International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Comparative Study on AI-Driven Anonymization Techniques for Protecting Personal Data

Mahendralal Prajapati[1], Alok Kumar Upadhyay[2], Mehdi Rezaie[3], Jyotshna Dongradive[4]

[1,2]Student, University of Mumbai
[3,4]Associate Professor, University of Mumbai

Abstract
In the Artificial Intelligence era, protecting individual users' data has become crucial. The collected data is stored in multiple databases having personally identifiable information (PII). This may provide a significant privacy concern for the database. Several privacy-preserving approaches have been proposed, including Differential Privacy, Homomorphic Encryption, Generative Adversarial Network and Federated Learning. In this paper, the above four anonymization techniques are compared. In addition, this study will review the strengths and weaknesses of these techniques. We also discuss the trade-off between data utility and privacy. The results of this study aim to guide researchers and practitioners in selecting suitable AI-driven anonymization techniques.

Keywords: AI-driven data Anonymization, Data privacy, Differential privacy, literature review, Homomorphic Encryption, Generative Adversarial Networks, Federated Learning

1. Introduction

The need for effective anonymization techniques has become crucial with the increasing volume and complexity of personal data being processed. These techniques are especially important for companies that heavily rely on personal data for their business and service provision, such as social media, healthcare, mobility, and financial services [1]. The implementation of these techniques is essential for these companies to follow the GDPR requirements and ensure the protection of individuals' data. The European Data Protection Board recognizes the challenges involved in balancing free expression and data protection and plans to issue guidance addressing this balance. Furthermore, the principle of data minimization under GDPR requires organizations to have a data retention policy in place, limiting the amount of personal data stored and the length of time for which it is kept to only what is necessary for processing purposes. Furthermore, organizations must also consider the potential risks associated with big data analysis, as the larger the dataset, the higher the probability of re-identifying individuals even in seemingly de identified datasets. To mitigate these risks and ensure compliance with data protection regulations, companies must securely drop personally identifiable information and other sensitive data when it is no longer needed for business purposes. This study will compare various AI-driven anonymization techniques, evaluating their effectiveness, efficiency, and potential drawbacks, to provide

recommendations for organizations looking to protect personal data while supporting the value of their data assets.

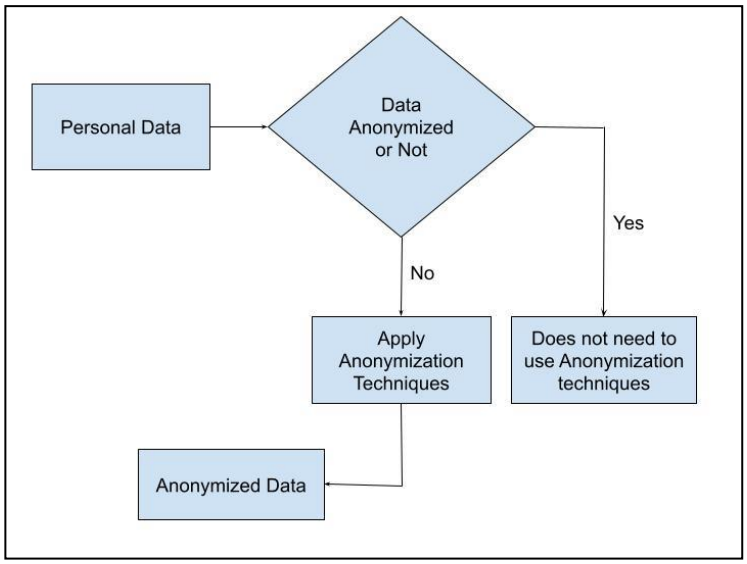

Figure 1: Concept of Data Anonymization

The above figure.1 depicts the decision-making process for deciding whether personal data should be anonymized as follows:

- The flowchart begins with a block titled "Personal Data," which represents the introduction of sensitive personal data into the process.
- An arrow points from the "Personal Data" block to a decision diamond labeled "Data Anonymized or Not." This judgment point determines whether the data has already been anonymized.
- If the data is found to be anonymized (the "Yes" branch), an arrow points to a block labeled "Does not need to useAnonymization techniques," suggesting that no further action is necessary.
- If the data is not anonymized (the "No" branch), an arrow points to a block labeled "Apply Anonymization Techniques," which indicates that a suitable anonymization technique must be applied to the data.
- After the anonymization procedures are used, an arrow travels to a block labeled "Anonymized Data," showing that the process produced anonymized data.

This study will focus on traditional anonymization techniques, such as Differential Privacy, Homomorphic Encryption, Generative Adversarial Network, and Federated Learning. These methods have been extensively researched and applied in various contexts [2][3][4][5].

