance these technical solutions while integrating ethical principles to ensure that privacy measures are balanced with fairness and utility in data sharing.

2.1.5 Data Anonymization

Data anonymization transforms personally identifiable information (PII) into non-identifiable formats, allowing data use for legitimate purposes while ensuring privacy (Secoda, 2024). Techniques such as k-anonymity, generalization, masking, and t-closeness each have distinct advantages and limitations.

- **K-Anonymity**: Ensures each record is indistinguishable from at least k-1 others but may suffer from homogeneity and background knowledge attacks (Hussien et al., 2013; Samarati & Sweeney, 2007).
- **Generalization**: Replaces specific data values with broader categories, potentially leading to significant information loss (Mandal & Nigam, 2012; Mishra, 2024).
- **Masking**: Substitutes sensitive data with non-revealing formats, useful for adhering to privacy regulations (Imperva, 2024).
- **l-Diversity**: Enhances k-anonymity by ensuring diverse representation of sensitive attributes but can be labour-intensive and vulnerable to certain attacks (Jain et al., 2016; Li et al., 2007).

Advanced Techniques

- **T-Closeness**: Ensures the distribution of sensitive attributes within equivalence classes is similar to the overall dataset, reducing exposure risks (Li et al., 2007).
- **Bucketization**: Groups records into buckets to obscure links between sensitive and identifying information (K. Wang et al., 2016).
- **Slicing**: Partitions data horizontally and vertically, preserving attribute correlations and preventing membership disclosure (Bhuvanesh et al., 2017).

While these advanced techniques offer improved privacy protection, they do not fully address the ethical implications of data sharing, particularly in balancing privacy and data utility. The proposed framework should evaluate these techniques and propose solutions that integrate ethical considerations, ensuring that data management practices are both effective and ethically sound.

Table 1. provides a clear comparison between what current frameworks and techniques offer (strengths) and where they fall short (gaps) in addressing both ethical and technical challenges in privacy-preserving data sharing. The table illustrates that while there are strong ethical and technical frameworks in place for privacy-preserving data sharing, they often lack flexibility, adaptability, and integration with ethical considerations, particularly in the face of emerging technologies and complex data-sharing environments.

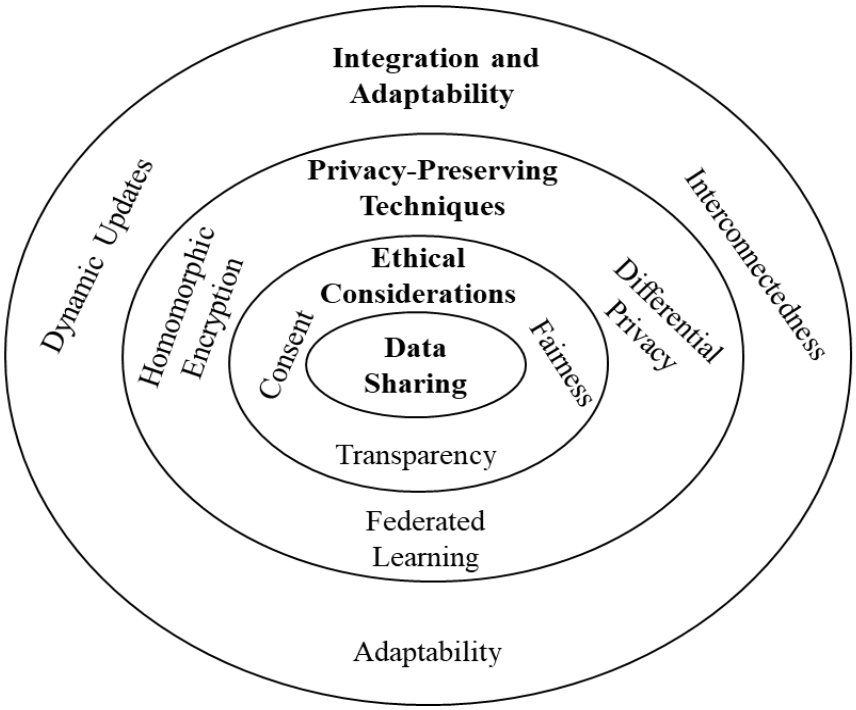
Table 1. Strengths and Gaps in Privacy-Preserving Frameworks and Techniques

