International Journal of Gender, Science and Technology

ISSN: 2040-0748

UGC Care Group I Journal

Vol-12 Issue-02 Dec 2023

# A Machine Learning Framework for Biometric Authentication Using Electrocardiogram

***Dr.Vaka Murali Mohan[1].,Harika Bandaru[2].,Manish Buchnola[3].,Likitha Papaiahgari[4].,Shivani Som[5].***

*[1] Professor & Principal, [2,3,4,5]StudentsB.Tech-IT.*

Malla Reddy Institute of Technology and Science.,Maisammaguda.,Medchal.,Telangana,India

*[1]vakamuralimohan@gmail.com,[2] bandaruharika2002@gmail.com, manureddy041@email.com,[4]likithapapaihgari@gmail.com,[5]reddyshivani108@gmail.com.*

## ABSTRACT

***This article presents a framework for developing biometric authentication systems that rely on electrocardiograms (ECGs) and how to properly implement and fine-tune machine learning (ML) approaches. Researchers and developers working on biometric authentication techniques based on electrocardiograms (ECGs) might benefit from the suggested framework by better defining the scope of necessary datasets and obtaining high-quality training data. Use case analysis is used to ascertain the extents of datasets. Our research on ECG-based authentication led us to identify three separate use cases, or types of authentication, to consider in our work. Improving the accuracy of ML-based ECG biometric authentication methods is as simple as providing more qualified training data to the relevant machine learning techniques. This system acquires high-quality ML training data using the ECG time slicing approach with R-peak anchoring. To assess the reliability of the ML datasets used for training and testing, the suggested framework incorporates four additional measures. Furthermore, a Matlab toolbox is created and released to the public for further research. It includes all suggested mechanisms, measurements, and sample data along with examples of different ML approaches.***

## I. INTRODUCTION

It is now common practice for users to identify themselves by their physical appearance while using application systems, since the majority of these systems provide Internet access to the general public. Because of this, biometric authentication is becoming a highly sought-after area of study. One benefit of ECG authentication over other biometric authentication techniques is that it uses real-time indications from the user's heart rate and other bodily signals to verify their identity. Typically, a verification model for user identification is built using machine learning methods using the individual's live ECG data. Numerous recent state-of-the-art literatures have focused on biometrics based on electrocardiograms [1]_[4]. Data acquisitions, authentication categorization, pre-processing for data quality improvement, Deep Learning (DL), and other Machine Learning classification algorithms are some of the remaining ECG biometrics difficulties that need further exploration [5]. This paper presents a machine learning framework for electrocardiogram (ECG) biometric authentication that aims to address the identified problems with ECG authentication. Identifying fundamental application scenarios via use-cases is crucial to have a better understanding of prospective application contexts for ECG authentication. The three main use cases for ECG authentication in the proposed framework are Hospital (HOS), Security Check (SCK), and Wearable Devices (WD). In addition, methods for preparing ECG data that account for power line interference (PLI), baseline correction of ECG frequency abnormalities, and the _ipping mechanism for ECG signals caused by improper electrode placement are suggested.

This novel framework model for ML-based ECG biometric authentication is shown in Figure 1, which provides an overview. Decision Tree (DT) and Support Vector Machine (SVM) are used for regression in the core process segment, while Artificial Neural Network (ANN) and Convolution Neural Network (CNN) are used for classification.

ML methods are used throughout. Also created and linked to the core process is a time-slicing method for electrocardiogram data.

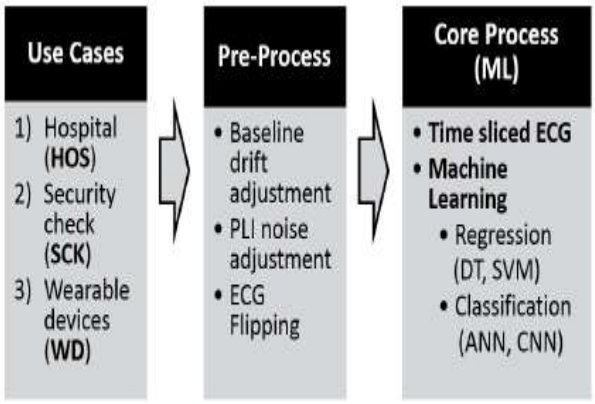



**FIGURE 1. Overview of the new framework model for ECG based biometric authentication.**

The processing flow for ECG biometric authentication utilizing Machine Learning methods is shown in Figure 2.

