ISTANBUL TECHNICAL UNIVERSITY ⋆ GRADUATE SCHOOL

A Unified Framework for Secure and Intelligent ECG Signal Processing via Chaotic Encryption, Fully Homomorphic Computation and Federated Learning

(Ph.D. THESIS)

Author: Beyazıt Bestami YÜKSEL
Supervisor: Assoc. Prof. Dr. Ayşe YILMAZER
Department: Computer Engineering
Date: March 2026

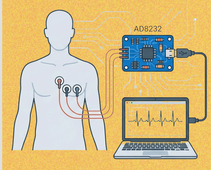
Abstract

This thesis presents a unified privacy-preserving ECG framework integrating real-time acquisition, adaptive chaotic encryption, AES-secured storage, TLS-protected transmission, and homomorphic federated learning. A learnable key generator produces signal-dependent chaotic parameters, enhancing structural confidentiality at the source level. Encrypted gradients are aggregated using homomorphic encryption, preventing data leakage during collaborative training. Experimental results demonstrate high entropy, strong randomness, near-lossless reconstruction, and up to 99% diagnostic accuracy under strict privacy constraints.

Gaps in Literature & Thesis Goal

Gap 1: Lack of Unified Architecture
Existing studies treat encryption, processing, and learning as isolated problems rather than an end-to-end flow.
Gap 2: Real-Time FHE Application
Literature is limited regarding the use of FHE for real-time signal monitoring due to its high computational cost.
Gap 3: Secure Collaborative Learning
While Federated Learning (FL) keeps data local, model updates can still leak information; this risk remains unaddressed in standard implementations.

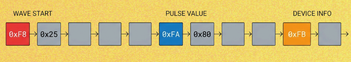
ECG Acquisition and Pre-processing Layer



Hardware Features
- **Sensor:** 3-Channel ECG Preamplifier (AD8232)
- **Transmission:** Serial Port (RS-232 / USB) @ 9600 baud
- **Sampling Rate:** 360 Hz

Preprocessing Pipeline
- Filtering: 4th Order Butterworth (0.5Hz - 45Hz)
- Segmentation: Decomposition of continuous data stream
- Normalization: Z-score standardization

The Language of the Stream: Marker Bytes



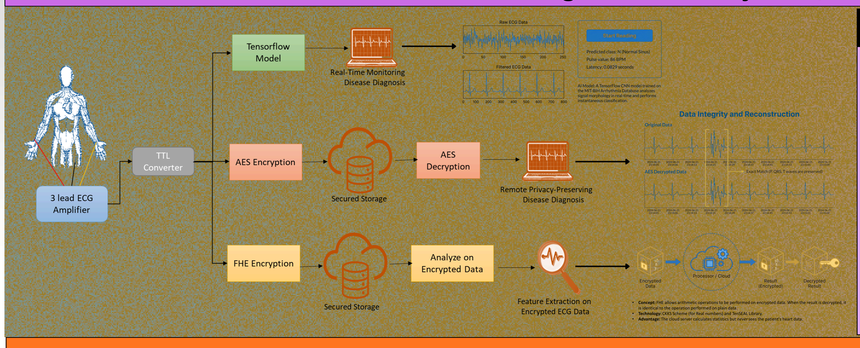
Hex Code	Meaning	Function
0xF8	**Wave Sample**	The subsequent byte represents the amplitude of the ECG signal to be plotted.
0xFA	**Pulse Value**	The subsequent byte is the calculated BPM (heart rate).
0xFB	**Device Info**	Carries status codes such as 'Lead Off' (electrode disconnect).

This marker structure ensures automatic re-synchronization at the next 0xF8 byte if any packet loss occurs.

Methodology

- In this layer, raw ECG data acquired from the hardware with a 300 Hz sampling rate and a 9600 bps baud rate via serial communication is transmitted without latency by utilizing special marker bytes (0xF8, 0xFA, 0xFB) to ensure automatic re-synchronization in case of packet loss.
- The mains noise and respiratory baseline wander present in these transmitted signals are cleaned using a zero-phase, 4th Order Butterworth Band-Pass Filter (0.5 - 45 Hz) to prevent any signal delay.
- Following this, a Discrete Wavelet Transform (DWT) utilizing soft thresholding is applied to eliminate subtle noise without distorting the sharpness of the QRS complex.
- Through these hardware and signal processing steps, raw biological data is transformed into a clinically reliable and clean format ready for feature extraction and AI classification.

