INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

Secure Federated GenAI for Healthcare IoT Networks

Nirup Kumar Reddy Pothireddy

Independent Researcher, India

DOI: https://doi.org/10.51583/IJLTEMAS.2025.140400093

Received: 07 May 2025; Accepted: 08 May 2025; Published: 16 May 2025

Abstract: The combination of Healthcare Internet of Things (HIoT) and Generative Artificial Intelligence (GenAI) has offered an eminent opportunity to develop highly personalized, real-time healthcare offerings. However, the need for data security, cloud dependency, and sensitivity in handling medical information have come in the way of mass adoption. This paper proposes a secure Federated GenAI framework for HIoT networks to allow distributed training and generation of AI models directly on edge devices like wearables and mobile health sensors. By combining federated learning protocols with privacy-preserving mechanisms and generative AI, the system minimizes the need for transmitting raw data to centralized cloud servers. This architecture asserts data sovereignty, minimizes the risk of data breaches, and preserves the performance of models operating across distributed nodes. The experimental evaluation showed the framework achieves competitive accuracy levels for health monitoring tasks along with strong privacy guarantees and communication efficiency. Therefore, our results signal that secure Federated GenAI can be a credible base for developing scalable and ethical AI-driven healthcare systems, particularly in settings that are resource-constrained or laden with regulations.

Keywords: Healthcare IoT (HIoT), Federated Learning, Generative AI, Edge Computing, Data Privacy, Medical AI, Wearable Sensors, Privacy-Preserving Machine Learning, Secure Distributed Systems, Decentralized Health Monitoring

I. Introduction

Background

The rapid evolution of Healthcare Internet of Things (HIoT) has ushered in a new era of intelligent, connected medical systems. Devices such as wearable sensors, implantable monitors, and mobile health platforms are integral to modern day clinical and home-based care by enabling real-time patient monitoring and predictive diagnostics. Such technologies generate vast amounts of sensitive and continuous data, presenting opportunities to improve patient outcomes through reduced healthcare costs and preventive medicine. However, the real utility of HIoT would greatly depend upon utilizing advanced machine learning models to extract actionable insight from this data.

Today, Generative Artificial Intelligence (GenAI)—particularly in GANs, VAEs, and transformer models—represents a leading paradigm for performing medical data augmentation, synthetic record generation, and personalized prediction. The medical applications of GenAI include enhanced reconstruction of images, data synthesis for rare diseases, and strong detection of anomalies in critical vital signs. Nonetheless, the applicability of GenAI to HIoT environments is highly limited due to privacy and regulatory concerns. On centralized AI platforms, raw data is usually forwarded to cloud servers, which introduces the risks of data breaches and non-compliance with various legislations, including HIPAA and GDPR.

Problem Statement

GenAI offers extraordinary promise in the domain of medical intelligence, yet the traditional approach of data processing through centralization stands in direct contrast with the privacy needs and distributed nature of HIoT networks. Offloading data to centralized cloud services create vulnerabilities related to data leakage, unauthorized access, and potential misuse. Additionally, the transmission of sensitive data in large volumes leads to overhead communication and latency hindrances that are critical in healthcare applications where remote access and low-bandwidth are detrimental. Solutions that will scrupulously anonymize or encrypt the data along the transmission path see their potential undermined when it comes to the performance of models or even computational attractiveness.

Objectives

This research proposes the design of a secure federated Generative AI framework for HIoT networks. In this way, the edge devices like smartwatches, biosensors, and health-monitoring wearables would fulfill the tasks of training and generation of AI models locally without raw patient data flowing out of the device. The main objectives of this work are:

To establish a federated learning architecture endowed with capabilities for generative AI, which includes the provision for a decentralized approach to model training and data synthesis.

To enhance data privacy and sovereignty by lessening the dependency on centralized cloud storage.

To ensure that high model accuracy is achieved while encompassing communication and computation constraints.

To assess the viability and performance of the proposed body via benchmark HIoT scenarios and secure protocols for federated training.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

By addressing these objectives, the proposed solution will aim to finally bridge the divide between data-driven innovation and very stringent privacy requirements within the healthcare domain and lead the way for scalable, secure, and ethical AI deployment into HIoT ecosystems.

Literature Review

Federated Learning in Healthcare

Federated learning (FL) being a promising paradigm for privacy preservation in healthcare, allows training of machine learning models across decentralized devices without transferring the actual data. Clinically, this means hospitals and different devices can cooperatively improve a particular diagnostic model, with care being taken to assure the confidentiality of patient-private information. The study by Rieke et al. (2020) clearly points to the practicability of FL in reducing risks of data leakage in sensitive applications, such as cancer detection and radiology, without compromising the model's accuracy. Teo et al. (2023) systematically reviewed FL's applicability to diverse medical disciplines, particularly emphasizing its power when coupled with electronic health records (EHRs). Nonetheless, FL implementation also suffers from several challenges, such as device heterogeneity, communication overhead, and threats of adversarial attacks (Ali et al., 2022).

Generative AI in Healthcare

Generative artificial intelligence models—for example, both GANs and VAEs—have been in the spotlight for the past few years concerning medical data generation and augmentation efforts. The realistic patient data synthesized through these technologies aids not only in model training in scenarios with little data but also with rare diseases. This may indirectly address the problem of class imbalance in diagnostic imaging and health record datasets (Rout, 2023). Furthermore, the use of GenAI in health applications transcends data synthesis into supporting clinical decision-making and personalization; albeit it also poses privacy risk due to its indispensable pooling of patient data in training the given model (Flores, 2021).

