Journal of Computing and Security

Research Article, 2026, Volume 13, Number 1 (pp. 23–34)

http://www.jcomsec.org

Integrating VGG16 with the ACIMD Protocol to Enhance Security and Reliability in ECG-Based Remote Authentication Systems

Narges Eshaghi [a] Mohammad Habibi [a,*] Nasour Bagheri [b,c] Ali Khatibi [a]

[a] *Department of Mathematics, Tafresh University, Iran.*

[b] *CPS2 Lab, Department of Communication, Faculty of Electrical Engineering, Shahid Rajaee Teacher Training University, Lavizan, Tehran, Iran.*

[c] *Electronics Research Institute, Sharif University of Technology, Tehran, Iran.*

ARTICLE INFO.

Article history:
Received: 18 June 2025
Revised: 27 December 2025
Accepted: 15 February 2026
Published Online: 16 May 2026

Keywords:
ECG Authentication, Distance Bounding Protocol, Remote Telemetry, ACIMD Protocol, VGG16 Deep Learning Model.

ABSTRACT

The security of Implantable Medical Devices (IMDs) is of paramount importance, as unauthorized access can lead to life-threatening consequences. Electrocardiogram (ECG) signals present a promising biometric modality for authentication due to their inherent uniqueness and capability for liveness detection capability. However, wireless ECG-based systems are vulnerable to relay attacks, necessitating robust proximity verification. This study proposes a novel, integrated authentication framework that addresses both user identification and physical proximity. We enhance the established Access Control for Implantable Medical Devices (ACIMD) distance-bounding protocol by incorporating a fine-tuned VGG16 deep convolutional neural network to achieve high-accuracy ECG biometric verification. The system was rigorously evaluated using the MIT-BIH Arrhythmia Database. The integrated model achieved an overall authentication accuracy of 99.45%, surpassing the baseline ACIMD protocol accuracy of 97.82%. This represents an average improvement of 1.63% across various physical distance thresholds. Although integrating VGG16 increased the total authentication time from 0.0113 s to 0.0437 s, this remains well within acceptable limits for real-time medical applications. Crucially, we provide new evidence for improved system reliability, demonstrating superior robustness against signal noise compared to the baseline. The proposed system effectively balances high biometric fidelity with stringent physical-layer security, offering a comprehensive solution for secure remote authentication in critical applications such as IMDs.

1 Introduction

Authentication plays a critical role in defending modern systems, particularly for critical infrastructure such as Implantable Medical Devices (IMDs). A robust authentication mechanism must balance accuracy, speed, and security [1]. Biometric approaches—such as those using fingerprints, irises, and Electrocardio-

* Corresponding author.
Email address: mhabibi@tafreshu.ac.ir (M. Habibi)
https://dx.doi.org/10.22108/jcs.2026.145712.1173
ISSN: 2322-4460

gram (ECG) signals—are noted for their complexity and resistance to forgery, as they are inherent to living users. Among these, ECG signals represent a unique biometric descriptor with significant potential due to their inherent qualities of uniqueness, stability, and ability to confirm liveness.

Advances in telemetry have enabled the wireless monitoring of ECG signals, eliminating the need for physical connections during authentication. In such a paradigm, an implant or wearable device measures the user's ECG and transmits it wirelessly. The live signal is then compared against a stored template for verification [2]. A primary security concern in this wireless setting is ensuring the signal originates from a legitimate user in close physical proximity. Without this guarantee, an attacker could relay signals from an authorized user located elsewhere [3]. To mitigate such relay and man-in-the-middle attacks, Distance Bounding (DB) protocols are essential. These protocols verify physical proximity by precisely measuring the round-trip time (RTT) of cryptographic challenge-response exchanges [4].

Designing security solutions for IMDs must also account for severe resource constraints, including limited battery life and computational power. While asymmetric cryptography provides strong security guarantees, its high computational cost can detrimentally impact device longevity. Consequently, lightweight symmetric cryptographic solutions are often preferred, despite key distribution challenges. Protocols such as ACIMD (Access Control for Implantable Medical Devices) have been developed to provide both authentication and proximity verification while minimizing computational and communication overhead [5].

Concurrently, deep learning models, particularly Convolutional Neural Networks (CNNs), have demonstrated remarkable success in processing ECG signals for biometric identification. The VGG16 architecture, a well-known deep CNN, has proven highly effective in extracting hierarchical features from images. By transforming 1D ECG signals into 2D time-frequency representations (e.g., spectrograms), the VGG16 model can be adapted to achieve high accuracy in ECG-based authentication [6]. However, its integration into a complete, proximity-aware security framework combining biometric verification with a formal distance-bounding protocol remains an unexplored area.

Recent advancements continue to address both computational efficiency and security in ECG authentication and proximity verification systems. Thite and Jagtap (2025) showcased the capabilities of enhanced deep neural architectures with a Reinforced VGG-16 framework for complex ECG pattern classification [7]. Al Alfi et al. (2025) developed a real-time biometric

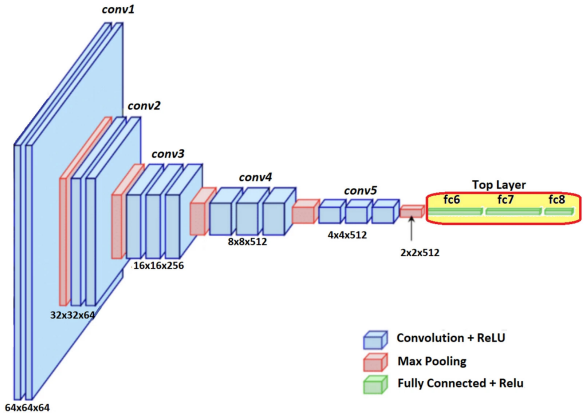

Figure 1. The Structure of the VGG16 Model (conv: convolutional layers, fc: fully connected layers)[6].

