Privacy-Enhancing Technologies in Collaborative Healthcare Analysis

Manar

[1]School of Computer Science and Informatics, Cardiff University [2]Self-Development

Published: 22 April 2025

Abstract

Healthcare data is often fragmented across different institutions, such as hospitals, clinics, and research centers, resulting in data silos. Privacy-enhancing technologies (PETs) play a crucial role in collaborative healthcare analysis by enabling healthcare providers to enhance care while protecting patient privacy. PETs offer a compliant framework for data sharing and research that adheres to strict regulations like HIPAA and GDPR. This survey investigates PETs in the healthcare industry, exploring privacy requirements and challenges specific to the field, and reviewing recent research trends and AI-related concerns.

1 Introduction

The digitization of health and patient data is significantly altering clinical, operating, and business models, and there has been a substantial increase in the volume of collected, stored, and processed data. The US International Data Corporation (IDC) predicted that by 2025, the amount of data created globally will reach approximately 163 zettabytes. This growth, coupled with a vast number of connected devices, raises significant concerns about security and privacy. While these changes have improved patient care and reduced costs, they also increase the probability of security and privacy breaches. According to Statista, the healthcare industry is highly vulnerable to cybercrime and was the most targeted sector in the US by cyber-attacks in 2023. These findings highlight the critical need for healthcare providers to adopt more proactive cybersecurity strategies. In response, techniques known as PETs have emerged to mitigate privacy threats and enable data sharing and preservation. This work aims to provide an overview of PETs in healthcare and identify future research opportunities.

2 Related Works

Numerous surveys have examined various aspects of PETs in fields such as AI and IoT, providing a detailed understanding of their evolution and trends. This paper systematically reviewed literature from major databases like ScienceDirect, IEEE Xplore, and Google Scholar, focusing on peer-reviewed studies from 2018-2024 that apply PETs and offer empirical insights.

2.1 Summary of Existing PET Methods

The document includes a summary table of existing works on PET methods, which I will recreate here using a `tabularx` environment. This table highlights the methods, strengths, and limitations of various studies.

Ref.	**Methods**	**Strengths**	**Limitations**
[?]	Various PETs/IoT area	Investigate privacy issues in wearable IoT health devices and review international guidelines and laws	Not specified in this part of the document
[?]	Various PETs	Classified PETs into three groups and eight categories	Point out which PETs best fit each personalized service category
[?]	Various PETs	Defined the legal foundation of PETs and provided a classification and selection of relevant PETs	Economic, social and usability aspects of PETS
[?]	Federated Learning/Healthcare	Design a privacy-preserving system named ADDETECTOR with assistance of IoT devices	Discover more effective features and evaluate feasibility on a larger dataset

3 Privacy Requirements and Challenges in Healthcare

Modern healthcare systems rely on technologies like IoT and cloud computing to collect and analyze sensitive health data, which raises significant privacy concerns. Protecting this data is as essential as providing quality healthcare services. The document identifies several key requirements and challenges for patient data privacy in healthcare IoT systems:

- **Content Privacy**: Ensures and preserves patient data to prevent attackers from revealing it.
- **Contextual Privacy**: Involves using pseudonyms to replace real identities (pseudonymity) and ensuring patient identities are unidentifiable from their data or actions (anonymity).

These requirements can be further categorized into regulatory, ethical, and technical requirements. Key challenges include health data security, consent management, data interoperability, and legal compliance.

4 Key Enabling Privacy-Enhancing Technologies (PETs)

This section provides an overview of key PETs that can be used to mitigate privacy attacks.

4.1 Data Minimization

Data minimization is the principle of collecting and using only the personal data necessary for a specific purpose. It is a core principle of regulations like GDPR, HIPAA, and CPRA. The goal is to limit data collection and retention to the minimum necessary for purpose-specific use and sharing.

4.2 Federated Learning (FL)

Federated learning is a powerful machine learning approach for protecting data privacy. It trains models on decentralized data without sharing the raw data. Instead, only local models are updated and exchanged between a parameter server and clients. This approach ensures the security of sensitive data and minimizes the risk of unauthorized access. FL is particularly useful in healthcare, where patient privacy is crucial.

4.3 Homomorphic Encryption (HE)

HE allows computations on encrypted data without first decrypting it. It uses public-key cryptography to ensure that identical operations on encrypted and decrypted data yield equivalent results. A significant limitation of Fully Homomorphic Encryption (FHE) is its high computational overhead and large storage requirements. HE is one of the most advanced PETs, but it's not yet capable of covering all real-world use cases.