First, the suggested framework goes through the training step to get matching user categories based on the target system environment.

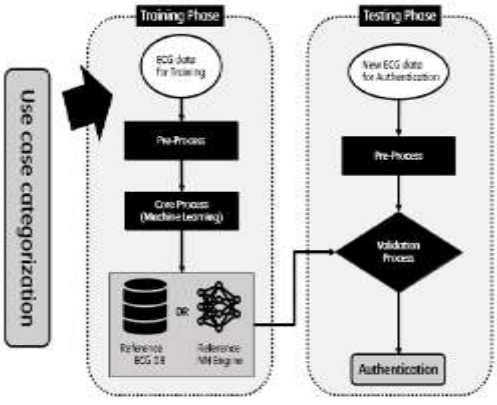



Image 2: The EGC biometric authentication framework processing flow using machine learning technology.

The training dataset consists of electrocardiogram data collected from the intended consumers. After the training data is obtained, it is processed using pre-processing methods to extract higher-quality (noise-less) data. Figure 1 shows a selection of basic process mechanisms that take the filtered data as input and produce an authentication assessment model. At present, the suggested central procedure is able to evaluate any ML-based ECG authentication system using either an ECG reference database or a trained Neural Network (NN) reference engine. After training is over, the NN Engine (or reference database) is created. During testing, the newly obtained ECG data must undergo data pre-processing to produce filtered data with better quality (reduced noise), and an authentication request based on the ECG data is created. After that, the filtered data is fed into the validation process, which confirms the user's identity by consulting the reference database or the NN Engine.

Furthermore, this paper's new Matlab toolbox includes all suggested processes, metrics, and example data with ML approach demos. We have created this toolkit and made it openly accessible for anybody to use in their future research.

## II. AUTHENTICATION CATEGORIZATION BASED ON USE CASES

A lot of research has focused on biometric authentication utilizing electrocardiogram data [6]_[11]. There is a plethora of research on ECG-based authentication, but it's all about different user settings and different ECG detection equipment. Electrocardiographs are often set up by researchers with medical engineering competence to acquire ECG data [6]_[8]. On the other hand, researchers that specialize in electrical engineering often install basic electrocardiogram (ECG) sensors, which are typically integrated into wearable devices, in order to collect ECG data [9]_[11]. Building an ECG-based biometric authentication strategy requires careful consideration of the user's surroundings and knowledge of the potential types of ECG detecting devices. A use case is a detailed account of the intended system's interactions with its end users. Use case analysis may explain important information for system processes and identify system needs during design [12]. By doing use case analysis, it would be possible to classify potential use cases. Figure 1 shows the three authentication categories that could be identified using the use case analysis technique applied to potential ECG based user authentication scenarios: hospital patients, building entrance identity checks, and continuous personal usage authentication. What follows is an examination of the associated user context and assumptions for each group. Keep in mind that the targets application

systems dictate the specific system performance requirements for each category with regard to authentication rate and speed.

What follows is a detailed explanation of the description and requirements for each group. Although there is little difference across authentication use cases, performance measurement methodologies will vary.

**A. Hospital-Based Patient Authentication (HOS)**

In the past, an electrocardiogram (ECG) was the gold standard for diagnosing cardiac illness or stress. Medical diagnostics sometimes need complex and intricate equipment to collect high-quality electrocardiogram (ECG) readings from patients. Since an electrocardiogram (ECG) test uses several leads, the sampling time for obtaining ECG data is rather considerable, ranging from a few minutes to hours. Hospital patient identification (Category 1; HOS use case) is a novel use of electrocardiogram (ECG) testing. Presumably, patients will need to pre-register their identities (names or legal ID numbers) and ECG data from the past.