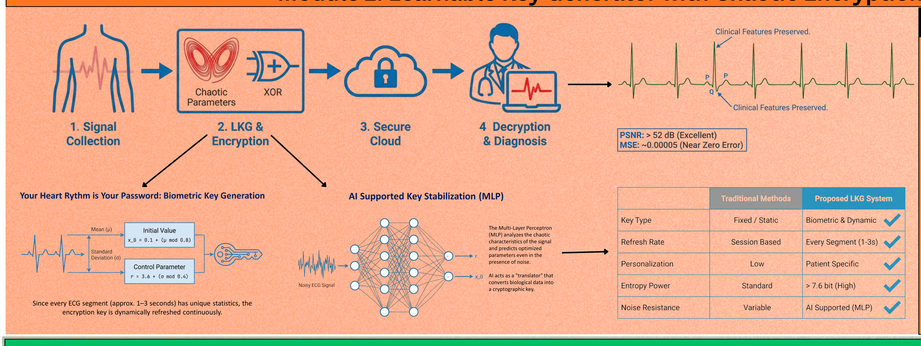
Module 1: Real Time ECG Monitoring and AES+FHE System (ECG-PPS Module)



Methodology

- Real-Time AI Classification: The cleaned ECG signals come from base layer are analyzed by a locally running TensorFlow CNN model in a short duration of approximately 0.08 seconds, providing patients with an instant and latency-free diagnosis.
- AES Pathway (Fast Transmission and Storage): In this speed-focused phase of the system, data is encrypted using AES and transmitted to the cloud with a latency of under 50 milliseconds, completely preserving the integrity of the original waveform (P, QRS, and T waves). Furthermore, secure key exchange is ensured via the ECDH protocol within a TLS framework.
- FHE Pathway (Analysis Without Decryption): Fully Homomorphic Encryption (FHE) is utilized to ensure patient privacy. This allows the cloud server to perform statistical and algorithmic analyses with high clinical accuracy (over 99%) without ever decrypting the data.

Module 2: Learnable Key Generator with Chaotic Encryption

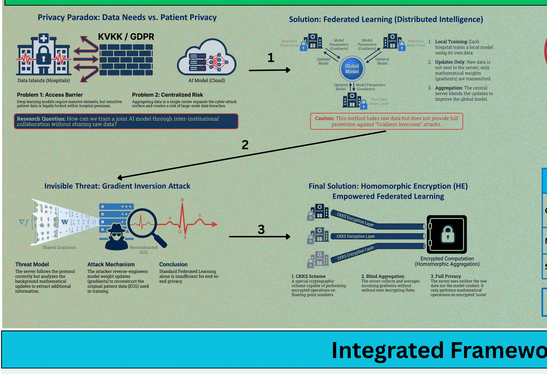


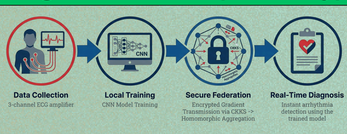
	Traditional Methods	Proposed LKG System
Key Type	Fixed / Static	Biometric & Dynamic ✓
Refresh Rate	Session Based	Every Segment (1-3s) ✓
Personalization	Low	Patient Specific ✓
Entropy Power	Standard	> 7.6 bit (High) ✓
Noise Resistance	Variable	AI Supported (MLP) ✓

Methodology

- The LKG (Learnable Key Generator) module is an innovative biometric security architecture in telemedicine systems that uses the patient's own ECG rhythm as a dynamic encryption key.
- The system generates continuously updated keys by processing statistical features (mean and standard deviation) extracted from 1–3 second signal segments through Chaos Theory, and supports this process with a Multi-Layer Perceptron (MLP) artificial intelligence network to enhance robustness against noise.
- Using these dynamically generated keys, ECG data is encrypted through permutation (shuffling) and XOR (masking) operations, making it completely indistinguishable (uniform) against statistical analysis attacks.
- Overall, this end-to-end system operates with a very low latency of approximately ~340 milliseconds, enabling real-time monitoring while preserving critical clinical diagnostic features such as P and Q waves without loss upon decryption (PSNR > 52 dB).

