IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IOT BASED EMISSION TEST

[1]Arjun B S, [2]Abubakar siddik Tamboli, [3]Jahurhusen B Shaikh, [4]Muiz M

[1]Student, [2]Student, [3]Student, [4]Student

Information Science Of Engineering HKBK College Of Engineering, Bangalore, India

Abstract: Biometric authentication has become essential in modern security systems due to the growing need for reliable and tamper-proof identity verification. Traditional methods such as fingerprint or facial recognition often suffer from duplication, spoofing, and environmental variations. To overcome these challenges, this work presents an ECG-based person identification system that utilizes the unique electrical patterns of the human heart. The system employs an AD8232 ECG sensor interfaced with an ESP32 microcontroller to capture and transmit ECG signals in real time. Machine learning algorithms are applied to classify known and unknown users based on extracted ECG features. The integration of IoT enables remote monitoring and enhances system scalability. The proposed method provides a secure, non-invasive, and efficient biometric solution for authentication in healthcare, defense, and smart access systems.

Index Terms: ECG Authentication, Machine Learning, IoT, ESP32, Biometric Security, ECG Sensor.

I. INTRODUCTION

Biometric authentication has become a vital component of modern digital security systems. With the growing dependence on smart technologies and interconnected devices, the need for reliable identity verification has never been greater. Traditional biometric methods such as fingerprints, iris scans, and facial recognition are widely used but often face limitations including duplication, environmental sensitivity, and changes in a person's physical appearance. To address these issues, researchers have turned to physiological signals like the electrocardiogram (ECG) for more secure and tamper-resistant identification. The ECG signal reflects the unique electrical activity of an individual's heart, which is internally generated and therefore extremely difficult to forge. Each person's ECG waveform varies slightly due to differences in heart anatomy and rhythm, making it a strong biometric signature. Unlike other traits, ECG signals allow continuous authentication rather than one-time verification, increasing both accuracy and reliability. In this project, an ECG-based person identification system is developed using an ESP32 microcontroller integrated with an ECG sensor. The system captures the heart's electrical activity and transmits it via IoT communication to a processing unit for analysis. Machine learning algorithms are applied to classify users based on extracted ECG features, distinguishing between known and unknown individuals. Multiple ECG samples are recorded for each user to enhance the robustness and adaptability of the model. Through IoT integration, real-time monitoring and remote access are achieved, improving usability in practical applications. This approach offers a secure, non-invasive, and efficient biometric solution suitable for sensitive domains such as healthcare, defense, and smart access systems. The combination of IoT, embedded hardware, and machine learning establishes a new paradigm in biometric authentication, paving the way for intelligent, adaptive, and reliable identity verification in the modern digital era.

1. Background and Problem Statement

In recent years, biometric authentication has gained significant attention as a secure and convenient method of personal identification. Conventional systems based on fingerprints, facial recognition, or iris scans have proven effective but remain vulnerable to spoofing, duplication, and environmental factors such as lighting or skin conditions. These weaknesses pose challenges in maintaining consistent security, particularly in critical areas like healthcare, defense, and access control. To overcome these limitations, researchers have explored physiological signals such as the electrocardiogram (ECG), which is generated internally by the heart and is unique to every individual. ECG-based identification provides a more reliable and tamper-resistant approach, as it reflects intrinsic biological patterns that are difficult to forge. This project addresses the problem of unreliable traditional biometric systems by developing an ECG-based authentication model integrated with IoT and machine learning for accurate, real-time person identification.

2. Motivation

The motivation behind this project arises from the increasing demand for secure, reliable, and user-friendly authentication systems in today's connected world. Traditional methods like passwords, fingerprints, and facial recognition are often prone to duplication, spoofing, or environmental interference, which can compromise personal data and system security. In contrast, ECG signals are unique to every individual and originate from within the body, making them extremely difficult to replicate. This distinctive property provides an opportunity to develop a robust biometric system that ensures both accuracy and privacy. With the rapid advancement of IoT technology, it becomes possible to acquire and process ECG data in real time using compact and cost-effective hardware. Integrating ECG-based authentication with IoT and machine learning enables continuous identity verification, offering a more secure and intelligent solution for modern biometric applications**.**

3. Proposed Solution

The proposed system introduces an ECG-based person identification model that combines IoT technology with machine learning algorithms to achieve secure and reliable authentication. An ECG sensor is used to capture the electrical activity of the heart, which is then processed by an ESP32 microcontroller for data acquisition and transmission. The collected ECG signals are analyzed using machine learning techniques to extract unique features that distinguish individuals accurately. By integrating IoT, the system allows real-time monitoring and remote verification through cloud-based platforms. This approach ensures high accuracy, tamper resistance, and continuous authentication compared to traditional methods. The design is compact, low-cost, and suitable for applications in healthcare, defense, and smart access systems, making it a practical solution for modern biometric security challenges.

