A Continuous Heart-Based Biometric Authentication for Healthcare Internet of Things

Laura R. Soares[1], Lucas Bastos[2], Bruno Martins[2], Iago Medeiros[2], Dênis Rosário[2], Jéferson C. Nobre[1], Eduardo C. Cerqueira[2]

[1]Institute of Informatics
Federal University of Rio Grande do Sul (UFRGS) – Porto Alegre, RS – Brazil

[2]Computer and Telecommunication Engineering Faculty
Federal University of Pará (UFPA) – Belém, PA – Brazil

{lrsoares,jcnobre}@inf.ufrgs.br,
{lucas.bastos,bruno.martins,iago.medeiros}@itec.ufpa.br,
{denis,cerqueira}@ufpa.br

Abstract. *The rapid spread of connected objects in healthcare environments, i.e. Healthcare Internet of Things (HIoT), has motivated concerns on data privacy. Thus, security mechanisms are required to restrict access to such data. Biometrics, measurements, and calculations related to human characteristics can be collected from the target biosignal (e.g., electrocardiogram - ECG) and employed for authentication. This work investigates a continuous heart-based biometric authentication system for HIoT. We propose a system to provide authentication mechanisms mainly targeted at preserving users' privacy and respecting low cost and scalability. This system employs fiducial features from Electrocardiogram (ECG) to produce a security token that corresponds to the user's identification. We evaluate our system through simulation experiments performed using a Proof of Concept (PoC) implementation and ECG samples from an open database. In these experiments, it is possible to observe the feasibility of our proposal as well as its desirable properties.* ***Keywords:*** *Healthcare Internet of Things (HIoT), Authentication, Biometrics, biosignal, Electrocardiogram (ECG), and privacy.*

1. Introduction

Healthcare Internet of things (HIoT) enable to collect, analyze, and distribute Healthcare sensor data to the interested users [Matni et al. 2020]. In this way, HIoT improves the e-Health environment by providing new medical therapies, faster diagnosis, and decision-making. HIoT systems have some common Internet of Things (IoT) characteristics, such as resources-restricted objects and communication networks, and some particularities, such as high privacy requirements [Wang 2018]. In this context, it is important to design an strong authentication system for the objects that compose a HIoT system, since physiological data expose sensitive information about HIoT user [Barros et al. 2020].

Biometrics have an advantage over traditional authentications methods, such as passwords. This is because biometric authentication depends on intrinsic characteristics of subjects that cannot be stolen [Barros et al. 2020], and are only lost under very specific circumstances. In HIoT facilities, one of the main biometric characteristics available is

the electrocardiogram (ECG). The ECG is present in all human beings and has great variability between different individuals, turning into an unparalleled choice for human authentication. These characteristics led the ECG to be an interesting solution for biometric authentication systems. For instance, there is an increasing number of research initiatives over the past few years using ECG for authentication system [Pinto et al. 2018].

A biometric authentication system is composed of an acquisition sensor, a storage module, and a biometric algorithm. The acquisition sensor captures the electrical activity of the heart (considering the ECG signal) and sends it to the storage module, which is responsible for storing models of user information [Bastos et al. 2022]. Specifically, the biometric algorithm is responsible for deciding whether an identity claim is legitimate or not, comparing the signal from the sensor and from the storage model. This user model consists either of fiducial features (measurements between heartbeat reference points) or non-fiducial features (where the entire signal is processed) [Barros et al. 2020].

Biometric authentication is crucial to offer confidentiality for legitimate users. In this context, biosignals, such as Electrocardiogram (ECG) and others, have essential advantages for such systems since they are hard to be stolen or replicated. It is because biosignals are something inherent in our organism that represents a peculiarity of hemodynamics and cardiovascular system for each individual [Bastos et al. 2021]. Recent studies prove that users' identification using these biosignals can achieve satisfactory accuracy for different user identification and authorization applications [Bastos et al. 2022].

This paper presents a biometric authentication system based on ECG signals, using computational low-cost techniques and algorithms to be applied in the resource-restricted HIoT scenario. The decision algorithm of the proposed system is based on Euclidean distance, a similarity metric of linear cost, and uses fiducial feature extraction from the ECG signal to reduce the amount of computation required for the authentication process. The system is then evaluated by means of computational cost, accuracy, and authentication time using a Proof of Concept (PoC) implementation. Evaluation results show biometric authentication with 0.018 (one trial), 0.116 (ten trials) milliseconds of computation time. This result is around 100 times faster than the current values from the related works in the literature.

