Article

Not peer-reviewed version

ppAIsec: Privacy-Preserving Artificial Intelligence Models in Healthcare Security—A Synthesis of AI Frameworks

Tanzina Sultana , Asura Akter Sunna , Mohammed Majbah Uddin , Naresh Kshetri *

Posted Date: 5 January 2026

doi: 10.20944/preprints202601.0250.v1

Keywords: artificial intelligence; privacy preserving AI frameworks; healthcare security; AI learning models

 doi:10.20944/preprints202601.0250.v1

Article

ppAIsec: Privacy-Preserving Artificial Intelligence Models in Healthcare Security—A Synthesis of AI Frameworks †

Tanzina Sultana [1], Asura Akter Sunna [2], Mohammed Majbah Uddin [3] and Naresh Kshetri [4,*]

[1] Tanzina Sultana, University of the Cumberlands, Williamsburg, KY, USA
[2] Asura Akter Sunna, Emporia State University, Emporia, KS, USA
[3] Mohammed Majbah Uddin, Clinical & Trans. Science Inst., Univ. of Florida, FL, USA
[4] Naresh Kshetri, Department of Cybersecurity, Rochester Institute of Technology, NY, USA
* Correspondence: kshetrinaresh@gmail.com

† This paper is submitted and accepted at IEEE 5th ICIAC 2026.

Abstract

As artificial intelligence (AI) technologies, particularly generative and collaborative learning models— are increasingly integrated into healthcare and other sensitive domains, data privacy, security, and fairness concerns have grown significantly. This paper focuses on a thorough examination of current privacy-preserving AI models, including federated learning (FL), differential privacy (DP), homomorphic encryption, and generative adversarial networks (GANs). Key contributions are reviewed across recent works that explore privacy-preserving mechanisms within domains such as clinical diagnostics, drug discovery, Internet of Medical Things (IoMT), and virtual health systems. Dynamic federated models (e.g., DynamicFL) that adjust model architecture based on computational heterogeneity and encryption-augmented FL architectures are presented to maintain data locality while ensuring equitable performance. GAN-based synthetic data generators (e.g., medGAN, CorGAN) offer alternative solutions to share healthcare data without compromising patient identity and introducing new threats if misused. Across these models, a multi-phase life cycle of threats is identified—spanning data collection, model training, inference, and system integration—highlighting the importance of proactive governance. Information compliance frameworks such as the EU AI Act and the U.S. AI Bill of Rights are counting for standardizing technological implementation in healthcare data management. This research work will cover explaining existing AI models and trying to identify the best one worked for ensuring data privacy and shareability with ethical responsibility for proposing a layered privacy-preservation paradigm essential for safely deploying AI in sensitive environments.

Keywords: artificial intelligence; privacy preserving AI frameworks; healthcare security; AI learning models

1. Introduction

Artificial Intelligence (AI) is reshaping the contemporary healthcare system through enhancement in patient monitoring, clinical decision-making and improving diagnosis. These advancements depend mostly on a big volume of sensitive medical data, which leads to a growing concern about privacy, security, and regulatory compliance. AI in healthcare brings transformative benefits from improving precision, reducing disparities, and empowering clinicians and patients to enhance discovery and decision-making, while still requiring careful navigation of technological, regulatory, and societal challenges to ensure its responsible and effective integration [1]. Uses of AI tools in health care must be continuously improved, ethically governed, and validated by experts to ensure safe and effective use in patient care [2].

 doi:10.20944/preprints202601.0250.v1

While use of AI in modern healthcare is being evident, preserving privacy in AI is also becoming a major concern. Deep learning systems have the potential to inadvertently memorize patient data which raises the risk of data breaches and unintentional exposure of sensitive patient data. Researchers are currently studying multiple privacy-preserving AI methods, including federated learning, differential privacy, homomorphic encryption, blockchain architectures, and synthetic data generation through GANs. In order to maintain openness and confidence in clinical settings, explainable AI (XAI) techniques such as SHAP which offers both global and local explanations and LIME which focuses solely on local explanations are increasingly gaining importance. Despite advancements, privacy leaks, inconsistent medical data, and low interpretability remain problems for current models. These weaknesses show that a more comprehensive strategy for healthcare AI security is required. In addition to reviewing recent research on PPAI techniques, this paper presents the PPAI Framework, a conceptual paradigm intended to detect risks, implement privacy-preserving techniques, and improve the security of AI and IoMT systems in healthcare.