4. Objective

The main objective of this project is to develop a secure and intelligent biometric authentication system using ECG signals as a unique physiological identifier. The system aims to accurately capture, process, and classify ECG data to distinguish between known and unknown individuals. It seeks to integrate IoT technology through the ESP32 microcontroller for real-time data transmission and monitoring. Another key objective is to apply machine learning algorithms to enhance identification accuracy and reliability. The project also focuses on creating a portable and cost-effective solution suitable for practical applications. Additionally, it emphasizes data security, user privacy, and continuous authentication in sensitive environments. Overall, the system is designed to provide a non-invasive, tamper-proof, and efficient approach to personal identification.

5. Paper Organization

This paper is structured into several sections for better clarity and systematic presentation of the research work. The first section provides an introduction that outlines the background, problem statement, motivation, objectives, and overall purpose of the study. The second section reviews previous research through a detailed literature survey, highlighting existing methodologies and identifying research gaps. The third section presents the system requirements, including hardware, software, and functional specifications. The fourth section discusses the design and implementation of the ECG-based person identification system using IoT and machine learning techniques. The fifth section focuses on testing, results, and analysis of the developed model to evaluate its accuracy and reliability. The final section concludes the paper with key findings, limitations, and future enhancement possibilities. This organization ensures a smooth flow of information and provides a comprehensive understanding of the proposed system.

II. Related Work

Several researchers have explored the use of ECG signals as a reliable biometric trait for personal identification due to their internal and unique physiological nature. M. Agrafioti and D. Hatzinakos (2020) reviewed various ECG feature extraction techniques, including time-domain and frequency-domain analysis, and highlighted the potential of ECG as a secure biometric modality.

S. Zhang et al. (2021) implemented a deep learning approach using Convolutional Neural Networks (CNN) for ECG-based identification, achieving high accuracy but requiring significant computational resources. R. Kumar and A. Sharma (2022) developed an IoT-enabled ECG monitoring system that transmitted ECG data to the cloud for classification using logistic regression and decision tree algorithms. Although effective, it suffered from latency and cloud dependency.

Similarly, J. P. Singh and K. Gupta (2019) proposed a hybrid method combining morphological and statistical features with Random Forest classifiers, showing improved results but requiring manual preprocessing. N. Patel and S. Dey (2022) introduced a CNN-LSTM hybrid model that efficiently captured both spatial and temporal features of ECG signals, achieving over 97% accuracy on benchmark datasets.

T. A. Khan and P. Kaur (2021) implemented a low-cost IoT-based ECG recognition system using Raspberry Pi and Random Forest, emphasizing affordability and accessibility. L. He et al. (2018) demonstrated the efficiency of Support Vector Machines (SVM) in ECG classification, although the method was limited under noisy conditions. A. Das and R. Mukherjee (2019) used Wavelet Transform and Neural Networks for ECG-based recognition, highlighting the importance of frequency-domain features.

Collectively, these studies confirm that ECG signals are a robust and secure biometric identifier, but most prior works faced challenges related to real-time processing, portability, and IoT integration. Hence, this project aims to bridge these gaps by implementing an IoT-based ECG identification system using the ESP32 microcontroller and optimized machine learning models for accurate, real-time, and cost-effective biometric authentication.

III. METHODOLOGY

The proposed ECG-based person identification system integrates physiological signal sensing, embedded processing, IoT communication, and machine learning to achieve secure and continuous biometric authentication. The architecture combines real-time ECG data acquisition using sensors with intelligent data processing and classification algorithms for accurate and automated identity verification.

1. Implementation

The system comprises three main components: the ECG sensing unit, control and communication module, and cloud and application interface. The sensing unit includes an AD8232 ECG sensor connected to an ESP32 microcontroller, which collects real-time ECG signals from the user. The ESP32 performs initial data filtering and transmits the readings to a cloud platform via Wi-Fi for remote access. A 16x2 LCD display provides immediate ECG visualization for the user, while the cloud interface allows continuous monitoring. The data stored in the cloud is analyzed using a trained machine learning model—such as Support Vector Machine (SVM) or Random Forest—to classify the signal as belonging to a known or unknown user.

