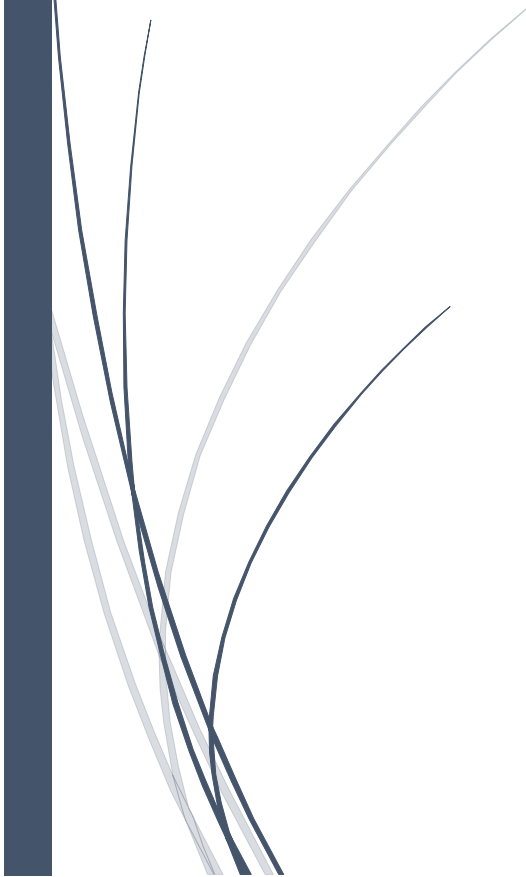


The logo for RADemics, featuring a dark blue vertical bar on the left and a blue arrow pointing right with the text "RADemics" inside.

RADemics

Federated Learning Models for Secure and Distributed Cardiac Health Monitoring in IoT Enabled Pacemaker Ecosystems

An abstract graphic consisting of several thin, curved lines in dark blue and light grey, originating from the bottom left and extending upwards and to the right.

Narasimha Chary Cholleti, Shaik Lal
John Basha

GURU NANAK INSTITUTIONS TECHNICAL CAMPUS,
VIT-AP UNIVERSITY

Federated Learning Models for Secure and Distributed Cardiac Health Monitoring in IoT Enabled Pacemaker Ecosystems

¹Narasimha Chary Cholleti, Associate Professor, Dept of CSE, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India. narasimhachary.dr@gmail.com

²Shaik Lal John Basha, Research Scholar and Assistant professor(C), School of Electronics Engineering, VIT-AP University, Amaravati, Guntur, Andhra Pradesh. sk.laljohn@gmail.com

Abstract

The integration of federated learning (FL) into IoT-enabled pacemaker ecosystems presents a promising solution to the dual challenge of personalized cardiac health monitoring and stringent data privacy requirements. Modern pacemakers continuously collect multi-modal physiological data critical for detecting arrhythmias and adjusting pacing strategies in real time. Conventional centralized learning methods require raw data to be transmitted externally, raising significant security and regulatory concerns. By enabling local model training on-device and sharing only encrypted model updates, FL preserves data locality while enhancing global predictive accuracy through collaborative learning. This chapter explores the architectural foundations, hardware-software co-design strategies, secure communication protocols, and adaptive personalization techniques necessary to deploy FL in resource-constrained, safety-critical pacemaker systems. Technical challenges such as non-IID data, catastrophic forgetting, and adversarial threats are examined alongside privacy-preserving mechanisms and continual learning pipelines. The role of physician oversight and closed feedback loops was highlighted to ensure algorithmic decisions align with clinical standards. By addressing these dimensions, the chapter establishes a blueprint for future research and practical deployment of secure, distributed learning frameworks that advance patient-specific cardiac care while maintaining trust, compliance, and safety within the broader medical IoT landscape.

Keywords: Federated Learning, IoT Pacemakers, Secure Cardiac Monitoring, Privacy-Preserving AI, Personalized Healthcare, Non-IID Data, Continual Learning, Edge AI, Medical IoT, Implantable Devices

Introduction

The evolution of cardiac pacemakers from simple [1], fixed-rate devices to sophisticated, connected systems marks a transformative chapter in cardiovascular medicine. Modern pacemakers, embedded with multi-modal sensors and wireless telemetry modules [2], generate continuous streams of physiological data that extend their role beyond basic rhythm correction [3]. These IoT-enabled implants now form an integral part of broader connected health ecosystems, allowing real-time monitoring, adaptive pacing, and remote clinical oversight [4]. The

convergence of biomedical engineering and digital health has created opportunities to embed intelligent learning capabilities directly within implantable devices [5].

One of the most compelling frontiers in this context was the integration of artificial intelligence to predict arrhythmias, optimize pacing parameters, and adapt to the evolving physiological states of individual patients [6]. Traditionally, machine learning models rely on centralized architectures where raw patient data was aggregated in cloud servers for training [7]. While effective for large-scale pattern recognition, this centralized paradigm conflicts with strict privacy laws [8], exposes sensitive medical information to breaches, and increases the risk of unauthorized misuse of highly personal health data [9]. For implantable devices like pacemakers, which produce deeply intimate biosignals, data sovereignty and privacy-preserving computation are critical [10].

Federated learning has emerged as a promising solution to these challenges by decentralizing model training [11]. Under this approach, each pacemaker processes and learns from its own locally collected data without transferring raw biosignals to external servers [12]. Instead, only encrypted model updates are exchanged with a central aggregator [13], which synthesizes global improvements by combining knowledge from distributed devices. This framework preserves patient privacy, aligns with data protection mandates [14], and harnesses the diversity of real-world cardiac data to enhance predictive accuracy and robustness [15].