This paper presents a in depth analysis of privacy-preserving AI models in healthcare in several key areas. The literature review section showcases recent insightful research on federated learning, blockchain-based security, synthetic data generation, explainable AI, and IoMT-driven systems, while highlighting persistent issues with interoperability, validation, and privacy protection. The growing risks of centralized AI models—such as data memorisation, reidentification vulnerabilities in GAN-generated synthetic data, limited explainability, and regulatory pressures like HIPAA and GDPR—are highlighted in the research problem section. The methodology section describes a qualitative approach that acknowledges the limitations associated with secondary data sources. This paper evaluates cutting-edge PPAI techniques and legal frameworks across clinical diagnostics, drug discovery, IoMT, prevention management and digital health. The proposed PPAI framework provides an integrated model composed of raw healthcare data processing, threat identification phases, core privacy-preserving mechanisms (GANs, FL, DP, HE), and safety tasks to enhance security , accessibility, and visibility. The PPAI framework is ultimately positioned as a feasible, future-centric solution for safe and reliable AI in healthcare. The analysis and results show that effective healthcare privacy depends on combining multiple protective strategies, aligning AI workflows with regulatory and ethical standards.

2. Literature Review

Researchers conducted experiments on arrhythmia databases and proposed a mechanism for reducing the probability of patient medical data reconstruction [3]. Authors preserved patient's privacy while using the data to train local disease diagnosis models. Federated Learning (FL) along with new technologies, such as Cloud Computing, Internet of Things (IoT), Internet of Medical Things (IoMT) and use of AI, highly penetrate the healthcare and medical industry. Either to save the medical costs or to combat the increasing death every year, a high percentage of global healthcare have implemented IoT solutions.

Another study in AI-based healthcare systems, [4] to improve security and safety via the use of blockchain technology was conducted. Authors proposed an AI-based healthcare blockchain model, healthAIchain, to delve into safety and security improvement in AI-based healthcare with implementing blockchain. While retaining critical data of medical patients, the highest security standards, blockchain can promote configurable openness. There is a compelling need for new frameworks to ensure safety and security as AI in healthcare traverse through emerging challenges.

Review by authors emphasizes several solutions to overcome cross-disciplinary challenges for AI data pipelines [5]. The progress in generative AI-driven applications for privacy-preserving data as the pharmaceutical sector is confronted with development and drug discovery challenges. Out of several issues, some of them are experimental workflows incorporation, validation of new molecular entities, and interoperability of results generated by AI. Privacy-preserving strategies into real-world AI systems and comparing their adaptability, scalability, and performance across various AI contexts using federated learning are done by researchers.

 doi:10.20944/preprints202601.0250.v1

Researchers introduced a healthcare model, HNMblock [6] for wellness enhancement, medical systems security, and epidemiological monitoring. The integration of a decentralized approach with compelling solutions from blockchain technology (with power of immutability and transparency within the nodes) helps to formulate the new healthcare model. The model also encourages patient involvement and data-informed decision making in light of widespread adoption of wearable technologies and Internet of Medical Things (IoMT) to combat the current issues of healthcare data regulations and security challenges.

A systematic evaluation and review of AI algorithms and techniques is conducted by the authors [7] to support sustainable practices in patient outcomes and diagnostic accuracy. The proposed integration framework provides a foundational guide to build energy-aware, high-performance AI systems in healthcare in resource constrained healthcare environments. Three groups of AI tools and algorithms by the researchers - (i) explicit AI algorithms for energy efficiency sustainability (e.g., Hybrid Quantum Classical Optimization, Federated Learning), (ii) traditional AI algorithms for sustainable healthcare (e.g., Bi-LSTM, BPNNs, CNNs), and (iii) sustainable AI techniques that support low power computing (e.g., AutoML for Model Compression).

3. Research Problem

Artificial Intelligence practice in the healthcare sector has yielded significant improvements in clinical decision-making, predictive diagnosis, and personalized treatment. The AI system relies on sensitive patient data and health records. As such, sharing patient data poses a significant risk to privacy and security, especially with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) in effect. With the traditional AI model, where centralized data aggregation is required, risks such as data breaches and unauthorized access are on the rise.