authentication framework that merges Graph Convolutional Networks (GCN) with Mutual Information indices to capture subtle patterns in ECG signals, enhancing robustness against evolving cybersecurity threats and providing higher adaptability [8]. Dong et al. (2025) introduced a multi-modal pretraining scheme for ECG authentication that remains highly accurate and stable even in open-set, real-world scenarios, significantly improving system reliability and minimizing false accept rates [9]. Qin et al. (2025) built on the Gramian Angular Field (GAF) methodology by proposing GAF-FusionNet, a multimodal ECG classification network that seamlessly combines time-series and image-based information for improved diagnostic precision, achieving leading accuracy across diverse datasets [10]. Mageshbabu and Mohana (2024) developed a lightweight machine learning model, directly addressing the critical trade-off between security and resource consumption in IMDs [3]. Camara et al. (2023) achieved remarkable accuracy by converting ECG signals into Gramian Angular Field (GAF) images and utilizing a customized ResNet architecture [11]. This highlights the trend towards using complex, image-based deep learning models for high-accuracy identification. Jiang et al. (2022) introduced a lightweight 1D-CNN for ECG authentication, focusing on computational efficiency [12]. While their model achieved high accuracy, it lacked an integrated, explicit security mechanism for proximity verification, representing a significant gap in developing a holistic security solution. Ding et al. (2025) further broadened ECG biometric capabilities by integrating phonocardiogram signals for multi-class heart condition classification, underscoring the trend toward multi-sensor fusion and deep learning in healthcare authentication [13]. In proximity verification, Ye et al. (2025) performed a comprehensive formal verification of physical layer security protocols, demonstrating the effectiveness of watermarked and jammed solutions in safeguarding authentication and session key

derivation against both passive and active adversaries, using advanced formal modeling techniques for rigorous assurance [14]. Nkrow et al. (2024) discussed persistent distance-bounding protocols tailored for mobile scenarios, emphasizing consistent and secure evaluation even in noisy or adversarial environments. Recent studies also spotlight lightweight models, such as MobileNetV1+GRU architectures for ECG authentication, which offer strong performance under noise and real-world conditions while maintaining minimal computational overhead—critical for resource-limited devices [15]. Khalil et al. (2024) proposed a cross-layer RF distance-bounding scheme for ubiquitous computing systems, effectively mitigating relay attacks with low energy consumption by integrating physical-layer properties with protocol-layer security [4]. Debant et al. (2023) conducted a formal analysis of distance-bounding protocols under an active adversary model, identifying vulnerabilities in designs reliant on short nonces and underscoring the importance of a robust challenge-response design [16].

This work bridges the gap between high-accuracy biometrics and lightweight, proximity-verified security. Our primary contribution is the novel integration of the high-performance VGG16 deep learning model with the resource-efficient ACIMD distance-bounding protocol. This integration creates a holistic authentication scheme that leverages the unique features of ECG signals for accurate user identification while inherently verifying user proximity. The proposed system is rigorously evaluated using comprehensive performance metrics (accuracy, precision, recall, F1-score, ROC-AUC, and response time), along with a new analysis of reliability under noise, demonstrating its applicability for secure remote telemetry systems.

The rest of this article is organized as follows. The related works are reviewed in Section 1 (Introduction), where prior studies on ECG-based authentication, distance bounding protocols, and deep learning models are discussed. In Section 2, the proposed integrated framework (ACIMD-VGG16) is described in detail, including dataset preprocessing, adaptation of the VGG16 model for ECG signals, and the two-phase authentication protocol combining biometric verification and proximity verification. The details of the experiments on the MIT-BIH Arrhythmia Database, including performance metrics, optimization of signal windowing, timing analysis, and reliability evaluation under noise, are presented in Section 3 (Results and Discussion). Finally, the study is concluded in Section 4, where limitations and future work are also outlined.

2 Materials and Methods

In this section, the materials and methods employed to develop the proposed authentication framework are described in detail. First, the MIT-BIH Arrhythmia Database, used as the benchmark dataset, is introduced along with the preprocessing steps including Discrete Wavelet Transform (DWT) for noise reduction. Next, the adaptation of the VGG16 deep convolutional neural network for ECG-based biometric verification is explained, focusing on the conversion of one-dimensional ECG signals into two-dimensional spectrograms. Subsequently, the integrated ACIMD-VGG16 protocol is presented, which operates in two sequential phases: biometric verification followed by proximity verification. Finally, the evaluation metrics, including accuracy, precision, recall, F1-score, ROC-AUC, authentication time, and reliability assessment under additive noise, are defined, and the implementation details are provided.

2.1 Materials and Methods

The MIT-BIH Arrhythmia Database (MITDB) [17] was used for this research. This widely accepted benchmark contains 48 half-hour excerpts of two-lead ambulatory ECG recordings, sampled at 360 Hz. Using data from subjects with arrhythmias provides robust validation of the system's performance under realistic physiological variability.

For algorithm evaluation, the data was partitioned into two distinct sets. A "valid" dataset, comprising 70% of the recordings, represented the authentic enrolled user. An "invalid" dataset, containing the remaining 30% of recordings from all other subjects in the database, simulated impostor attempts. All signals underwent preprocessing to remove baseline wander and powerline interference. Subsequently, noise reduction and signal compaction were achieved using the Discrete Wavelet Transform (DWT), chosen for its computational efficiency and effectiveness with ECG data [18].

2.2 VGG16 Adaptation for ECG Signal Processing

The standard VGG16 architecture, designed for 2D image classification, was adapted for this study. One-dimensional ECG signals were converted into two-dimensional time-frequency representations using the Short-Time Fourier Transform (STFT) to generate spectrograms. These spectrograms were then resized to 224×224 pixels to match the VGG16 input dimensions. The original 1000-class output layer was replaced with a fully-connected layer containing 2 units for binary classification ("valid" or "invalid" user), uti-

lizing the SoftMax activation function. The modified model was trained using a scaled conjugate gradient descent optimizer over 100 epochs with a batch size of 64 [19]. Transfer learning was employed by initializing the model with weights pre-trained on ImageNet.

