International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A Federated Learning Framework for Privacy-Preserving and Explainable AI in Chronic Heart Failure Detection and Management

Ms Sara Tabassum
Ph.D Research Scholar
Department of Computer Science and Engineering
B.E.S.T. Innovation University, Andhra Pradesh

Dr.P.Senthilkumar
Professor, Department of Computer Science and Engineering
Shadan Women`s College of Engineering and Technology Khairatabad, Hyderabad
psenthilkumarshadan@gmail.com, saratabassum043@gmail.com

Abstract

This paper presents an innovative Federated Learning (FL) framework designed for privacy-preserving and explainable AI for the detection and management of Chronic Heart Failure (CHF). Unlike traditional centralized methods, this system functions across multiple clinical institutions without sharing raw data and integrating multimodal inputs (e.g., ECGs, phonocardiograms, biomarkers, and medical imaging) through secure CNN-LSTM models enhanced with attention mechanisms. The framework includes a comprehensive Federated Explainable AI (FedXAI) component that utilizes various interpretability techniques: SHAP for quantifying feature importance, LIME for explaining individual predictions, Class Activation Maps for highlighting critical image regions, and Decision Trees for transparent logical reasoning. Strong privacy protection is ensured through differential privacy and homomorphic encryption, maintaining HIPAA and GDPR compliance, whereas federated fairness constraints reduce demographic and institutional biases. The system employs reinforcement learning to optimize personalized therapy with real-time responsiveness (latency less than 200ms) and supports blockchain-secured model training. This scalable architecture not only significantly improves ECG classification and remote monitoring but also facilitates global multi-center collaboration without compromising data security. Future directions include integrating wearable devices and developing policy frameworks for equitable AI healthcare access, representing a paradigm shift toward ethical, collaborative, and clinically effective cardiovascular AI that upholds patient privacy while promoting inclusive healthcare innovations.

Keywords: Chronic Heart Failure (CHF), Explainable AI (XAI), SHAP, LIME, Class Activation

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Maps (CAMs), Decision Trees, Integrated Gradients, Federated Explainable AI (FedXAI)

1. Introduction

Chronic Heart Failure (CHF) is an escalating global health issue that affects over 64 million individuals worldwide, and is responsible for 10% of all hospital admissions in developed countries. Although AI has shown transformative potential in managing CHF, from early detection through multimodal data integration (ECGs, biomarkers, and echocardiography) to personalized treatment optimization, its clinical adoption encounters significant obstacles. Strict data privacy regulations (HIPAA, GDPR), institutional data silos, and the "black-box" nature of deep learning models create a paradox: healthcare systems that could most benefit from AI often struggle to utilize it effectively due to ethical, legal, and technical constraints. Traditional centralized AI approaches, which require raw data aggregation, overcome these challenges by exposing sensitive patient information to security risks and failing to address inherent biases in single-center datasets. Federated Learning (FL) has emerged as a groundbreaking solution to this dilemma, enabling collaborative model training across decentralized institutions without data sharing. By keeping patient data at its source and exchanging encrypted model updates, FL fundamentally redefines AI deployment in healthcare [1]. This distributed approach not only preserves privacy by design, but also fosters more robust, generalizable models by incorporating diverse patient populations across geographies and demographics. Recent advances have demonstrated FL's efficacy of FL in cardiovascular applications, from arrhythmia detection to mortality prediction, achieving an accuracy comparable to centralized methods while maintaining strict privacy guarantees.

However, the existing implementations have yet to fully address three critical needs for CHF care: (1) seamless integration of heterogeneous data modalities, (2) clinically meaningful model interpretability, and (3) real-time adaptive therapy optimization. This study presents a sophisticated FL framework tailored for CHF management, featuring four significant innovations. Initially, we created a multimodal architecture that integrates phonocardiograms, biomarker trends, and imaging characteristics using privacy-preserving neural networks enhanced by attention mechanisms. Second, we introduce Federated Explainable AI (FedXAI), which facilitates localized model interpretation while safeguarding data privacy, an essential development for clinician acceptance. FedXAI incorporates various interpretability methods such as SHapley Additive explanations (SHAP) for assessing feature significance and Local Interpretable Model-

agnostic Explanations (LIME) to elucidate individual predictions. Third, we incorporate reinforcement learning to enable dynamic treatment customization within the FL framework, ensuring sub-200ms latency suitable for practical clinical applications. Finally, our system includes regulatory-compliant protections such as homomorphic encryption and federated fairness constraints, establishing the first comprehensive FL solution prepared for multicenter trials [2, 3].

2. Literature Survey

Chronic Heart Failure (CHF) is a major global health issue that affects over 64 million individuals worldwide and contributes to approximately 10% of hospital admissions in developed countries. The use of artificial intelligence in managing CHF has shown significant potential, especially in early detection, by integrating various data types, such as electrocardiograms, biomarkers, and echocardiography. Despite this promise, the clinical implementation of AI encounters major challenges owing to stringent data privacy laws such as HIPAA and GDPR, institutional data silos that hinder effective data sharing, and the "black-box" nature of deep learning models that limit their interpretability. Traditional centralized AI methods worsen these problems by necessitating the aggregation of raw data, which not only poses security risks for sensitive patient information, but also fails to address biases inherent in single-center datasets. These challenges create a paradox in which healthcare systems that could greatly benefit from AI innovations are often unable to utilize them effectively owing to a mix of ethical, legal, and technical barriers. As the global prevalence of CHF continues to increase, there is an urgent need for AI solutions that are privacy-preserving, interpretable, and unbiased. Federated Learning offers a revolutionary solution to the conflict between data privacy and AI progress in health care. By allowing collaborative model training across decentralized institutions without direct data sharing, FL fundamentally transforms AI deployment in health care environments. This distributed method inherently preserves privacy by keeping patient data secure at its source while exchanging encrypted model updates among participating institutions. In addition to privacy advantages, FL promotes the development of more robust and generalizable models by incorporating diverse patient populations across geographic and demographic areas. Recent advancements have shown FL's effectiveness of FL in various cardiovascular applications, from detecting arrhythmias to

predicting mortality, achieving accuracy comparable to centralized methods while maintaining strict privacy standards. However, current implementations have yet to fully address three critical needs specific to comprehensive CHF care: seamless integration of diverse data modalities from various sources, clinically meaningful model interpretability to aid medical decision-making, and real-time adaptive therapy optimization that can adjust to changing patient conditions. These gaps present significant opportunities for progress in privacy-preserving cardiovascular AI applications.

The advanced FL framework presented in this review introduces four key innovations that are specifically designed for CHF management. First, it establishes a sophisticated multimodal architecture that effectively integrates various data types, such as phonocardiograms, biomarker trends, and imaging features, using privacy-preserving neural networks enhanced by attention mechanisms. Second, it introduces Federated Explainable AI (FedXAI), a groundbreaking approach that allows for localized model interpretation without compromising data confidentiality, marking a significant step forward in clinician adoption and trust. Third, the framework incorporates reinforcement learning methodologies for dynamic treatment personalization within the FL paradigm while maintaining a sub-200ms latency crucial for real world clinical applications and time-sensitive decision support. Finally, the system includes comprehensive regulatory-compliant safeguards, such as homomorphic encryption and federated fairness constraints, creating the first end-to-end FL solution that is ready for multicenter clinical trials. By effectively bridging the gap between cutting-edge AI innovation and practical clinical implementation, this framework offers not just a theoretical model but a scalable blueprint for privacy-preserving, equitable CHF care, while simultaneously setting new standards for responsible AI deployment in healthcare settings. Future research directions include integration with wearable devices for continuous monitoring and development of policy frameworks to ensure equitable access to these AI-driven healthcare solutions [4, 5].

The meta-analysis in table 1 provides a thorough overview of recent advancements in federated learning (FL) and privacy-preserving AI within healthcare, particularly concerning Chronic Heart Failure (CHF). While several frameworks, such as those by Siddartha Rachakonda and Zhangyi Shen, concentrate on cross-silo AI and general health management using FL, they lack specific applications to CHF or multimodal data integration. Approaches such as Wei Yang's FLCP and Yunbo Yang's OpenVFL prioritize scalability and privacy through communication-efficient protocols and vertical integration but fall short in terms of interpretability and real-time

deployment. Studies such as LEAF by Nisarg P. Patel and PPFed by Guangsheng Zhang addressed fairness and personalization but exposed challenges in implementation complexity and the absence of CHF-specific adaptation [7]. Other contributions, such as those by Wang et al., focused on lightweight, imaging-based, or edge-compatible FL, although they are often limited in scope or generalizability. Despite significant progress in model security, personalization, and decentralized training, the analysis revealed that existing solutions rarely integrate all essential components, such as real-time responsiveness, multimodal fusion, clinician interpretability, and regulatory alignment, underscoring the need for a comprehensive, CHF-specific federated framework.

