Biometric Authentication System

ECG Authentication

B. Nithisha@ , B. Sreeja#, G Hari Chandana\*

*@Department of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana, India.*

*#Department of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana, India.*

*\*Department of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana, India.*

Abstract— Unimodal or Single factor biometric systems refer to biometric systems that employ only one form of biometric data to authenticate an individual’s identity. These kinds of biometrics are susceptible to higher error rates and security vulnerabilities because it relays on a single trait for authentication. These biometrics systems increase integrity and privacy since it will contain several biometric features of every customer. So, here designed a unimodal biometrics project utilizing deep learning to enhance authentication security by Electrocardiogram (ECG) signals. VGG-16 model, a deep learning architecture used to capture complex patterns in accurate individual identification with ECG data. The high-resolution convolutional filters captured intricate details of the ECG waveform, ensuring high accuracy in distinguishing different individuals.

Keywords— Biometrics, ECG, VGG16, Unimodal, Security, Dataset, Authentication.

I. INTRODUCTION

Biometric authentication can be considered a very important component in security practice, aiming at using physiological and behavioural characteristics of people to ascertain their identity. This technique is much superior to the conventional forms of authentication where passwords or physical tokens such as key chain token may get misplaced, forgotten or even be stolen. Finger prints, facial features, or voice structure are unique features of an individual and cannot be mimicked by others; hence such type of data serves as reliable solutions for the purpose of authentication.

The security and privacy issues have remained a worry from the time that Internet started. The most conventional techniques of the user authentication strategies mainly rely on passwords, which are also more frequently used. In the past, passwords were used to authenticate users to a central computer in an Intranet environment where the chance of getting the passwords compromised was very small due to the non-connectivity of the Intranet to other networks. However, in the present context, the devices are more connected to the Local Area Networks and the Internet is always available. Also, as a result of numerous IoT devices integration into the nowadays world, there are more and more individuals whose personal data is transmitted and stored. Consequently, implementing stringent access control policies is essential to ensure effective security and privacy [1].

Unimodal biometric authentication is a process that uses one distinct biometric trait, either physiological or behavioral, to confirm an individual's identity. It operates in two main phases: enrollment and authentication. During enrollment, the user's biometric data is captured, processed, and stored in a secure database. During authentication, the system compares the captured data against the stored template to verify the user's identity. This approach offers simplicity and lower cost, making it widely used in applications like unlocking smartphones, secure access to buildings, and financial transactions. However, unimodal systems face challenges such as higher error rates, external factors, and the possibility of spoofed single biometric modalities. Additionally, they have limitations for users who cannot provide the required biometric due to injury or disabilities. Despite their ease of use, higher security environments often prefer multimodal biometric systems that combine multiple traits to enhance accuracy, robustness, and resistance to fraud.

ECG based biometric modalities, apply the unique electrical impulses generated by the heart for the identification and authentication of persons. ECG signals are highly personal dependent on the differences in cardiac structure and function and therefore ECG based biometrics are consistent and robust across time. In contrast to the biometric algorithms like fingerprints, face recognition, ECG biometrics provides non intrusive and continuous form of authentication with least amount of interaction from the user once the signal is taken. The security of ECG-based systems can be further improved by the fact that is difficult to imitate or spoof the above said internal physiological signals which in turn makes the system safe from fraud and impersonation attacks. ECG BIs can be extended for various fields including healthcare, finance and IoT since it is highly immunes to different environment challenges. Present researches in ECG Biometric systems seek at optimizing noise reduction process, investigating variability due to physiological parameters and establishing uniform acquisition and processing methodologies so that they can make ECG biometric system more accurate and dependable. Therefore, ECG biometrics implies one of the most effective approaches toward enhancing identification while employing the physiological natures of the subject’s cardiac signals.