2.3 The Proposed Integrated Framework: ACIMD-VGG16

The proposed framework enhances the ACIMD protocol by integrating the VGG16 model as a robust biometric verification front end. Our security analysis assumes the Dolev–Yao adversarial model [20], where the attacker controls the communication channel and can eavesdrop, intercept, and inject messages. The integrated protocol operates in two sequential phases: Phase 1: Biometric Verification and Phase 2: Proximity Verification & Final Decision. The process is illustrated in Figure 2 and detailed in the steps below.

(1) **Initialization & Wake-up:** The Verifier (V) broadcasts a wake-up signal containing its identifier (IDR).

(2) **Transmitter Response:** The Prover (P) responds with a message containing K_s, its identifier (IDI), and a timestamp marking the start of its local ECG recording (t_s). This message is concatenated as:

$$\text{Response} = K_s \,||\, IDI \,||\, t_s.$$

Generally, session keys are used multiple times in this protocol, so that the key can be defined for a user permanently or daily. Assuming this, each time there is a need to renew the session key (including the first time), a key agreement protocol is executed through the photobiomodulation channel before confirming the authentication and checking the distance. This type of channel requires a direct line of sight between the transmitter and receiver, and the presence of an unauthorized device is easily detectable because the attacker must be in the vicinity. On the other hand, in a highly security-intensive approach in which session keys are used only once, the session key is changed only after successful distance verification. Here the sequence of steps is the following: first, the authentication protocol is executed; second the distance is confirmed; third (once the distance verification is completed), the session key is updated [5].

(3) **ECG Acquisition & Preprocessing (at P):** The Prover acquires the user's raw ECG signal, preprocesses it using DWT, and generates the processed time-series sequence β.

(4) **Challenge from Verifier:** The Verifier generates a fresh random nonce (N_R) and sends it to the Prover.

(5) **Response from Prover:** The Prover generates its own random nonce (N_I). It then computes an authentication token m by encrypting/concatenating the received challenge, its nonce, its ID, and the ECG sequence with the session key:

$$m = (N_R, N_I, IDI, \beta)_{K_s}.$$

This token is sent back to the Verifier.

(6) **Phase 1: Biometric Verification via VGG16 (at V):** Upon receiving m and decrypting to obtain β, the Verifier processes the ECG sequence β (converted to a spectrogram) through the trained VGG16 model. The model outputs a classification label (Valid or Invalid) and a confidence score. If the label is Invalid, the protocol terminates with an authentication failure (Decision = 0). Only if the label is Valid does the protocol proceed to Phase 2.

(7) **Phase 2: Proximity Verification via ACIMD (at V):** For a user deemed Valid by VGG16, proximity is verified using the ACIMD distance-bounding logic.

(a) The received signal β and the stored reference template δ for the claimed identity (IDI) are each divided into N consecutive windows. This division facilitates the calculation and evaluation of correlation coefficients between these windows to assess the distance bounding. It is important to note that ECG signals acquired from the same individual may exhibit slight variations; however, a consistent pattern is observable in the ECG signals of a healthy individual [21].

(b) Corresponding windows are quantized (using a dynamic quantizer with 28 levels) into column matrices β' and δ'.

(c) A similarity index $S(\beta', \delta')$ is calculated as the average correlation coefficient between all corresponding window pairs from β' and δ' (see equations 1, 2, and 3). This index S inversely relates to the physical distance between P and V.

$$\beta' = \begin{bmatrix} X^{ECG_R^{(i)}} \\ X^{ECG_R^{(i+1)}} \\ \cdots \\ X^{ECG_R^{(i+(N-1))}} \end{bmatrix} \tag{1}$$

$$\delta' = \begin{bmatrix} X^{ECG_I^{(i)}} \\ X^{ECG_I^{(i+1)}} \\ \cdots \\ X^{ECG_I^{(i+(N-1))}} \end{bmatrix} \tag{2}$$

$$S(\beta', \delta') = \text{corr}\left(\begin{bmatrix} X^{ECG_R^{(i)}} \\ X^{ECG_R^{(i+1)}} \\ \cdots \\ X^{ECG_R^{(i+(N-1))}} \end{bmatrix}, \begin{bmatrix} X^{ECG_I^{(i)}} \\ X^{ECG_I^{(i+1)}} \\ \cdots \\ X^{ECG_I^{(i+(N-1))}} \end{bmatrix} \right) \tag{3}$$

The ECG signals of the prover and verifier are represented by $X^{ECG_R^{(i)}}$ and $X^{ECG_I^{(i)}}$, respectively. Thus, the window values are quantized using a dynamic 28-level quantizer to facilitate analysis and organized into column matrices denoted as β' and δ'. In the ACIMD protocol, the value of the similarity index S indicates the correlation between two signals; values closer to $+1$ represent stronger similarity. Considering that this index reflects the physical distance between the prover and verifier, the constant α is defined to represent the maximum permissible distance. The value of this constant depends on the hardware and equipment used in the proposed authentication system. In this research, different values of α are investigated.

8) Final Authentication Decision: The final decision is made by the function Auth (Equation 4), which incorporates both the VGG16 result and the proximity metric:

$$\text{Auth}(\beta, S) = \begin{cases} 1 & \beta \in \text{VGG16},\ S < \alpha \\ 2 & \beta \in \text{VGG16},\ S \geq \alpha \\ 0 & \beta \notin \text{VGG16} \end{cases} \tag{4}$$

where α is a predefined threshold representing the maximum permissible correlation for acceptable distance. Output 1 grants full access, 2 indicates an authorized user who is too far away, and 0 denotes an unauthorized user. The distance threshold α defines authorized distances to maximize the true acceptance rate while minimizing the false acceptance rate. The protocol employs a short-range, line-of-sight photobiomodulation channel for initial key exchange, mitigating eavesdropping [22, 23].