As a consequence of the introduction of a deep learning model for healthcare data, patients' traditional deep neural networks unintentionally memorize data used in providing trials, and that data later becomes available to unauthorized users. Here, [8] proposed an adaptive differentially private deep learning algorithm; this algorithm applies minimizing Gaussian noise linearly to gradients during training, instead of a constant noise scale, which can be detectable. They also adopt truncated concentrated differential privacy (tCDP) approach, which provides a tighter and more explicit privacy bound compared to TensorFlow's moments accountant approach. The study highlights that fixed-noise approaches, such as TensorFlow Privacy's DPSGD, can cause poor model utility in healthcare. Their adaptive approach mitigates this, but the trade-off between privacy and accuracy remains an ongoing challenge.

Additionally, the Generative Adversarial Network machine learning algorithm is used to reduce the risk of exposing patients' original data through mixing it with synthetic EHR data that approximates the statistical distributions of real data, according to [9]. Challenges increase when sharing or using sensitive healthcare data for machine learning while preserving patients' privacy. In EHR data access is often restricted due to legal or compliance requirements; to overcome this situation, generating synthetic data could be an alternative to obtaining permission. In medical machine learning, the model is trained using synthetic patient data that closely resembles the original data. The author in this research work proposed a privacy-preserving GAN model that can generate synthetic EHR data, which is both. High quality in terms of capturing the statistical properties of the original data. Privacy preserving in the sense of limiting the risk of reidentification or membership inference.

Explainable AI (XAI) refers to an artificial intelligence system that is responsible for decision-making processes that are transparent, interpretable, and understandable to humans, particularly clinicians, patients, and regulators. XAI addresses this problem by employing specialized techniques that open the black box and reveal the reasons behind each prediction. This method directs the application of features towards people's realization (like blood pressure, age, or X-ray image areas) that affect the AI's decision and by how much. In healthcare, this is crucial because AI models

 doi:10.20944/preprints202601.0250.v1

influence life-critical decisions such as diagnosis, treatment, and prognosis. According to [10], AI is becoming a common practice in healthcare for storing and analyzing data, as well as supporting disease diagnosis, risk prediction, and decision-making for doctors.

As the use of AI is expanding at a rapid pace, many AI systems are still in the innovation stage and operate like a black box. These systems provide results that people cannot easily understand. Explainable AI (XAI) makes AI decisions clear and understandable to doctors and patients. The authors [10] reviewed 100 studies to examine the application of XAI in healthcare. The most identifiable six methods are feature-based methods, such as SHAP (features infused in the result), global methods that explain how the model works overall, concept models that mimic a complex model, pixel-based models used for medical images, and a human-centric approach that focuses on explanations of results. The review revealed that most medical AI systems employ methods such as SHAP and LIME to explain predictions derived from patient data or medical images.

Table 1. Application of XAI in healthcare [10].

Method	Privacy / Governance Role	Explanation Use in EHR
SHAP (Shapley Additive Explanations)	Provides local feature attribution without exposing complete patient data; it supports differential privacy by summarizing influence weights.	Used in Parkinson's Disease EHR, heart-disease prediction, and sepsis-risk models; highlights feature contribution (age, vitals, medications) without direct identifier exposure.
LIME (Local Interpretable Model-agnostic Explanations)	Generates synthetic perturbations rather than using actual patient data → protects individual records.	Applied to Hepatitis and Glioblastoma models; can be adapted for EHR auditing and anonymized explainability.
Grad-CAM / CAM	Visual heatmaps limited to non-textual data; for EHR, can visualize tabular feature "importance maps."	Used primarily for imaging; can complement tabular EHR dashboards.
PDP (Partial Dependence Plots)	Summarizes feature effects globally; safe for publication because results are aggregated.	Useful in population-level EHR risk modeling.
Human-Centric Explanations & Surrogate Models	Incorporate clinician feedback; ensures explainability aligns with data-use consent under HIPAA / GDPR.	Supports informed decision and ethical transparency.