Aspect	Existing Frameworks/Techniques	Identified Gaps
Ethical Considerations	- GDPR and DPDPA emphasize transparency, consent, and fairness. - VSD integrates autonomy, justice, and beneficence in technology.	- Lack of adaptability to emerging technologies (e.g., AI, big data). - Insufficient focus on ethical implications of vendor practices.
Privacy-Preserving Data Sharing	- Techniques like de-identification, anonymization, and differential privacy protect sensitive information.	- Predominantly technical focus, with limited integration of ethical considerations. - Challenges in balancing privacy with data utility.
Privacy-Preserving Techniques	- Homomorphic encryption allows computation on encrypted data. - Federated learning decentralizes model training to enhance privacy.	- Overemphasis on technical solutions, overlooking fairness and ethical implications. - Difficulty in adapting to dynamic threats.
Data Anonymization Techniques	- K-anonymity and t-closeness ensure privacy by making data indistinguishable or balancing distribution of attributes.	- Susceptibility to specific attacks (e.g., homogeneity attacks) and significant information loss. - Lack of comprehensive ethical oversight.
Ethical Frameworks	- Belmont Report and OECD Guidelines emphasize principles like respect, beneficence, and accuracy.	- Struggles with integrating emerging technologies and managing cross-border data sharing. - Need for more dynamic and adaptable frameworks.

Ethics and Fair Use Framework for Privacy Preserving Data Sharing

Figure 1 presents a structured approach to managing data privacy by integrating ethical principles with advanced technical solutions. The framework includes five key layers, (1) the Core Framework Layer, which establishes foundational principles; (2) Ethical Considerations, focusing on transparency, consent, fairness which evolving standards; (3) Privacy-Preserving Techniques, covering both basic and advanced methods, including homomorphic encryption, differential privacy, and federated learning; (4) Integration and Adaptability, ensuring responsiveness to new technologies and regulations, with dynamic updates and interconnectedness, (5) the outcome layer, aiming for robust data protection and responsible management. This framework provides a cohesive and dynamic model for balancing effective data protection with ethical practices.

Figure 1. Holistic Data Sharing Framework



Source: By Authors.

The Comprehensive Data Sharing and Privacy-Preserving Framework is unique in its integrated approach, bridging the gap between ethical considerations and technical solutions in data management. Unlike traditional frameworks that often treat these aspects separately, this model combines them in a structured, layered format. It addresses the gaps in the literature by covering both basic and advanced privacy-preserving techniques, ensuring a comprehensive approach to data protection.

The framework's emphasis on adaptability allows it to remain relevant in the face of emerging technologies and evolving regulations, a feature commonly overlooked in existing models. By proactively addressing the ethical implications of new technologies, it ensures that data management practices are both effective and aligned with contemporary societal values, providing a dynamic and cohesive solution for modern data privacy challenges.

2.2 Content analysis

Following the literature review, content analysis is employed to systematically interpret and analyze the textual data gathered (Bengtsson, 2016). This involves coding and categorizing the information to uncover patterns, trends, and insights. Content analysis helps in identifying recurring themes and gaps in existing methods and frameworks, enabling the formulation of a comprehensive framework that integrates privacy-preserving techniques with ethical principles (Parry et al., 2014). The findings from this analysis inform the development of a robust framework designed to enhance data management and privacy protection, addressing identified gaps and aligning with ethical standards.

For coding, we meticulously reviewed the textual data to identify key themes and concepts relevant to our study. This process involved developing a coding scheme with specific labels to represent these themes. Each section of the text was assigned a code that best matched the identified theme, ensuring a systematic approach to organizing the data. This approach helped break down complex information into manageable pieces, facilitating easier analysis and interpretation (Erlingsson & Brysiewicz, 2017). The coding process for the context data included:

- **Privacy Techniques**: Codes such as 'Differential Privacy', 'Homomorphic Encryption', and 'K-Anonymity'.
- **Ethical Principles**: Codes such as 'Informed Consent', 'Transparency', and 'Data Security'.
- **Gaps**: Codes like 'Lack of Integration', 'Insufficient Ethical Considerations', and 'Implementation Challenges'.

In the categorizing phase, we grouped similar codes into broader categories to organize the data into meaningful clusters. This involved aggregating related codes under overarching themes to identify patterns and trends more clearly. By categorizing the data, we uncovered recurring themes and gaps in existing methods and frameworks. This structured approach allowed us to formulate a comprehensive framework that integrates privacy-preserving techniques with ethical principles (Erlingsson & Brysiewicz, 2017). The categorization included:

- **Privacy Techniques**: Grouping codes related to methods like differential privacy and homomorphic encryption.
- **Ethical Principles**: Grouping codes related to principles such as informed consent and data security.
- **Gaps and Opportunities**: Grouping codes related to missing elements and areas for improvement, such as integrating ethical considerations into privacy techniques and addressing implementation challenges.

3. Results

The analysis of current privacy-preserving frameworks and techniques reveals significant gaps in both ethical and technical aspects, particularly in the context of emerging technologies and complex data-sharing environments. The results are organized around three key areas, (1) the limitations of existing privacy-preserving technologies, (2) the inadequacies in ethical frameworks, and (3) the integration challenges of ethical principles with technical advancements.