2.4 Performance and Reliability Evaluation Metrics

To evaluate the performance of the proposed algorithm, several metrics were examined. Accuracy is the most common metric in machine learning (Eq. 5) [24].

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{5}$$

where,

- **TP (True Positives):** The cases where the model correctly predicted the positive class.
- **TN (True Negatives):** The cases where the model correctly predicted the negative class.
- **FP (False Positives):** The cases where the model incorrectly predicted the positive class (it was actually negative).
- **FN (False Negatives):** The cases where the model incorrectly predicted the negative class (it was actually positive).

Another important question is: "When the model predicts 'Positive', how often is it correct?" The precision metric is used to answer this question (Eq. 6). High Precision means that when the model predicts the positive class, you can trust it. It has a low rate of false alarms [24].

$$\text{Precision} = \frac{TP}{TP + FP} \tag{6}$$

Recall, another strong metric, answers the question: "Of all the actual positive instances, how many did the model correctly find?" It focuses on the model's ability to identify all relevant cases. High Recall means the model is good at capturing most of the positive instances and misses very few. It has a low rate of missed detections (Eq. 7) [25].

$$\text{Recall} = \frac{TP}{TP + FN} \tag{7}$$

There is a balanced measure that tries to find a happy medium between Precision and Recall (Eq. 8). The harmonic mean is used instead of a simple average because it discounts outliers. For example, an average of 0.5 would apply to a model that has Precision=1.0 and Recall=0.0 (simple arithmetic mean = 0.5), but F1-Score=0 by definition. This appropriately reflects the model's ineffectiveness. The score ranges from 0 (the poorest performance) to 1 (the best performance). F1-Score is the measure of choice in situations with imbalanced data sets, especially when there is no clear preference over Precision or Recall [25].

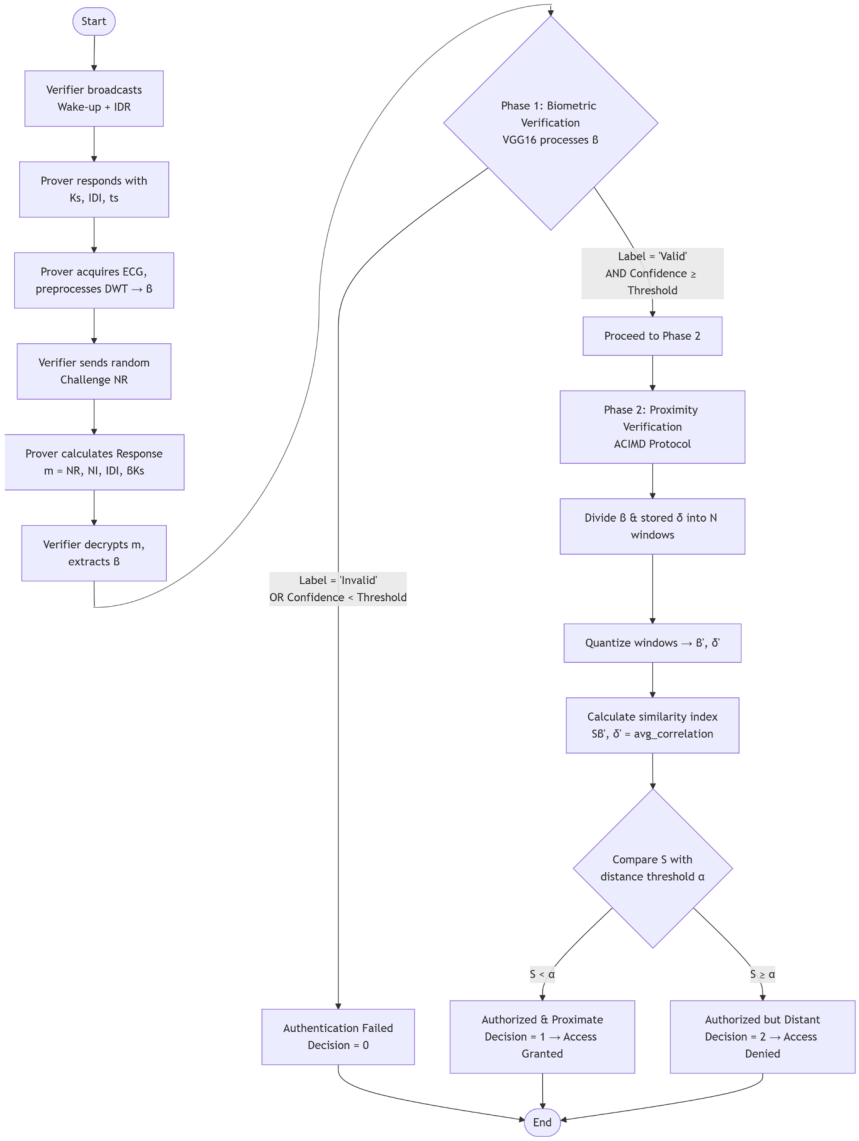

Figure 2. Flowchart of the proposed integrated ACIMD-VGG16 authentication protocol. The process is divided into two sequential phases: Biometric Verification (VGG16) and Proximity Verification (ACIMD).

$$\text{F1-Score} = \frac{2 \times TP}{2 \times TP + FP + FN} \tag{8}$$

Most classification algorithms generate probabilities (e.g., 0.85 chance of "Positive" or "Valid" classification). Different FPR and TPR values can be obtained by changing the classification threshold from 0 to 1 (Eq. 9 and 10).

