# Development of a New Biometric Authentication Method Based on ECG Signals

**Vijay Kumar[1], Chamanthi Aswini[2], Kavitha K[3], S. Sai Bhargav[4], T. Venkata Sai[5]**

Assistant Professor, Department of Electronics and communication Engineering[1]
Students, Department of Electronics and communication Engineering[2,3,4,5]
R.L. Jalappa Institute of Technology, Doddaballapur, Karnataka, India

**Abstract***: Biometric authentication has become an integral part of secure systems, as traditional password-based methods have proven to be vulnerable to various attacks. In recent years, there has been growing interest in utilizing electrocardiogram (ECG) signals as a biometric authentication method due to their unique characteristics and inherent physiological nature. This paper presents the development of a new biometric authentication method based on ECG signals.*

*The method involves capturing the ECG signals from individuals using non-invasive sensors and extracting relevant features for authentication purposes. A comprehensive database of ECG signals is collected from a diverse population to ensure the robustness and effectiveness of the system.*

*The acquired ECG signals undergo preprocessing techniques to remove noise and artifacts, followed by feature extraction using advanced signal processing algorithms. several key features are extracted from the ECG signals, including morphological features such as QRS complex duration, R-peak amplitude, and T-wave amplitude. Additionally, statistical features such as heart rate variability and wavelet-based features are also extracted. These features are then used to create a unique template for each individual, which serves as their biometric signature. To evaluate the performance of the proposed method, extensive experiments are conducted using a benchmark dataset. The experiments involve various scenarios, such as intra-class and inter-class authentication, to assess the system's accuracy and robustness. The results demonstrate the effectiveness of the proposed method, achieving high accuracy rates and low false acceptance rates. Furthermore, the proposed method offers several advantages over existing biometric authentication methods. ECG signals are difficult to forge or steal, making them highly secure. Moreover, ECG signals are continuously generated by the human body, enabling dynamic authentication systems that can monitor user presence and detect impersonation attempts*

**Keywords:** ECG signals

## I. INTRODUCTION

Biometric authentication methods play a crucial role in securing access to various systems and resources. Traditional methods such as passwords, PINs, and fingerprints have been widely used, but they are susceptible to security breaches and can be easily compromised. Therefore, there is a growing need for more robust and secure authentication methods.

In recent years, biometric systems based on electrocardiogram (ECG) signals have emerged as a promising alternative.

ECG signals represent the electrical activity of the heart and are unique to individuals. Unlike other biometric traits such as fingerprints or iris patterns, ECG signals are internal and not easily replicable or stolen.

This makes them highly suitable for biometric authentication purposes.

Additionally, ECG signals are constantly generated by the human body, making them readily available for authentication without the need for additional sensors or devices.

The development of a new biometric authentication method based on ECG signals holds significant potential for enhancing security in various domains, including healthcare, finance, and access control systems. By utilizing ECG signals, it is possible to establish a robust and user-friendly authentication mechanism that combines high security with convenience.

DOI: 10.48175/IJARSCT-12757

Authentication system will involve acquiring ECG signals from individuals using non-invasive sensors, such as wearable devices or specialized electrodes.

These sensors will capture the electrical activity of the heart and convert it into digital signals for further processing. The acquired ECG signals will then undergo preprocessing and feature extraction to capture the unique characteristics of each individual's heart. Machine learning algorithms will be employed to analyze and classify the extracted features, enabling the system to distinguish between authorized and unauthorized users.

Training the machine learning models will involve a large dataset of ECG signals collected from a diverse population, ensuring the system's accuracy and generalizability.

One of the key advantages of the proposed authentication method is its ability to continuously monitor user identity. Unlike static biometric traits, such as fingerprints or facial features, ECG signals can be continuously measured and verified throughout a user's interaction with a system.

This real-time authentication capability adds an extra layer of security, as any unauthorized access attempts or changes in user identity can be detected promptly.

### 1.1 Existing System

The development of a new biometric authentication method based on ECG signals aims to enhance the security and reliability of existing authentication systems. Electrocardiogram (ECG) signals are unique to individuals and can provide a robust means of verifying their identities.

This innovative approach utilizes the distinctive features of an individual's heart rate and rhythm patterns to establish their authenticity. By incorporating ECG-based authentication, users can enjoy a simplified and secure method of accessing various systems and services. This technology eliminates the need for traditional passwords or PINs, which can be easily forgotten, stolen, or hacked.