Furthermore, for both the training (registration) and testing (frication) stages of an ECG-based authentication method, it is assumed that the recorded ECG signals from the same patient are consistent enough, meaning that the recorded ECG signal levels fall within a normal range. After then, the next time such patients come to the hospital, they may be identified using a biometric authentication technique that is based on electrocardiograms. In contrast to a nurse asking the patient for their name and legal identification number, which could take several minutes, a well-trained ECG user authentication model (or scheme) can identify a patient in a very short amount of time (less than a couple of seconds) [13]. Users or patients who lose consciousness in the emergency department may be readily identified using electrocardiogram (ECG) based authentication. Among the many potential use cases for electrocardiogram (ECG) based authentication systems is patient authentication in healthcare facilities. The healthcare and medical industry's most extensively used research environment is this HOS use case [14]. Historical electrocardiogram (ECG) data is available in many publicly accessible databases, such as PhysioBank [15].

**B. SCK authentification of building occupants**

If required, the second use case for user authentication using ECG data is implemented during the security check (Category 2; SCK use case) at the building and room entrances. The majority of businesses use security checkpoints to verify the identities of their personnel and customers. Along with fingerprint scanning, face recognition, voice identification, iris recognition, and retina scan, ECG based biometric authentication systems will soon be available as portable ECG detection devices or sensors become widely available. To distinguish between registered regular workers and unfamiliar people, including guests, this SCK use case employs an authentication mechanism based on electrocardiograms (ECGs). It is presumed that all lawful workers have already identified themselves to this ECG authentication system by providing their names or legal identification numbers, as well as their ECG data from the past. Furthermore, it is presumed that the recorded electrocardiogram signals from the same worker are consistent enough to be used for both the verification and registration processes.

**C. Ongoing Verification for Individual Use (WD)**

One other use case for electrocardiogram (ECG) based user authentication is in wearable devices, such as smart watches, which may constantly check the owner's identity (Category 3; WD use case). The primary need for most wearable devices is the ability to continually verify the owner's identity.

To standardize the received ECG signals by filtering out potential signal noise caused by user body status, a new framing technique may be necessary. This is because a person's heart beat period (R-R peak period) and the amplitude of ECG signals can change dramatically when they are under different body states, such as when they are walking, running, or sleeping. The ability to add second factor authentication to a wearable device is possible with the addition of an electrocardiogram (ECG) sensor and an authentication module. A user may exert more control over the security of their wearable gadget by using a two-factor authentication mechanism, such as logging in with both the user's password and their electrocardiogram data.

Database boundaries classified according to authentication use cases (TABLE 1).

| Cat No. | Cat. Name | Known ID classification | Unknown ID | Personal Status |
|---|---|---|---|---|
| 1 | Hospital (HOS) | O | X | X |
| 2 | Security Check (SCK) | O | O | X |
| 3 | Wearable Devices (WD) | X* | O | O |

* There is only one known ID in the WD case

Due to difference in intended application, the sampling frequency of electrocardiogram (ECG) signals should be much lower than that of ECG signals produced by conventional medical measuring equipment. Furthermore, since different kinds of ECG equipment are used in the HOS scenario and the WD case, human operation problems such lead misplacement will not be included in the WD category.

## III. PRE-PROCESS FOR ECG DATA QUALITY ENHANCEMENT

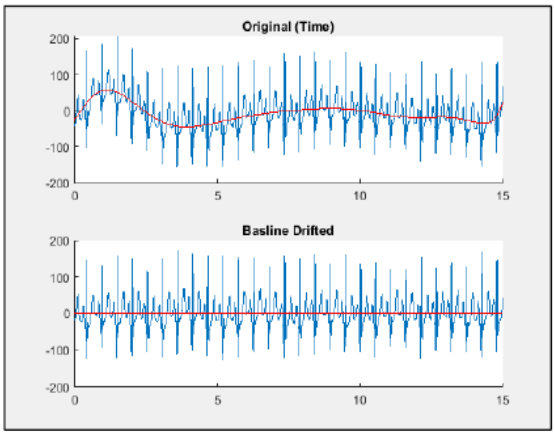
Data adjustments prior to beginning the main process (the machine learning process) are what the pre-process is all about. Since electrocardiogram (ECG) data may be thought of as signals, signal processing methods have been extensively used to modify ECG data.