II. CONTRIBUTIONS AND OBJECTIVES OF THE RESEARCH

The major theme of this study is to establish new unimodal biometric ECG (electrocardiogram) recognition to boost security access measures in different hazardous fields. Through the identification of the electrical activity profiles each person’s heart possesses, with the aid of this study, this research intends to devise an exceptionally safe, accurate, and nn- invasive way for identification. Coming up with ways of obtaining ECG signals at high quality during diverse exercises and in order to eliminate or reduce the noise and additional artifacts to acquire better results. Employing current generation data processing methods and computer algorithms, including pattern matching and machine learning, to analyse ECG data and ascertain the uniqueness of the feature and enhance the speed and reliability of the identity recognition process. Securing ECG biometric system from spoofing and other attendant cyber threats through multi-factor authentication and encryption. Proactively identifying and meeting the customers’ needs by creating easily-navigation interfaces and ensuring that the system can be used by heart disease or physically impaired persons. Carrying out extensive experimental and operational trials of ECG biometric systems in practice in order to prove their efficiency and stability when integrating in the preexisting security systems. And bring the development of advanced biometric face recognition systems to increase the security measures in the access and authorization of different regions. Thus, rendering the specifically identified and localized facial features, this work is going to offer a highly accurate, trusted and contactless approach to identity confirmation. Here are some prior objectives:

* Enhances system's resilience against spoofing attacks by integrating authentication and anti-spoofing technologies.
* Improve user experience by designing user-friendly interfaces.

III. LITERATURE REVIEW EXISTING BIOMETRIC AUTHENTICATION

Biometric authentication systems are increasingly used for security due to their ability to verify individuals based on unique biological traits.Biometric identification technologies are advanced; that is, the physiological and behavioral characteristics, which include fingerprints, facial expressions, iris scans, voice recognition, and gait analysis, are more secure and elastic. Biometric modalities already exist as fingerprints and iris scans and are already very efficient and secure especially for use in sensitive places such as mircochips being Pros include high accuracy and reliability Its Cons include spoofing, and its efficiency reduces with changes in environment or physiological states. Modern advances in artificial intelligence and machine learning allow setting up complex feature extraction, elaborated pattern recognition, as well as learning adaptations enhancing accuracy and stability. For instance, CNNs have been quite successful in applications like face recognition, and newest transformer structures work also fine for multimodal biometrics, demonstrating better scalability and speed. Moreover additional modalities including ECG and vein patterns recognition have been developed in order to address issues of universality or liveness detection. Two rather newly popular techniques, the homomorphic encryption and federated learning, have also been used to try to mitigate the ethical issues regarding data privacy and potential bias. Nevertheless, there are several problems for practical implementation of the methods remain: the problem of costs and scalability to arbitrary number of people, the problem of ethics that comes with wider usage of biometrics, all the above calls for further research on the topic.

*B. Research On ECG-Based Authentication*

There are many previously worked ECG-based researches exist. In that we have gone through few papers like: Security concerns are also relevant in Wireless BSNs especially where\_instance, authentication is paramount for the secure communication between the sensor nodes existing in the network. As discussed in the previous subsection, ECG generated by these nodes has real time readout and therefore has inherent liveness. While there are extensive works on the ECG-based intranode authentication in WBSNs, privacy preservation of ECG-sensitive data has received more consideration. The present paper presents an ECG-Based Authentication System with Privacy Preservation Assume a noninvertible transform called the manipulable Haar transform (MHT). This system also protects the intranode authentication as well as the rather sensitive ECG data from disclosure. ECG has proven to be a reliable biometric for human identification as it provides seamless and none stop identification without much possibility of imitation. In many cases, however, many of the current algorithms necessitate long data of ECG, making its applicability a bit restricted. In this paper, a two-phase of authentication using the neural network which we named 3-seconds-user-authentication-NN with a reliable performance is proposed. In the first phase applied and tested on 50 subjects using mobile collected finger ECG signals with general condition the general NN model and then the personal NN model is used. By analyzing the results shown in the graph, one can conclude that the algorithm is effective when applied on the whole set of products as well as on the subgroups of various sample size. Some of the medical IoT applications are used by patients for health monitoring whereby they allow physical examination through sending their own health records to the hospitals. However, security and privacy concerns emanates from the fact that health information is sensitive. Widgets and traditional cryptographic methods with passwords are insufficiently protective in the context of health monitoring’s privacy and security requirements. Biometric authentication particularly using ECG signal is therefore an effective method of human characteristic verification. Nevertheless, ECG seems to be highly appropriate for biometric applications, it is in most cases even usable practical realization of ECG-based authentication which encounter such problems as data noise and concern for privacy.