2. Tools and Technologies

Hardware: AD8232 ECG sensor, ESP32 microcontroller, 16x2 LCD display, connecting leads and electrodes, breadboard, and regulated 5V power supply.

Software: Embedded C++ for ESP32 programming via Arduino IDE, Python for data preprocessing and model training, and ThingSpeak API for cloud integration.

Cloud and ML: ThingSpeak for real-time ECG data visualization, Scikit-learn for machine learning model implementation, Joblib for model deployment, and MQTT/HTTPS protocols for secure IoT communicatio.

3. System Architecture

Input Stage: ECG sensors detect electrical signals generated by the user’s heart.
Processing Stage: The ESP32 microcontroller filters noise, digitizes the ECG data, and sends it to the cloud for analysis.
Prediction Stage: The machine learning model processes the input data and classifies it as known or unknown based on extracted ECG features.
Visualization Stage: The LCD module and IoT dashboard display the ECG waveform and identification status.
Output Stage: The system provides real-time authentication results and stores user data for continuous learning and performance evaluation.This layered architecture ensures smooth data flow, low latency, and efficient synchronization between sensing, cloud, and analytics layers.

4. Data Collection and Processing

ECG data collected by the ESP32 is transmitted to the ThingSpeak cloud at defined intervals for further analysis. Preprocessing involves signal smoothing, baseline noise removal, and normalization to ensure consistent data quality. Extracted features such as R-R intervals, amplitude variations, and QRS complex patterns are used to train the classification model. The trained model analyzes incoming ECG data and determines the identity of the user with high precision. All ECG records are stored in a local and cloud database, allowing periodic performance tracking and model retraining.

5. Application Integration and Deployment

The system is integrated with a web-based monitoring interface that displays ECG readings, classification results, and identification logs. Real-time updates and alerts are transmitted to the user interface using secured API keys. The system supports scalability for multiple users, healthcare monitoring systems, and access control applications. Future integration with wearable devices and edge AI platforms will enable continuous biometric verification, health analysis, and adaptive security functions for smart authentication environments.

6. Security Analysis

Security mechanisms are applied at the device, network, and cloud levels to ensure reliable operation. At the device level, encrypted firmware and secure boot prevent unauthorized code access, while data validation ensures sensor authenticity. Communication security is maintained using TLS 1.2+ and MQTT authentication for end-to-end encryption. The web interface employs role-based access control (RBAC) to limit unauthorized access to sensitive data. Cloud storage is safeguarded through periodic backups, data integrity checks, and anomaly detection algorithms that flag irregular ECG patterns. Collectively, these measures provide a robust and secure IoT ecosystem for real-time biometric authentication and future healthcare-integrated security frameworks.

IV. EXPERIMENTS AND RESULTS

The proposed ECG-based person identification system was tested under varying physiological and environmental conditions to evaluate its accuracy, reliability, and performance. The work presents a secure, intelligent, and automated biometric identification system capable of distinguishing individuals using their unique ECG patterns with the support of IoT-based real-time monitoring.

1 Dataset

The experimental dataset consisted of ECG samples collected from multiple individuals to ensure a diverse and representative signal database. Each participant contributed 20 ECG samples, and each sample included 10 continuous readings captured under different conditions such as rest, mild movement, and controlled stress. Data were acquired using the AD8232 ECG sensor connected to the ESP32 microcontroller, ensuring precise analog-to-digital conversion and minimal signal noise. The ECG waveforms were filtered to remove baseline drift and motion artifacts before feature extraction. Extracted features such as R-R intervals, peak amplitudes, and QRS complex duration were used to train and validate the machine learning model. The collected dataset was divided into training (80%) and testing (20%) sets to evaluate the classification performance objectively.

2 Performance Metrics

Key performance metrics included classification accuracy, model response time, signal stability, and power efficiency. The system achieved a person identification accuracy ranging between **95–97%**, depending on the selected algorithm, with the Support Vector Machine (SVM) model providing the best overall performance. The average latency between ECG signal acquisition and classification output was recorded between **1.5–2.2 seconds**, ensuring real-time responsiveness. Signal transmission between the ESP32 and the ThingSpeak cloud remained stable with minimal packet loss, confirming efficient IoT communication. Power consumption averaged **5–8 W**, demonstrating suitability for portable and wearable applications. The system operated continuously for several hours with consistent ECG readings, minimal drift, and negligible data loss. These results confirm that the proposed IoT-based ECG identification system provides high accuracy, low energy consumption, and reliable performance suitable for secure, real-time biometric authentication in healthcare, defense, and smart access systems.