To improve ECG detection, several signal processing techniques are used, such as filter designs [16]_[18] and Fourier Transforms [19], [20]. It is advised to use three pre-processes to enhance ECG data before commencing the machine learning process, even if numerous pre-processes are employed for signals.

### A. Adjusting the Baseline

A low-frequency distortion in electrocardiograms (ECGs) caused by breathing and electrically charged electrodes is known as the baseline drift (or baseline wander) [21]. Removing baseline drift is the baseline adjustment method. In most cases, setting the high-pass filter's cut-off frequency higher than the signal's lowest frequency is necessary to eliminate baseline wander completely. Cancelling the low-frequency components of the signal is a commonality throughout most baseline wander reduction approaches. In most cases, the baseline wander high-pass filter's frequency is adjusted to be somewhat lower than 0.5 Hz [22]. It is important to know in advance how often to remove the baseline drift, even if these methods have been extensively researched and employed [23]. In addition to low-frequency noise, certain applicant movements may potentially cause baseline drift during ECG data collection.

Thus, these filtering methods can be useless in the HOS instance if we don't have a good indication of the cut-off frequency or if we don't know what an applicant is likely to do.



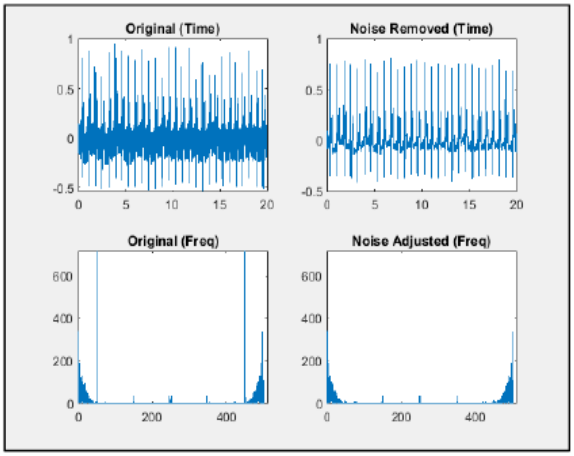

Adjusting the baseline using polynomial curve fitting [15] is shown in Figure 3.

Section B: Eliminating Power Line Interference Noise

Baseline wander and PLI noise coupled to signal carrying cables is especially problematic in medical equipment. This is especially true in hospital settings (HOS case), where seamless supply lines can cause electromagnetic interference (EMI) of frequency on the cables that carry signals from exam rooms to monitoring equipment [26]. Common sources of noise in electrocardiograms (ECGs) include electromagnetic fields (EMFs) generated by power lines, which may introduce 50 or 60 Hz sinusoidal interference and, in some cases, multiple harmonics. Due to the introduction of spurious and unreliable waveforms, such narrow band noise makes low amplitude wave interpretation difficult [27]. One common method for eliminating PLI noise is the Innate Impulse Response (IIR) notch _lter [28]. In order to pass signals above and below a certain frequency range—the stop band frequency range—a

notch filter attenuates or rejects the signals within this range [29].

To eliminate the baseline drift, one might use these filters; however, before doing so, one should establish an appropriate target frequency. On the flip side, you can achieve the same results by using a notch filter to remove aberrant peak points in the frequency domain—all without knowing the desired frequency in advance. This method might be used to eliminate PLI noise in Figure 4 since PLI exhibits strong frequency domain peaks.




A noise modification to remove the PLI frequency is shown in Figure 4 [30].

In the frequency domain, the Fourier Transform has been used to identify anomalous peak locations. In order to improve the original ECG data, noise-like anomalous peak spots in the frequency domain, such as PLI frequencies (usually 50-150 times larger than an average magnitude), are eliminated.