First, the review of privacy-preserving technologies, such as k-anonymity, l-diversity, and differential privacy, highlights both their strengths in protecting data and their limitations in practical applications. K-anonymity ensures that each record is indistinguishable from at least k-1 others, making it a foundational technique in privacy protection (El Emam & Dankar, 2008; Sweeney, 2002). However, it is vulnerable to homogeneity and background knowledge attacks, which can compromise its effectiveness in protecting sensitive information (Q. Wang et al., 2011).

L-diversity improves upon k-anonymity by ensuring that sensitive attributes are well-represented within groups (Machanavajjhala et al., 2007), but it faces challenges related to labour-intensive implementation and susceptibility to skewed distributions in the dataset (Mseer & Ahmed, 2024; Tamuhla et al., 2023).

Differential privacy introduces noise to data queries to prevent the identification of individuals, thus offering a robust privacy guarantee (Li et al., 2010). However, the added noise can significantly reduce data utility, particularly in small or sensitive datasets, making it difficult to strike a balance between privacy protection and data usability (X. Yang et al., 2017).

Technologies like t-closeness, bucketization, and slicing offer enhanced privacy protections by addressing specific vulnerabilities of earlier methods (Jayapradha & Prakash, 2022; Kumar et al., 2018). However, these approaches are primarily technical solutions and often fail to consider broader ethical implications, such as fairness, transparency, and user consent in data management (Sokolovska & Kocarev, 2018; Thapa & Camtepe, 2021). This limitation underscores the need for a more integrated approach that combines technical rigor with ethical considerations.

Second, the evaluation of ethical frameworks, such as the GDPR, DPDPA, and the Belmont Report, reveals that while they establish foundational principles for data privacy, they fall short in several critical areas. Ethical frameworks often struggle to keep pace with rapid technological advancements (Grover et al., 2024; Rigotti & Fosch-villaronga, 2024). For example, emerging technologies such as AI and blockchain introduce new ethical dilemmas, such as algorithmic bias and the opacity of AI decision-making processes (Owolabi et al., 2024), which existing frameworks are not fully equipped to handle.

This gap highlights the need for frameworks that are more adaptable to evolving technological landscapes. Current frameworks inadequately address the ethical implications of vendors adhere to ethical standards, particularly in global and complex data ecosystems .This gap suggests a need for more robust guidelines that ensure ethical consistency across the entire data lifecycle. The global nature of data sharing necessitates harmonized standards across jurisdictions. However, existing frameworks often lack the flexibility to address the complexities of cross-border data flows, leading to potential ethical and legal conflicts (Andanda & Mlotshwa, 2024). This challenge is particularly relevant in the context of international collaboration and data exchanges that require compliance with multiple, and sometimes conflicting, legal requirements.

Third, the results indicate that while there is a growing recognition of the need to integrate ethical principles into technical privacy-preserving solutions, significant challenges remain. Achieving a balance between privacy and data utility is a persistent challenge (N. Yuvaraj et al., 2022). Privacy-preserving techniques often prioritize privacy at the expense of data utility, which can limit the effectiveness of data-driven decision-making processes (Dhinakaran et al., 2024; Yuping Zhang et al., 2023).

Ethics and Fair Use Framework for Privacy Preserving Data Sharing

There is a critical need for solutions that maintain privacy while preserving the usefulness of data, particularly in sectors like healthcare and finance where data accuracy and utility are paramount. Techniques such as homomorphic encryption and federated learning often promising privacy-preserving capabilities (L. Zhang et al., 2023). However, these technologies require further refinement to address ethical concerns such as fairness and transparency (Q. Yang, 2021). For instance, federated learning reduces the risk of data breaches by keeping data local, but it raises questions about fairness in model training and transparency in data usage (Bouacida & Mohapatra, 2021; Yifei Zhang et al., 2024). The results emphasize the importance of developing context-special ethical frameworks that consider the unique challenges of different data-sharing environments. These frameworks should integrate ethical reasoning with technical solutions to ensure that privacy-preserving measures are not only effective but also fair and transparent.

The analysis highlighted opportunities to enhance current frameworks by bridging the identified gaps. Specially, the integration of ethical principles into privacy-preserving technologies and the adoption of a more holistic approach to data management were identified as key areas for improvement. These results underscore the importance of developing a framework that not only preserves data privacy but also upholds ethical standards, thereby fostering responsible and transparent data sharing practices.

3.1 Comprehensive Ethical Data Sharing Framework

The Comprehensive Ethical Data Sharing Framework, as illustrated in Figure 2, addresses the critical need for a robust approach to data sharing that integrates ethical principles with privacy-preserving techniques. Central to this framework is the Holistic Ethical Framework, which ensures that data sharing practices are both technically effective and ethically sound. This central element emphasizes the balance between technical solutions and ethical considerations, providing a foundation for all other components of the framework. It ensures that data management practices align with societal values and ethical standards.