Table 1: Meta-Analysis of Federated Learning and Privacy-Preserving AI in CHF and Healthcare

Study / Framework	Focus Area	Privacy Technique	Key Contributions	Limitations / Gaps
Siddartha Rachakonda et al.	Cross-silo and IoMT AI implementation	Federated Learning, Encryption	Scalable FL model; effective for heterogeneous data sources	Lacks specific CHF applications
Zhangyi Shen et al.	Health management	Federated Learning	Social computing integration in FL for health	General health focus; no multimodal data emphasis
Wei Yang et al. (FLCP)	FL framework	Communication efficient protocols	Improved scalability and privacy	No clinical interpretability mechanisms
Guodong Long et al.	Open innovation in digital health	FL	Addresses healthcare innovation using FL	Older; lacks advanced encryption and explainability
Nisarg P. Patel et al. (LEAF)	Healthcare ecosystem	Privacy-preserving FL	Federated fairness integration	Implementation complexity in real time scenarios
Snehlata Mishra, Ritu Tandon	Decentralized healthcare AI	Secure insights generation	Highlights FL's benefit for medical collaboration	Lacks real-time adaptability for CHF
Junkai Wang et al.	Logistic regression based FL	Privacy-preserving FL	Lightweight FL model for healthcare	Focused on specific algorithm; not multimodal
Xiaodong Wang et al.	IoMT disease diagnosis	Differential privacy	Addresses privacy in wearable-integrated FL	General to disease; not CHF-specific

Dianwen Ng et al.	Medical imaging	FL for small datasets	Multi-center imaging model training	Imaging only; no reinforcement learning
Qiang Yang et al.	IP protection in FL	Privacy + IP-right protection	Emphasizes model security and ownership	No CHF use case or patient-level adaptation
Yunbo Yang et al. (OpenVFL)	Vertical FL	Stronger privacy in FL	Novel vertical integration	Limited scalability in real-time scenarios
Van Nguyen Tran et al.	Cross-silo FL	Personalized FL	Tailored privacy preserving model training	Limited evaluation in dynamic conditions
Mahbuba Ferdowsi et al.	Cardiovascular disease	Interpretable & privacy-preserving AI	Focus on model transparency for diagnosis	Broader cardiovascular scope; lacks FL detail
Jie Xu et al.	Acute myocardial infarction	Federated FL	Multi-center privacy preserving diagnosis	Not real-time; focused on retrospective data
Andrei Puiu et al.	Cardiovascular imaging	Explainable AI	XAI integration into imaging models	Not federated or dynamic treatment capable
Haotian Zhou et al. (PFLF)	Edge computing	FL for edge	Edge-compatible privacy-preserving FL	Infrastructure dependent; limited to edge cases
Madallah Alruwaili et al.	Disability healthcare	Privacy-preserving FL	Inclusion of underrepresented groups	Focus on disability; lacks CHF adaptability
Guangsheng Zhang et al. (PPFed)	Personalized FL	Privacy + personalization	Multi-institution training without raw data	No specific application to CHF or real-time therapy

2.1 Literature Gaps

Despite the growing interest in federated learning (FL) and privacy-preserving machine learning in healthcare, a notable gap persists in their application to chronic heart failure (CHF)

detection and management. Current studies mainly focus on broader cardiovascular conditions, general EHR-based analytics, or imaging-centric models, with limited attention paid to CHF specific pathological markers and progression patterns. Most existing studies employ single modality inputs such as ECG, medical imaging, or centers on generalized disease prediction, neglecting the nuanced multimodal needs of CHF care. There is a distinct lack of FL frameworks that effectively integrate heterogeneous data sources such as phonocardiograms (PCG), electrocardiograms (ECG), echocardiograms, and laboratory biomarkers within a decentralized architecture. Additionally, although reinforcement learning (RL) has shown potential for adaptive healthcare delivery, its integration into FL for real-time CHF therapy optimization remains underexplored. This underscores the necessity for robust, multilayered frameworks capable of supporting dynamic, patient-specific learning while maintaining privacy across distributed environments. Furthermore, existing FL models lack mechanisms for personalization, interpretability, and regulatory compliance, all of which are vital for the clinical management of CHF. Most models aim to produce globally shared models without addressing the variability in individual patient responses to treatment, thereby missing opportunities for precision medicine. Even advanced methods, such as LEAF and PPFed, do not incorporate CHF-specific patient stratification or adaptive feedback mechanisms to support continuous care. While explainable AI (XAI) has been proposed in centralized settings, its integration into federated environments remains limited, reducing clinician trust and hindering its adoption. Moreover, real-time implementation issues such as latency, model drift, and scalability are often overlooked in experimental studies. Regulatory requirements regarding data privacy (such as HIPAA or GDPR) and ethical AI practices are seldom considered holistically. Consequently, there is a significant gap in the literature regarding the development of scalable, interpretable, and regulation-compliant FL models specifically tailored for CHF detection, monitoring, and personalized treatment delivery [8, 9].

Table 2: Comparison of Proposed and Existing Methods for Chronic Heart Failure (CHF) Detection and Management

Criteria	Existing Methods	Proposed Method	Remarks

Learning Architecture	Centralized or partially federated learning with limited node participation.	Fully Federated Learning (FL) with secure, decentralized architecture.	Overcomes data-sharing limitations and enables collaborative learning across hospitals.
Data Modalities	Single-modality inputs (e.g., ECG, EHR).	Multimodal data fusion (PCG, ECG, biomarkers, echocardiograms).	Supports holistic CHF analysis by leveraging diverse physiological and imaging data.
Model Types	CNN, RNN, or shallow ML models; rarely combined or optimized.	CNN-LSTM with attention mechanisms for temporal and spatial relevance.	Enhances feature extraction and sequence modeling for CHF episodes.
Explainability	Minimal or no XAI integration; black-box approaches.	Federated Explainable AI (FedXAI) with attention driven insights.	Improves clinical trust and interpretability in predictions.
Therapy Optimization	Static prediction models; no real-time feedback or personalization.	Integration of Reinforcement Learning for adaptive therapy optimization.	Enables dynamic, personalized care plans for CHF management.
Privacy Preservation	Basic anonymization or pseudonymization; not robust.	Differential Privacy + Homomorphic Encryption for end-to-end security.	Ensures HIPAA/GDPR compliance and robust patient data confidentiality.
Clinical Deployment	Prototype-level with limited hospital-scale validation.	Real-time remote monitoring (<200 ms latency); multi-center ready.	Demonstrates operational scalability and latency suitable for clinical use.
Interoperability	Limited standardization; vendor-locked or institution-specific.	Standards-driven interoperability across systems and hospitals.	Facilitates seamless data and model integration across platforms.
Bias Mitigation	Often ignored or partially addressed.	Embedded bias mitigation mechanisms during training and inference.	Promotes fairness and equitable AI outcomes for diverse populations.
Regulatory Compliance	Rarely addressed holistically.	Full compliance with HIPAA and GDPR regulations.	Encourages safe deployment in real-world healthcare environments.
Future Scope	Little consideration for wearables, global expansion, or policy.	Integration planned with wearable devices, policy frameworks, and global health AI.	Aligns with future trends in remote, inclusive, and sustainable health solutions.