On the other hand, you might eliminate the sounds that occur at certain frequencies. In the case of PLI, the frequency is 50 Hz, while in the case of baseline wander, it is 1 Hz. Removing these frequencies using the Fourier Transform might enhance the ECG data, even without the use of filters.

### C. Signal Reversal

Experts are usually needed to set up and assess ECG signals from medical equipment, such as an electrocardiograph. The incorrect placement of electrodes is only one example of how even experts may make a mistake. It is quite unusual for hospital personnel to inadvertently flip an ECG signal. Fig. 5 is an example of ECG _ipping, and it is preferable to verify whether a target ECG data is _ipped or not during either the training or testing stages. If the original data is _ipped, this pre-process will alter it; otherwise, it will keep the original data and any adjustments made will be applied. A more simplified approach to _ipping ECG data involves _piping status determination using mean value testing of subsets of data rather than whole data inspection.

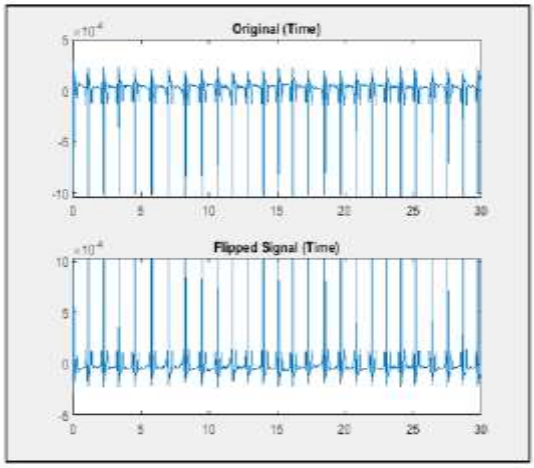



FIGURE 5. Flipping ECG data example [31].

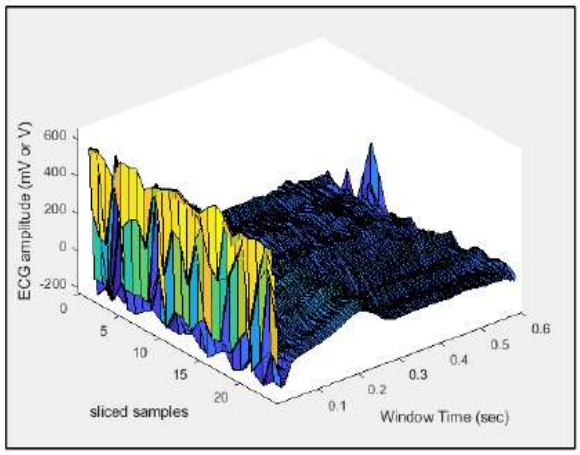
## IV. TIME SLICING AND MACHINE LEARNING

When constructing the dataset for machine learning training, the temporal slicing approach is taken into consideration. For the purpose of constructing the training data for machine learning, this method is very useful. The ECG data is divided using the R-peak anchoring method, which involves a slice (window) time commonly referred to as a sliding window. This approach has the potential to provide a sufficient number of data samples, with each data slice serving as a training input for the machine learning system. The time-sliced ECG dataset may be easily combined with other training inputs and used with a variety of ML training techniques, as discussed in subsection B. A. Automated ECG Segmentation for Deep Learning As the most prominent and important section of the tracing, the QRS complex is a composite of three of the graphical defections found on a typical electrocardiogram (ECG) [32].

The highest point of a QRS complex, also known as an R-peak. The anchor of the QRS complex, which

includes R-peak detection and optimizing the sliding window time, is often based on the moment of the R-peak, and it signals one pulse [33]. By dividing the ECG signal from its R-peak moment to its sliding window period and then stacking the parts according to the R-peak moment, time slicing may be used for ECG data in the time domain, which is ideal for R-peak anchoring. The machine learning training uses each slicing peace as an input sample, according to the R-peak anchoring in Figure 6. In this study, a slicing time (i.e., sliding window) of 0.6 seconds, which is consistent with a heartbeat rate of 100 bps, is selected as the average minimum of a heartbeat interval from abnormal heart rates [34].