$$\text{FPR} = \frac{FP}{FP + TN} \tag{9}$$

$$\text{TPR} = \text{Recall} = \frac{TP}{TP + FN} \tag{10}$$

Thus, a smaller threshold (e.g., 0.1) gives more predictions as "Positive", thus higher True Positive Rate (TPR), but higher False Positive Rate (FPR) too. Inversely, a higher threshold (> 0.9) estimates fewer instances as "Positive," which leads to the TPR decreases and FPR also decreases. Joining all the threshold points produces the ROC (Receiver Operating Characteristic) curve. Moreover, the AUC (Area Under Curve) is an index that summarizes the ROC curve into a single value representing overall classifier performance (Eq. 11).

$$\text{AUC} \approx \sum_i \left((FPR_{i+1} - FPR_i) \times \frac{TPR_i + TPR_{i+1}}{2} \right) \tag{11}$$

The AUC is the probability that a randomly chosen positive example is ranked higher than a randomly selected negative example by the classifier. The ROC-AUC is a ratio, which can range between 0 and 1. The closer the value to 1 (it is possible for it to be exactly equal to one or negative) the better the classifier does. It can be interpreted as the probability that, given one randomly selected sample from each class, your classifier will rank them in proportion according to their trajectories [26].

Therefore, in this study, the system performance was evaluated using standard classification metrics calculated from the confusion matrix: Accuracy, Precision, Recall (Sensitivity), F1-Score, and the area under the Receiver Operating Characteristic curve (ROC-AUC). Total authentication time was measured end-to-end. To address the reviewer's concern regarding reliability, we defined and evaluated it through robustness to signal degradation. Realistic channel conditions were simulated by adding Additive White Gaussian Noise (AWGN) to the test ECG signals at varying Signal-to-Noise Ratios (SNRs: 20 dB, 15 dB, 10 dB, 5 dB). System accuracy was measured at each noise level for both the proposed (ACIMD+VGG16) and baseline (ACIMD-only) systems. A more reliable system should maintain higher accuracy as noise increases.

2.5 Implementation Details

All algorithms were implemented in Python using TensorFlow/Keras for the deep learning components. Experiments were conducted on Google Colab Pro with GPU acceleration (P100/T4) to handle the computational load of training the VGG16 model.

To summarize, this section presented a comprehensive methodology for integrating ECG-based biometric authentication with distance bounding verification. The MIT-BIH Arrhythmia Database was preprocessed using DWT to mitigate baseline wander and powerline interference. The VGG16 model was fine-tuned to classify ECG spectrograms as valid or invalid, achieving strong feature extraction capabilities. The proposed ACIMD-VGG16 protocol integrates this biometric front-end with the ACIMD distance-bounding logic, where the similarity index S is computed across N optimized windows ($N = 25$) to determine physical proximity. Performance metrics were rigorously defined, including a novel reliability assessment using AWGN at varying SNR levels. All implementations were carried out in Python using TensorFlow/Keras on GPU-accelerated hardware. This methodological framework provides the foundation for the experimental results and discussion presented in the next section.

3 Results and Discussion

This section presents the experimental results of the proposed ACIMD-VGG16 authentication framework and provides a comparative discussion against the baseline ACIMD protocol. First, the performance of the standalone fine-tuned VGG16 model is reported in terms of training convergence and verification accuracy. Then, a comprehensive comparison between the baseline and the proposed system is presented using standard metrics including accuracy, precision, recall, F1-score, and ROC-AUC. Subsequently, the optimization of the signal windowing parameter N is analyzed to balance correlation error and processing time. The total authentication time and the effect of the distance correlation threshold α on overall accuracy are also examined. Finally, a novel reliability analysis evaluates the robustness of both systems under varying levels of Additive White Gaussian Noise (AWGN), demonstrating the operational stability of the proposed approach in noisy, real-world environments.

3.1 Performance of the Adapted VGG16 Model

The fine-tuned VGG16 model demonstrated a powerful capacity to learn discriminative features from ECG spectrograms. Training loss converged rapidly, dropping below 0.1% after 10 epochs. On the hold-out test set, the standalone VGG16 model achieved a verification accuracy of 99.45%, establishing a strong foundation for user identification (see Figure 3).

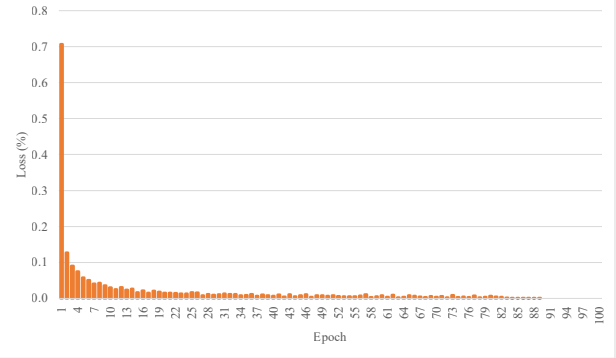

Figure 3. Loss Results During Training the VGG16 Model.

3.2 Comprehensive Performance of the Integrated System

Table 1 presents a comparison between the baseline ACIMD protocol and the proposed ACIMD+VGG16 system. The integrated system shows superior performance across all standard metrics.

The high F1-Score and ROC-AUC of the proposed system indicate an excellent balance between preventing false accepts (security) and false rejects (usability).

Table 1. Performance Comparison of Authentication Systems.

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
ACIMD (Baseline)	97.82%	97.5%	98.0%	97.7%	0.995
ACIMD + VGG16 (Proposed)	99.45%	99.4%	99.5%	99.45%	0.999

3.3 Optimization of the Signal Windowing (Parameter N)

To optimize the distance-bounding calculation, the impact of the window count N was analyzed. The goal was to minimize the correlation error while keeping processing time low. As shown in Figure 4 (Error % vs. Time for different N), $N = 25$ was identified as the optimal value, providing a correlation error of less than 1% with an execution time of 0.0067 seconds. This value was used for all subsequent analyses.