*C. Research on Unimodal Biometric Authentication*

Unimodal biometric systems are widely used for verifying identity using a single biometric trait like fingerprints, iris patterns, or voice recognition. These systems are simple, cost-effective, and easy to integrate into existing technologies like smartphones and secure access control systems. However, they face challenges such as spoofing risks, environmental impact, high error rates, and failure to enroll.Single traits are susceptible to presentation attacks, which can bypass unimodal systems without adequate security measures. External factors like lighting, noise, or physical damage can degrade performance. Unimodal systems often experience higher False Acceptance Rates (FAR) and False Rejection Rates (FRR) due to limited redundancy. Some users may not have suitable biometric data for certain modalities, such as those with physical disabilities affecting fingerprints. Efforts to mitigate these vulnerabilities focus on enhancing Presentation Attack Detection (PAD) techniques, which integrate hardware and software tools to detect non-genuine biometric inputs. Emerging biometric traits like electrocardiogram (ECG) signals are being explored to complement traditional unimodal systems, offering resistance to spoofing and potentially increasing robustness when integrated into a multimodal framework. Unimodal biometric authentication systems are used in consumer devices, government systems, and banking. However, their limitations in robustness and error resilience suggest that integrating PAD techniques or transitioning to multimodal systems may provide enhanced performance and security.

IV. METHODOLOGY

*B. ECG Data Collection*

For the ECG biometric authentication dataset, we considered the MIT-BIH Arrhythmia Database. MIT-BIH Arrhythmia Database comprises 48 half-hour excerpts from two-channel resting ECG recordings of 30 patients examined at the BIH Arrhythmia Laboratory between 1975 and 1979. The recordings were digitized at 360 samples per second per channel at 11 bits resolution within delta mode of 10 mV range. Two or more cardiologists did label each record and disagreement reached a consensus so as to get computer readable reference annotation for each beat. All the records of the MIT-BIH Arrhythmia Database are kept in this directory and around 50% of the data since the inception of PhysioNet in 1999.

.*D. ElectroCardioGram Signal Extracting.*

ECG data was collected from MIT-BIH Arrhythmia Database. Signal restoration goal is to improve signal clarity through reduction of interference. This involved using a bandpass filter technique in which it became easier to select a certain frequency of the signal that is most appropriate for analysis. Thus, by confining interest to these specific frequency bands—While functionally comparable in some aspects of the signal filtering methodology, the use of the mathematical Fourier Transform has major advantages in later analysis.—the system was able to filter out response components that were of little use in analysing the ECG waveform for the medical diagnostics application in this paper. Following noise removal, the signals are then divided into different regions representing different phases or events in the cardiac cycle. These segmented images were then stored for more analysis and visualization to get clearer view of ECG data without any noises that were not needed. It is not only enhancing the performance of ECG signal interpretation, but also guarantees that the extracted data from ECG signal are useful and contain meaningful information for medical diagnosing or further researches.