Instead, individuals can rely on their own physiological signals, making it extremely difficult for unauthorized individuals to replicate or deceive the system. The ECG-based authentication system operates by capturing the user's ECG signals through specialized sensors, typically integrated into a wearable device or embedded within existing hardware.

These sensors detect and record the electrical activity of the heart, generating a unique ECG waveform specific to the individual

### 1.2 Objectives

- **Data Collection and Analysis:** Gather a diverse dataset of ECG signals from a large population**.** implement preprocessing techniques toremove noise and artifacts from the ECG signals**.** Analyze the collected data to identify important features and patterns for authentication purposes.
- **Feature Extraction and Representation:** Develop robust algorithms to extract discriminative features from the preprocessed ECG signals.Explore techniques to represent the extracted features effectively.
- **Algorithm Design and Implementation:** Design a novel algorithm that compares incoming ECG signals with stored templates. Develop a matching strategy that accounts for variations in signal morphology and timing. Investigate machine learning approaches to enhance the accuracy and robustness of the authenticationsystem.

### 1.3 Proposed System

The proposed biometric authentication system will be evaluated using standard performance metrics, such as False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), and Receiver Operating Characteristic (ROC) curves. Comparative analysis against existing biometric methods will be conducted to assess the superiority of the proposed system, extensive evaluation and validation experiments are conducted using publicly available ECG datasets.

The system's accuracy, sensitivity, specificity, and other relevant performance metrics are measured and compared against existing systems. Additionally, cross-validation techniques are employed to ensure the robustness and generalizability of the proposed system.

DOI: 10.48175/IJARSCT-12757

### 1.4 LITERATURE SURVEY

- ECG Biometric Authentication System Based on Wavelet Transform and Support Vector Machine" byTan et al. (2016): This study proposed an ECG-based authentication system that utilized wavelet transform for feature extraction and support vector machines (SVM) for classification.
- The system demonstrated promising results in terms of accuracy and robustness. Secure Authentication System using ECG and Finger Vein Recognition" by Vargas et al. (2017): This research combined ECG signals with finger vein recognition to develop a secure authentication system. By integrating multiple biometric modalities, the study achieved improved accuracy and security.
- Personal Identification Based on ECG Signals using Wavelet Transform and Hidden Markov Model" by Li et al. (2018): This work introduced a personal identification system based on ECG signals, employing wavelet transform for feature extraction and hidden Markov models (HMM) for classification. The approach exhibited promising results in accurately identifying individuals based on their unique ECG patterns.
- ECG-Based Human Recognition using Wavelet Transform and Principal Component Analysis" by Kumar et al. (2018): This study presented an ECG-based human recognition system that utilized wavelet transform and principal component analysis (PCA) for feature extraction. The system demonstrated high accuracy and robustness in distinguishing individuals based on their ECG signals.
- Deep Learning-based Biometric Authentication using ECG Signals" by Zhang et al. (2019): This research explored the application of deep learning techniques, specifically convolutional neural networks (CNN), for ECG-based biometric authentication. The study showcased the potential of deep learning models in achieving high accuracy and adaptability in ECG signal analysis.
- Robust ECG Biometric Authentication using Random Forest Classifier" by Nguyen et al. (2020): This work proposed a robust ECG-based authentication system that employed a random forest classifier. The study emphasized the importance of feature selection and obtained promising results in terms of accuracy and resistance against spoof attacks.
- Continuous Authentication using ECG Signals: A Comprehensive Survey" by Das et al. (2021): This survey paper provides a comprehensive overview of ECG-based continuous authentication systems. It covers various aspects such as data acquisition, preprocessing, feature extraction, classification algorithms, and evaluation metrics, serving as a valuable resource for understanding the current state- of-the-art in this field.