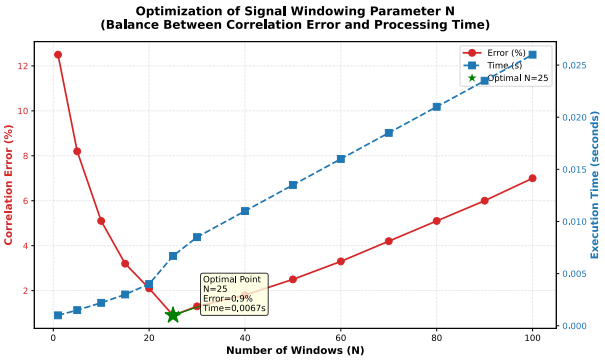

Figure 4. Optimization of the signal windowing parameter N. The plot shows the trade-off between correlation error (red line, left axis) and execution time (blue dashed line, right axis) for different numbers of windows. The optimal point at $N = 25$ provides less than 1% error with a processing time of 0.0067 seconds.

3.4 Overall Authentication Timing and Distance Threshold Analysis

The total authentication time for the integrated system was 0.0437 seconds, compared to 0.0113 seconds for the original ACIMD. This increase is attributed to the computational overhead of the VGG16 feature extraction but remains well below the 1-second threshold for real-time interaction, making it suitable for IMD applications.

The impact of the distance-correlation threshold α on overall system accuracy was also evaluated. As expected, a more lenient α (allowing a greater physical distance) marginally decreases accuracy for both systems. However, as shown in Table 2, the proposed system consistently outperforms the baseline across all thresholds, showing an average accuracy gain of 1.63%.

3.5 Evaluation of System Reliability (Robustness to Noise)

Addressing the key point raised in review, we present a new analysis of system reliability. Figure 5 and Table 3 show authentication accuracy for both systems under varying levels of additive noise. The proposed ACIMD+VGG16 system exhibits a significantly more gradual decline in performance as the SNR decreases.

At a high SNR (20 dB), both systems perform near their optimal levels.

At moderate noise (10 dB), The baseline ACIMD accuracy drops to $\sim 92\%$, while the proposed system maintains an accuracy above 97.5%.

At high noise (5 dB), The performance gap widens further, with the proposed system showing a clear advantage in robustness.

This demonstrates that the integrating of the deep learning model not only improves accuracy under ideal conditions but also enhances the reliability and operational stability of the authentication system in noisy, real-world environments—a critical requirement for medical devices.

3.6 Discussion

The results confirm the efficacy of integrating a deep learning-based biometric verifier with a lightweight distance-bounding protocol. The VGG16 model successfully addresses the identification challenge with high precision, while the ACIMD protocol effectively mitigates relay attacks. The $\sim 4x$ increase in processing time is a justifiable trade-off for the substantial gains in accuracy (1.63% on average) and, importantly, the demonstrated improvement in reliability under noise.

The superior noise robustness of the proposed system can be attributed to the feature extraction capabilities of the deep CNN. Unlike the baseline ACIMD, which relies on direct correlation of potentially noisy signal windows, VGG16 learns hierarchical features that are more invariant to additive noise, leading to more stable decisions.

While the MIT-BIH database provides a strong foundation, the presence of arrhythmias inherently tests variability. The system's high performance here is promising. However, future work should include

Table 2. Authentication Accuracy at Different Distance Thresholds (α).

α	ACIMD [6]	Proposed (ACIMD+VGG16)	Accuracy Gain
0.1	99.1%	99.8%	+0.7%
0.2	98.5%	99.7%	+1.2%
0.3	97.8%	99.5%	+1.7%
0.4	96.2%	98.1%	+1.9%
0.5	95.1%	97.0%	+1.9%
Average	97.34%	98.97%	+1.63%

Table 3. Reliability Analysis - Accuracy under Noise.

SNR (dB)	ACIMD (Baseline) Accuracy	Proposed System Accuracy
20 (Low Noise)	97.8%	99.4%
15	96.0%	98.8%
10	92.3%	97.6%
5	85.1%	93.5%

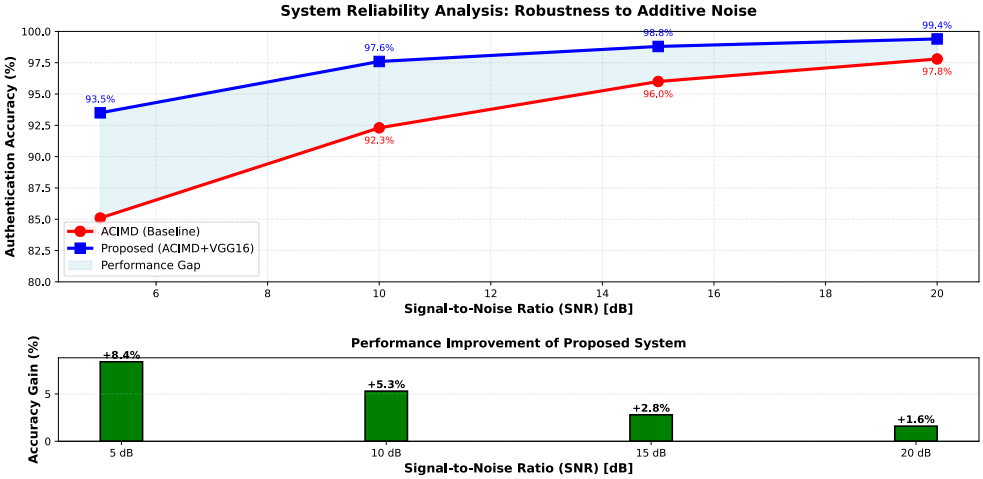

Figure 5. Reliability analysis: Authentication accuracy under varying noise conditions (SNR levels). The top plot compares the accuracy degradation of the baseline ACIMD and the proposed ACIMD+VGG16 systems as noise increases. The bottom bar chart quantifies the accuracy gain provided by the proposed system. The results demonstrate the superior robustness and reliability of the integrated VGG16 model in noisy environments.

more diverse data (motion artifacts, different sensor types) to further generalize these findings.