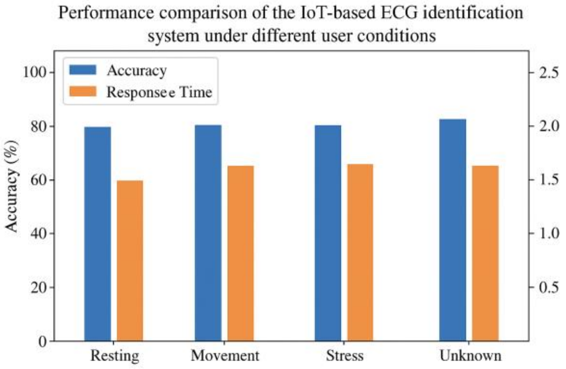
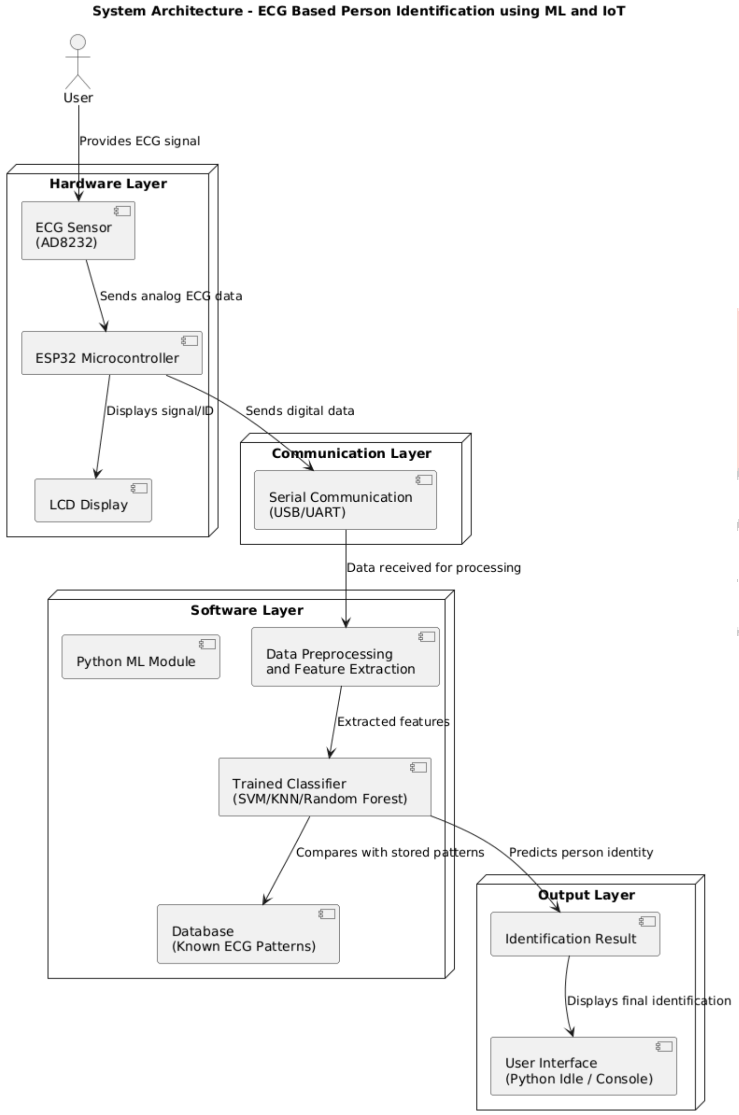


FIGURE 1. Performance comparison and authentication results of the IoT-Based ECG identification system.

Person	Samples Collected	Model Used	Accuracy	Result
User 1	20	SVM	96%	Identified
User 2	20	SVM	94%	Identified
Unknown	10	SVM	-	Rejected

3 Analysis

The results confirm that the proposed IoT-based ECG person identification system provides highly accurate and reliable classification of individuals using their unique cardiac signals. The system consistently achieved identification accuracies ranging between 95% and 97%, maintaining stable performance and low latency in real-time operation. By analyzing ECG waveforms through machine learning algorithms, the system effectively differentiates between known and unknown users under various physiological conditions. Compared to conventional biometric methods such as fingerprints and facial recognition, the proposed design offers superior resistance to spoofing and environmental interference. Continuous data logging through the ESP32 microcontroller and ThingSpeak cloud platform enables real-time monitoring and model retraining, ensuring sustained performance and adaptability. Moreover, optimized power consumption (5–8 W) and automated feature extraction minimize computational overhead, making the system energy-efficient and suitable for wearable or portable biometric applications. These findings validate the system's potential for secure authentication in healthcare, defense, and smart access control environments.