According to [10], It is challenging to create models that are both accurate and easy to explain, and there are no standard rules for evaluating the quality of an explanation. Doctors also prefer visual explanations, whereas data scientists tend to prefer mathematical ones. Another significant concern is maintaining patient data privacy and security, particularly when AI systems utilize extensive amounts of sensitive medical information.

RP I. As TensorFlow model, introduced by the Google Brain team, this is a versatile machine learning library; however, its design basis focuses on scalability instead of privacy. This leads to vulnerability to data exposure during data preparation, training, or inference when external privacy layers are not added.

RP II. Risk of not complying with HIPAA compliance, which is mandatory in the healthcare industry. TensorFlow provides AI as a service; however, a third-party service does not comply with regulatory concepts.

 doi:10.20944/preprints202601.0250.v1

RP III. Lack of domain-specific constraints - In real EHR data, data is collected from different domains, where the GAN model generating synthetic data can have limitations of medical logic, correlations, consistency, missing data patterns, and longitudinal dependencies.

RP IV. In the GAN Model, creating EHR synthetic data based on real-life data, proposed defense strategies are broad without quantitative or theoretical guidance; it is unclear how to choose parameters or design those defenses in practice. In total, naive design on synthetic data generation models through GAN can be a point of vulnerability.

4. Methodology

The research methodology we use in this study is qualitative, and it synthesizes existing privacy preserving AI models drawing insights from state-of-the-art techniques, including federated learning (FL), differential privacy (DP), homomorphic encryption, and generative adversarial networks (GANs). It attempts to comprehend the implications and current state of AI preserving models in different healthcare domains such as clinical diagnostics, drug discovery, Internet of Medical Things (IoMT), and virtual health systems. It reviews and compliments the findings of the previous literature that was done in this area, specially using Explainable AI (XAI), SHAP AND LIME model in clinical decision making particularly in disease prediction. This research considers the legal guidelines of Information compliance frameworks such as the EU AI Act and the U.S. AI Bill of Rights directives in technological implementation in healthcare data management. The secondary data was analyzed about experiments on arrhythmia databases and uses of broad ranges of Information technology in healthcare and the proposal of HealthAIchain, a dedicated blockchain technology for healthcare to ensure privacy and safety of the patient data. In this paper we identified how existing AI models pose multifaceted life cycles of threat in the widely used GAN-based synthetic data generators. Additionally, we have proposed a framework: PPAI framework that included Basic PPAI model, threat identification, raw healthcare data, and safety tasks analyzing all existing AI frameworks. The limitation of this research is its reliance on published models and secondary data, which may not fully capture real-world ever changing privacy risks or implementation challenges in diverse healthcare domains.

5. Proposed Framework - PPAI Framework

As usage of AI is growing every day, we have proposed the PPAI conceptual model (Privacy-Preserving AI model) for healthcare security and IoMT security. We have identified several threats for several phases that help in determining the safety tasks for the same. The four primary components of the PPAI models are (a) raw healthcare data, (b) threat identification, (c) Basic PPAI model, and (d) safety tasks.

a. **Raw healthcare data** - Several raw healthcare data (images data, speech data, text data, and other data) via data collection for system integration and training of the proposed model, PPAI model (privacy-preserving AI model) for healthcare security and IoMT security.

b. **Threat identification** - One of the important phases in our multi-phase model for identification of potential threats as healthcare is the most attacked domains by attackers. Based on the training and processing of the raw healthcare data, we identified threats from 1 to N from Phase P_1 to Px.

c. **Basic PPAI model** - As stated before, our conceptual PPAI model (privacy-preserving AI model) for healthcare security contains generative adversarial networks (GANs with synthetic data generators as medGAN, corGAN etc.), with dynamic federated learning models (Dynamic FL), along with differential privacy (DP) including homomorphic encryption.

d. **Safety tasks** - Numerous safety tasks being pointed out from Safety Task T1 to Safety Task Tn, as part of PPAI model (privacy-preserving AI model) with identification of best one for ensuring data privacy and shareability. As the integration of learning models and AI technologies continue, concerns of data privacy and security have grown.