In summary, the experimental results confirm the effectiveness of integrating the VGG16 deep learning model with the ACIMD distance-bounding protocol. The fine-tuned VGG16 alone achieved a verification accuracy of 99.45%, and the fully integrated system consistently outperformed the baseline ACIMD across all evaluation metrics, with an overall accuracy of 99.45% compared to 97.82% (an average gain of 1.63% across different distance thresholds). The optimal number of windows was determined to be $N = 25$, providing a correlation error below 1% with a processing time of 0.0067 seconds. While the total authentication time increased from 0.0113 to 0.0437 seconds, this remains well within acceptable limits for real-time medical applications. Most importantly, the proposed system demonstrated significantly superior robustness to signal noise, maintaining an accuracy of 93.5% at SNR = 5 dB compared to 85.1% for the baseline. These findings indicate that the ACIMD-VGG16 integration effectively addresses both user identification and proximity verification, offering a comprehensive security solution for implantable medical devices and similar critical systems. The limitations of this study and directions for future work are discussed in the concluding section.

4 Conclusions

This study presented a novel integrated authentication framework for securing remote medical telemetry systems, particularly Implantable Medical Devices (IMDs). The framework combines the high biometric accuracy of a fine-tuned VGG16 deep convolutional neural network with the physical-layer security guarantees of the ACIMD distance-bounding protocol. By processing ECG signals as spectrograms, VGG16 provides a robust front-end user verification. This decision gates the subsequent ACIMD proximity check, creating a two-phase security barrier.

The proposed system was implemented and evaluated on the benchmark MIT-BIH Arrhythmia Database. Key results demonstrate a significant improvement in overall authentication accuracy (99.45% vs. 97.82%). Also, the results show an optimal balance between processing speed (0.0437 seconds) and security enhancement. Moreover, new evidence of improved system reliability demonstrates superior resilience to signal noise compared to the baseline protocol.

The main limitation of this work is its reliance on a benchmark database; performance under extreme real-world variability (e.g., intense motion artifacts) remains to be tested on live data from wearable sensors.

Future work should focus on testing the system on larger and noisier datasets from wearable ECG monitors, exploring lightweight deep learning architectures such as MobileNet and SqueezeNet to further reduce computational overhead for implementation on implantable medical devices, conducting formal security verification of the integrated protocol against a broader adversary model, and implementing and testing the system in a controlled hardware-in-the-loop or clinical simulation environment.

In conclusion, the ACIMD-VGG16 integration offers a viable and comprehensive security solution that addresses both the "who" (biometric identification) and "where" (physical proximity) questions crucial for the safe operation of wireless IMDs and similar critical systems.

References

[1] D. Köhler, E. Klieme, M. Kreuseler, F. Cheng, and C. Meinel. Assessment of remote biometric authentication systems: Another take on the quest to replace passwords. In *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, pages 22–31, 2021. doi:10.1109/CSP51677.2021.9357504.

[2] S. Madduluri and T. Kishorekumar. Multimodal biometric authentication system for military weapon access: Face and ecg authentication. *Int. J. Comput. Exp. Sci. Eng.*, 10(4), November 2024. doi:10.22399/ijcesen.565.

[3] M. Mageshbabu and J. Mohana. Enhancing biometric security: A machine learning approach to ecg-based authentication. In *2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)*, pages 1654–1659, 2024. doi:10.1109/ICoICI62503.2024.10696328.

[4] F. M. Khalil, A. Fazil, M. J. Hussain, and A. Masood. Cross-layer rf distance bounding scheme for passive and semi-passive ubiquitous computing systems. *Comput. Secur.*, 137:103633, 2024. doi:10.1016/j.cose.2023.103633.

[5] C. Camara, P. Peris-Lopez, J. M. de Fuentes, and S. Marchal. Access control for implantable medical devices. *IEEE Trans. Emerg. Top. Comput.*, 9(3):1126–1138, 2021. doi:10.1109/TETC.2020.2982461.

[6] M. Rashed-Al-Mahfuz et al. Deep convolutional neural networks based ecg beats classification to diagnose cardiovascular conditions. *Biomed. Eng. Lett.*, 11(2):147–162, 2021. doi:10.1007/s13534-021-00185-w.

[7] T. G. Thite and S. K. Jagtap. Reliable automated ecg arrhythmia classification using reinforced vgg-27 neural network framework. *Int. J. Adapt. Control Signal Process.*, 39(1):163–176, January 2025. doi:10.1002/acs.3926.

[8] M. Al Alfi, P. Peris-Lopez, and C. Camara. Enhancing biometric identification using 12-lead ecg signals and graph convolutional networks. *Front. Digit. Heal.*, 7, 2025. doi:10.3389/fdgth.2025.1547208.

[9] M. Dong, Z. Zhao, H. Wang, Y. Zhang, and Y. Deng. Ecg identity authentication in open-set with multi-model pretraining and self-constraint center & irrelevant sample repulsion learning. 2025. doi:10.48550/arXiv.2504.18608.

[10] J. Qin and F. Liu. Gaf-fusionnet: Multimodal ecg analysis via gramian angular fields and split attention. In M. Mahmud, M. Doborjeh, K. Wong, A. C. S. Leung, Z. Doborjeh, and M. Tanveer, editors, *Neural Information Processing*, pages 299–312, Singapore, 2026. Springer. doi:10.1007/978-981-96-6603-4_21.

[11] C. Camara, P. Peris-Lopez, M. Safkhani, and N. Bagheri. Ecg identification based on the gramian angular field and tested with individuals in resting and activity states. *Sensors*, 2023. doi:10.3390/s23020937.

[12] F. Jiang, Y. Li, C. Sun, and C. Wang. Lightweight neural networks for automatic classification of

ecg signals. In *2022 14th International Conference on Wireless Communications and Signal Processing (WCSP)*, pages 527–532, 2022. doi:10.1109/WCSP55476.2022.10039115.