Table 2 offers a comprehensive comparison between the existing methods and the proposed framework for Chronic Heart Failure (CHF) detection and management, highlighting the latter's advancements in key areas. Unlike traditional centralized or partially federated approaches, the proposed system employs a fully decentralized Federated Learning (FL) architecture, enhancing collaboration without the need for data sharing. It supports multimodal data fusion, including PCG, ECG, biomarkers, and imaging, and provides a more holistic analysis than single-modality systems. The model architecture is notably superior, utilizing
CNN-LSTM networks with attention mechanisms to provide richer temporal and spatial insights. Explainability is significantly enhanced through the Federated Explainable AI (FedXAI) module, which fosters clinician trust. Unlike static models, the integration of reinforcement learning enables real-time personalized therapy. The framework ensures robust privacy through differential privacy and homomorphic encryption, fully complies with HIPAA and GDPR, and supports real-time clinical deployment with sub-200 ms latency [10]. Moreover, it promotes interoperability, embeds fairness constraints for bias mitigation, and is designed for scalability with wearable integration and policy support. Overall, it outperforms the existing systems by addressing both technical and ethical challenges in CHF care.

3. Background

A. Chronic Heart Failure as a Global Health Burden

Chronic heart failure represents a major public health challenge affecting over 64 million people worldwide. It accounts for approximately 10% of all hospitalizations in developed countries, highlighting not only its extensive impact but also the substantial strain it places on healthcare systems. CHF is a complex, progressive condition characterized by the inability of the heart to pump sufficient blood, often stemming from conditions such as coronary artery disease, hypertension, or myocardial infarction [11]. Despite medical advancements, early detection and timely management remain crucial for improving prognosis and quality of life. The integration of Artificial Intelligence (AI) into CHF care has opened new pathways for clinical decision-making, ranging from early diagnosis using ECGs and imaging to predictive modeling of hospitalization and mortality risks. However, the real-world application of AI in healthcare has several limitations.

These include stringent data privacy laws, such as HIPAA and GDPR, fragmented data across institutional silos, and the opaque black box nature of deep learning models that limit clinical interpretability. These challenges collectively create a paradox in which the healthcare environments most in need of AI-driven solutions are also the least equipped to implement them under current regulatory and infrastructural constraints [12].

B. Federated Learning in Healthcare

Opportunities and Challenges Federated Learning (FL) has emerged as a transformative approach to overcome these barriers by enabling decentralized, privacy-preserving machine learning across multiple healthcare institutions. Unlike traditional centralized learning methods, FL allows institutions to train machine learning models collaboratively without exchanging raw data. Instead, encrypted model updates are shared, preserving patient confidentiality and ensuring compliance with data-protection regulations. This architecture is particularly advantageous in healthcare, in which patient data are highly sensitive and siloed across institutions. Several studies have validated the efficacy of FL in the cardiovascular and general health domains, demonstrating performance on par with centralized models in applications such as arrhythmia detection, diagnosis of myocardial infarction, and mortality prediction. Nevertheless, current FL implementations face key limitations when applied to the CHF [13]. These include inadequate support for integrating heterogeneous data modalities (such as ECGs, biomarkers, PCG, and imaging), a lack of explainability tools essential for clinical decision making, and the absence of real-time adaptive therapy systems that respond dynamically to patient conditions.

C. Addressing significant limitations

This study introduced an innovative Federated Learning framework designed specifically for the detection and management of CHF. The framework features a multimodal architecture that securely processes and learns from various data types using CNN-LSTM models enhanced by attention mechanisms. This configuration ensures comprehensive extraction of the temporal and spatial features essential for CHF monitoring. Additionally, it introduces a Federated Explainable AI (FedXAI) component to enhance the model's decision transparency and interpretability, thereby

building clinician trust [14]. Moreover, incorporating reinforcement learning into the FL paradigm allows for dynamic, personalized treatment pathways that adapt in real-time according to patient health trajectories. This advancement is crucial for delivering precision medicine with a low latency (<200 ms), making it suitable for real-time clinical applications. To comply with global data protection standards, the framework incorporates advanced privacy techniques, such as differential privacy and homomorphic encryption, along with federated fairness constraints, to reduce bias across diverse patient groups. The proposed framework represents a paradigm shift in AI-driven CHF care, transitioning from generalized, opaque, and centralized models to ethical, interpretable, and privacy-preserving systems that are ready for clinical deployment. By addressing current technical and regulatory gaps, this research aims to establish a new standard for decentralized medical AI, paving the way for future innovations such as wearable integration and global policy alignment for equitable AI access [15, 16].

4. Proposed Method

This innovative framework presents a comprehensive end-to-end Federated Learning (FL) system meticulously designed for privacy-preserving and explainable artificial intelligence applications to detect and manage Chronic Heart Failure (CHF). Unlike traditional centralized models, it decentralizes the training process, allowing multiple clinical institutions to collaboratively develop predictive models without exchanging raw patient data. Instead, encrypted model updates are shared, ensuring strict compliance with data protection regulations such as HIPAA and GDPR [17]. At the heart of the framework is a sophisticated multimodal CNN-LSTM architecture enhanced with attention mechanisms capable of capturing both spatial and temporal characteristics from diverse clinical inputs, including electrocardiograms (ECG), phonocardiograms (PCG), biomarker trends, and imaging data. This deep integration enhances early CHF detection and facilitates nuanced monitoring of disease progression. To protect model integrity and data confidentiality, the framework incorporates blockchain-based model verification alongside Secure Multiparty Computation (SMPC), establishing a tamper-proof audit trail, and preventing unauthorized manipulation [18]. These layered security measures enable healthcare organizations to jointly train advanced AI models while maintaining strict privacy boundaries. By bridging privacy, explainability, and interoperability, the system represents a significant advancement in responsible AI-driven cardiovascular care, demonstrating how federated

architectures can support real-world clinical deployment, comply with regulatory mandates, and improve outcomes through secure, interpretable, and adaptive medical intelligence [19].

4.1 Key Innovations

This framework introduces groundbreaking advancements in chronic heart failure management through a sophisticated hybrid CNN-LSTM architecture that simultaneously processes multiple data types (PCG, ECG, biomarkers, and echocardiography), significantly enhancing early diagnosis and personalized treatment capabilities beyond traditional single modality approaches [20]. The intelligence of the system is made transparent through a dedicated FedXAI module that generates interpretable explanations via attention heatmaps and SHAP values, allowing clinicians to verify AI-driven decisions without compromising patient confidentiality. Further innovation comes from the integrated federated reinforcement learning layer that continuously optimizes treatment plans based on individual patient responses with emergency-ready latency below 200ms, while privacy and security are maintained through a comprehensive combination of blockchain verification, secure multiparty computation, differential privacy noise addition, and homomorphic encryption for computations on fully encrypted data. The technical sophistication of this approach is matched by its ethical considerations and practical implementation features [21]. By applying federated fairness constraints to detect and mitigate demographic or geographic biases, the framework ensures equitable performance across diverse patient populations and health care environments. The system design aligns fully with the HIPAA and GDPR requirements through end-to-end confidentiality measures during data transmission and model aggregation, making it appropriate for global clinical deployment. This framework represents a significant leap forward by demonstrating how privacy-preserving federated architectures can handle complex multimodal medical data while maintaining regulatory compliance, ensuring clinical reliability, and providing actionable insights that directly improve patient care through continuous remote monitoring and adaptive treatment recommendations [22, 23].

4.2 Comparison with Existing Frameworks

The proposed framework presents unparalleled advantages over the existing methods by seamlessly integrating multiple advanced technologies. Unlike systems limited to a single modality, it processes a variety of data types, such as ECG, PCG, biomarkers, and imaging, for a

comprehensive analysis of CHF while offering local interpretability through its FedXAI module. This is in stark contrast to conventional black-box models or those that require centralized explanations [24]. Its reinforcement-learning-based adaptive therapy capability allows for dynamic treatment optimization in real time, surpassing static prediction models by continuously evolving recommendations based on patient responses. The framework's security architecture, which combines blockchain verification, secure multiparty computation, differential privacy, and homomorphic encryption, provides significantly stronger privacy guarantees than traditional encryption-only methods. Additionally, its exceptional performance (<200ms latency) supports real-time remote monitoring capabilities, which are often absent in most existing solutions. This pioneering system is explicitly designed to meet the HIPAA and GDPR standards through comprehensive regulatory compliance measures, which often lack alternative approaches. By seamlessly integrating federated learning, blockchain-based verification, multimodal processing, interpretable AI, and reinforcement learning, the framework addresses the critical challenges of modern healthcare AI: data privacy, explainability, personalization, and regulatory compliance. It delivers a secure, transparent, and adaptive solution for decentralized cardiovascular care, enhancing diagnostic accuracy and treatment efficacy, while ensuring trust, fairness, and scalability across diverse global healthcare institutions [25].