The framework is organized along two main dimensions: Integration and Adaptability. Dynamic Adaptability is crucial for maintaining the framework's relevance in the face of rapidly evolving technologies and ethical challenges. This includes regular updates, continuous integration of new research, and feedback loops to refine and improve the framework. Integration of Vendor Practices ensures that third-party vendors comply with ethical standards through regular audits, ethical contracts, and training. Furthermore, Cross-Border Considerations address the complexities of

international data sharing by developing harmonized standards and facilitating cooperation across jurisdictions to ensure consistent ethical practices.

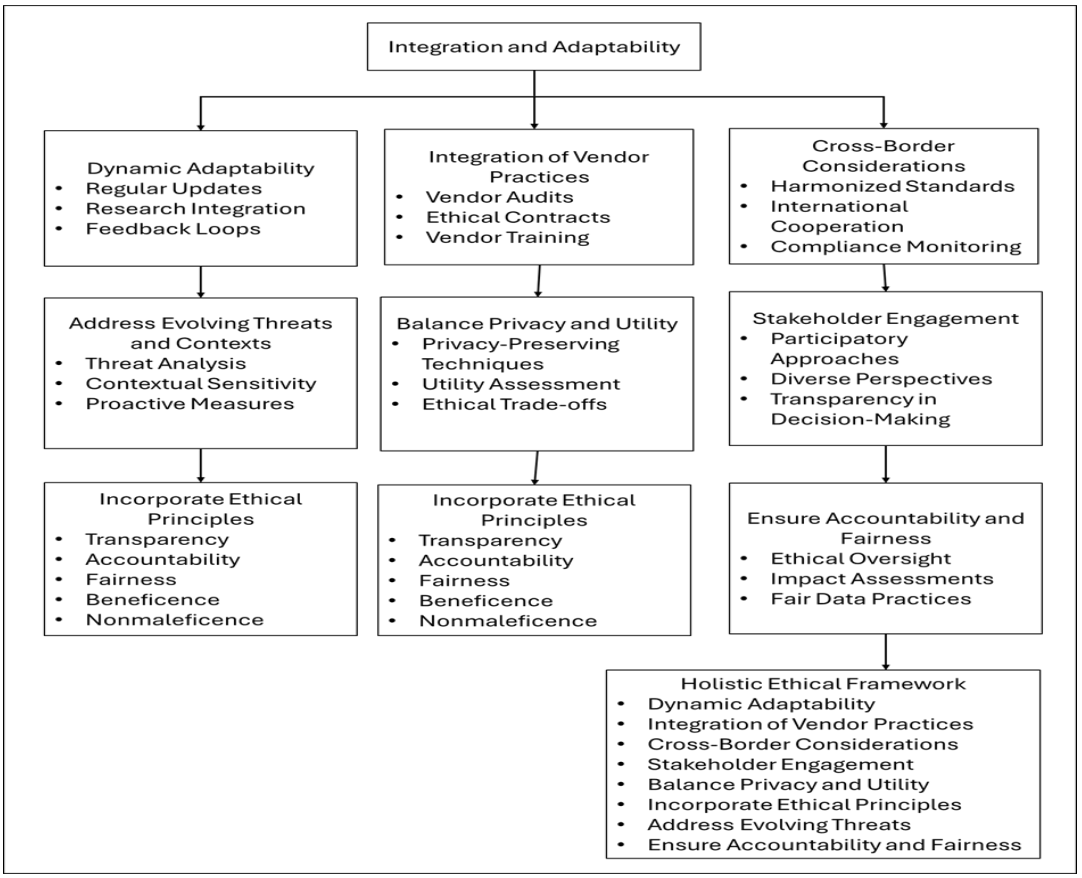
Balancing Privacy and Utility is achieved through the application of privacy-preserving techniques such as homomorphic encryption, differential privacy, and federated learning, which protect privacy while allowing data to be useful. Addressing Evolving Threats and Contexts involves proactive measures to mitigate risks and adapt to new threats. Incorporating Ethical Principles, including transparency, accountability, fairness, beneficence, and nonmaleficence, ensures that the framework is ethically grounded. Stakeholder Engagement and Ensuring Accountability and Fairness further enhance the framework by incorporating diverse perspectives and maintaining high standards of responsibility.

Together, these components create a comprehensive system that enhances data management and privacy protection effectively and ethically. Engaging with stakeholders ensures that the framework reflects diverse perspectives and addresses various concerns. This component involves participatory approaches that involve stakeholders in the decision-making process, considering input from various groups to ensure inclusivity, and ensuring transparency in decision-making. Engaging stakeholders helps to create a framework that is more responsive to the needs and values of different communities.