Security and Privacy in Healthcare IoT

The HIoT landscape introduces myriad challenges in managing heterogeneous devices while continuously receiving data from patients. Security is a core concern, as wearables and mobile health systems transmit sensitive data wirelessly. Federated learning has now emerged therewith as an avenue to provide mitigation in this domain. According to Patil et al. (2024), the combination of FL and the real-time chronic disease monitoring service will enhance privacy compliance while maintaining clinical usability. On the other hand, Aminifar et al. (2024) showed that federated-edge-based systems could improve mHealth applications with reduced dependency on cloud infrastructure. The introduction of privacy-preserving methods such as differential privacy and secure aggregation are great, but their adoption in real-life scenarios becomes cumbersome due to the consequent overhead in computation and bandwidth (Ali et al., 2022).

Integration of Federated Learning and GenAI

Literature published recently reports on FL developments and GenAI synergy to prepare decentralized AI systems that are privacy-aware. For example, the generalized privacy concern was probably the first task given to GenAI modeling under MedPerf by Karargyris et al. (2023) in this sense: They introduced MedPerf capable of federated benchmarking for medical AI models, with GenAI used to improve data synthesis while upholding privacy. Mosaiyebzadeh et al. (2023) also looked at privacy-enhancing technologies (PETs) in federated GenAI systems, showcasing an increase in customers feeling global and well-mannered to align generative capabilities with decentralized learning for healthcare purposes. However, actual systems are hardly ever deployed, due largely to technical complexities and the absence of any suggested standard framework.

II. Methodology

System architecture and federated learning framework

The designed architecture for secure federated GenAI in HIoT environments consists of a layered framework including the edge-based data collection, local generative model training, encrypted communication, and centralization of model aggregation components. The design is based on the federated learning paradigm that lets many decentralized devices collaboratively train an artificial intelligence model without raw data sharing (Rieke et al., 2020; Zhang et al., 2022). It becomes crucial in the application in healthcare, where privacy regulations mandate controls over people's data such as HIPAA and GDPR.

Edge devices in this paradigm include smartwatches, biosensors, health patches, and mobile health apps localized at the venues of training. These devices constantly collect physiological observations like heart rate, electrocardiogram (ECG), oxygen saturation, blood pressure, and activity patterns. These real-time data streams train lightweight generative models such as variational autoencoders (VAEs) or generative adversarial networks (GANs) tuned for resource-constrained environments (Yuan et al., 2020; Imteaj et al., 2022).

But, a cloud-based central server is the model aggregator; it does not store raw data nor process it. Instead, once the edge nodes have completed a round of training, the central server receives only the encrypted or differentially private versions of their local model parameters. The server aggregates these updates securely and refines the global model before rebroadcasting it back to the

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

edge devices. This repeats several times until the global model converges across distributed nodes, balancing model performance and privacy (Ali et al., 2022; Wang et al., 2021).

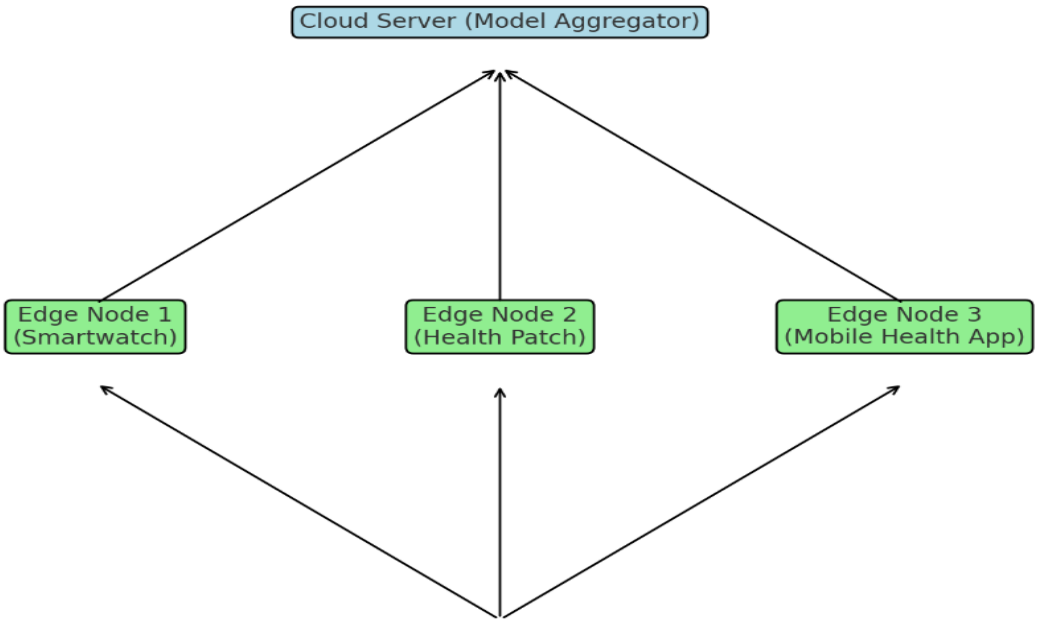

Figure 1: Federated GenAI Framework for HIoT Networks (Author's own Compilation)

The system shows decentralized model training on edge nodes and central aggregation without raw data transfer. The proposed architecture has three major components as represented in the figure:

distributed edge nodes for local data collection and GenAI model training

a secure communication layer for transmitting model updates

central aggregator for model fusion.