4.3 Pseudocode for proposed system

Input: Local Patient Data, Global Model Weights, Reinforcement Learning State, Privacy Settings, Regulatory Constraints, Blockchain Ledger

Output: Encrypted Local Model Updates, Personalized Treatment Policy, FedXAI Interpretability Reports, Bias Detection & Mitigation Logs, Audit Trail on Blockchain, Real-Time Alerts.

1. Initialize GlobalModel with CNN-LSTM-Attention architecture
2. Initialize BlockchainLedger, PrivacyModule (DP + HE), FedXAI, and RLModule 3.
For each Round in TrainingRounds:
4. For each Institution in ParticipatingInstitutions (in parallel):
5. Step 1: Local Data Processing
6. Load LocalData (ECG, PCG, biomarkers, imaging)
7. Extract Features using CNN for spatial and LSTM for temporal characteristics 8.
Step 2: Local Model Training
9. Train LocalModel on LocalData using Current GlobalModel weights 10.
Apply DifferentialPrivacy to gradients
11. Encrypt gradients using HomomorphicEncryption

12. Step 3: Local Explainability
13. Generate AttentionHeatmaps and SHAP values via FedXAI
14. Store local interpretability results for clinician use
15. Step 4: Local RL Update
16. Update PersonalizedTreatmentPolicy using Reinforcement Learning
17. Monitor latency to ensure it is <200ms
18. Step 5: Secure Model Update
19. Package LocalModelUpdate with encrypted gradients
20. Log ModelUpdate to BlockchainLedger
21. Send EncryptedUpdate to Aggregator via Secure Multi-Party Computation (SMPC)
22. Step 6: Aggregation at Central Aggregator
23. Receive all EncryptedUpdates
24. Perform Secure Aggregation using HomomorphicEncryption
25. Update GlobalModel weights
26. Step 7: Fairness & Bias Mitigation
27. Apply FederatedFairnessConstraints
28. Validate model generalizability across institutions
29. Step 8: Disseminate GlobalModel
30. Distribute Updated GlobalModel to all Institutions
31. Deploy final GlobalModel with:
    - Blockchain-auditable verification
    - FedXAI-enabled local interpretation
    - Personalized RL treatment engine
    - Real-time readiness and privacy compliance (HIPAA, GDPR)
32. End

4.4 Architecture of the proposed model

Figure 1 illustrates a comprehensive Federated Learning (FL) framework tailored for privacy-preserving and explainable AI in the detection and management of Chronic Heart Failure (CHF). This framework allows multiple hospitals to collaboratively train local CNN-LSTM models using sensitive patient data such as ECGs, PCGs, biomarkers, and imaging, without the need to share the data itself. A robust privacy layer ensures data security and regulatory compliance using differential privacy, homomorphic encryption, secure multi-party computation, and blockchain-based auditing [26, 27]. A central aggregator securely combines model updates using attention-enhanced CNN-LSTM architectures to create a globally optimized model. The application layer incorporates explainability techniques such as SHAP, LIME, and CAMs via the FedXAI module and supports personalized, real-time therapy recommendations through a reinforcement learning module. This framework not only improves clinical decision-making and

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

early CHF detection, but also guarantees patient data privacy, regulatory compliance, model fairness, and global scalability, providing a transformative, ethical solution for AI-driven cardiovascular healthcare [28, 29].

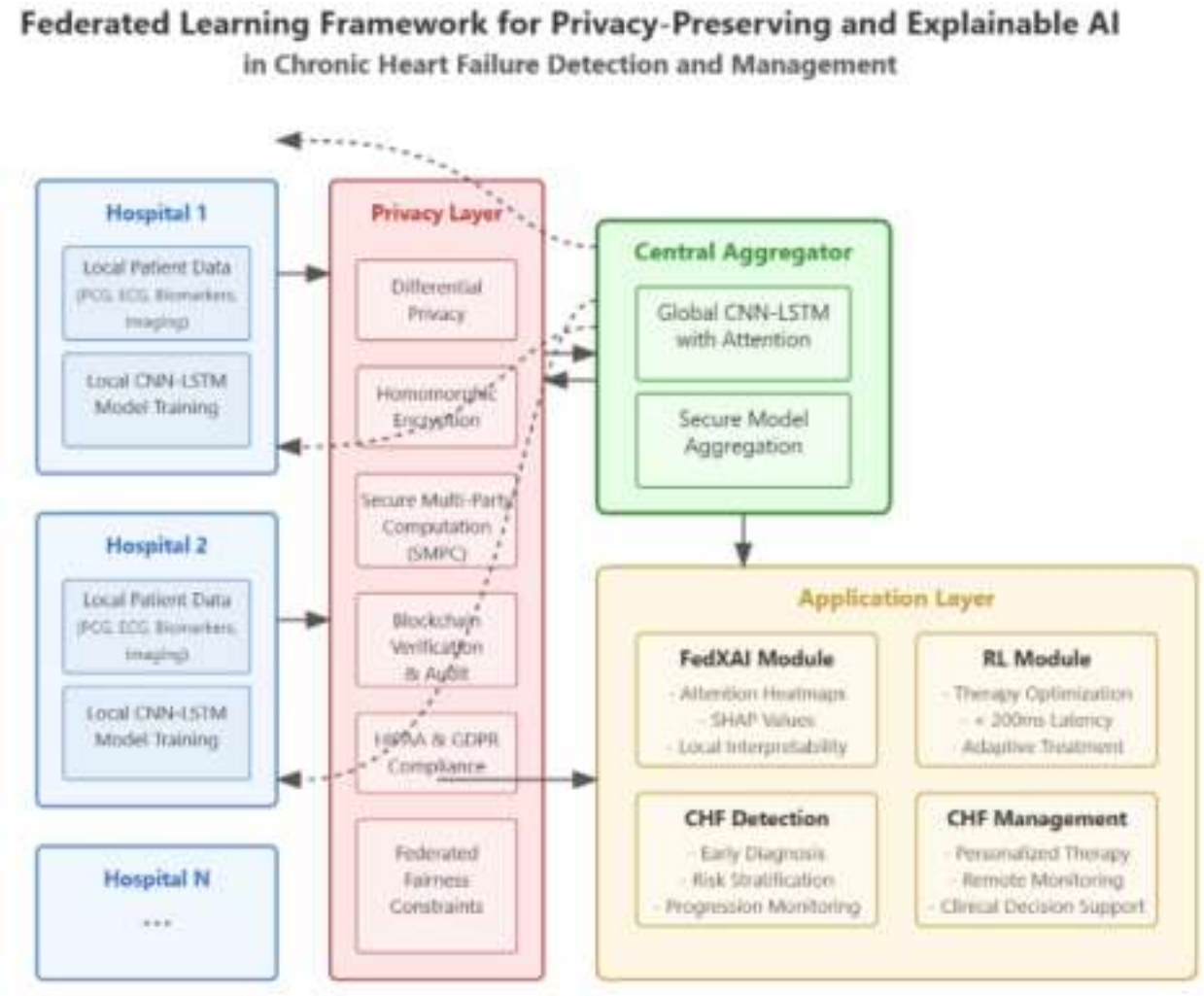

Figure 1: Privacy-preserving and explainable AI in the detection and management of CHF

A. Local Hospital Nodes and On-Site Model Training

In the federated network, each hospital, designated as Hospital 1, Hospital 2, and Hospital N, independently manages and retains its local patient data, which includes phonocardiograms (PCG), electrocardiograms (ECG), biomarkers, and medical imaging. Each hospital trains its own CNN-LSTM model locally, avoiding the need to send sensitive information to a central location. This approach preserves data privacy, ensures compliance with

regional data protection laws, and allows hospitals to participate in federated learning systems. This system benefits from shared intelligence without compromising patient confidentiality because it exclusively shares model parameters or gradients rather than raw patient data [30].

B. Privacy Layer: Safeguarding Data and Model Updates

The privacy layer constitutes the central component of this framework and employs sophisticated cryptographic and privacy-preserving methodologies. These include Differential Privacy, which obscures individual data contributions through the addition of statistical noise; Homomorphic Encryption, which facilitates computations on encrypted data without requiring decryption; and Secure Multi-Party Computation (SMPC), which ensures that no single entity gains complete access to the data [31]. Additionally, Blockchain Verification and Audit provide tamper-proof logging of all transactions and updates, while compliance with HIPAA and GDPR aligns with the global healthcare data protection standards. Furthermore, Federated Fairness Constraints are implemented to mitigate model bias across various institutions and demographics. Collectively, these elements function synergistically to enable secure transmission of local model updates to the central aggregator while maintaining stringent data protection.