*E. Deep Learning Algorithm – VGG16:*

The VGG16 engine is a computational tool which can be used to identify various objects or pictures in a particular image. They are made up of more than one layer that are; the convolutional layer, the pooling layer, then the fully connected layer. VGG16 mimics the human visual system and proved to be able to extract features of different abstraction levels as well to detect spatial relations within the images. Due to its construction, VGG16 puts together unseen layers in a certain sequence to enable the model to learn about hierarchical attributes. The pre-processing in VGG16 is like the human’s brain where it only focuses on very crucial features that will help it make a better decision.

*1) VGG16 Architecture*

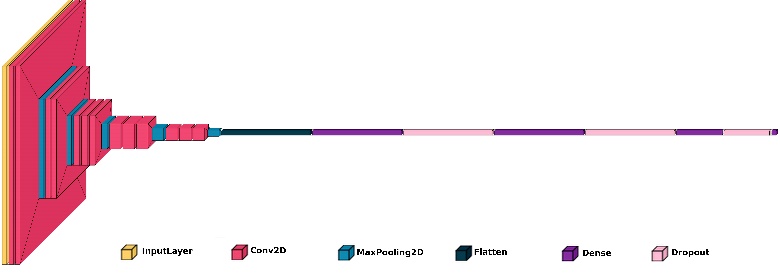


Fig. 1. VGG16 Architecture which we used for and ECG

The VGG model modification aims to enhance the speed in training and improve the optimization for certain classification learning tasks for feature learning. To make the understanding of our model easier, Fig. 1 below depicts a graphical representation of our model. Here, the base model is the VGG16, which is first started with out the final layers so that it can contain individual classifier layers. The first and foremost, all layers of the network are frozen with the exception of the layers that are responsible for feature extraction and by doing so computational resources are conserved yet the ability to extract intricate visual features from images are retained.

Moreover, the VGG16 model has introduced new classifier layers with an aim of making it more flexible. It is basically a deep learning based model, having three fully connected layers with rectified linear unit activation incorporated in between to avoid problem of overfitting, which are followed by dropout layers. The dense layers consist of neurons amounting to 4096 in each of the layer and the next layer containing 2048 neurons and the final layer; soft max layer contain 30 classes for specific purposes of classification. First, it adheres to the primary development of the deep learning model for identification of hierarchical patterns in the target visual data source; second, it aligns with the standard recommendations used in model refinement for enhancing the intended model accuracy.

*H. Method for Authentication.*

By analysing the fig. 2 we can easily understand that data preprocessing of ECG .For the grayscale while for ECG data the noise was removed and the signals segmented. Then feature extraction done with VGG16 architecture, model vgg16.To combine and access the ECG a biometric model used logical ‘and’ operator. The system then processes these inputs by loading the respective pre-trained models: The ECG model compare an uploaded ECG signal for identification by using a threshold score. Then after that if model confirms the model result that the ECG data belong to the person the system announces “Authentication for Weapon successful. ‘Person (no. ) Unlocked. ” and the system records the result. Otherwise it will display “Authentication Failed”. Such an integration guarantees a fast and efficient biometric authentication since it combines the best features of ECG signals recognition.

V. RESULTS AND DISCUSSIONS

*A. Performance Evaluation*

To thoroughly assess our classification models, we have included several key metrics and visualizations.

The **modal accuracy graph** gives the user an understanding of the classifier whereby the y-axis represents the improved class and the x-axis represents the reduced class over the total classes implemented for the classifier.

A **model loss graph** shows the error function based on training wherein the convergence of the model and the ability to minimize the mistakes are presented.

The **ROC** curves are used to portray the diagnostic capacity of the binary classifier frameworks crosswise over discrimination points, it is basically a graph of the true positive rate versus false positive rate measurement.

Lastly, the **confusion matrix** also provides a detailed view of the classification results in that it shows the number of examples which have been correctly classified and misclassified by the model, thereby providing a deeper insight of the efficiency of the model.