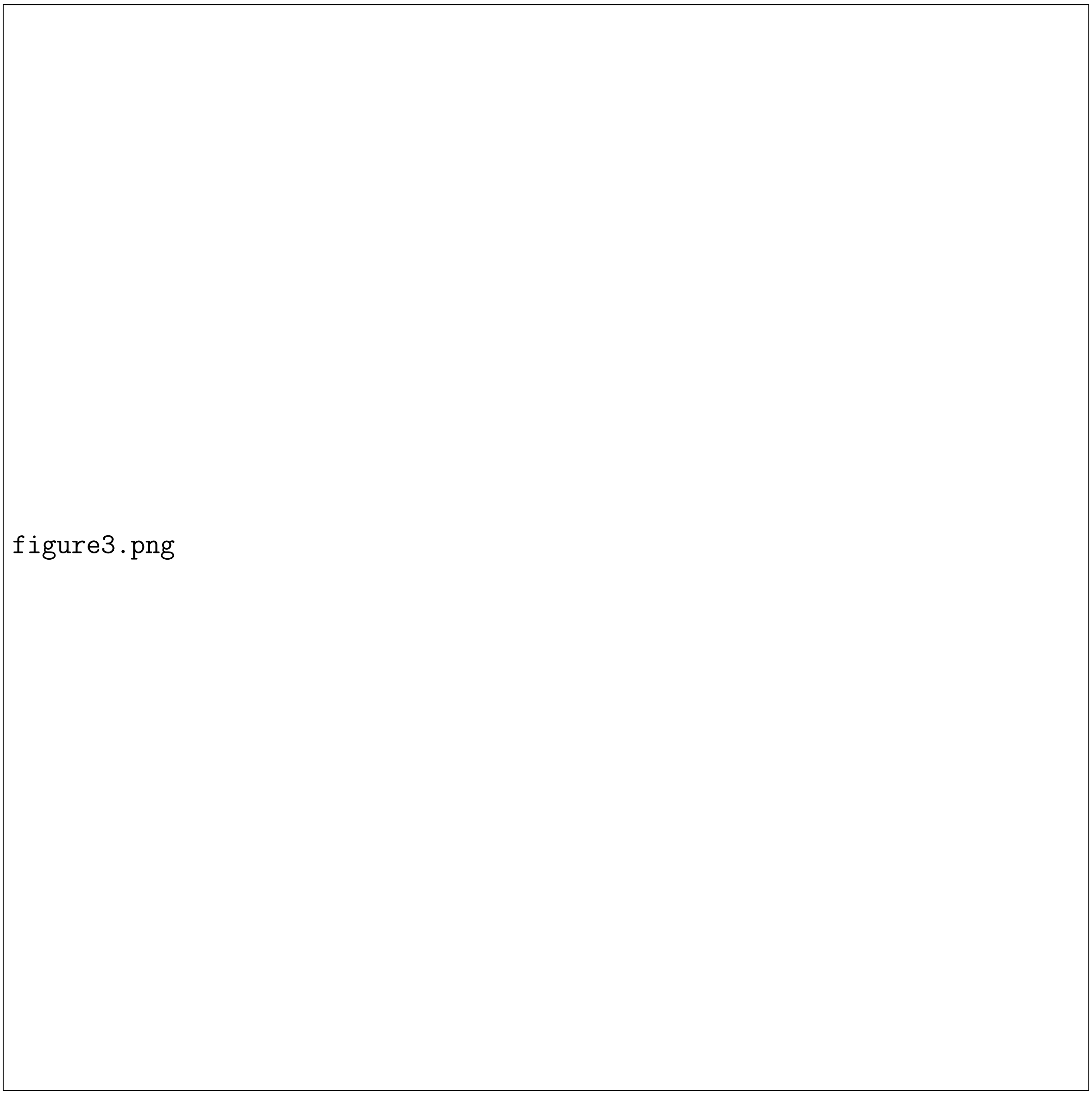

Figure 1: Privacy Requirements and Challenges in Healthcare industry. (a) Essential Privacy requirements; (b) Key challenges.

4.4 Anonymization

Data anonymization uses various techniques to protect private information during data collection by removing, altering, or encrypting identifiers that could reveal identities. It is a mature technology with high usability and is widely accepted. However, insufficient anonymization can lead to re-identification attacks, particularly in healthcare. Anonymization technologies can be categorized into syntactic and semantic groups.

5 Conclusion

This report has surveyed privacy-enhancing technologies (PETs) and their applications in collaborative healthcare analysis. It has highlighted the growing need for robust privacy solutions due to the increasing digitization and fragmentation of healthcare data. The document reviewed key PETs, including Data Minimization, Federated Learning, Homomorphic Encryption, and Anonymization, and discussed the privacy requirements and challenges specific to the healthcare industry. These insights can help guide future research to enhance privacy in healthcare.

References

[1] Alnasser, M.; Li, S. Privacy-Enhancing Technologies in Collaborative Healthcare Analysis. *Cryptography* **2025**, 9, 24.

[2] Kaaniche, M.; Ben-Othman, J. Privacy-Preserving Techniques. *IEEE Trans. Depend. Secur. Comput.* **2020**, 17, 185-199.

[3] Liu, X.; et al. Privacy-Preserving Federated Learning: A Survey. *IEEE Access* **2020**, 8, 14317-14334.