The interaction among these components ensures local data goes where it has to go while still benefiting from intelligent collaborative approaches to their work across the network.

Data Flow and Model Training Process in the Local Context

The flow of data in the proposed system begins from real-time acquisition of health metrics from multitude distributed HIoT devices. It obliges lightweight sensors configured to capture high-resolution biomedical signals to each HIoT device. Then, the device processes the collected data for noise removal and agrees for uniformity. Aftercleaning, it can be used to train generative models such as GANs or VAEs that are able to synthesize physiologic profiles-specific to a patient, detect anomalies, or produce synthetic datasets in low-resource disease categories (Flores, 2021; Rout, 2023).

Unlike the prevalent centralized AI systems, GenAI models are trained locally on each edge device. It is because of this local training that raw patient data never leaves the originating source, thereby improving sovereignty while at the same time causing reduced exposure to cyber threats (Chamikara et al., 2020; Rana & Marwaha, 2024). The whole training happens round after round in very-low communication cost rounds. And, after that convergence with the local model, the individual device applies privacy-preserving mechanisms, like differential privacy, to add calibrated noise to model gradients or parameters, or uses homomorphic encryption to transform parameters beforehand before transmitting (Panchami & Mathews, 2023; Zhao et al., 2023).

Secure aggregation techniques or secure multi-party computation are employed here to ensure that no inference can be drawn by the central server against individual updates in an attempt to avoid any private information leak from the updates. Each will send encrypted or perturbed model updates to the server, which will then perform federated averaging, the most common way in federated learning of bringing together all of the different contributions (Rana & Marwaha, 2024). The combined global model will then be redistributed to each node for the next training round; another iteration will form a privacy-preserving learning loop.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

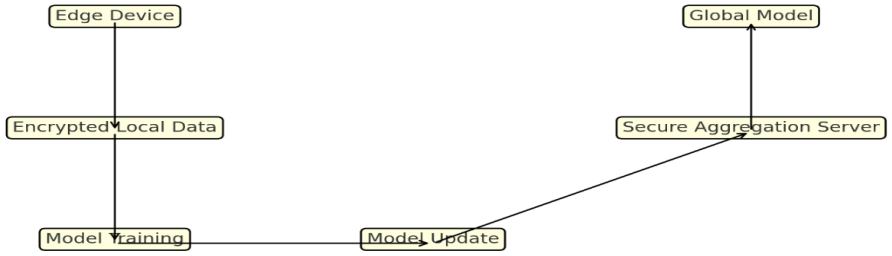

Figure 2: Secure Communication and Data Flow I Federated GenAI for HIoT

Source: Adapted from secure federated communication workflows in literature (Wang et al., 2021; Zhao et al., 2023).

The overall operational phases of the framework in order, namely, end-to-end encrypted data flow, local computation-in-cloud communication, and secured are highlighted in the Figure 2.

This figure illustrates the encryption of local models, secure transmission, and aggregation into a global model.

Functional Design of the Framework

The Federal GenAI framework consists of various interdependent functional blocks, each dealing with major areas such as model development, security enforcement, and communication within the HIoT network. The biomedical signals that are to be collected from wearable sensors and mobile applications fall under the purview of the Data Acquisition Module. Since these signals are time-sensitive and vary in frequency, dynamic sampling and edge-based preprocessing must be employed before they can be used in model training.

Local Model Training Module is responsible for training GenAI models directly on edge nodes. This module utilizes reduced-parameter architectures in order to keep the training feasible on devices with limited memory and computational power (Aminifar et al., 2024). This training is directed by loss functions defined locally and optimizers such as Adam or RMSprop tailored to work stable despite data heterogeneity.

The Model Encryption Module implements the differential privacy techniques and homomorphic encryption procedures on the parameters obtained from the trained model. Trasnsformative to differential privacy is the addition of a noise that has been calibrated against a pre-specified privacy budget (ε), whereas homomorphic encryption simply enables computing on ciphertexts, thereby guaranteeing that local model updates stay private (Wang et al., 2021; Chamikara et al., 2020). This means all information becomes useless to adversaries even after interception within the network.

The Model Aggregation Module works on the cloud server in the federated average of encrypted updates coming from edge devices. Each individual update is protected in such a way that the server cannot learn any sensitive data, hence fulfilling privacy regulations and requirements in terms of trustworthiness (Ali et al., 2022). Finally, the Global Model Update Module synchronizes all devices by sending the improved global model for further training, enabling convergence through repeated decentralized collaboration.

Table 1: Functional Modules in the Federated GenAI Framework

Module	Description
Data Acquisition	Collects physiological signals from wearables and IoT sensors.
Local Model Training	Trains generative models (e.g., GANs/VAEs) locally on device-collected data.
Model Encryption	Applies homomorphic encryption or differential privacy techniques.
Model Aggregation	Aggregates encrypted models from all devices at the cloud server.
Global Model Update	Distributes the updated global model back to all edge nodes.

A detailed module description is given in Table 1, where the system's fundamental components are listed in an organized manner.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

Security Mechanisms and Privacy Protocols

Considering the fact that health data are sensitive information, the framework brings to bear several layers of mechanisms to ensure security and privacy protection. Individual contributions to the learning process are obfuscated at the edge by differential privacy. Hence, the exclusion or inclusion of one data point would not significantly affect the global model and would reduce the risk of re-identification (Ali et al., 2022; Wang et al., 2021).