Module 3: Federated Learning with Homomorphic Encryption





Security Analysis: Threats and Defense

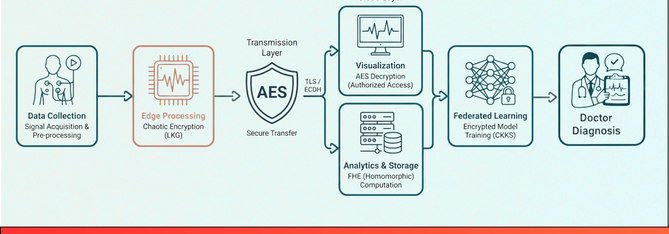
Threat Type	Standard FL (Unprotected)	Proposed FL-HE System
Gradient Inversion	Vulnarable (Data reconstructible) ✗	**Fully Protected** (Encrypted gradients cannot be decrypted) ✓
Model Inference	Possible ✗	**Prevented** (Parameters are hidden) ✓
Server Trust	Requires trust in server	**Resistant** to 'Honest-but-Curious' model

Conclusion: Data never becomes plaintext at any point during the training process (Transmission, Processing, Collection)

Methodology

- The FL-HE module is an architecture that combines Homomorphic Encryption (CKKS scheme) and Federated Learning to ensure data privacy during AI model training across collaborating hospitals.
- In this system, hospitals encrypt the weights (gradients) of their locally trained models before transmitting them to the central server, completely preventing the theft of original patient data via "Gradient Inversion" attacks.
- The central server securely updates the global model by performing "blind aggregation" solely on encrypted noise, without ever decrypting the data at any stage.
- This encryption process does not degrade the AI model's learning capacity, it delivers high accuracy rates equivalent to unencrypted systems, achieving 99.91% in Vertical, 98.18% in Hybrid, and 97.82% in Horizontal Federated Learning scenarios.
- Although the training duration increases between 30% and 456% due to the encryption overhead, this trade-off does not impact the real-time diagnosis (inference) speed provided to patients.
- Consequently, the system delivers end-to-end data privacy that is fully compliant with KVKK and GDPR requirements without compromising clinical performance or inference speed.

Integrated Framework and Cross Module Analysis



Pipeline Architecture & Data flow and security boundaries

- The unified privacy-preserving pipeline establishes a multi-layered, defense-in-depth architecture by mapping distinct cryptographic mechanisms to formally defined security boundaries across the ECG data lifecycle.
- Boundary B1 (Source/Acquisition): Raw ECG signals are immediately secured at the edge device via biometric-adaptive chaotic encryption. This acts as a data-level confidentiality primitive that protects the signal prior to any external exposure.
- Boundary B2 (Transmission and Storage): To protect against network-based adversaries, the already chaotic-encrypted segments are further secured using AES encryption over TLS with ECDH key exchange. This boundary ensures robust confidentiality during channel transmission and cloud storage.
- Boundary B3 (Computation/Analytical): Within the cloud and federated learning domains, Fully Homomorphic Encryption (FHE via the CKKS scheme) is deployed to enable statistical analytics and computations directly on encrypted data. In this isolated security boundary, collaborating institutions share only FHE-encrypted model updates (gradients), effectively preventing data reconstruction or gradient inversion attacks by an honest-but-curious central server.
- Ultimately, this boundary-aligned cryptographic allocation ensures that a compromise at any single point in the data flow does not expose the underlying plaintext patient data.

Publications on the Thesis

- Yuksel, B. B., and Yilmazer-Metin, A., (2026). HEART: A high-efficiency adaptive real-time telemonitoring framework for secure ECG signal transmission using chaotic encryption, ***Electrica***, doi: 10.5152/electrica.2026.25232.
- Yuksel, B. B., & Yilmazer Metin, A. (2026). Federated learning with homomorphic encryption for secure real-time ECG anomaly detection: A multi-institutional privacy-preserving framework. ***Biomedical Signal Processing and Control***, 116, 109557. https://doi.org/10.1016/j.bspc.2026.109557
- Yuksel, B. B., and Yilmazer Metin, A., (2026). Artificial Intelligence Breakthroughs and Data Futures: A Retrospective and Prospective Review, ***APJESS***, vol. 14, no. 1, pp. 1–16, Jan. 2026, doi: 10.21541/apjess.1705042.
- Yuksel, B. B., & Yilmazer-Metin, A. (2024). ECG-PPS: Privacy Preserving Disease Diagnosis and Monitoring System for Real-Time ECG Signals, 2024, ***17th International Conference on Security of Information and Networks (SIN)***.
- Yuksel, B. B., & Yilmazer-Metin, A. (2024). (2025). Advancing Biomedical Signal Security: Real-Time ECG Monitoring with Chaotic Encryption, ***1st ITU Software Developers Meeting Symposium***.

All projects codes are available github.com/bbyuksel