 doi:10.20944/preprints202601.0250.v1

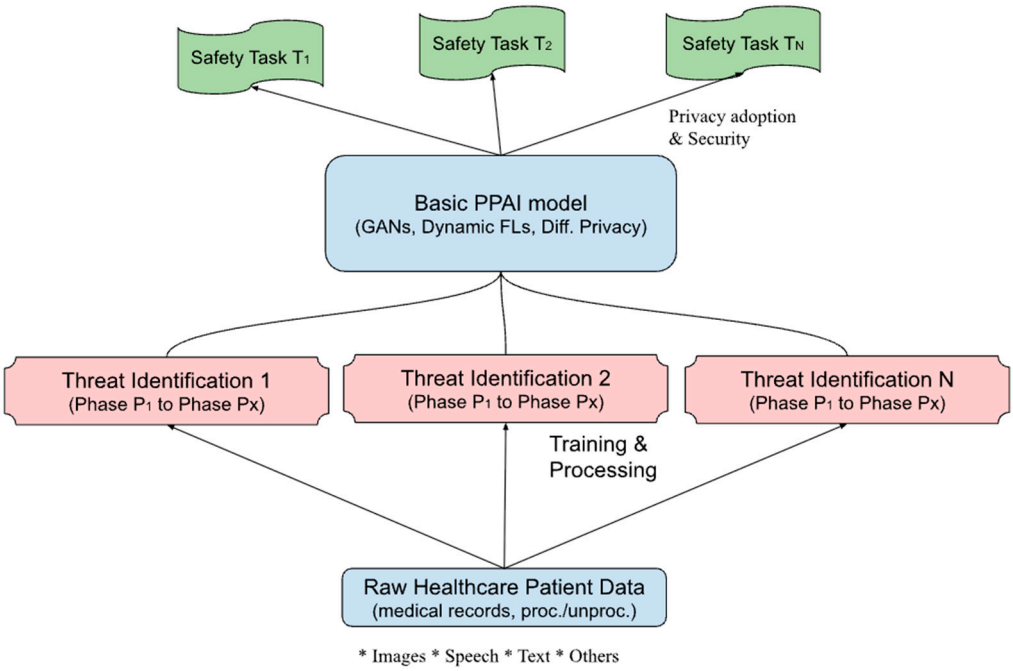

Figure 1. Proposed conceptual framework, PPAI (Privacy-Preserving AI model) for Healthcare and IoMT security.

6. Analysis and Findings

Our investigation indicated that privacy-preserving AI in healthcare works best when diverse techniques are appropriately integrated together. Federated learning can help keep data at its source, but it cannot ensure complete privacy on its own. Adding measures like differential privacy and secure encryption reduces the chance of personal data leaking, even during collaborative model training. Although generative models, like GANs, enable the sharing of synthetic data for research, they still carry the risk of reidentification if they are not robustly developed, so further precautions must be taken when applying them to delicate health situations.

We also find the ongoing conflict between data utility and privacy in real-world healthcare contexts, such as hospitals and IoMT networks. The most effective systems—like the conceptual PPAI model proposed in our research—adapt to technical, legal, and practical threats at each stage. These cover integrating compliance frameworks (like HIPAA and GDPR), explainable AI (like SHAP and LIME), and governance controls into a single workflow.

Finally, our results indicate that strong privacy protection and meaningful explainability can be achieved together, not "either-or." Healthcare practitioners need to trust and interpret AI judgments, thus transparent, well-designed explanations must be embedded from the start—not just added as an afterthought. By basing our approach on these industry-tested tactics and aligning it in today's compliance standards, the proposed PPAI framework offers a viable, future-ready pathway for keeping healthcare data safe, shareable, and ethically maintained.

7. Conclusion and Future Scope

a. Conclusion

Artificial Intelligence's integration into healthcare systems revolutionized its capacity of clinical decision-making, diagnosis, and prevention planning. Simultaneously automation intensify concerns regarding patient privacy, data security, and adherence to regulatory compliance [11]. This paper synthesizes current privacy-preserving AI frameworks, examining federated learning, differential privacy, homomorphic Encryption, and Generative adversarial networks, Explainable AI to

 doi:10.20944/preprints202601.0250.v1

identify optimal approaches for ensuring data privacy and sharing in sensitive healthcare environments.