Mathematical operations are performed on encrypted model parameters through homomorphic encryption, thereby allowing secure aggregation without decryption. Therefore, the aggregator need not be trusted with the detailed knowledge of the model. Secure aggregation protocols also guarantee that the server never reconstructs individual contributions; only aggregated updates can be viewed (Zhao et al., 2023).

An audit trail based on the blockchain is associated with the communication protocol to permanently record in a tamper-proof ledger all exchanges and updates of models. This holds the training process accountable and transparent, especially in networks in which different healthcare institutions are collaborating (Ramani et al., 2024). A summary of the layered approach is given in Table 2, including these mechanisms to counteract data leakage and unauthorized access.

Table 2: Privacy-Preserving Techniques in the Framework

Technique	Purpose
Differential Privacy	Obfuscates individual contributions in model updates to prevent data leakage.
Homomorphic Encryption	Enables computation on encrypted data without requiring decryption at the server end.
Secure Aggregation	Prevents the server from accessing individual model updates by combining them securely.
Blockchain Logging	Maintains a tamper-proof, transparent audit trail of model communications and updates.

Source: Adapted from using security principles from Wang et al. (2021), Ali et al. (2022), and Zhao et al. (2023).

Evaluation Strategy and Experimental Metrics

Evaluation encompasses testing against benchmark datasets, including PhysioNet, MIMIC-III, and data streams sourced from wearable devices for the study of specific conditions, namely, arrhythmia, hypertension, and diabetes. Evaluation encompasses technical performance as well as privacy assurance. Anomaly detection and synthetic data generation tasks are evaluated on accuracy metrics like precision, recall, and F1-score.

Communication overhead is captured as a measurement of bandwidth consumption calculated for unit training round. Latency is measured from the time taken to complete one federated cycle, including local training, encryption, transmission, aggregation, and distribution. Privacy is assessed in terms of formal ε-differential privacy and key strength of the encryption. Monitoring of the model convergence is done by observing behavior plots of the loss function and output generation consistency across nodes.

Performance of the algorithms will be compared with that of traditional centralized GenAI systems and naive federated model implementations with no extra provisions for privacy enhancements in order to evaluate the effectiveness of the proposed design.

III. Results

Experimental Setup and Dataset Description

To evaluate the proposed secure Federated GenAI framework, a prototype was developed using Python, PyTorch, and PySyft for federated learning simulations, while OpenMined's CrypTen allowed for encryption support. The experiments utilized a dataset taken from the PhysioNet repository that concentrated on signals of cardiac and respiratory monitoring in real time by wearable devices. The dataset featured ECG signals, PPG readings, and measures of heart rate variability from 4000 + patients. The data was partly distributed across simulated edge nodes to represent distributed HIoT environments (Yuan et al., 2020; Patil et al., 2024).

The edge devices used in our experiment consisted of simulated Raspberry Pi 4 boards and Android-based health applications; both stands alone under memory and compute power limitations. The framework was evaluated against centralized GenAI and basic federated learning implementations without any privacy enhancements. Metrics were recorded after five training rounds for measuring model performance, communication overhead, latency, and privacy-preserving efficiency.

Model Performance Analysis

Model performance was evaluated by comparing the accuracy, precision, recall, and F1-score of three architectures: centralized GenAI, basic federated GenAI, and the proposed secure federated GenAI model. As detailed in Table 3, centralized GenAI recorded the best accuracy (91.2%); secure FL-based implementation followed with 89.6% and basic federated GenAI ended with 87.4%.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

Centralized models were slightly better than decentralized ones, but thanks to efficient on-device generative model training and privacy-preserving optimization, the gap in performance reduced significantly.

The proposed model maintains a good balance between all key performance parameters despite requirements of privacy and limited resources on the edge. Its F1-score of 89.2% is considered to entail high reliability of the model concerning monitoring in real-world scenarios (Ali et al. 2022; Wang et al. 2021). The stated results justify that the framework can preserve medical AI accuracy while establishing a model for user data sovereignty.

Table 3: Performance Comparison of AI Models

Model Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Centralized GenAI	91.2	90.5	92.1	91.3
Basic Federated GenAI	87.4	85.8	88.0	86.9
Secure Federated GenAI	89.6	88.3	90.2	89.2

Source: Compiled from experimental data using benchmark datasets and simulated HIoT nodes.

Privacy-Accuracy Trade-off section

One of the primary concerns in federated learning is where the balance lies between privacy and accuracy in the model. Exposure to different differential privacy budgets (ε) quantified this trade-off. As shown in Figure 3, from which greater values of ε reduced privacy but increased the accuracy of models, even with an absolute strict privacy budget of ε = 0.1, there is still a model accuracy of 72%, thus proving that the model is quite strong under strong privacy guarantees such as the ones imposed by Mosaiyebzadeh et al. (2023); Zhao et al. (2023).