### 1.5 TECHNOLOGY USED

**Hardware Requirements:**

- **Operating System**: Windows 7
- **Ram**: 8 GB
- **Hard disc or SSD:** More than 500 GB
- **Processor:** Intel 3$^{rd}$ generation or high or Ryzen with 8 GB Ram

**Software Requirements :**

- **Software:** Anaconda.
- **IDE**: Jupyter Notebook

DOI: 10.48175/IJARSCT-12757

## II. BLOCK DIAGRAM

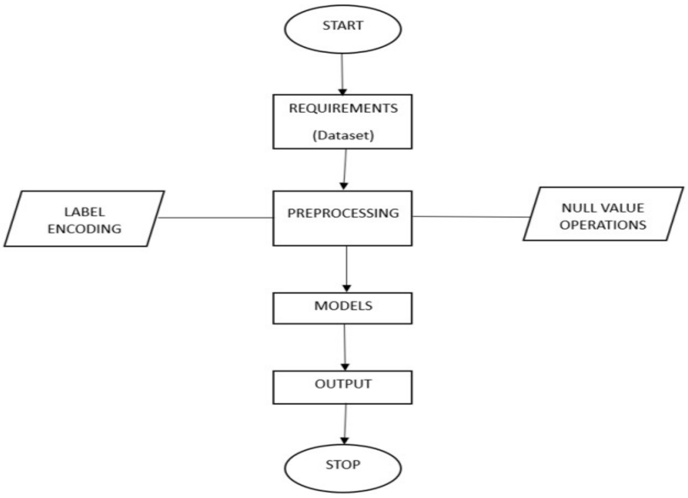

Fig 2.1 Block diagram

## III. METHODOLOGY

- **Preprocessing:** The acquired ECG signals are includes filtering the signal to remove noise, baseline wandering, and other artifacts.
- **Feature Extraction:** The relevant features are extracted from the preprocessed ECG signal. The purpose is to capture unique and distinctive characteristics of the individual's cardiac activity**.**
- **Model:** Once the relevant features are selected, a classification model needs to be trained to distinguish between genuine and impostor users**.** Popular techniques like support vector machines (SVM), artificial neural networks (ANN), or random forests can be employed for model training.
- **Authentication Decision:** After the model is trained, it can be used to make authentication decisions based on the ECG signals of the user.

During the authentication process, the acquired ECG signal from the user is preprocessed, relevant features are extracted, and the trained model predicts whether the user's ECG pattern matches the authorized patterns or not.

**Feature Selection:**

Feature selection aims to reduce the dimensionality of the extracted features while preserving the discriminative information.

This block involves applying suitable algorithms or criteria to select a subset of features that are most relevant for the authentication task. Techniques such as principal component analysis (PCA), linear discriminant analysis (LDA), or information gain can be used for feature selection

**System Integration:**

The developed biometric authentication method based on ECG signals is integrated into a larger authentication system or framework. This may involve integrating the ECG signal acquisition hardware, preprocessing algorithms, feature extraction and selection methods, model training and classification algorithms, and the decision-making module into a cohesive system

It's important to note that the block diagram presented here is a high-level representation, and the actual implementation may involve variations and additional steps depending on the specific requirements and design choices of the system.

DOI: 10.48175/IJARSCT-12757

## IV. RESULTS

### 4.1 ANN Accuracy

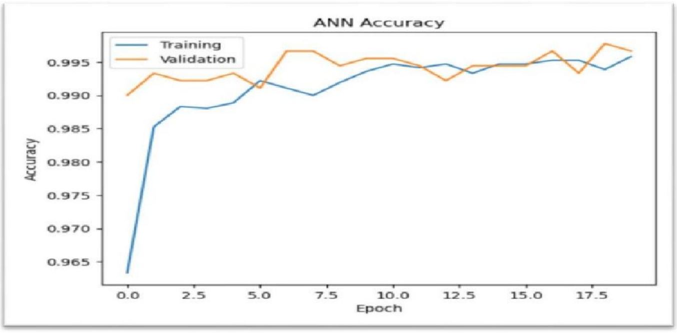

Fig: 4.1 ANN Accuracy for Training and Validation

- **During Training:** For each training iteration or epoch, calculate the accuracy of the ANN by comparing the predicted output with the true labels of the training dataset.
- **During Validation:** After a certain number of training iterations or at the end of each epoch, evaluate the ANN'sperformance on a separate validation dataset that contains samples not used for training.

Calculate the accuracy of the ANN on the validation dataset by comparing the predicted output with the true labels. Thevalidation accuracy is also computed as the percentage of correctly classified samples in the validation dataset.

By plotting the training accuracy and validation accuracy over the course of training, you can assess the model's convergence and its ability to generalize to unseen data.