Literature review shows that, any individual privacy-preserving technique cannot provide a complete solution. According to [12] effective privacy protection requires a layered, coordinated strategy using different complimentary technologies. Federated learning maintains data locality but remains vulnerable to inference attacks without additional safeguards [8,14]. Differential privacy protection approach provides mathematical guarantees but requires careful calibration to prevent degradation of clinical performance [13]. Whereas Homomorphic Encryption preserves data access confidentiality during processing by limiting computation overhead in real-time applications [15]. GAN framework enables synthetic data generation; however, this approach also has risks when improperly designed.

In the proposed PPAI framework define the limitations of multiple singular framework implementation on the healthcare system. This proposed framework showcases the inefficiency corner of multiple privacy preserving mechanisms across the entire AI lifecycle while incorporating explainable AI (XAI) techniques such as SHAP and LIME to ensure clinical interpretability to enhance general acceptance. According to [10] SHAP is a specific method that provides future attribution without exposing complete patient data alongside LIME protects data through synthetic perturbations. In recent times combining blockchain with XAI have shown promising outcomes in ensuring transparency and trust in healthcare AI systems.

Our proposed framework also emphasizes regulatory compliance with HIPAA, GDPR, the EU AI Act and the U.S. AI Bill of Rights to provide legal and ethical boundaries for ensuring clients and patients privacy. Blockchain technology combined with separate storage of data sources defines healthAIchain and HNMblock. It adds immutability and transparency in decentralized settings that support traditional privacy-protecting methods.

In a nutshell, safe AI implementation in Healthcare demands a holistic approach to balance data visibility and security with privacy protection, clinical interpretability with security and innovation with regulatory compliance. The PPAI framework synthesizes current best practices into a cohesive paradigm essential for ensuring AI enhancement of patient care without compromising confidentiality.

b. Future Research Scope

From this proposed framework towards the next step will be developing dynamically elevated mechanisms to adjust privacy parameters based on data sensitivity, clinical urgency and following regulatory compliance. According to [16] though clinical diagnosis in Breast Cancer achieved 91% success by using AI yet standardized method for privacy perimeter section across diverse healthcare domain is a challenge. GAN architecture ensures data privacy by generating synthetic data however current generative models needs interdisciplinary collaboration to incorporate clinical constraints and longitudinal dependencies.

More research is needed to improve privacy preserving AI for healthcare to reduce risk in patient confidentiality while developing a more reliable, and safe intelligent system. Future research may focus on enhancing privacy-preserving deep learning for medical imaging and developing federated learning to better handle a variety of clinical data. Researchers may also investigate privacy aware large language models that can safely learn from clinical data, as well as secure models for real-time monitoring through IoMT devices. This inclusion of IoMT in healthcare facilities adds vulnerabilities for model inversion and membership inference, attacks, and secure protocols for such devices. More studies are needed for creating interoperable frameworks for safe cross-hospital data sharing. In order to ensure healthcare organizations, adopt AI systems, future research needs to focus on optimizing the balance between privacy and model performances while maintaining regulatory compliance.

The majority of current Privacy-Preserving AI research methods relies on simulated environments where benchmark data sets simulate whole scenarios which are limited for capturing dynamic insights of patients' clinical data. Comprehensive pilot studies on diversified chunks of

 doi:10.20944/preprints202601.0250.v1

datasets should apply to capture distinct cases. Stakeholder centered long-term research on healthcare data to determine how each participant precise and interacts with privacy-preserving AI systems.