The goal of ECG-based projects determines the optimal sliced window time, and ECG slicing time considerably affects various machine learning performance metrics. Other intriguing ECG-based security research issues include improving window time for biometrics, however we are not currently addressing this optimization challenge.




ECG time slicing using the R-peak anchoring method (Figure 6) [15].

**B. A Method for Teaching Data to Machines**

One branch of AI, machine learning allows computers to learn how to do a job well even when given no human-level guidance. Without being explicitly coded, machine learning algorithms may construct a mathematical model from training data and use it to make judgments (classification/pattern recognition) or predictions (regressions) [35]. There has been a lot of research on utilizing AI approaches to analyze ECG data [5, 6, 8, 36, 39].

Training the time-sliced ECG data using ML approaches is the main emphasis of this study. Different methods are offered to illustrate the incorporation of a machine learning model into the ECG-based biometric identification system.

Table 2: DT and SVM Comparison.

| DT | | SVM | |
|---|---|---|---|
| **Results** | | **Results** | |
| RMSE | 33.761 | RMSE | 36.168 |
| R-Squared | 0.59 | R-Squared | 0.54 |
| MSE | 1139.8 | MSE | 1308.1 |
| MAE | 19.164 | MAE | 19.01 |
| Prediction speed | ~740000 obs/sec | Prediction speed | ~600 obs/sec |
| Training time | 5.2194 sec | Training time | 2008.2 sec |

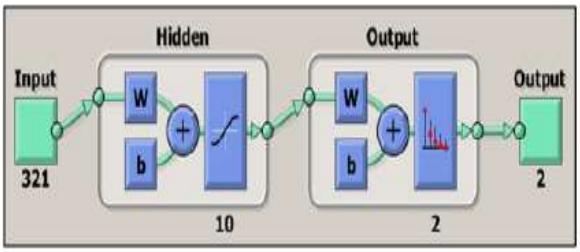



**FIGURE 7.** Design of 10 hidden layer convolution neural network (WD).

## V. DATA QUALITY MEASURES

Every machine learning (ML) project must include testing the algorithms' performance, and providing high-quality samples is critical for this purpose [51]. The values of assessment findings of sample data quality and authentication systems based on regression procedures are examples of performance measurements (evaluation metrics) [52]. Here are some common metrics for evaluating the quality of data and the effectiveness of a regression approach:

the mean squared error, the mean absolute error, the sum of squares error, and the sum of squares total

In addition to the usual quality metrics, the article also introduces several novel metrics for evaluation. Both the requirements for validating samples and regression-approached machine learning systems make use of these quality indicators. I have updated the data quality measures to the following:

* Accuracy percentage inside ranges* Accuracy per upper control limit* Mean absolute error rate* Upper and lower range control limits

The following sections elaborate on the aforementioned new data quality metrics.

**Section A. The MAER**

To evaluate a machine learning model, the Mean Square Error (MSE) and the root Mean Square Error (RMSE) are helpful metrics to track mistakes. One measure of accuracy in estimation is the mean squared error (MSE) [53]. Two often used metrics for evaluating machine learning are the root-mean-squared error (RMSE) and the mean-squared error (MSE). Most regression-based machine learning model assessments employ either the mean squared error (MSE) or the root mean squared error (RMSE), however it is difficult to tell by looking at either of these metrics alone whether the model is excellent or terrible. This study introduces a new metric for evaluating machine learning engines or training datasets. One way to define the MAER is as follows:

$$MAER = \frac{1}{N}\sum_{n=1}^{N}\frac{|Y_n - \mu_n|}{\mu_n + \epsilon}, \quad \epsilon \sim 0 \qquad (1)$$

**B. Limits of Upper and Lower Range (UCL, LCL)**

Quality engineers often use the terms statistical process control (SPC) and statistical quality control (SQC) interchangeably; both terms refer to the use of statistical methods to the control of a process manufacturing method [54]. Two of SPC's most common uses are quality control and control charts (also known as acceptance sampling) [55]. There are two varieties of control charts: X-charts, which show the data's mean, and R-charts, which show the data's range, or variance or standard deviation. If you look at a control chart, you'll see horizontal lines called control limits. These lines are often drawn at a distance of _3 standard deviations (or _6 standard deviations) from the mean of the data.