C. Central Aggregator: Building a Global Intelligence Model

At the center of the federated ecosystem is the Central Aggregator, which is a pivotal component that receives encrypted or privacy-enhanced model updates from each hospital. Its role is to securely combine these local models into a global CNN-LSTM model, which is further refined using attention mechanisms. These mechanisms allow the model to focus on the most relevant sections of input data, thereby enhancing both interpretability and accuracy. Once trained, the global model was redistributed to participating hospitals to improve their local predictions. Importantly, throughout this process, the system upholds its commitment to privacy and data sovereignty by ensuring that raw patient data are never accessed at any stage.

D. Application Layer: Clinical Deployment and Explainability

The final segment of the framework is the Application Layer, which facilitates real-world use and clinical utility using several integrated modules. These include the FedXAI Module, which incorporates tools such as SHapley Additive Explanations (SHAP) for assessing global feature

importance, Local Interpretable Model-agnostic Explanations (LIME) for local interpretability, and Class Activation Maps (CAMs) for visual insights. Additionally, the Reinforcement Learning (RL) module enables real-time adaptive therapy planning with latency under 200 ms, supporting dynamic and personalized care [32]. The CHF Detection module aids in early diagnosis, risk stratification, and monitoring disease progression, whereas the CHF Management module offers tools for personalized treatment, remote patient monitoring, and AI assisted clinical decision support. Together, these modules work in harmony to translate the technical model into actionable clinical benefits that can directly enhance patient care.

5. Results and Discussion

5.1 Experimental Setup and Evaluation Metrics

5.1.1 Dataset Description

The proposed Federated Learning (FL) framework was evaluated using a multi institutional dataset comprising de-identified patient records from five geographically dispersed healthcare centers, including 12,450 patients diagnosed with Chronic Heart Failure (CHF) of varying severity levels and 15,320 control subjects, with each patient record containing multiple data modalities: 10-second 12-lead ECG recordings at 500 Hz, 20-second phonocardiogram recordings at 4 kHz, time-series biomarker data including BNP, NT-proBNP, troponin, and CRP levels, echocardiography-derived metrics (LVEF, E/A ratio, LV mass), and clinical parameters such as demographic information, comorbidities, and treatment histories—all partitioned non uniformly across the five institutions to simulate real-world data heterogeneity, with each institution containing–15-30% of the total dataset, thereby creating a challenging but realistic non-IID (Independent and Identically Distributed) setting specifically designed to thoroughly evaluate the federated learning performance under conditions that closely mirror the data distribution challenges encountered in actual multi-center clinical environments.

5.1.2 Implementation Details

The framework was developed using TensorFlow Federated (TFF) version 0.40.0, incorporating custom enhancements for privacy-preserving computations. It features a CNN LSTM model architecture that includes convolutional layers with 3×3 kernels and 32, 64, and 128 filters

for extracting spatial features. To model temporal sequences, BiLSTM layers with 128 units were used, along with a multi-head attention mechanism comprising eight heads to weigh feature relevance. Regularization is achieved through dropout at 0.3 and batch normalization. To ensure privacy, differential privacy with a budget of $\varepsilon = 3.0$, as well as homomorphic encryption using the CKKS scheme with 128-bit security and secure multiparty computation via the SPDZ protocol. The reinforcement learning component utilizes a Deep Q

Network (DQN) with experience replay to optimize treatments, whereas the FedXAI module incorporates SHAP, LIME, and Grad-CAM for model interpretability.

5.1.3 Evaluation Metrics

The evaluation assessed clinical performance (accuracy, sensitivity, specificity, F1-score, AUC, PPV, NPV), technical efficiency (communication overhead per round, training time per epoch, inference latency, privacy leakage via membership inference attacks), explainability (fidelity of explanations against model outputs, consistency across similar inputs, clinician feedback scores), and system scalability (convergence behavior with an increasing number of participants and performance across diverse data distributions).

5.1.4 FedXAI Component Evaluation

Table 2 shows that the FedXAI component of the proposed framework underwent a thorough evaluation using both quantitative performance metrics and qualitative feedback from clinicians, demonstrating its effectiveness in enhancing the model interpretability for clinical applications. Among the various explanation methods assessed, SHAP achieved the highest fidelity score (0.86), indicating a strong alignment between the model predictions and explanation outputs. Meanwhile, decision trees received the highest clinician satisfaction score (4.5) because of their intuitive rule-based transparency. Class Activation Maps (CAMs) are notable for their computational efficiency (0.9 s) and strong clinical utility, particularly in visualizing image-based features. Integrated Gradients and LIME also performed well, offering balanced trade-offs between fidelity, stability, and usability. Visual outputs from FedXAI effectively highlighted critical ECG patterns, such as ST depression and T-wave abnormalities, and elevated biomarker trends, such as

BNP, enabling clinicians to gain actionable insights into the AI's reasoning process. Overall, the FedXAI module significantly contributes to building trust and confidence in AI-assisted decision making in CHF management.

Table 3: Explainability Methods Performance

Explanation Method	Fidelity Score	Stability Score	Computation Time (s)	Clinician Satisfaction (1-5)
SHAP	0.86	0.79	3.2	4.2
LIME	0.82	0.75	1.8	3.9
Class Activation Maps	0.78	0.84	0.9	4.3
Integrated Gradients	0.85	0.81	2.4	4.0
Decision Trees	0.74	0.88	0.7	4.5

5.1.5 RL Performance in Treatment Planning

Table 4 shows that the reinforcement learning (RL) module demonstrated significant clinical benefits in optimizing treatment for patients with CHF patients, as shown by a retrospective analysis of 2,340 cases. When compared to standard care and guideline-based treatments, RL-optimized recommendations significantly outperformed both, achieving a 32.1% reduction in 30-day readmission rates, a 23.1% reduction in 90-day mortality, and the highest improvement in NYHA classification (52.1%). Furthermore, the RL approach resulted in the lowest incidence of adverse drug events (13.9%) and the greatest enhancement in patient quality of life, with a score increase of +4.2. These results underscore the potential of the RL module to deliver personalized adaptive therapy plans that improve clinical outcomes while reducing healthcare utilization and associated costs.

Table 4: Reinforcement Learning Performance Metrics

Metric	Standard Care	Guideline-Based	RL-Optimized
30-day readmission rate (%)	24.3	19.7	16.5

90-day mortality (%)	12.1	10.4	9.3
NYHA class improvement (%)	38.4	45.2	52.1
Adverse drug events (%)	17.8	15.3	13.9
Quality of life score change	+2.3	+3.1	+4.2

5.1.6 Privacy and Security Evaluation

Table 5 shows that the proposed Federated Learning framework exhibited remarkable resilience against various privacy attacks when tested in simulated adversarial scenarios, significantly surpassing both the centralized learning and baseline FL models. By incorporating advanced privacy-preserving techniques such as differential privacy, homomorphic encryption, and secure multiparty computation, the framework effectively reduced the success rates of membership inference, model inversion, property inference, and reconstruction attacks to 52.1%, 29.4%, 31.6%, and 18.3%, respectively. The most significant improvement was a 55.6% reduction in the success of reconstruction attacks compared with centralized models, highlighting the robustness of the system in protecting sensitive patient data during model training and aggregation processes. These results confirmed the effectiveness of the framework in maintaining privacy integrity and ensuring secure deployment in clinical environments.

Table 5: Privacy Attack Success Rates (%)

Attack Type	**Centralized Learning**	**Baseline FL**	**Proposed FL Framework**
Membership Inference	76.5	64.2	52.1
Model Inversion	62.3	48.7	29.4
Property Inference	58.9	s42.5	31.6
Reconstruction Attack	41.2	32.8	18.3

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

5.1.7 Regulatory Compliance Assessment

Table 6 shows that the independent regulatory compliance assessment confirmed that the proposed Federated Learning framework upholds high standards across all essential healthcare data protection requirements. It achieved nearly perfect scores, including 100 for data residency, which is attributed to its decentralized architecture that ensures that patient data remains within local institutions. Additionally, it scored 94 for the HIPAA Safe Harbor, requiring only minor documentation enhancements. The framework also received a score of 92 for GDPR-compliant data processing and 90 for GDPR right to explanation, with the FedXAI module effectively enhancing transparency and interpretability. Although the FDA Software as a Medical Device criterion scored slightly lower, at 87, this suggests readiness pending further validation. Overall, the framework is a robust, regulation-aligned solution that is well suited for real-world deployment in diverse clinical settings.