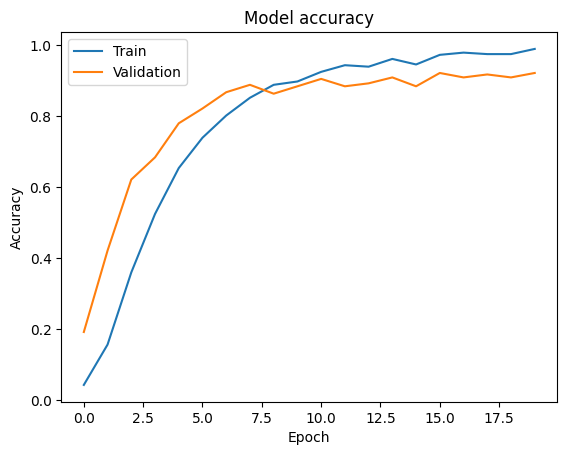


Fig.2 Model accuracy graph

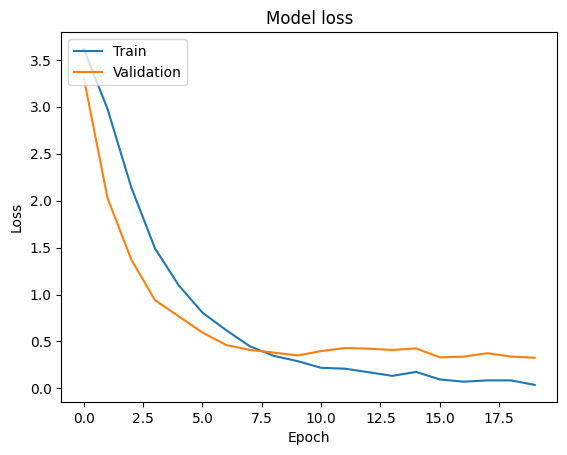


Fig.3 Model loss graph

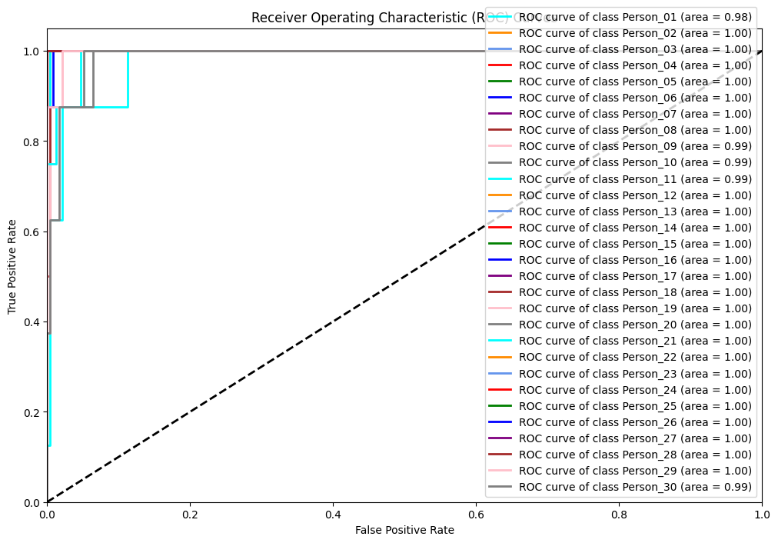


Fig.4 Receiver Operating Characteristic(ROC)