References

1. Koski, E. and Murphy, J. (2021) *AI in Healthcare, Studies in health technology and informatics*. Available at: https://pubmed.ncbi.nlm.nih.gov/34920529/
2. Bala, I. ., Pindoo, I. ., Mijwil, M. M. ., Abotaleb, M. ., & Yundong, W. . (2024). *Ensuring Security and Privacy in Healthcare Systems: A Review Exploring Challenges, Solutions, Future Trends, and the Practical Applications of Artificial Intelligence. Jordan Medical Journal, 58(3).* Retrieved from https://jjournals.ju.edu.jo/index.php/JMJ/article/view/2527
3. Wang, X., Hu, J., Lin, H., Liu, W., Moon, H., & Piran, M. J. (2022). Federated learning-empowered disease diagnosis mechanism in the internet of medical things: From the privacy-preservation perspective. *IEEE Transactions on Industrial Informatics*, *19*(7), 7905-7913.
4. Kshetri, N., Hutson, J., & Revathy, G. (2023, December). healthAIChain: Improving security and safety using Blockchain Technology applications in AI-based healthcare systems. In *2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)* (pp. 159-164). IEEE.
5. Mahendra, P., & Verma, A. (2025, June). Privacy-Preserving Data Pipelines for AI: A Comprehensive Review of Scalable Approaches. In *2025 3rd International Conference on Inventive Computing and Informatics (ICICI)* (pp. 350-355). IEEE.
6. Kshetri, N., Mishra, R., Rahman, M. M., & Steigner, T. (2024, April). HNMblock: Blockchain technology powered Healthcare Network Model for epidemiological monitoring, medical systems security, and wellness. In *2024 12th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 01-08). IEEE.
7. Alzoubi, Y. I., Topcu, A. E., & Elbasi, E. (2025). A Systematic Review and Evaluation of Sustainable AI Algorithms and Techniques in Healthcare. *IEEE Access*.
8. Zhang, X., Ding, J., Wu, M., Wong, S. T., Hien, V. N., & Pan, M. (2021). *Adaptive privacy preserving deep learning algorithms for medical data.* https://openaccess.thecvf.com/content/WACV2021/html/Zhang_Adaptive_Privacy_Preserving_Deep_Learning_Algorithms_for_Medical_Data_WACV_2021_paper.html
9. Venugopal, R., Shafqat, N., Venugopal, I., Tillbury, B. M. J., Stafford, H. D., & Bourazeri, A. (2022). *Privacy preserving Generative Adversarial Networks to model Electronic Health Records. Neural Networks, 153, 339–348.* https://doi.org/10.1016/j.neunet.2022.06.022
10. Sadeghi, Z., Roohallah Alizadehsani, Mehmet Akif CIFCI, Kausar, S., Rehman, R., Priyakshi Mahanta, Pranjal Kumar Bora, Almasri, A., Alkhawaldeh, R. S., Hussain, S., Bilal Alatas, Afshin Shoeibi, Hossein Moosaei, Hladík, M., Saeid Nahavandi, & Pardalos, P. M. (2024). *A review of Explainable Artificial Intelligence in healthcare. Computers & Electrical Engineering, 118, 109370–109370.* https://doi.org/10.1016/j.compeleceng.2024.109370
11. Pati, S., Kumar, S., Varma, A., Edwards, B., et al. (2024). Privacy preservation for federated learning in health care. *Patterns*, 5(7), 100974. https://doi.org/10.1016/j.patter.2024.100974
12. Brauneck, A., Schmalhorst, L., Majdabadi, M. M. K., Bakhtiari, M., Völker, U., Baumbach, J., & Baumbach, L. (2023). Federated machine learning, privacy-enhancing technologies, and data protection laws in medical research: Scoping review. *Journal of Medical Internet Research*, 25, e41588. https://doi.org/10.2196/41588
13. Ali, M., Naeem, F., Tariq, M., Kaddoum, G., et al. (2022). Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. *IEEE Journal of Biomedical and Health Informatics*, 27(2), 778-789. https://doi.org/10.1109/JBHI.2022.3181823
14. Ahmed, I., Maddikunta, P. K. R., Gadekallu, T. R., Alshammari, N. K., & Hendaoui, F. A. (2024). Efficient differential privacy enabled federated learning model for detecting COVID-19 disease using chest X-ray images. *Frontiers in Medicine*, 11, 1409314. https://doi.org/10.3389/fmed.2024.1409314
15. Mantey, E. A., Zhou, C., Anajemba, J. H., Arthur, J. K., Hamid, Y., Atif Chowhan, & Obinna Ogbonnia Otuu. (2024). Federated Learning Approach for Secured Medical Recommendation in Internet of Medical

 doi:10.20944/preprints202601.0250.v1

Things Using Homomorphic Encryption. *IEEE Journal of Biomedical and Health Informatics*, *28*(6), 3329–3340. https://doi.org/10.1109/jbhi.2024.3350232

16. Shukla, S., Rajkumar, S., Sinha, A., Esha, M., Elango, K., & Sampath, V. (2025). Federated learning with differential privacy for breast cancer diagnosis enabling secure data sharing and model integrity. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-95858-2