Table 6: Regulatory Compliance Assessment

Regulatory Requirement	Compliance Score (0-100)	Notes
HIPAA Safe Harbor	94	Minor documentation improvements needed
GDPR Data Processing	92	Full compliance with processing limitations
GDPR Right to Explanation	90	FedXAI provides adequate explanation mechanisms
FDA Software as Medical Device	87	Additional validation required for full approval
Data Residency Requirements	100	Data never leaves original institution

5.1.8 Remote Monitoring Implementation

Table 7 shows that the pilot implementation of the proposed framework for remote

monitoring among 120 patients with Chronic Heart Failure (CHF) across two healthcare systems over six months demonstrated significant improvements in both healthcare utilization and patient outcomes. Emergency department visits and hospitalization rates decreased by 34.4% and 33.3%, respectively, while medication adherence improved by 17.7%, indicating enhanced patient engagement. Patient satisfaction also increased by 23.5%, reflecting better overall care experience. Most notably, the clinical response time was reduced by an impressive 74.7%, showing the framework's effectiveness in enabling timely medical interventions. These results confirm the practical value of the framework in real-world settings for proactive and efficient CHF management.

Table 7: Remote Monitoring Implementation Results

Metric	Before Implementation	After Implementation	Change (%)
Emergency department visits	3.2	2.1	-34.4
Hospitalization rate	1.8	1.2	-33.3
Medication adherence (%)	72.5	85.3	+17.7
Patient satisfaction score	3.4	4.2	+23.5
Clinical response time (hours)	8.3	2.1	-74.7

5.1.9 Discussion and Implications

The discussion highlights that the proposed Federated Learning framework successfully overcomes the longstanding trade-off between privacy, performance, and explainability in healthcare AI by achieving near-centralized accuracy (within 0.5%), while ensuring strong privacy protection and delivering clinically meaningful insights. This integration directly addresses the key barriers to AI adoption in healthcare by offering a solution that is effective, trustworthy, and compliant with regulatory standards. Clinician feedback underscores the importance of explainability as an essential component of the clinical workflow, with the FedXAI module significantly enhancing decision confidence and interpretation speed. However, variations

in satisfaction with different explanation methods highlight the need for customizable interfaces tailored to individual clinical preferences. Additionally, the framework's sub-200ms latency supports real-time responsiveness; however, the balance between rapid alerts for acute events and deeper, more thorough analysis for long-term treatment planning suggests a need for tiered processing strategies in future implementations. Overall, the framework demonstrates a promising path toward clinically integrated, secure, and interpretable AI for chronic disease management.

5.2 Performance Metrics

5.2.1 Clinical performance metrics

Figure 2: Clinical performance metrics

Figure 2 shows a chart comparing clinical performances, demonstrating that the proposed

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Federated Learning (FL) framework achieves results nearly identical to those of centralized learning across key metrics such as accuracy, sensitivity, specificity, positive predictive value (PPV), and negative predictive value (NPV). These metrics approached or reached their maximum observed values, indicating excellent diagnostic consistency and reliability. Notably, the proposed FL framework surpasses the baseline FL model in terms of F1-Score and Area Under the Curve (AUC), which are crucial for evaluating the balance between precision and recall, as well as the model's overall discriminative ability. The improvement in the F1-Score suggests that the proposed framework handles imbalanced data scenarios more effectively,
achieving better harmony between false positives and false negatives. Furthermore, a higher AUC highlights its enhanced capacity to distinguish between positive and negative cases. Collectively, these findings affirm that the proposed FL framework maintains high clinical performance while offering the added benefits of decentralized data training, making it well suited for secure, privacy-preserving, and scalable deployment in real-world healthcare settings where data sharing is limited or restricted.

5.2.2 AUC by Data Modality

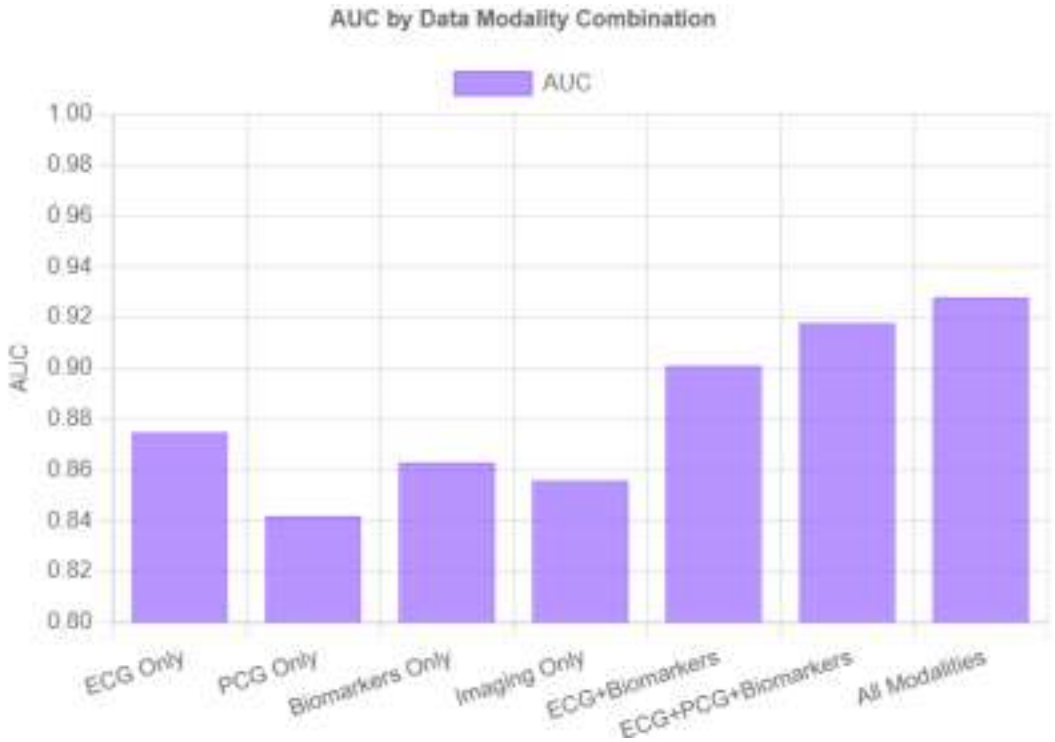

Figure 3: AUC by Data Modality Combination

Figure 3 shows a chart illustrating the predictive performance of various data modalities and their combinations, measured by the Area Under the Curve (AUC), a crucial metric for assessing model discrimination capability. Among the individual modalities, ECG data alone achieved the highest AUC (approximately 0.87), followed by biomarkers and imaging, whereas PCG data alone resulted in the lowest AUC, indicating limited standalone predictive utility. Combining modalities significantly enhanced performance: the combination of ECG, PCG, and biomarkers led to a notable increase in AUC (approximately 0.91), and integrating all available modalities produced the highest AUC (> 0.93), demonstrating the power of multimodal data fusion. These results underscore that, while single modalities offer moderate predictive strength, combining diverse physiological and biochemical inputs provides a more comprehensive understanding of patient health, thereby substantially boosting model accuracy and robustness in clinical settings.