Ensuring Accountability and Fairness guarantees that data sharing practices are both fair and responsible. This involves establishing ethical oversight bodies or mechanisms to oversee compliance, conducting regular impact assessments to evaluate the effects of data sharing practices, and ensuring fair data practices that are just and equitable. This component ensures that the framework maintains high standards of responsibility and fairness in data management.

This comprehensive framework integrates ethical principles and privacy-preserving techniques to create a robust system for data sharing. By addressing gaps in current methods and ensuring adaptability to new challenges, this framework aims to enhance data management and privacy protection in a manner that is both effective and ethically sound.

Figure 2. Comprehensive Ethical Data Sharing Framework



Source: By Authors.

4. Conclusion

This study has critically examined the current state of privacy-preserving technologies and ethical frameworks in data sharing, identifying significant gaps and proposing a comprehensive approach to address these challenges. The findings underscore the need for a more integrated and dynamic framework that balances privacy protection with data utility while embedding ethical principles into technical solutions. By analysing the limitations of current privacy-preserving technologies, this study highlights the need for more robust and adaptable methods that can effectively protect privacy without compromising data utility.

The study advocates for a comprehensive framework that integrates ethical principles with privacy-preserving practices. this framework addresses the complexities of data sharing by considering key ethical dimensions, including fairness transparency, and user consent, thereby enhancing the ethical management of data across various contexts. The study emphasizes the

importance of developing context-specific frameworks that extend data sharing is secure, equitable, and respectful of individual rights.

Future research should explore interdisciplinary approaches that integrate legal, ethical, and technical perspectives to develop more comprehensive privacy-preserving frameworks. As technology continues to evolve, there is a need for ongoing research into dynamic ethical standards that can adapt to new challenges and ensure that continued relevance and effectiveness of privacy frameworks. Further studies should focus on real-world applications of the proposed ethical framework, particularly in complex data-sharing environments, to assess its practically and effectiveness in addressing privacy and ethical challenges.

References

Andanda, P., & Mlotshwa, L. (2024). Streamlining the ethical-legal governance of cross-border health data sharing during global health emergencies. *Research Ethics*. https://doi.org/10.1177/17470161241261907

Aslam, T., & Shyam Kishore, V. (2024). Study of Digital Transformation and Personal Data Protection in the Era of Globalization [Alliance University]. In *Alliance School of Law, Alliance University*. https://gnanaganga.inflibnet.ac.in:8443/jspui/handle/123456789/15767

Belmont Report. (1979). Read the Belmont Report. In *The Belmont Report*. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open*, *2*, 8–14. https://doi.org/10.1016/j.npls.2016.01.001

Bhuvanesh, S., V N, A., Gladies, A. X. S., & M, V. (2017). Micro data Privacy Preserving Using Slicing. *Ijarcce*, *6*(3), 358–362. https://doi.org/10.17148/ijarcce.2017.6382

Bouacida, N., & Mohapatra, P. (2021). Vulnerabilities in Federated Learning. *IEEE Access*, *9*, 63229–63249. https://doi.org/10.1109/ACCESS.2021.3075203

Brey, P. A. E. (2012). Anticipatory Ethics for Emerging Technologies. In *NanoEthics* (pp. 1–13). Springer. https://link.springer.com/article/10.1007/s11569-012-0141-7

Christodoulou, E., & Iordanou, K. (2021). Democracy Under Attack: Challenges of Addressing Ethical Issues of AI and Big Data for More Democratic Digital Media and Societies. *Frontiers in Political Science*, *3*(July), 1–17. https://doi.org/10.3389/fpos.2021.682945

Dhinakaran, D., Sankar, S. M. U., Selvaraj, D., & Raja, S. E. (2024). Privacy-Preserving Data in IoT-based Cloud Systems: A Comprehensive Survey with AI Integration. *Sustainable Energy Technologies and Assessments*, *57*(2). https://doi.org/https://doi.org/10.1016/j.seta.2023.103144

Dwork, C. (2006). Differential privacy. *Differential Privacy, in: International Colloquium on Automata, Languages and Programming, in: 33rd International Colloquium*, 1–12. https://link.springer.com/chapter/10.1007/11787006_1

El Emam, K., & Dankar, F. K. (2008). Protecting privacy using k-anonymity. *Journal of the American Medical Informatics*, *15*(5), 1–5. https://doi.org/10.1197/jamia.M2716.Introduction

Erlingsson, C., & Brysiewicz, P. (2017). A hands-on guide to doing content analysis. *African Journal of Emergency Medicine*, *7*(3), 93–99. https://doi.org/10.1016/j.afjem.2017.08.001