Both with and without the reference values, R-charts may be constructed. The control values might be used to exclude outliers before training the data, and both figures illustrate the data quality. Here are the upper and lower control limits (UCL and LCL) for the range of values R:

$$UCL = \overline{R}_Y + \sigma(b)\overline{R}_Y, \qquad (2)$$

$$LCL = Max\left(0, \overline{R}_Y - \sigma(b)\overline{R}_Y\right), \qquad (3)$$

**C. Range-Based Accuracy Percentage (APR)**

An ECG's Accuracy Percentage within Ranges (APR) is its proportion of data falling between zero and the upper confidence limit (UCL).

The entire number of sliced ECG data samples is divided into ranges, and the counting numbers inside each range make up this total.

$$APR = \frac{n(\{R \le UCL\})}{n(\Omega_R)} \qquad (4)$$

Even before verifying data, the APR shows how well the time-sliced ECG data is, and a higher APR means greater performance. Additionally, this number serves as the cutoff for disregarding the experimental ECG results prior to comparing them to the control data. A higher APR number indicates that the dataset and ML system are of higher quality.

**Section D. Accuracy per UCL (APU)**

One measure of training efficacy is the Accuracy percentage within ranges per the upper control limit (APU), which is calculated as the ratio of the APR to the UCL. As the UCL decreases, the APR may remain modest despite the great accuracy. Here is how the APU is determined:

$$APU = \frac{APR}{UCL} \qquad (5)$$

## VI. MATLAB TOOLBOX

Sections I through IV lay out the groundwork for implementing ML approaches into biometric identification systems that use electrocardiograms (ECGs). The suggested Matlab functions serve as the toolbox that demonstrates the procedures and strategies in each area. Here are a few examples of the functions included in the amgecg Toolbox, which is short for "Amang ECG Toolbox," a collection of Matlab routines that researchers may utilize for their own ECG authentication studies.

**A. Pre-Process and Time-Slicing Instruments**

As part of the preprocessing for the Machine Learning adaptations, the following three procedures have been included to the toolbox: adjusting the baseline drift (Figure 3), adjusting the noise (Figure 4), and processing the _ipping ECG data (Figure 5).

- *baselinedrift*
- *enhancednoiseadjust*
- *pseudoflip*

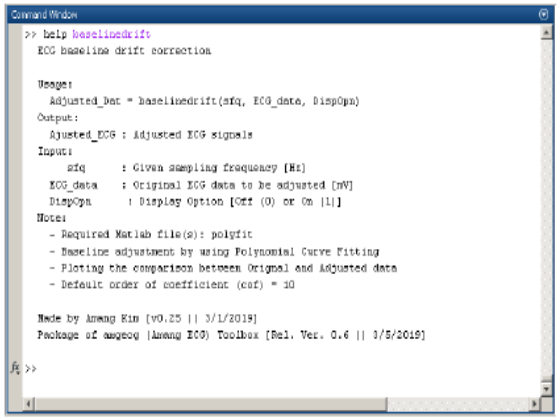



FIGURE8, The Matlab command window's "help" feature in action.

One of the main reasons to include ML approaches into ECG authentication projects is the timeslicedecg function, which opens up possibilities for using different ML techniques on ECG data. The ECG data might be time-sliced for use in designing the ML system, with each slice serving as input for the system. The amgecg Toolbox allows users to create ML systems, but it does not offer true Machine Learning implementations like the DT regression and CNN classification (Figure 7).

**Section B: Data Quality Tools**

You may find the tools you need to assess data quality in the amgecg Toolbox as well. The following related functions are available in the toolbox, which contains the data quality indicators discussed in Section V:

- *rangecontrol*
- *maer*
- *mseamg*
- *maerdataqualityengine*
- *msedataqualityengine*

Figure 9: MAER-based data quality analysis demonstration.