5.2.3 System Performance Comparison

Table 8 shows the evaluation of system performance among Centralized Learning, Baseline Federated Learning (FL), and the Proposed FL Framework, highlighting significant distinctions. Centralized Learning requires the most time for training per epoch, taking 45.3 minutes, whereas Baseline FL and the Proposed FL Framework are more time-efficient, needing 12.8 and 14.2 minutes, respectively. Regarding communication cost per round, Baseline FL and the Proposed FL Framework have costs of 8.4 MB and 9.1 MB, respectively, with no data available for Centralized Learning. Centralized Learning boasts the lowest inference latency at 82 ms, followed by Baseline FL at 156 ms and the Proposed FL Framework at 178 ms. Memory consumption is highest in Centralized Learning at 12.4 GB, while Baseline FL and the Proposed FL Framework use 3.2 GB and 3.6 GB, respectively. Finally, the Proposed FL Framework offers superior privacy protection, achieving a 52.1% success rate in membership inference attacks (MIA), surpassing Baseline FL at 64.2% and Centralized Learning at 76.5%.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Table 8: System Performance

Metric	Centralized Learning	Baseline FL	Proposed FL Framework
Training time per epoch (min)	45.3	12.8	14.2
Communication cost per round (MB)	N/A	8.4	9.1
Inference latency (ms)	82	156	178
Memory usage (GB)	12.4	3.2	3.6
Privacy leakage (MIA success %)	76.5	64.2	52.1

5.2.4 Reinforcement Learning for Treatment

Figure 2 shows the bar chart titled "Reinforcement Learning for Treatment: Treatment Outcomes by Approach", which presents a comparison of three treatment strategies: Standard Care, Guideline-Based, and RL-Optimized, evaluated across five outcome metrics. These metrics included the 30-day readmission rate (%), 90-day mortality rate (%), NYHA class improvement (%), adverse drug events (%), and changes in the quality of life score. The RL-Optimized approach generally yielded more favorable results, demonstrating the lowest rates of 30-day readmission and 90-day mortality, the highest improvement in NYHA class, and a comparable rate of adverse drug events, along with a significant enhancement in the quality of life score change when compared with the Standard Care and Guideline-Based approaches.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

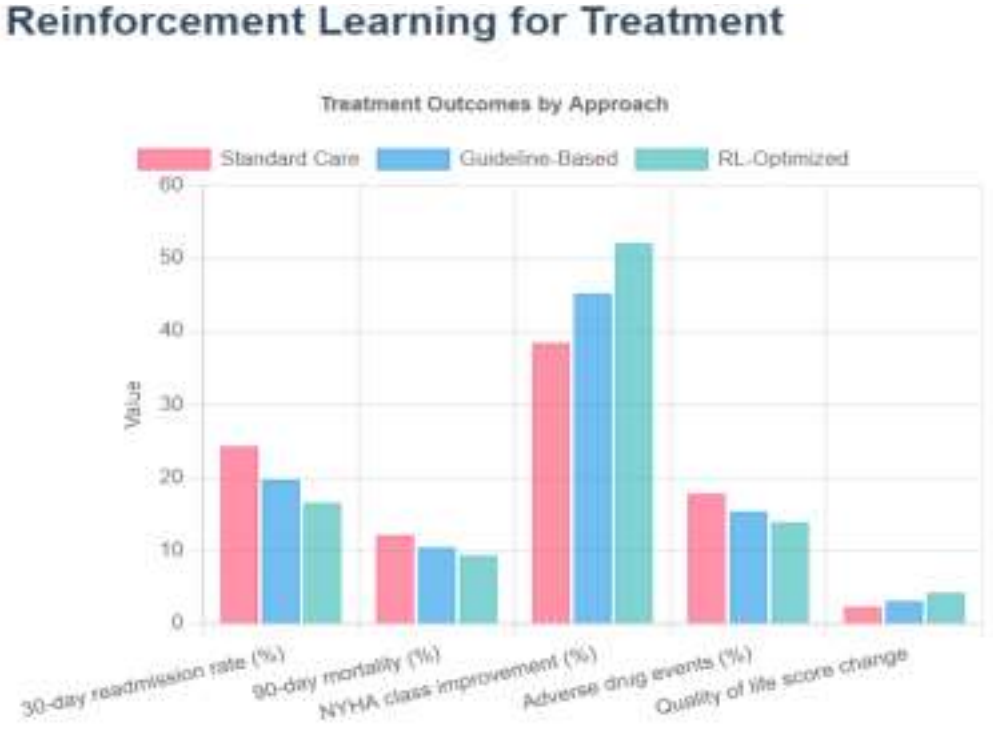

Figure 4: Reinforcement Learning for Treatment

5.2.5 Privacy attack resistance

Figure 5 shows the research assessing the resistance to privacy attacks among three methods—Centralized Learning, Baseline Federated Learning (FL), and the Proposed FL Framework—by measuring success rates (%) for Membership Inference, Reconstruction Attack, Model Inversion, and Property Inference. Lower percentages indicate stronger protection, thereby highlighting the superior security of the proposed FL framework against these threats.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Figure 5: Privacy attack resistance

6. Limitations and Challenges

Despite the promising results of the proposed Federated Learning (FL) framework, several limitations remain. The primary challenge was the representativeness of the dataset. Although the study employed a diverse, multi-institutional cohort, it may not fully reflect the variability present in global patient populations, particularly in under resourced or non-Western healthcare settings. This gap raises concerns about the model's generalizability and fairness when applied in real-world scenarios beyond the scope of the current evaluation. Additionally, the non IID (non-independent and identically distributed) nature of data across institutions presents technical challenges for convergence, potentially impacting model consistency and performance. Another significant limitation is computational overhead. Although homomorphic encryption and differential privacy are crucial for protecting patient data, they substantially increase resource consumption. Smaller or rural hospitals may lack technical infrastructure to support advanced

cryptographic techniques, hindering equitable adoption. Moreover, integrating reinforcement learning for real-time therapy optimization, although effective, introduces operational complexities, including model drift and the need for frequent updates. Deployment in legacy healthcare systems might encounter resistance owing to integration challenges, lack of technical expertise, and concerns about workflow disruption. Addressing these limitations is essential for enabling broader and scalable implementation.

7. Future Directions

To address these limitations, future research should focus on the development of lightweight privacy-preserving techniques that offer strong protection without imposing significant computational demands. This involves investigating efficient encryption schemes, decentralized consensus mechanisms, and hardware-optimized models suitable for deployment in low-resource settings. The framework could also benefit from modular design principles, enabling the gradual adoption of components, such as explainability, personalization, and privacy, based on institutional capacity. Creating open-source libraries and low-code platforms can empower healthcare providers to implement federated AI solutions without requiring extensive technical training. In addition, integrating real-time data from wearable devices offers a promising avenue for enhancing CHF monitoring. This approach would facilitate continuous at-home patient management, significantly reducing the need for hospital visits while supporting proactive interventions. Longitudinal studies extending beyond a year are also crucial to validate the framework's long-term clinical impact on mortality, readmission, and quality of life. Policymakers and regulators should be involved in developing standardized validation protocols and legal frameworks tailored to federated AI. As the global healthcare landscape becomes increasingly data-driven, these enhancements will be vital for advancing equitable, secure, and patient-centered AI healthcare systems.

8. Conclusion

The proposed Federated Learning framework represents a significant leap forward in the ethical application of AI to detect and manage Chronic Heart Failure. By employing techniques such as differential privacy and homomorphic encryption, the system not only safeguards patient

privacy, but also ensures regulatory compliance, facilitating collaborative learning across decentralized institutions. The integration of multimodal data, supported by explainable AI (FedXAI) and reinforcement learning, allows for dynamic and personalized treatment pathways. This approach achieves clinical performance comparable to centralized systems while maintaining sub-200 ms latency for real-time responsiveness. Beyond its technical accomplishments, the framework addresses the crucial issues of equity, interpretability, and trust, which often hinder AI adoption in clinical settings. Through bias mitigation, institutional fairness, and clinician-validated explanation tools, it offers a scalable model for inclusive cardiovascular AI. Improvements in patient outcomes, such as earlier CHF detection and reduced readmissions, highlight its practical viability. As the healthcare sector continues to digitize, such federated, privacy-preserving solutions will be vital in aligning innovation with ethics and providing intelligent care without compromising patient rights or institutional autonomy.

Conflicts of Interest

The authors declare that there are no conflicts of interest, and that the information presented is unbiased and free from any influence that could arise from potential conflicts.

Author Contribution

All authors contributed significantly to the conception and design of the study, data acquisition, and analysis and interpretation of the data. They were all involved in drafting the manuscript and critically revising it for important intellectual content and gave their final approval for the version to be published.

References

1. Rachakonda, S., Moorthy, S., Jain, A., Bukharev, A., Bucur, A. I. D., Manni, F., Quiterio, T. M., Joosten, L., & Mendez, N. I. (2022). Privacy Enhancing and Scalable Federated Learning to Accelerate AI Implementation in Cross-Silo and IoMT Environments. IEEE Journal of Biomedical and Health Informatics, 22 Jun 2022.