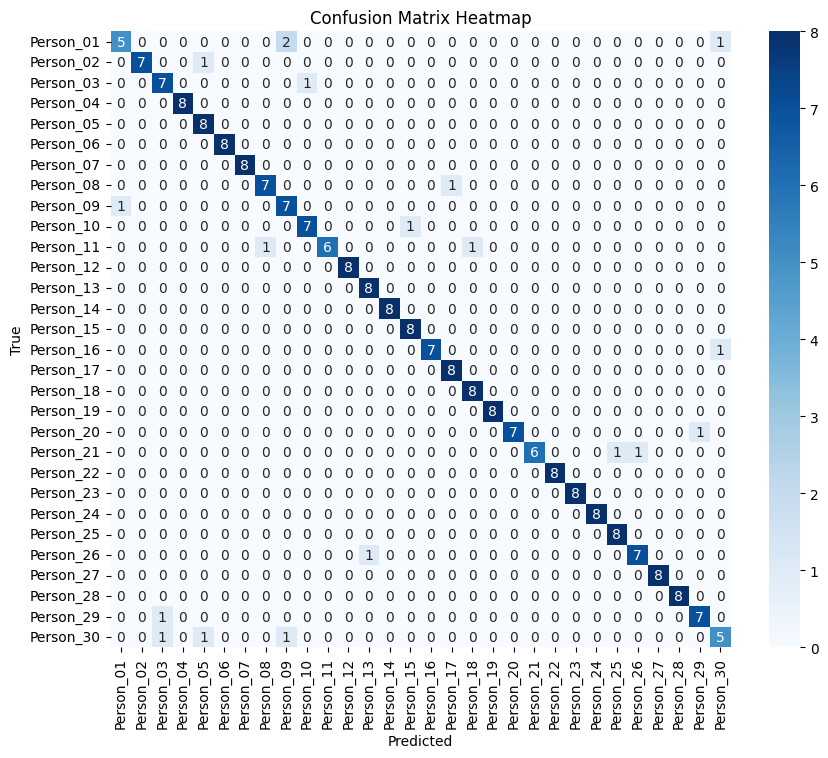


Fig.5 Confusion Matrix

The system uses ECG data to preprocess information and feed it into VGG16. The VGG16 compares the data against a database to check for matches in ECG signals.

VI. CONCLUSION

In conclusion, our study strongly highlights the problems of employing the unimodal biometric systems that are based on the single modes such as fingerprints or face. These systems are prone to exhibit higher errors and security threats because they rely on one factor of identity. To overcome these challenges, the paper supports the use of ECG biometric systems.ECG waveforms as well as the structure. The development of our proposed ECG system means that improvements in terms of accuracy and reliability. Particularly, the proposed approach based on the VGG16 model provided results with a 92. 08% of accuracy for ECG data. This shows of unimodal biometric increases the reliability of the authentication process, increases integrity levels, and protects users from privacy invasions in different applications.