GDPR.EU. (2024). *What is GDPR, the EU's new data protection law?* Proton AG. https://gdpr.eu/what-is-gdpr/

Grover, R., Jang, K., & Su, L. W. (2024). *Beyond Digital Protection(ism): Comparing Data Governance Frameworks in Asia* (Vol. 14). Journal of Information Policy. https://doi.org/10.5325/jinfopoli.14.2024.0005

Groves, R. M., & Harris-Kojetin, B. A. (2017). Innovations in federal statistics: Combining data sources while protecting privacy. In *Innovations in Federal Statistics: Combining Data Sources While Protecting Privacy*. THE NATIONAL ACADEMIES PRESS. https://doi.org/10.17226/24652

Habbal, A., Hamouda, H., Alnajim, A. M., Khan, S., & Alrifaie, M. F. (2024). Privacy as a Lifestyle: Empowering assistive technologies for people with disabilities, challenges and future directions. *Journal of King Saud University - Computer and Information Sciences*, *36*(4), 102039. https://doi.org/10.1016/j.jksuci.2024.102039

Hai, X., & Liu, J. (2022). PPDS: Privacy Preserving Data Sharing for AI applications Based on Smart Contracts. *Proceedings - 2022 IEEE 46th Annual Computers, Software, and Applications Conference, COMPSAC 2022*, 1561–1566. https://doi.org/10.1109/COMPSAC54236.2022.00248

Hussien, A. A., Hamza, N., & Hefny, H. A. (2013). Attacks on Anonymization-Based Privacy-Preserving: A Survey for Data Mining and Data Publishing. *Journal of Information Security*, *4*(2). https://doi.org/10.4236/jis.2013.42012

Imperva. (2024). *Anonymization*. Imperva.

https://www.imperva.com/learn/data-security/anonymization/#:~:text=from the data.-,Data Anonymization Techniques,*" or "x".

Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: a technological perspective and review. *Journal of Big Data*, *3*(1). https://doi.org/10.1186/s40537-016-0059-y

Jayapradha, J., & Prakash, M. (2022). A Survey on Privacy-Preserving Data Publishing Methods and Models in Relational Electronic Health Records. In *Sustainable Advanced Computing*. Springer. https://link.springer.com/chapter/10.1007/978-981-16-9012-9_52

Jiang, L., Xia, Z., & Sun, X. (2021). Chapter Three - Review on privacy-preserving data comparison protocols in cloud computing. In S. W. Ali R. Hurson (Ed.), *Advances in Computers* (Vol. 120, pp. 81–119). Elsevier. https://doi.org/https://doi.org/10.1016/bs.adcom.2020.09.002

Knijnenburg, B. P., Page, X., Wisniewski, P., Lipford, H. R., Proferes, N., & Romano, J. (2022). The Ethics of Privacy in Research and Design: Principles, Practices, and Potential. In *Modern Socio-Technical Perspectives on Privacy* (pp. 395–426). Springer. https://doi.org/10.1007/978-3-030-82786-1_1

Kumar, A., Gyanchandani, M., & Jain, P. (2018). A comparative review of privacy preservation techniques in data publishing. *Proceedings of the 2nd International Conference on Inventive Systems and Control, ICISC 2018*, *Icisc*, 1027–1032. https://doi.org/10.1109/ICISC.2018.8398958

L. Floridi, & Taddeo, M. (2016). What is Data Ethics? *Philosophical Transactions of the Royal Society*, *374*(2083), 1–8. http://dx.doi.org/10.1098/rsta.2016.0112

Li, N., Li, T., & Venkatasubramanian, S. (2007). t-Closeness : Privacy Beyond k-Anonymity and-Diversity t -Closeness : Privacy Beyond k -Anonymity and -Diversity. *IEEE*, *July*, 106–115. https://doi.org/10.1109/ICDE.2007.367856

Li, N., Qardaji, W., & Su, D. (2010). CERIAS Tech Report 2010-27 Provably Private Data Anonymization: Or, k-Anonymity Meets Differential Privacy Provably Private Data Anonymization: Or, k-Anonymity Meets Differential Privacy. In *Purdue University*. https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2010-24.pdf

Liu, J., Chen, C., Qu, Y., Yang, S., & Xu, L. (2023). RASS: Enabling privacy-preserving and authentication in online AI-driven healthcare applications. *ISA Transactions*, *141*, 20–29. https://doi.org/10.1016/j.isatra.2023.03.049

Machanavajjhala, A., Kifer, D., Gehrke, J., & Venkitasubramaniam, M. (2007). ℓ-diversity: Privacy

beyond k-anonymity. *ACM Transactions on Knowledge Discovery from Data*, *1*(1). https://doi.org/10.1145/1217299.1217302