Data quality functions are a hybrid of more fundamental and integrated ones. In Matlab, the "help" function provides information on each function. Figure 9 further shows that the demo _le is accessible with the Toolbox.

The Matlab source codes, namely the amgecg Toolbox, may be found on GitHub1 and are freely used by readers. Furthermore, YouTube has demonstrations of how to use the amgecg Toolbox's features.2

## VII. CONCLUSION

Massive application systems throughout the globe will soon use ECG-based biometric identification as new ECG detection devices grow smaller, lighter, embeddable with cell phones and wearable's, and connectable with distant servers via wireless technologies. It is common practice to apply ML approaches to construct a more reliable assessment model for ECG based biometric authentication in order to achieve high user authentication accuracy.

This research introduces a generic machine learning framework for biometric authentication based on electrocardiogram (ECG). To facilitate the design and evaluation of an ML-based ECG user authentication strategy, the proposed framework details the general data processing flow of such a mechanism, in addition to a number of functional aspects. Among

these features are three new authentication categories for ECG users, three new methods for pre-processing data, a method to slice time in order to create high-quality ECG datasets, four new metrics for measuring data quality, and a publically accessible Mat lab Toolbox called magic Toolbox. Researchers can still benefit from the suggested framework's various data pre-processing techniques and newly defined measure metrics, which can speed up the development of their ML-based schemes, even if they are not using ML technologies to study ECG-based biometric authentication.

## REFERENCES

*[1] Q. Zhang, D. Zhou, and X. Zing, ``HeartID: A multiresolution convolutional neural network for ecg-based biometric human identi_cation in smart health applications,'' IEEE Access, vol. 5, pp. 11805_11816, 2017.*

*[2] J. R. Pinto, J. S. Cardoso, and A. Lourenço, ``Evolution, current challenges, and future possibilities in ECG biometrics,'' IEEE Access, vol. 6, pp. 34746_34776, 2018.*

*[3] E. J. da Silva Luz, G. J. P. Moreira, L. S. Oliveira, W. R. Schwartz, and D. Menotti, ``Learning deep off-the-person heart biometrics representations,'' IEEE Trans. Inf. Forensics Security, vol. 13, no. 5, pp. 1258_1270, May 2018.*

*[4] H. Kim and S. Y. Chun, ``Cancelable ECG biometrics using compressive sensing-generalized likelihood ratio test,'' IEEE Access, vol. 7, pp. 9232_9242, 2019.*

*[5] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, ``Machine learning and deep learning methods for cybersecurity,'' IEEE Access, vol. 6, pp. 35365_35381, 2018.*

*[6] H. J. Kim and J. S. Lim, ``Study on a biometric authentication model based on ECG using a fuzzy neural network,'' Proc. IOP Conf. Ser., Mater. Sci. Eng., vol. 317, Mar. 2018, Art. no. 012030.*

*[7] J. R. Pinto, J. S. Cardoso, A. Lourenço, and C. Carreiras, ``Towards a continuous biometric system based on ECG signals acquired on the steering wheel,'' Sensors, vol. 17 no. 10, p. 2228, 2017.*

*[8] M. Sansone, R. Fusco, A. Pepino, and C. Sansone, ``Electrocardiogram pattern recognition and analysis based on arti_cial neural networks and support vector machines: A review,'' J. Healthcare Eng., vol. 4, no. 4, pp. 465_504, Jun. 2013.*

*[9] A. E. Saddik, J. S. A. Falconi, and H. A. Osman, ``Electrocardiogram (ECG) biometric authentication,'' U.S. Patent 9 699 182 B2, Jul. 4, 2017.*

*[10] S. Y. Chun, J.-H. Kang, H. Kim, C. Lee, I. Oakley, and S.-P. Kim, ``ECG based user authentication for wearable devices using short time Fourier transform,'' in Proc. 39th Int. Conf. Telecommun. Signal Process. (TSP), Jun. 2016, pp. 656_659.*