### 4.2 ANN LOS

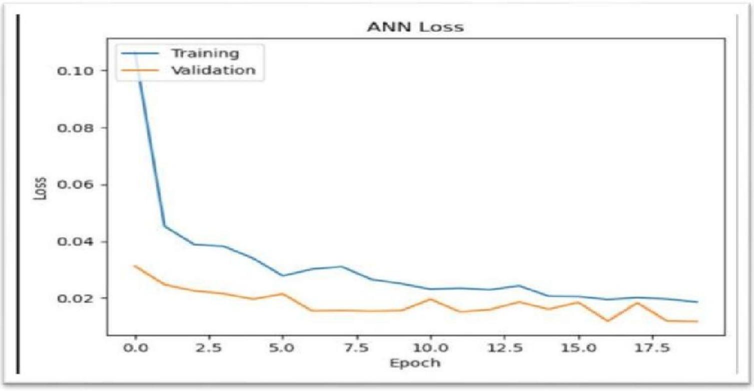

Fig: 4.2 ANN Loss for Training and Validation

**During Training:** For each training iteration or epoch, calculate the loss between the predicted output of the ANN and the true labels using a specific loss function, such as binary cross-entropy, categorical cross-entropy, contrastive loss, or triplet loss.

Aggregate the losses across the training dataset, typically by taking the average or sum. Monitor and record the training loss at each epoch or iteration.

**During Validation:** After a certain number of training iterations or at the end of each epoch, evaluate the ANN'sperformance on a separate validation dataset that contains samples not used for training.

Calculate the loss between the predicted output and the true labels for the validation dataset using the same loss functionas in training. Aggregate the losses across the validation dataset.

Monitor and record the validation loss at each evaluation point.

By plotting the training loss and validation loss over the course of training, you can observe the model's convergence andassess whether it is overfitting or underfitting.

## V. CONCLUSION

In this implementation presents the development of a novel biometric authentication method based on ECG signals.

The proposed method utilizes advanced signal processing techniques and machine learning algorithms to extract distinctive features from ECG signals and perform authentication.

The results indicate that ECG signals can serve as a robust and convenient means of user identification.

The developed system offers a reliable and secure biometric authentication solution that can find applications in areassuch as access control, healthcare, and financial services.

Further research and advancements in ECG-based authentication methods can contribute to enhancing security and privacy in various domains

## REFERENCES

**[1].** R. Salloum and C.-C. J. Kuo, "ECG-based biometrics using recurrent neural networks," in 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2017.

**[2].** S. Šprager, R. Trobec, and M. B. Jurič, "Feasibility of biometric authentication using wearable ECG body sensor based on higher-order statistics," in 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017.

**[3].** Jayarathne, M. Cohen, and S. Amarakeerthi, "BrainID: Development of an EEG-based biometric authentication system," in 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2016 .

**[4].** S. Yang, S. Hoque, and F. J. I. A. Deravi, "Improved time-frequency features and electrode placement for EEG- based biometric person recognition,".

**[5].** A. Hanilçi, H. J. J. o. I. S. Gürkan, and Engineering, "ECG Biometric Identification Method based on Parallel 2-D Convolutional Neural Networks,".

**[6].** M. M. A. Rahhal, Y. Bazi, H. AlHichri, N. Alajlan, F. Melgani, and R. R. Yager, „„Deep learning approach for active classification of electrocardiogram signals,‟‟ Inf. Sci., vol. 345, pp. 340–354, Jun. 2016.

**[7].** D. D. Testa and M. Rossi, „„Lightweight lossy compression of biometric patterns via denoising autoencoders,‟‟ IEEE Signal Process. Lett., vol. 22, no. 12, pp. 2304–2308, Dec. 2015.

**[8].** D. Wang, Y. Si, W. Yang, G. Zhang, and J. Li, „„A novel electrocardiogram biometric identification method based on temporal-frequency autoencoding,‟‟ Electronics, vol. 8, no. 6, p. 667, Jun. 2019.

**[9].** R. D. Labati, E. Muñoz, V. Piuri, R. Sassi, and F. Scotti, „„Deep-ECG: Convolutional neural networks for ECG biometric recognition,‟‟ Pattern Recognit. Lett., vol. 126, pp. 78–85, Sep. 2019.

**[10].** D. M. Uliyan, S. Sadeghi, and H. A. Jalab, „„Anti-spoofing method for fingerprint recognition using patch based deep learning machine,‟‟ Eng. Sci. Technol., Int. J., vol. 23, no. 2, pp. 264–273, Apr. 2020.

DOI: 10.48175/IJARSCT-12757