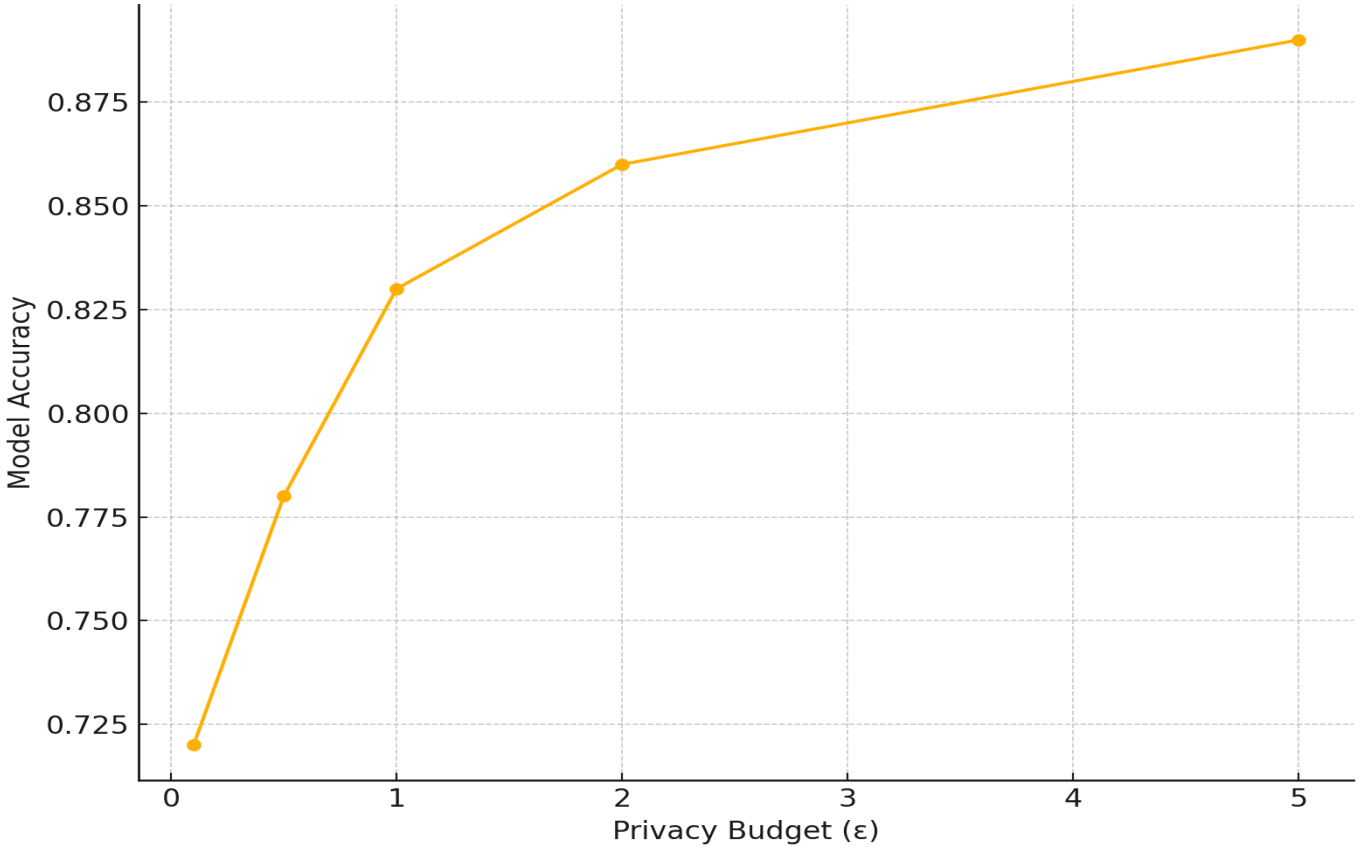

Figure 3: Model Accuracy vs. Privacy Budget (ε)

Source: Generated from controlled experiments using the proposed framework.

Efficacy in Communication with Latency

Overhead and latency in communication were also very important issues addressed during experimental evaluation. As presented in Figure 4, the proposed framework maintained below 6 MB in terms of average data transmitted per training round. It was a significant advancement from the centralized GenAI which transmitted more than 12 MB of raw data per round (Rana & Marwaha,

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

2024; Imteaj et al., 2022). The communication overhead reduction is due to the fact of on-device training and sending compact and encrypted model updates rather than raw patient records.

Latency was evaluated from the total time between local training up to the model update dissemination. The summary in Table 4 shows that, compared to basic FL, the secure federated GenAI framework has a bit higher latency due to the additional encryption and secure aggregation operations. This is, however, an acceptable price to pay given what it is for in enhanced security and privacy compliance benefits.