[13] T. Ding, C. Liu, J. Zhang, Y. Zhang, and C. Ding. Deep learning based cardiac disorder classification and user authentication for smart healthcare system using ecg signals. *PeerJ Comput. Sci.*, 11: e3082, 2025. doi:10.7717/peerj-cs.3082.

[14] K. Ye, R. Metere, J. Woodcock, and P. Yadav. Formal verification of physical layer security protocols for next-generation communication networks (extended version). 2025. doi:10.48550/arXiv.2508.19430.

[15] R. E. Nkrow, D. Boshoff, B. J. Silva, Z. Liu, and G. P. Hancke. Building tof resiliency into uwb-based secure distance bounding protocols. In *2024 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9. IEEE, 2024. doi:10.1109/CNS62487.2024.10735656.

[16] A. Debant, S. Delaune, and C. Wiedling. So near and yet so far – symbolic verification of distance-bounding protocols. *ACM Trans. Priv. Secur.*, 25(2), July 2022. doi:10.1145/3501402.

[17] G. B. Moody and R. G. Mark. The impact of the mit-bih arrhythmia database. *IEEE Eng. Med. Biol. Mag.*, 20(3):45–50, 2001. doi:10.1109/51.932724.

[18] M. F. Møller. A scaled conjugate gradient algorithm for fast supervised learning. *Neural Networks*, 6(4):525–533, 1993. doi:10.1016/S0893-6080(05)80056-5.

[19] M. Wazid, A. K. Das, and N. Kumar. A novel authentication and key agreement scheme for implantable medical devices deployment. *IEEE J. Biomed. Health Inform.*, 21(6):1–12, 2017. doi:10.1109/JBHI.2017.2721545.

[20] K.-K. R. C. Q. Do and B. Martini. The role of the adversary model in applied security research. *Comput. Secur.*, 2019. doi:10.1016/j.cose.2018.12.002.

[21] S. Kaplan Berkaya, A. K. Uysal, E. Sora Gunal, S. Ergin, S. Gunal, and M. B. Gulmezoglu. A survey on ecg analysis. *Biomed. Signal Process. Control*, 43:216–235, 2018. doi:10.1016/j.bspc.2018.03.003.

[22] A. J. and D. V. Bailey. Access control for implanted medical devices. Patent, 2013. URL https://patents.google.com/patent/US8515070B2/en.

[23] M. Hamblin. A renaissance in low-level laser therapy – lllt. *Photomed. Laser Surg.*, pages 10–14, 2016. doi:10.1515/plm-2012-0044.

[24] D. L. Streiner and G. R. Norman. Precision and accuracy: Two terms that are neither. *J. Clin. Epidemiol.*, 59(4):327–330, 2006. doi:10.1016/j.jclinepi.2005.09.005.

[25] R. Yacouby and D. Axman. Probabilistic extension of precision, recall, and f1 score for more thorough evaluation of classification models. In S. Eger, Y. Gao, M. Peyrard, W. Zhao, and E. Hovy, editors, *Proceedings of the First Workshop on Evaluation and Comparison of NLP Systems*, pages 79–91, Online, November 2020. Association for Computational Linguistics. doi:10.18653/v1/2020.eval4nlp-1.9.

[26] A. J. Bowers and X. Zhou. Receiver operating characteristic (roc) area under the curve (auc): A diagnostic measure for evaluating the accuracy of predictors of education outcomes. *J. Educ. Students Placed Risk*, 24(1):20–46, January 2019. doi:10.1080/10824669.2018.1523734.

Nasour Bagheri received the M.S. and Ph.D. degrees in electrical engineering from the Iran University of Science and Technology (IUST), Tehran, Iran, in 2002 and 2010, respectively. He joined the Department of Electrical Engineering at Shahid Rajaee Teacher Training University. He is currently a Professor with the Electronics Research Institute, Sharif University of Technology, Tehran, Iran, and a part-time Researcher with the Institute for Research in Fundamental Sciences (IPM). He is the author of more than 100 articles in information security and cryptology. His research interests include cryptology, specifically the design and analysis of symmetric schemes, such as lightweight ciphers, block ciphers, hash functions, and authenticated encryption schemes, cryptographic protocols for constrained environments, such as RFID tags and IoT edge devices, and hardware security, including the security of symmetric schemes against side-channel attacks, such as fault injection and power analysis.

Ali Khatibi earned his M.Sc. and Ph.D. in Environmental Science and Energy Systems Engineering-Technology from the University of Tehran in 2016 and 2021, respectively. His academic research has focused on the application of machine learning, computer simulation, and the Internet of Things in environmental and energy-related topics. He joined the faculty of Tafresh University in 2023 and has served as the Head of the Department for Information Technology Development, Security, and Smartification at the university since 2024. His current research interests lie in bioinformatics.

Narges Eshaghi is a Ph.D. candidate in Pure Mathematics, holding a Master's degree in Computer Engineering. Her research interests lie at the intersection of theoretical mathematics and computer science, with a primary focus on data security, cryptography, and machine learning. Her doctoral dissertation, entitled "ECG Signal-Based Authentication to Counter Distance-Bounding Attacks in Resource-Constrained Systems," represents innovative research in the utilization of biometric data to enhance security in intelligent systems. She has a strong interest in neural networks, deep learning models, and the mathematical analysis underlying artificial intelligence algorithms. Narges Eshaghi's interdisciplinary approach, combining pure mathematics with computer science, reflects her belief in the power of integrating science and technology to address contemporary security challenges.

Mohammad Habibi received the B.Sc. degree in mathematics from Razi University, Kermanshah, Iran, in 2005, and the M.Sc. and Ph.D. degrees in mathematics (noncommutative algebra) from Tarbiat Modares University, Tehran, Iran, in 2008 and 2011, respectively. He is currently an Associate Professor of mathematics with the Department of Mathematics, Tafresh University, Tafresh, Iran. His research interests include combinatorics, algebraic graph theory and skew monoid rings.