2. Literature Review

In the era of ubiquitous data collection and advanced analytics, the need to protect individual privacy has become paramount. The rapid growth of "Big Data" has presented both opportunities and challenges, as the vast troves of information offer valuable insights but also raise significant privacy concerns. [10], [11] Ensuring the security and privacy of this data is essential to support public trust and enable responsible innovation.

One key approach to addressing these challenges is the development of differential privacy, a rigorous mathematical framework for quantifying and limiting the privacy risks associated with data analysis.[9],

[12] Differential privacy provides a formal guarantee that the output of an analysis on a data-set will be statistically indistinguishable from the output that would have been produced had any individual's data been excluded. This powerful technique allows for the extraction of useful insights from data while probably bounding the potential harm to individual privacy.

Complementing differential privacy, homomorphic encryption offers another avenue for preserving privacy in data-driven applications. Homomorphic encryption enables computation on encrypted data, allowing analytics to be performed without ever exposing the underlying sensitive information [13]. By combining these techniques, organizations can unlock the value of Big Data while ensuring the confidentiality of personal information.

Generative Adversarial Networks (GANs) have also appeared as a promising tool for privacy preserving data generation. These neural network-based models can synthesize new, realistic data samples that retain the statistical properties of the original dataset, but without reproducing the private details of individual records [10],[13].

Finally, Federated Learning presents an innovative approach to distributed machine learning that prioritizes data privacy. Rather than centralizing data, Federated Learning trains models on decentralized data sources, allowing each participant to keep control over their personal information. By aggregating model updates rather than raw data, Federated Learning minimizes the risk of privacy breaches [18].

Through the synergistic application of these innovative technique's differential privacy, homomorphic encryption, Generative Adversarial Networks, and Federated Learning organizations can harness the power of Big Data analytics while upholding the fundamental right to privacy. [9],[10],[13],[14],[15],[16],[17] As data-driven innovation continues to transform our world, this comprehensive approach to privacy-preserving technology will be essential to realizing the full potential of the information age.

3. AI-Driven Anonymization Techniques

When distributing anonymized data, the primary priority is to protect individuals' sensitive information from exposure. There are three categories of information exposure: identification, attribute, and inference.

Identification threat increases when a less productive algorithm and incapable Anonymization techniques are used that allow the threat of identification by linking with a specific record in the anonymized data. This linking of data is known as the Quasi- Identifier. According to that, "A set of attributes where the attributes are not identifiers by themselves, but when combined, may enable the unique identification of records in the database."

Table 1: Attribute vs Anonymization Techniques

Attribute	Differential Privacy	Generative Adversarial Networks (GANs)	Federated Learning	Homomorphic Encryption
Privacy Protection	High	Medium-High	High	Very High
Data Utility	Medium	High	High	Medium
Computational Efficiency	Medium	Medium-high	High	Low
Robustness	High	Medium	High	Very High

Table 1 above illustrates the notable privacy protection, data utility, computational effectiveness, and

robustness of different anonymization strategies, such as Differential Privacy, Homomorphic Encryption, Generative Adversarial Networks (GANs), and Federated Learning. The aforementioned table demonstrates how businesses and organizations can successfully employ these strategies to safeguard individuals' privacy. These methods offer high security for safeguarding personally identifiable information (PII).

3.1 Differential Privacy

Differential privacy is a mathematical approach to protecting people whose data is utilized in datasets. It provides privacy when studying and exchanging data. To guarantee individual privacy, different processes are utilized, including the LaPlace mechanism, the Gaussian mechanism, and the exponential strategy (for non-numeric inquiries).

3.2 Homomorphic Encryption (HE)

Homomorphic encryption (HE) is a kind of encryption that enables computation on encrypted material without first decrypting it. This allows secure data processing in untrustworthy contexts while maintaining data privacy throughout the computing process. In encryption, Plaintext data is encrypted using an encryption technique, and a key is generated. Using this key one can convert this ciphertext into plaintext. In HE, you may conduct operations on encrypted data that correspond exactly to operations on plaintext data.

3.3 Generative Adversarial Networks (GANs)

Generative adversarial networks (GANs) are made up of two neural networks, the generator and the discriminator, which are trained concurrently using an adversarial process. This approach generates realistic synthetic data by understanding the original data's underlying patterns. GANs generating network generates synthetic data samples from random noise. In addition, the discriminator network assesses the legitimacy of the data samples.

3.4 Federated Learning (FL)

Federated Learning is a decentralized machine learning strategy in which several devices collaborate to build a model without sharing local data. Rather of sending raw data to a centralized server, each device trains a model locally and only shares model changes. This reduces the risk of the individual's data being exposed to others. These changes are then combined to create a global model that protects data privacy and security.

4. Methodology

4.1 Define the Research Scope

4.1.1 Objective: The main objective of this review paper is to compare AI-driven anonymization techniques, evaluate their effectiveness in protecting personal data, and provide a balance view of their strengths and weaknesses.