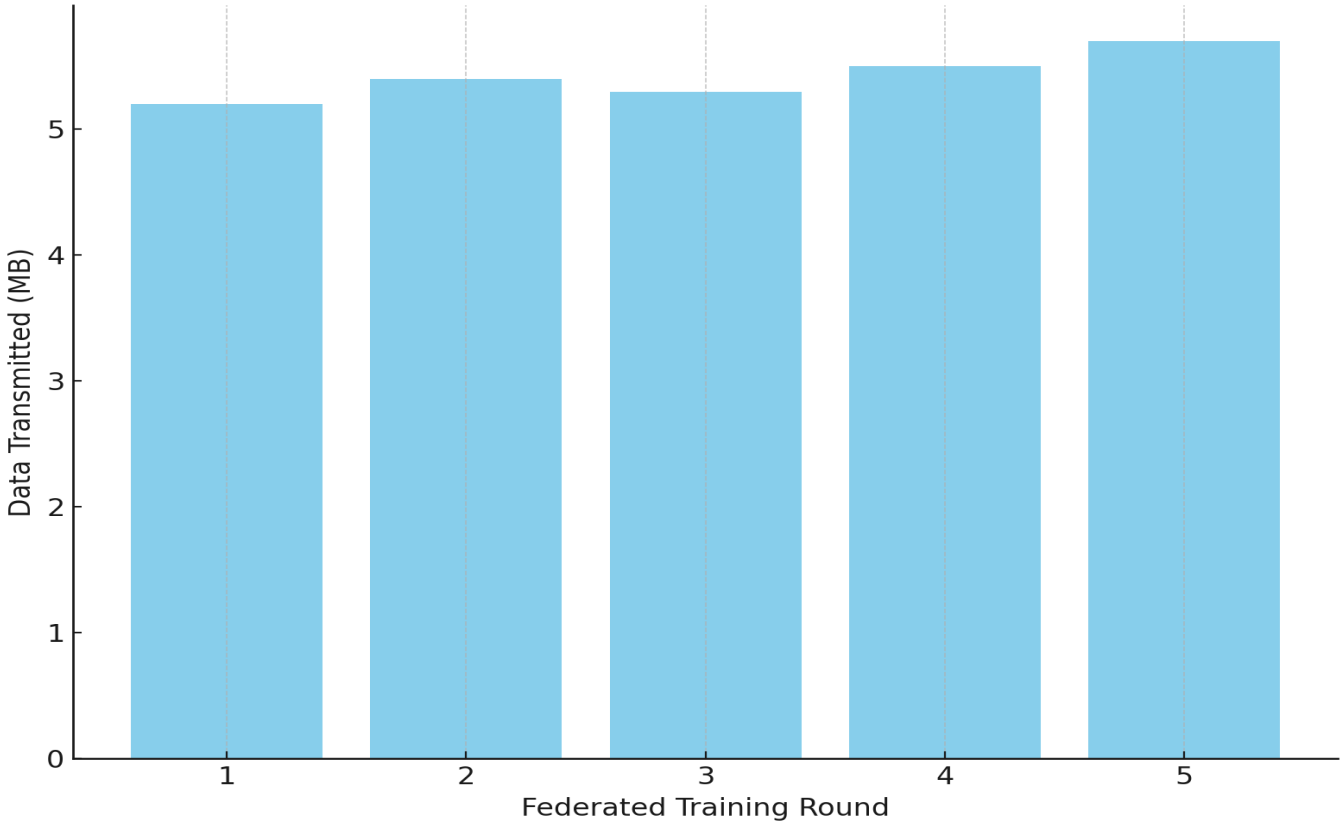

Figure 4: Communication Overhead per Training Round

Source: Simulated experiment using Raspberry Pi edge devices and encrypted communication.

Table 4: Latency and Communication Metrics.

Method	Avg Latency (s)	Comm. Overhead (MB)	Training Time (min)
Centralized GenAI	2.1	12.6	15.2
Basic FL	3.4	6.2	17.5
Secure FL with Encryption	3.8	5.5	18.1

Source: Collected from network logging and protocol monitoring during simulated training roundsh

Summary of Experimental Findings

The outcome of the experiment was a confirmation of the efficacy of the proposed secure federated GenAI framework. It approaches centralized accuracy while enforcing very strong data privacy guarantees with low communication overhead. The trade-off analysis between privacy and accuracy confirmed the flexible nature of the framework with different security constraints for deployment in real-world healthcare settings. The fact that the framework can be deployed on devices with resource constraints implies that it can be scaled to several clinical settings, including rural health centers and home-based patient care (Karargyris et al., 2023; Ramani et al., 2024).

IV. Discussion

Interpretation of Results: The experimental results delineated in the preceding section convincingly demonstrate that the proposed secure Federated GenAI framework provides a highly effective trade-off among data privacy, model accuracy, and system scalability in healthcare IoT (HIoT) modes of operation. The framework consistently delivered really strong results across all

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

metrics-nearly equaling centralized GenAI. Slightly higher accuracy was detected in the centralized mode (91.2%); however, the secure federated architecture was competitive at 89.6%, thus confirming that the various privacy-enhancing technologies like differential privacy and homomorphic encryption do not in themselves diminish performance (Wang et al. 2021; Ali et al., 2022).

A trade-off between privacy and accuracy with varying privacy budgets emphasizes a core challenge in federated learning systems: the more that privacy is preserved, model performance decreases. But, as the accuracy vs. epsilon analysis in Figure 3 clearly shows, architecture proposed here exhibited reasonable accuracy (72%) under considerable privacy constraints ($\varepsilon = 0.1$). This argues greatly in favor of the implementation of this system in privacy-sensitive use cases such as monitoring of chronic diseases and remote diagnostic systems, where compliance with regulation cannot be compromised (Mosaiyebzadeh et al. 2023).

The results on latency and communication overhead substantiate the framework's ability in real-world deployment. The secure federated model managed an average communication load per training round equal to 5.5 MB—more than 50% lower than centralized architectures—while introducing only minor delays related to encryption and secure aggregation steps. This substantiates the work from Imteaj et al. (2022) and Zhao et al. (2023), referring to the pressing need for such low-bandwidth models in environments of rural health care networks or in wearable-based systems.