Mandal, A., & Nigam, M. K. (2012). A Review On Data Anonymization Technique For Data Publishing. *International Journal of Engineering Research & Technology (IJERT)*, *1*(10), 46–54. https://d1wqtxts1xzle7.cloudfront.net/64342587/a-review-on-data-anonymization-technique-for-data-publishing-IJERTV1IS10210-libre.pdf?1599121871=&response-content-disposition=inline%3B+filename%3DIJERT_A_Review_On_Data_Anonymization_Tec.pdf&Expires=1716968

Medium. (2023). *Ethical Considerations in Data Privacy and Security*. Medium. https://medium.com/@armaanakhan91/ethical-considerations-in-data-privacy-and-security-1874a10061f0

Mishra, A. (2024). Privacy-Preserving Data Sharing Platform. *INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, *8*(4). https://doi.org/10.55041/IJSREM32225

Mseer, I. N., & Ahmed, S. M. (2024). Artificial Intelligence and Security Challenges. In *Studies in Systems, Decision and Control* (Vol. 487). https://doi.org/10.1007/978-3-031-35828-9_13

N. Yuvaraj, Praghash, K., & Karthikeyan, T. (2022). Privacy preservation of the user data and properly balancing between privacy and utility. *International Journal of Business Intelligence and Data Mining*, *20*(4). https://doi.org/10.1504/IJBIDM.2022.123216

OECD. (2023). *Report on the implementation of the OECD Privacy Guidelines* (Issue 361). https://www.oecd-ilibrary.org/content/paper/cf87ae8f-en

Owolabi, O. S., Uche, P. C., Adeniken, N. T., Ihejirika, C., Islam, R. Bin, & Chhetri, B. J. T. (2024). Ethical Implication of Artificial Intelligence (AI) Adoption in Financial Decision Making. *Computer and Information Science*, *17*(1), 49. https://doi.org/10.5539/cis.v17n1p49

Parry, K., Mumford, M. D., Bower, I., & Watts, L. L. (2014). Qualitative and historiometric methods in leadership research: A review of the first 25years of The Leadership Quarterly. In *Leadership Quarterly* (Vol. 25, Issue 1, pp. 132–151). Elsevier Inc. https://doi.org/10.1016/j.leaqua.2013.11.006

Phillips, M. (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Human Genetics*, *137*(8), 575–582. https://doi.org/10.1007/s00439-018-1919-7

Pop, C. (2023). *India's Digital Personal Data Protection Act: Key Provisions and Business Implications*. CoSoSys. https://www.endpointprotector.com/blog/indias-personal-data-protection-bill-what-we-know-so-far/

Raab, C. D. (2020). Information privacy, impact assessment, and the place of ethics ∗. *Computer Law and Security Review*, *37*, 105404. https://doi.org/10.1016/j.clsr.2020.105404

Rasheed, K., Qayyum, A., Ghaly, M., Al-Fuqaha, A., Razi, A., & Qadir, J. (2022). Explainable, trustworthy, and ethical machine learning for healthcare: A survey. *Computers in Biology and Medicine*, *149*(August), 106043. https://doi.org/10.1016/j.compbiomed.2022.106043

Richards, D., Vythilingam, R., & Formosa, P. (2023). A principlist-based study of the ethical design and acceptability of artificial social agents. *International Journal of Human Computer Studies*, *172*(April 2022), 102980. https://doi.org/10.1016/j.ijhcs.2022.102980

Rigotti, C., & Fosch-villaronga, E. (2024). How might the GDPR evolve? A question of politics, pace and punishment. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, *53*(April), 105966. https://doi.org/10.1016/j.clsr.2024.106033

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers and Security*, *49*, 70–94. https://doi.org/10.1016/j.cose.2014.11.007

Samarati, P., & Sweeney, L. (2007). Protecting Privacy When Disclosing Information: K Anonymity and its Enforcement Through Suppression. *IEEE Xplore*.

Secoda. (2024). *What is Data Anonymization?* Secoda. https://www.secoda.co/glossary/what-is-data-anonymization#:~:text=Data anonymization serves the purpose,individuals associated with the data.