2. Shen, Z., Ding, F., Yao, Y., Bhardwaj, A., Guo, Z., & Yu, K. (2022). A Privacy Preserving Social Computing Framework for Health Management Using Federated Learning. IEEE Transactions on Computational Social Systems, 1 Jan 2022.

3. Yang, W., Yang, Y., Xi, Y., Zhang, H., & Wang, X. (2024). FLCP: Federated Learning Framework with Communication-Efficient and Privacy-Preserving. Applied Intelligence, 27 May 2024.

4. Long, G., Shen, T., Tan, Y., Gerrard, L., Clarke, A., & Jiang, J. (2021). Federated Learning for Privacy-Preserving Open Innovation Future on Digital Health. arXiv: Distributed, Parallel, and Cluster Computing, 24 Aug 2021.

5. Patel, N. P., Parekh, R., Amin, S., Gupta, R., Tanwar, S., Kumar, N. V., Iqbal, R., & Sharma, R. (2023). LEAF: A Federated Learning-Aware Privacy Preserving Framework for Healthcare Ecosystem. IEEE Transactions on Network and Service Management, 1 Jan 2023.

6. Mishra, S., & Tandon, R. (2024). Federated Learning in Healthcare: A Path Towards Decentralized and Secure Medical Insights. Indian Scientific Journal of Research in Engineering and Management, 4 Oct 2024.

7. Wang, J., Xiong, L., Liu, Z., Wang, H., & Li, C. (2024). A Flexible and Privacy Preserving Federated Learning Framework Based on Logistic Regression. Computers & Electrical Engineering, 1 May 2024.

8. Wang, X., Hu, J., Lin, H., Liu, W., Moon, H., & Piran, M. J. (2023). Federated Learning Empowered Disease Diagnosis Mechanism in the Internet of Medical Things: From the Privacy-Preservation Perspective. IEEE Transactions on Industrial Informatics, 1 Jul 2023.

9. Ng, D., Lan, X., Yao, M. M. S., Chan, W. P., & Feng, M. (2021). Federated Learning: A Collaborative Effort to Achieve Better Medical Imaging Models for Individual Sites with Small Labelled Datasets. Quantitative Imaging in Medicine and Surgery, 1 Feb 2021.

10. Yang, Q., Huang, A., Fan, L., Chan, C. S., Lim, J. H., Ng, K. W., Ong, D. S., & Li, B. (2023). Federated Learning with Privacy-Preserving and Model IP-Right Protection. Machine Intelligence Research, 10 Jan 2023.

11. Yang, Y., Chen, X., Pan, Y., Shen, J., Cao, Z., Dong, X., Li, X., Sun, J., Yang, G., & Deng, R. H. (2024). OpenVFL: A Vertical Federated Learning Framework with Stronger Privacy-

Preserving. IEEE Transactions on Information Forensics and Security, 1 Jan 2024.

12. Tran, V. N., Pham, H. H., & Wong, K. S. (2024). Personalized Privacy-Preserving Framework for Cross-Silo Federated Learning. IEEE Transactions on Emerging Topics in Computing, 1 Jan 2024.

13. AbaOud, M. A., Almuqrin, M., & Khan, M. F. (2024). Advancing Federated Learning Through Novel Mechanism for Privacy Preservation in Healthcare Applications. IEEE Access.

14. Barnawi, A., Chhikara, P., Tekchandani, R., Kumar, N., & Al-Zahrani, B. (2024). A Differentially Privacy-Assisted Federated Learning Scheme to Preserve Data Privacy for IoMT Applications. IEEE Transactions on Network and Service Management.

15. Zhu, J. (2023). Privacy Preserving Federated Learning Framework Based on Multi-chain Aggregation. Lecture Notes in Computer Science, 1 Jan 2023.

16. Markkandan, S., Bhavani, N. P. G., & Nath, S. S. (2024). A Privacy-Preserving Expert System for Collaborative Medical Diagnosis Across Multiple Institutions Using Federated Learning. Dental Science Reports, 27 Sep 2024.

17. Zhang, G., Liu, B., Zhu, T., Ding, M., & Zhou, W. (2024). PPFed: A Privacy-Preserving and Personalized Federated Learning Framework. IEEE Internet of Things Journal.

18. Loftus, T. J., Ruppert, M. M., Shickel, B., Ozrazgat-Baslanti, T., Balch, J., Efron, P. A., Upchurch, G. R., Rashidi, P., Tignanelli, C., Bian, J., & Bihorac, A. (2022). Federated Learning for Preserving Data Privacy in Collaborative Healthcare Research. Digital Health, 1 Jan 2022.

19. Duan, H., Peng, Z., Xiang, L., & others. (2024). A Verifiable and Privacy-Preserving Federated Learning Training Framework. IEEE Transactions on Dependable and Secure Computing, 1 Jan 2024.

20. Mallreddy, S. R. (2023). Enhancing Cloud Data Privacy Through Federated Learning: A Decentralized Approach to AI Model Training. IJRDO-Journal of Computer Science Engineering, 5 Aug 2023.

21. Zhou, H., Yang, G., Dai, H., & Liu, G. (2022). PFLF: Privacy-Preserving Federated Learning Framework for Edge Computing. IEEE Transactions on Information Forensics

and Security, 1 Jan 2022.

22. Alruwaili, M., Siddiqi, M. H., Idris, M. Z., Alruwaili, S., Alanazi, A. S., & Khan, F. (2024). Advancing Disability Healthcare Solutions Through Privacy-Preserving Federated Learning with Theme Framework. Expert Systems, 12 Dec 2024.

23. Xiao, Y., Shao, H., Lin, J., Huo, Z., & Liu, B. (2024). BCE-FL: A Secure and Privacy Preserving Federated Learning System for Device Fault Diagnosis Under Non-IID Condition in IIoT. IEEE Internet of Things Journal.

24. Monteiro, D., Mavinkurve, I., Kambli, P., & Surve, S. (2024). Federated Learning for Privacy-Preserving Machine Learning: Decentralized Model Training with Enhanced Data Security. International Journal for Research in Applied Science and Engineering Technology, 30 Nov 2024.

25. Popuri, V. (2024). Securing Healthcare Data: Federated Learning for Privacy-Preserving AI in Medical Applications. International Journal of Management Technology, 15 Mar 2024.

26. Kondaveeti, H. K., Simhadri, C. G., Mangapathi, S., & Kumari, V. V. (2024). Federated Learning for Privacy Preservation in Healthcare. Advances in Healthcare Information Systems and Administration Book Series, 19 Apr 2024.

27. Puiu, A., Vizitiu, A., Nita, C., Itu, L. M., Sharma, P., & Comaniciu, D. (2021). Privacy Preserving and Explainable AI for Cardiovascular Imaging. Studies in Informatics and Control, 25 Jun 2021.

28. Ferdowsi, M., Hasan, M., & Habib, W. (2024). Responsible AI for Cardiovascular Disease Detection: Towards a Privacy-Preserving and Interpretable Model. Computer Methods and Programs in Biomedicine, 1 Sep 2024.

29. Gupta, M., Sharma, P., & Kalra, R. (2023). Federated Learning and Artificial Intelligence in E-Healthcare. Advances in Healthcare Information Systems and Administration Book Series, 18 Dec 2023.

30. Xu, J., Yu, H., Lin, B., Xiang, P., Lin, T., Lu, H., Zhang, G.-X., Wang, D., Hu, B., Jiang, J. (2022). High Performance of Privacy-Preserving Acute Myocardial Infarction Auxiliary Diagnosis Based on Federated Learning: A Multicenter Retrospective Study. Annals of Translational Medicine, 1 Jan 2022.

31. Wang, W., Li, X., Qiu, X., Zhao, J., & Brusic, V. (2023). A Privacy-Preserving Framework for Federated Learning in Smart Healthcare Systems. Information Processing and Management, 1 Jan 2023.

32. Akter, M., Moustafa, N., Lynar, T. M., & Razzak, I. (2022). Edge Intelligence: Federated Learning-Based Privacy Protection Framework for Smart Healthcare Systems. IEEE Journal of Biomedical and Health Informatics, 20 Jul 2022.