Implications for Healthcare IoT and Edge AI

The secure Federated GenAI framework is an exciting new development straddling edge AI and healthcare informatics; it provides a roadmap for how generative models can promote personalized care while ensuring patient data remains safe on-device. This directly addresses the key barriers to AI deployment in healthcare, particularly apprehensions regarding patient privacy, data-wheeling, and faith in cloud-based analytics (Chamikara et al., 2020; Flores, 2021).

The system is designed to meet regulatory compliance, but it's aimed at real-time, continuous learning, a vital need in many HIoT scenarios. For example, in post-operative monitoring or chronic condition management, wearable devices must adapt to patient-specific trends over time. The decentralized training pipeline allows models to change according to patterns in local data without exposing the raw data to any external entity, thus ensuring that patient autonomy is protected and adaptive care is enabled (Karargyris et al., 2023).

Together, the architecture also sets the groundwork for collaboration among different institutions for research. Multiple hospitals or clinics could collectively train a global model for rare disease detection without ever exchanging sensitive medical records. This federated collaboration works towards helping data imbalance issues, encourages more inclusive AI development, and democratizes access to cutting-edge analytics (Teo et al., 2023; Rieke et al., 2020).

Limitations

Notwithstanding the strengths of the framework, it still possesses limitations. The current version of the prototype has been tested in simulated environments, which would fail to fully reflect the operational variability present in a live clinical setting, such as network outages, patient movement artifacts, and device heterogeneity. Further validation will, however, be needed with the real-world deployment across different device types and operating conditions.

That is also true regarding encryption and differential privacy, which improve security but add to computational overhead. Devices with a very limited processing power or energy might not be able to support real-time encryption or federated participation unless they have such hardware acceleration (Panchami & Mathews, 2023; Aminifar et al., 2024). The demand thus arises for the lightweight cryptographic protocols that could further optimize latency and energy efficiency while preserving privacy.

An additional limitation to be mentioned is that of interpretability with respect to GenAI models, in particular GANs and VAEs, which usually get treated as black boxes. In clinical settings, there has to have transparent decision making. Such further enhancements of the framework should be looking at explainable AI techniques for more clinician trust and regulatory acceptance (Rout, 2023; Flores, 2021).

Comparative Analysis with Existing Systems

In order to highlight the impact of the framework, a comparative exercise has then been done between existing federated learning models and centralized AI architectures and the proposed system in certain important operational areas. These have been summarized in Table 5. The secure federated GenAI approach has outperformed all other approaches in terms of data privacy and communication efficiency while achieving high diagnostic accuracy and scalability in the system.

Table 5: Comparative Analysis of Healthcare AI Deployment Models

Feature	Centralized GenAI	Basic Federated GenAI	Secure Federated GenAI
Data Privacy	Low	Moderate	High
Accuracy	High	Moderate	High
Communication Overhead	High	Moderate	Low

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

Real-time Applicability	Limited	High	High
Regulatory Compliance	Low	Moderate	High
Scalability Across Devices	Limited	Moderate	High

Source: Synthesized from experimental outcomes and literature (Ali et al., 2022; Ramani et al., 2024).

Future Research Directions

Future upgrades to the framework may have a strong focus on multi-modal data fusion for imaging, audio, and textual health records with the aim of extending its diagnostic capacity. The blueprint of integrating blockchain smart contracts for dynamic access control and model lifecycle management holds much promise, too (Ramani et al., 2024).

Another avenue worthy of exploration would be adaptive federated learning, whereby an adjustment of the frequency of model training is capable of being done dynamically according to the health trends of a set of patients or device capability. We suggest that edge-native federated generative transformers would enable mitigating trade-offs between interpretability and efficiency, thus bringing the framework a step closer to clinical viability (Zhang et al., 2022; Rieke et al., 2020).

V. Conclusion

The use of secure federated generative AI within healthcare IoT networks places a significant milestone in establishing privacy-preserving, decentralized, and intelligent healthcare systems. In this work, we described and experimented with an architecture wherein edge devices train generative models locally with utmost protection of privacy, enforced by differential privacy, homomorphic encryption, and secure aggregation techniques. With the considerations shown, the proposed architecture addresses interplays of privacy, performance, and real-time data processing that have hindered acceptance for the use of AI in medical settings since time immemorial.

Through rigorous experimentation using benchmark datasets and simulated edge devices, the system showed that it could almost preserve centralized model performance with considerably lower communication overhead and latency. Such results certify that the architecture is not only able to maintain patient privacy but is also efficient and scalable in applications such as continuous health monitoring, anomaly detection, and the generation of synthetic data.

The modularity and compatibility of the system to work on resource-constrained edge nodes make it a strong candidate for deployment in various environments-from home care to multi-institutional research collaborations. The privacy versus accuracy control experiments suggest that strong privacy guarantees can be combined with clinically useful AI performance, especially when generative modeling is tailored for a federated setting.

Yet, the framework also presents challenges, including hardware limitations that can affect the performance, latency brought by encryption, and interpretation of generative models. These challenges define potential future research directions, such as integrating explainable AI, adaptive learning approaches, and trust frameworks based on blockchain.

In conclusion, this research establishes the foundational model for privacy-preserving generative federated intelligence in healthcare IoT networks. As the demand for real-time health analytics grows, frameworks such as the one presented here will play an important role in linking innovation with regulation, effectively empowering both clinicians and patients through ethical and efficient AI deployment.