Sokolovska, A., & Kocarev, L. (2018). Integrating Technical and Legal Concepts of Privacy. *IEEE Access*, *6*, 26543–26557. https://doi.org/10.1109/ACCESS.2018.2836184

Sweeney, L. (2002). k-Anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(5), 1–14. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=2ab47454f59d9d8e55d4d8a69530562a3690794a

Tamuhla, T., Lulamba, E. T., Mutemaringa, T., & Tiffin, N. (2023). Multiple modes of data sharing can facilitate secondary use of sensitive health data for research. *BMJ Global Health*, *8*(10), 1–11. https://doi.org/10.1136/bmjgh-2023-013092

Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in Biology and Medicine*, *129*(November 2020), 104130. https://doi.org/10.1016/j.compbiomed.2020.104130

Tripathy, B. K. (2019). 4 - De-Anonymization Techniques for Social Networks. In *Social Network Analytics* (pp. 71–85). Elsevier. https://doi.org/https://doi.org/10.1016/B978-0-12-815458-8.00004-9

Vegesna, V. V. (2023). Privacy-Preserving Techniques in AI-Powered Cyber Security: Challenges and Opportunities. *International Journal of Machine Learning for …*, *5*(4), 1–8. https://ijsdcs.com/index.php/IJMLSD/article/view/408

Wagner, B. (2019). Ethics As An Escape From Regulation. From "Ethics-Washing" To Ethics-Shopping? In *Being Profiled: Cogitas Ergo Sum*. Amsterdam University Press. https://doi.org/10.1515/9789048550180-016

Wanbil Lee, Zankl, W., & Chang, H. (2016). An Ethical Approach to Data Privacy Protection. *Isaca*, *6*(January), 1–9. https://www.researchgate.net/publication/338331380_An_Ethical_Approach_to_Data_Privacy_Protection?enrichId=rgreq-15d13a6484ab8374af67173f9cd7afae-XXX&enrichSource=Y292ZXJQYWdlOzMzODMzMTM4MDtBUzo4NTAxMTk1NzQ0Mzc4ODhAMTU3OTY5NTcwOTAwNA%3D%3D&el=1_x_2&_esc=p

Wanbil W. Lee, Wolfgang Zankl, & Henry Chang. (2016). An Ethical Approach to Data Privacy Protection. *ISACA Journal*, *6*, 1–9. www.isaca.org

Wang, K., Wang, P., Fu, A. W., & Wong, R. C. W. (2016). Generalized bucketization scheme for flexible privacy settings. *Information Sciences*, *348*, 377–393. https://doi.org/10.1016/j.ins.2016.01.100

Wang, Q., Xu, Z., & Qu, S. (2011). An enhanced k-anonymity model against homogeneity attack. *Journal of Software*, *6*(10), 1945–1952. https://doi.org/10.4304/jsw.6.10.1945-1952

Watson, D., & Jones, A. (2013). Chapter 5 - Risk Management. In *Digital Forensics Processing and Procedures* (pp. 109–176). Elsevier. https://doi.org/https://doi.org/10.1016/B978-1-59749-742-8.00005-4

Xu, C., Qu, Y., Xiang, Y., & Gao, L. (2023). Asynchronous federated learning on heterogeneous devices: A survey. *Computer Science Review*, *50*(August 2022), 100595. https://doi.org/10.1016/j.cosrev.2023.100595

Yang, Q. (2021). Toward Responsible AI: An Overview of Federated Learning for User-centered Privacy-preserving Computing. *ACM Transactions on Interactive Intelligent Systems*, *11*(3–4). https://doi.org/10.1145/3485875

Yang, X., Wang, T., Ren, X., & Yu, W. (2017). Survey on Improving Data Utility in Differentially Private Sequential Data Publishing. *IEEE Transactions on Big Data*, *7*(4), 1–1. https://doi.org/10.1109/tbdata.2017.2715334

Yazici, İ., Shayea, I., & Din, J. (2023). A survey of applications of artificial intelligence and machine learning in future mobile networks-enabled systems. *Engineering Science and Technology, an International Journal*, *44*. https://doi.org/10.1016/j.jestch.2023.101455

Zhang, L., Xu, J., Vijayakumar, P., Sharma, P. K., & Ghosh, U. (2023). Homomorphic Encryption-Based Privacy-Preserving Federated Learning in IoT-Enabled Healthcare System. *IEEE Transactions on Network Science and Engineering*, *10*(5), 2864–2880. https://doi.org/10.1109/TNSE.2022.3185327

Zhang, Yifei, Zeng, D. U. N., Luo, J., Fu, X., & Chen, G. (2024). A Survey of Trustworthy Federated Learning : Issues , Solutions , and Challenges. *ACM Transactions on Intelligent Systems and Technology*. https://doi.org/10.1145/3678181

Zhang, Yuping, Qu, Y., Gao, L., Luan, T. H., Jolfaei, A., & Zheng, J. X. (2023). Privacy-preserving data analytics for smart decision-making energy systems in sustainable smart community. *Sustainable Energy Technologies and Assessments*, *57*(December 2021), 103144. https://doi.org/10.1016/j.seta.2023.103144

Zhang, Z., Wang, L., & Lee, C. (2023). Recent Advances in Artificial Intelligence Sensors. *Advanced Sensor Research*, *2*(8), 1–27. https://doi.org/10.1002/adsr.202200072