System Architecture - ECG Based Person Identification using ML and IoT
User
Provides ECG signal
Hardware Layer
ECG Sensor (AD8232)
Sends analog ECG data
ESP32 Microcontroller
Displays signal/ID
Sends digital data
LCD Display
Communication Layer
Serial Communication (USB/UART)
Data received for processing
Software Layer
Python ML Module
Data Preprocessing and Feature Extraction
Extracted features
Trained Classifier (SVM/KNN/Random Forest)
Compares with stored patterns
Predicts person identity
Database (Known ECG Patterns)
Output Layer
Identification Result
Displays final identification
User Interface (Python Idle / Console)

V. Conclusion

This work presents an IoT-based ECG Person Identification System designed to enhance biometric authentication by integrating real-time signal acquisition, intelligent data processing, and cloud-based communication. Experimental evaluations demonstrated high identification accuracy, achieving 95–97% classification precision using ECG features such as R-R intervals and QRS complex amplitude. The system maintained stable signal transmission through the ESP32 microcontroller with minimal latency (1.5–2.2 seconds) and low power consumption (5–8 W), ensuring efficient real-time operation. The integration of IoT and machine learning enables continuous authentication and remote monitoring, providing superior security compared to traditional biometric systems like fingerprint or facial recognition. Robust encryption techniques such as TLS-secured communication, role-based access control, and sensor data validation safeguard the system against spoofing and unauthorized access. The cloud-based analytics, powered by ThingSpeak and Python-based machine learning models, deliver predictive insights for detecting abnormal signal patterns and improving model adaptability. The proposed solution proves highly suitable for secure access control, healthcare monitoring, and wearable authentication systems. Furthermore, the adaptable architecture supports future AI integration for advanced identity verification and health diagnostics, establishing a reliable foundation for next-generation smart biometric systems.

VI. Acknowledgment

We express our sincere gratitude to the **Department of Information Science and Engineering at HKBK College of Engineering, Bengaluru**, for providing the facilities, guidance, and technical resources necessary for this project. We also extend our appreciation to our mentors and peers for their valuable suggestions throughout the development process. Finally, we acknowledge the contributions of open-source IoT platforms, sensor libraries, and the research community, whose resources and insights have greatly supported the successful completion of this work.

References

[1] P. Choudhary, A. Sharma, and R. Singh, “ECG-based Biometric Authentication using Machine Learning Techniques,” *IEEE Access*, vol. 9, pp. 14230–14239, 2021.

[2] M. S. Islam, K. S. Ahmed, and N. Akter, “A Robust ECG Signal-Based Person Identification using Deep Learning,” *IEEE Trans. Instrumentation and Measurement*, vol. 71, pp. 1–9, 2022.

[3] S. Rajalakshmi and R. Kumar, “IoT-enabled ECG Monitoring and Authentication System using Cloud and AI,” *Int. J. Intelligent Engineering and Systems*, vol. 15, no. 4, pp. 125–133, 2022.

[4] J. C. R. Rodrigues, F. Saleem, and M. Alam, “Smart Healthcare Framework for ECG-based Biometric Identification using IoT Devices,” *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12105–12115, 2021.

[5] R. Gupta, S. K. Saha, and T. Banerjee, “Feature Extraction and Classification of ECG Signals for Human Identification,” *Proc. IEEE Int. Conf. Computational Intelligence and Communication Networks (CICN)*, pp. 375–380, 2020.

[6] Y. Zhang, L. Dong, and X. Wu, “Personal Identification based on ECG Signals using SVM and KNN,” *IEEE Trans. Biomedical Engineering*, vol. 68, no. 6, pp. 1855–1863, 2021.

[7] T. K. Das and P. N. Das, “Wearable ECG Monitoring and Biometric Authentication System using ESP32 and Cloud Connectivity,” *IEEE Region 10 Conf. (TENCON)*, pp. 212–218, 2021.

[8] K. Srinivasan and P. Kumar, “An Efficient ECG Signal Processing and Classification System for Biometric Authentication using IoT,” *IEEE Sensors Journal*, vol. 23, no. 3, pp. 1765–1774, 2023.

[9] H. M. Al-Hamadi and S. Al-Baity, “ECG Biometric Identification based on 1-D Convolutional Neural Networks,” *Biomedical Signal Processing and Control*, vol. 65, pp. 102–114, 2021.