4.1.2 Research Questions:

- HowdoDifferential Privacy, Homomorphic Encryption, GenerativeAdversarial Networks, and Federated Learning keep personal information safe?
- What are the advantages and disadvantages of each technique?
- What are the challenges faced by these techniques?
- how businesses and organizations can successfully employ these strategies to safeguard individuals' privacy?

4.2 Literature Search Strategy

4.2.1 Source Identification:

- **Academic Databases:** IEEE Xplore, SpringerLink, ResearchGate, GoogleScholar, arXiv (Cornell University library).
- **Journals and conferences:** Computer law and security Report, Communications in computer & Information science, Journal of Econometrics, Machine Learning and Knowledge Extraction, IEEE Signal Processing Magazine.

4.2.2 Search Keywords:

- **"Differential Privacy"**
- **"Homomorphic Encryption"**
- **"Generative Adversarial Networks for Anonymization"**
- **"Federated Learning"**
- **"AI-Driven Anonymization techniques"**

4.3 Presentation of Findings

4.3.1 Structured Review:

- **Introduction:** Context and importance of protecting personal data , introduction to AI-driven anonymization techniques, and objective of the review.
- **Literature Review:** Provides a summary about the relevant work done in the AI-Driven anonymization techniques and gaps.
- **Methodology:** Detailed explanation of the literature search strategy, Research scope, and Presentation of findings.
- **AI-Driven Anonymization Techniques:** Provides a detail understanding of AI-driven anonymization techniques and comparison of them.
- **Challenges faced by AI-driven anonymization techniques:** Explains the challenges faced by AI-driven anonymization techniques in implementing, effectiveness, computational costs, etc.
- **Conclusion:** Summary of the main findings, recommendations for researchers and practitioners, and suggestions for future research.

5. Challenges Faced by AI-Driven Anonymization Techniques

5.1 Differential Privacy

- Data quality can be lowered by adding noise to data or query results in order to protect privacy, which will reduce the data's usefulness for analysis and machine learning activities. Striking the correct balance between data utility and privacy protection is still quite difficult.
- Correctly implementing differential privacy necessitates giving the privacy budget and query sensitivity considerable thought. Misconfiguration may result in unneeded data utility loss or inadequate privacy protection.
- The effectiveness of privacy protection may be progressively diminished by cumulative privacy loss resulting from repeated inquiries or analyses on the same dataset.
- Large datasets and complicated queries, which can be slow and computationally demanding, require the noise addition process to scale.

5.2 Homomorphic Encryption

- Fully Homomorphic Encryption (FHE) is sluggish and computationally expensive, making it unsuitable for real-time applications even if it permits arbitrary calculations on encrypted data.
- Although partial and partially homomorphic encryption systems are more effective, their utility is limited because they only support a limited number of operations.
- It is crucial and difficult to securely distribute and manage encryption keys, particularly in decentralized contexts.
- Large-scale data environments and high-frequency data streams can exacerbate the performance limitations of homomorphic encryption.

5.3 Generative Adversarial Networks

- It is difficult to generate diversified, high-quality synthetic data that preserves privacy while properly representing the original information. Analysis results that are misleading can be caused by low-quality synthetic data.
- GANs can suffer from mode collapse, where the generator produces limited varieties of outputs, failing to capture the full diversity of the original data.
- Re-identification problems could arise from GANs producing data that is overly similar to real data if they are not appropriately handled.
- Much processing power and resources are needed for GAN training, which might be prohibitive for many businesses.

5.4 Federated Learning

- Federated learning requires frequent communication between local devices and a central server to aggregate model changes, which results in significant communication costs and delay.
- Data shared across multiple devices might differ greatly in terms of quality and distribution, making it difficult to train a globally consistent model.
- Even if raw data is not shared, model updates might nonetheless reveal critical information via gradient adjustments. It is difficult to ensure strong privacy safeguards, such as differential privacy, in federated learning.
- Local devices involved in federated learning may have limited compute power and battery life, limiting their capacity to participate efficiently to the model training procedure.

6. Conclusion

This review study investigated AI-Driven Anonymization techniques' significance in protecting personal data. primarily focuses on the four aspects of privacy protection, data utility, computational efficiency, and robustness of these techniques. Every technique has distinct strengths and limitations, making it appropriate for a variety of scenarios. Differential Privacy is appropriate for circumstances that require tight privacy assurances, whereas Homomorphic Encryption is best for secure computing on sensitive data. GANs provide a versatile method for creating anonymised datasets, whereas Federated Learning provides a scalable solution for privacy-preserving model training across several data sources.

In practice, organisations should use a hybrid approach, using the capabilities of numerous strategies to provide maximum privacy and utility. For example, integrating Differential Privacy with Federated Learning can improve privacy in decentralised contexts, whereas combining Homomorphic Encryption with GANs helps safeguard sensitive data throughout the synthetic data creation process.