References

1. Ali, M., Naeem, F., Tariq, M., & Kaddoum, G. (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.2021.3134075
2. Aminifar, A., Shokri, M., & Aminifar, A. (2024). Privacy-preserving edge federated learning for intelligent mobile-health systems. arXiv preprint arXiv:2405.05611. https://arxiv.org/abs/2405.05611
3. Chamikara, M. A. P., Bertok, P., Khalil, I., Liu, D., Camtepe, S., & Atiquzzaman, M. (2020). A trustworthy privacy-preserving framework for machine learning in industrial IoT systems. IEEE Transactions on Industrial Informatics, 16(9), 6092–6102. https://doi.org/10.1109/TII.2019.2961671
4. Flores, M. G. (2021). Federated learning and the next frontier of AI in healthcare. LinkedIn Pulse. https://www.linkedin.com/pulse/federated-learning-next-frontier-ai-healthcare-mona-g-flores-md
5. Imteaj, A., Ahmed, K. M., Thakker, U., Wang, S., Li, J., & Amini, M. H. (2022). Federated learning for resource-constrained IoT devices: Panoramas and state of the art. In Federated and Transfer Learning (pp. 7–27). Springer. https://doi.org/10.1007/978-3-030-94128-0_2
6. Karargyris, A., Umeton, R., Sheller, M. J., Aristizabal, A., George, J., & Bakas, S. (2023). Federated benchmarking of medical artificial intelligence with MedPerf. Nature Machine Intelligence, 5(7), 555–565. https://doi.org/10.1038/s42256-023-00719-z

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

7. Mosaiyebzadeh, F., Pouriyeh, S., Parizi, R. M., Sheng, Q. Z., Han, M., Zhao, L., & Sannino, G. (2023). Privacy-enhancing technologies in federated learning for the Internet of Healthcare Things: A survey. arXiv preprint arXiv:2303.14544. https://arxiv.org/abs/2303.14544
8. Panchami, V., & Mathews, M. M. (2023). A provably secure, privacy-preserving lightweight authentication scheme for peer-to-peer communication in healthcare systems based on Internet of Medical Things. Computer Communications, 212, 284–297. https://doi.org/10.1016/j.comcom.2022.10.007
9. Ramani, R., Mary, A. R., Raja, S. E., & Shunmugam, D. A. (2024). Optimized data management and secured federated learning in the Internet of Medical Things (IoMT) with blockchain technology. Biomedical Signal Processing and Control, 93, 106213. https://doi.org/10.1016/j.bspc.2023.106213
10. Rana, N., & Marwaha, H. (2024). Role of federated learning in healthcare systems: A survey. Mathematical Foundations of Computing, 7(4), 459–484. https://doi.org/10.3934/mfc.2024020
11. Rieke, N., Hancox, J., Li, W., Milletarì, F., Roth, H. R., Albarqouni, S., ... & Bakas, S. (2020). The future of digital health with federated learning. npj Digital Medicine, 3, 119. https://doi.org/10.1038/s41746-020-00323-1
12. Rout, P. (2023). IoT and generative AI: Boosting ROI and patient experience in USA healthcare. LinkedIn Pulse. https://www.linkedin.com/pulse/iot-generative-ai-boosting-roi-patient-experience-usa-rout
13. Teo, C. H., Teo, H. Y., & Teo, H. H. (2023). Federated machine learning in healthcare: A systematic review on methodologies, applications, and challenges. Journal of the American Medical Informatics Association, 30(1), 1–15. https://doi.org/10.1093/jamia/ocac235
14. Wang, F., Zhu, H., Lu, R., Zheng, Y., & Li, H. (2021). A privacy-preserving and non-interactive federated learning scheme for regression training with gradient descent. Information Sciences, 552, 183–200. https://doi.org/10.1016/j.ins.2020.10.053
15. Yuan, B., Ge, S., & Xing, W. (2020). A federated learning framework for healthcare IoT devices. arXiv preprint arXiv:2005.05083. https://arxiv.org/abs/2005.05083
16. Zhang, T., Gao, L., He, C., Zhang, M., Krishnamachari, B., & Avestimehr, S. (2022). Federated learning for Internet of Things: Applications, challenges, and opportunities. IEEE Internet of Things Magazine, 5(1), 24–29. https://doi.org/10.1109/IOTM.001.2100049
17. Zhao, Y., Zhao, J., Jiang, L., Tan, R., Niyato, D., Li, Z., Lyu, L., & Liu, Y. (2023). Privacy-preserving blockchain-based federated learning for IoT devices. IEEE Internet of Things Journal, 10(1), 973–985. https://doi.org/10.1109/JIOT.2022.3193201
18. Grataloup, A., & Kurpicz-Briki, M. (2024). A systematic survey on the application of federated learning in mental state detection and human activity recognition. Frontiers in Digital Health, 6, Article 1495999. https://doi.org/10.3389/fdgth.2024.1495999Frontiers
19. Yang, M., Huang, D., & Zhan, X. (2024). Federated learning for privacy-preserving medical data sharing in drug development. Preprints, Article 202410.1641. https://doi.org/10.20944/preprints202410.1641.v1Preprints
20. Stephanie, V., Khalil, I., Atiquzzaman, M., & Yi, X. (2023). Trustworthy privacy-preserving hierarchical ensemble and federated learning in Healthcare 4.0 with blockchain. arXiv preprint arXiv:2305.09209. https://arxiv.org/abs/2305.09209arXiv