VII. REFERENCES

* Odinaka, P. -H. Lai, A. D. Kaplan, J. A. O'Sullivan, E. J. Sirevaag and J. W. Rohrbaugh, "ECG Biometric Recognition: A New Comparative Study,” published in IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, pp. 1812–1824, December 2012, doi: 10.1109/TIFS.2012.2215324. keywords: Electrocardiography; Feature extraction; Authentication; Training; Heart beat; Databases; Authentication;biometrics, classification, ECG; EKG
* M. Ingale, R. Cordeiro, S. Thentu, Y. Park and N. Karimian, "ECG Biometric Authentication: ” A Comparative Analysis,” International Journal of IEEE Access, vol. 8, pp. 117853-117866, 2020, doi: 10.1109/ACCESS.2020.3004464 keywords: {Electrocardiography;Biometrics (access control);Feature extraction;Authentication;Databases;Biomedical monitoring
* K. N. Plataniotis, D. Hatzinakos and J. K. M. Lee, "ECG Bio.metric Recognition Without Fiducial Detection," 2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference, Baltimore, MD, USA, 2006, pp 1-6.
* {ECG;Biometric;Human;SW PWM;Detector;Finger print;Heart beat;DCT;Iris;Sr}• Eberz, S; Paoletti, N; Roeschlin, M; Kwiatkowska, M; Martinovic, I; Patané, A.baugh, "ECG Biometric Recognition: A Comparative Analysis," in IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, pp. 1812-1824, Dec. 2012, doi: 10.1109/TIFS.2012.2215324. keywords: {Electrocardiography;Feature extraction;Authentication;Training;Heart beat;Databases;Authentication;biometrics;classification;ECG;EKG;electrocardiogram;fusion;identification;recognition;verification}
* M. Ingale, R. Cordeiro, S. Thentu, Y. Park and N. Karimian, "ECG Biometric Authentication: A Comparative Analysis," in IEEE Access, vol. 8, pp. 117853-117866, 2020, doi: 10.1109/ACCESS.2020.3004464. keywords: {Electrocardiography;Biometrics (access control);Feature extraction;Authentication;Databases;Biomedical monitoring;ECG biometric;authentication;segment;off-the-person;on-the-person;Kalman filter;feature extraction;ECG datasets}
* K. N. Plataniotis, D. Hatzinakos and J. K. M. Lee, "ECG Biometric Recognition Without Fiducial Detection," 2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference, Baltimore, MD, USA, 2006, pp. 1-6, doi: 10.1109/BCC.2006.4341628.
* {Electrocardiography;Biometrics;Humans;Space vector pulse width modulation;Detectors;Fingerprint recognition;Heart beat;Discrete cosine transforms;Iris;Strontium}
* Eberz, S, N Paoletti, M Roeschlin, M Kwiatkowska, I Martinovic, and A Patané. 2017. “Broken Hearted: In today’s article, I will explain how to attack ECG biometrics. The authors published this paper in Network and Distributed System Security Symposium in 2017. Internet Society.
* S. I. Safie, J. J. Soraghan and L. Petropoulakis, "Electrocardiogram (ECG) Biometric Authentication Using Pulse Active Ratio (PAR)," in IEEE Transactions on Information Forensics and Security, vol. 6, no. 4, pp. 1315-1322, Dec. 2011, doi: 10.1109/TIFS.2011.2162408 keywords: {ECG; feature extraction; biometric; authentication; indexes; biometric ECG; feature extraction; pulse active ratio (PAR)}
* K. A. Sidek, I. Khalil and H. F. Jelinek, "ECG Biometric with Abnormal Cardiac Conditions in Remote Monitoring System," in IEEE Transactions on Systems, Man, and Cybernetics: Switched, vol. 44, no. 11, pp. 1498–1509, Nov. 2014, doi: 10.1109/TSMC.2014.2336842 keywords: {Electrocardiography;Databases;Feature extraction;Heart;Accuracy;Robustness;Abnormal cardiac condition; Biomedical; Biometric
* S. -C. Wu, P. -L. Hung and A. L. Swindlehurst, "ECG Biometric Recognition: Unlinkability, Irreversibility, and Security,” Internet of Things, IEEE, vol. 8, no. 1, pp. 487–500, Jan. 1, 2021, doi: 10.1109/JIOT.2020.3004362. keywords: {ECG signals;Biometric;IoT security;Feature extraction;Monitoring;Database;Authentication;ECG biometrics;
* E. Al Alkeem et al., "An Enhanced Electrocardiogram Biometric Authentication System Using Machine Learning," in IEEE Access, vol. 7, pp. 123069-123075, 2019, doi: 10.1: \* 1109/ACCESS.2019.2937357 Keywords: Electrocardiography; Authentication; Training; Testing; Mutual information; Matlab; Authentication; biomedical signal processing; electrocardiogram signal ECG; machine learning; mutivariable regression.
* Chamatidis, A. Katsika and G. Spathoulas, "Using deep learning neural networks for ECG based authentication," 2017 International Carnahan Conference on Security Technology (ICCST), Madrid, Spain, 2017, pp. 1-6, doi: 10.1109/CCST.2017.8167816.
* L. Wieclaw, Y. Khoma, P. Fałat, D. Sabodashko and V. Herasymenko, "Biometrie identification from raw ECG signal using deep learning techniques," 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Third IEEE International Conference on Technology and Applications , Bucharest, Romania ,2017,pp 129-133,doi no: 10.1109/IDAACS.2017.8095063