6.1 Suggestions for Future Research Directions

Future research should concentrate on increasing the computational efficiency and scalability of these techniques, creating rigorous ways to assess the privacy and value of anonymized data, and investigating unique hybrid approaches. Additionally, standardized criteria and evaluation frameworks are required to assist the comparative assessment of anonymization techniques.

7. References

1. C. Tikkinen-Piri, A. Rohunen, and J. Markkula, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies," *Computer Law and Security Report/Computer Law & Security Report*, vol. 34, no. 1, pp. 134–153, Feb. 2018, doi: 10.1016/j.clsr.2017.05.015.
2. A. Pawar, S. Ahirrao, and P. P. Churi, "Anonymization Techniques for Protecting Privacy: A Survey," Nov. 2018, doi: 10.1109/punecon.2018.8745425.
3. P. Lison, I. Pilán, D. Sanchez, M. Batet, and L. Øvrelid, "Anonymisation Models for Text Data: State of the art, Challenges and Future Directions," Jan. 2021, doi: 10.18653/v1/2021.acl-long.323.
4. D. Narula, P. Kumar, and S. Upadhyaya, "Privacy Preservation Using Various Anonymity Models," in *Advances in Intelligent Systems and computing*, 2018, pp. 119–130. doi: 10.1007/978-981-10-8536-9_13.
5. L. Bolognini and C. Bistolfi, "Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation," *Computer Law and Security Report/Computer Law & Security Report*, vol. 33, no. 2, pp. 171–181, Apr. 2017, doi: 10.1016/j.clsr.2016.11.002.
6. Y. Hu *et al.*, "SoK: Privacy-Preserving Data Synthesis," *arXiv.org*, Jul. 05, 2023. https://arxiv.org/abs/2307.02106
7. H. Hukkelås, R. Mester, and F. Lindseth, "DeepPrivacy: A Generative Adversarial Network for Face Anonymization," in *Lecture notes in computer science*, 2019, pp. 565–578. doi: 10.1007/978-3-030-33720-9_44.
8. F. Liu, "A Statistical Overview on Data Privacy," *arXiv (Cornell University)*, Jan. 2020, doi: 10.48550/arxiv.2007.00765.
9. N. Grislain and J. Gonzalvez, "DP-XGBoost: Private Machine Learning at Scale," *arXiv (Cornell University)*, Jan. 2021, doi: 10.48550/arxiv.2110.12770.
10. H. Jiang, Y. Gao, S. M. Sarwar, L. GarzaPerez, and M. Robin, "Differential Privacy in Privacy-Preserving Big Data and Learning: Challenge and Opportunity," in *Communications in computer and information science*, 2022, pp. 33–44. doi: 10.1007/978-3-030-96057-5_3.
11. L. E. Haourani, A. A. E. Kalam, and A. A. Ouahman, "Big Data security and privacy techniques," Mar. 2020, doi: 10.1145/3386723.3387841.
12. OliverH. Lowry, NiraJ. Rosebrough, A. L. Farr, and RoseJ. Randall, "PROTEIN MEASUREMENT WITH THE FOLIN PHENOL REAGENT," *Journal of Biological Chemistry/the Journal of Biological Chemistry*, vol. 193, no. 1, pp. 265–275, Nov. 1951, doi: 10.1016/s0021-9258(19)52451-6.
13. X. Bi and X. Shen, "Distribution-invariant differential privacy," *Journal of Econometrics*, vol. 235, no. 2, pp. 444–453, Aug. 2023, doi: 10.1016/j.jeconom.2022.05.004.

14. S. T. Arasteh *et al.*, "Preserving fairness and diagnostic accuracy in private large-scale AI models for medical imaging," *Communications Medicine*, vol. 4, no. 1, Mar. 2024, doi: 10.1038/s43856-024-00462-6.
15. M. Senekane, "Differentially Private Image Classification Using Support Vector Machine and Differential Privacy," *Machine Learning and Knowledge Extraction*, vol. 1, no. 1, pp. 483–491, Feb. 2019, doi: 10.3390/make1010029.
16. A. A. Ding, S. S. Wu, G. Miao, and S. Chen, "Reducing Noise Level in Differential Privacy through Matrix Masking," *arXiv (Cornell University)*, Jan. 2022, doi: 10.48550/arxiv.2201.04211.
17. F. Mireshghallah, M. Taram, P. Vepakomma, A. Singh, R. Raskar, and H. Esmaeilzadeh, "Privacy in Deep Learning: A Survey," *arXiv (Cornell University)*, Jan. 2020, doi: 10.48550/arxiv.2004.12254.
18. T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50–60, May 2020, doi: 10.1109/msp.2020.2975749.