This paper is organized as follows. Section 2 discuss the Related work. In Section 3, our proposed solution and its associated concepts are described. The experimental evaluation, encompassing simulation setups, is presented in Section 4. Finally, we present the concluding remarks and future work in Section 5.

2. Related Work

Huang et al. [Huang et al. 2019] proposed an ECG-based authentication with noise detection and elimination in real-time, making the system reliable even with noisy inputs. The application of ECG-based authentication becomes more practical than ordinary ones for daily use, especially for long-term health monitoring. The most common daily exercises, i.e., walking, running, and jumping, are included. The privacy of ECG templates is protected by providing indistinguishability. The sensitivity of ECG signals is considered while the authentication accuracy is preserved after optimized privacy enhancement

Peter et al. [Peter et al. 2016] presented a biometric authentication protocol that intrinsically reflects the statistical properties of the uncertainties, which systematically

balance the risk of false rejected authentications and false accepted attempts. They addressed these issues in two stages. Design and implement a sensor platform, including suitable data processing and feature detection methods.

Seepers et al. [Seepers et al. 2015] evaluated the security performance of heartbeat-based security in the context of entity authentication. Specifically, this work thoroughly characterizes the strength of the Inter-Pulse-Interval (IPI) based keys, investigating several aspects that may occur in practice. Specifically, they considered 1) subjects with different degrees of heart-rate variability (HRV); 2) different sensor sampling frequencies; 3) realistic inter-sensor variability (VAR) based on measurements obtained from ECG and blood-pressure recordings; and 4) average and worst-case authentication time.

Tan et al. [Tan and Perkowski 2017] proposed a two-stage subject verification system that takes advantage of both fiducial and non-fiducial features, and combines a probabilistic random forest classifier with a one-to-many template matching classifier based on wavelet coefficients. To objectively assess the performance of the proposed algorithm, a new ECG database is created by combining ECG data from four sources, including the ECG from a mobile phone, the ECG in the presence of arrhythmia, the ECG with normal sinus rhythm, and the ECG data measured over 6 months.

Choi et al. [Choi et al. 2016] proposed a practical biometric authentication method using ECG signals acquired via mobile sensors. Validating the actual utility of the present method for biometric authentication via ECG signals acquired by a low-cost mobile sensor. This work designed a bandpass filter by cascading a low-pass filter and a high-pass filter to remove the noises embedded in the ECG signals acquired by the mobile sensors. As the authentication unit, they presented a segmentation from ECG signals into a heartbeat unit and a feature extraction procedure together with empirically tuned values of parameters. Finally, a classifier-based authentication scheme is proposed to achieve a satisfactory performance, where training data is constructed to avoid the unbalanced problem in the one-against-all authentication.

In this section, we analyzed some works employing ECG signals for authentication and identification tasks, sensor handshaking, and others. These works use both fiducial features (using signal reference points for processing) and non-fiducial methods (using the entire signal for processing). However, none of the analyzed works have both the same authentication scenario and the resource constraint requirements as proposed in this work. Therefore, further research on the combination of fiducial features with less costly techniques in a healthcare scenario is necessary.

3. Heart-Based Biometric Authentication System

In this section, we present the scope and requirements of this work. Then, we introduce the fiducial feature set used for user authentication in the proposed system. At last, we introduce the decision algorithm based on Euclidean distance used for the template-matching.

3.1. Requirements

This work is intended as a lightweight ECG-based biometric authentication system to be applied in resource-constrained devices inside a HIoT environment. The ECG is the

biometric trait of choice due to its wide availability in this environment. In addition, the authentication functionality could be integrated into the sensor without demanding further computation, mainly in patients limited to hospital beds. This resource optimization is important due to the mentioned limitation in the computational capability of the target devices, e.g., HIoT sensors.

Most HIoT systems are divided into a three-layer architecture, namely, sensor, server, and the gateways responsible for the communication between them. The goal of the proposed system is to be resource-friendly enough to be applied to the sensor node of the biometric system, since The sensor node is where the computational resources are the most scarce. Therefore, there is a need for the decision algorithm to be as less costly as possible.

For the classification of resource-constrained environments, there is a need for a common and succinct terminology that can roughly translate each device's capabilities. In this work, we use International Engineering Task Force (IETF) terminology (RFC 7228 [Bormann et al. 2014]), which defines classes to divide the constrained devices regarding available data and code size, as shown in Table 1.

Table 1. Terminology

Name	Data size (e.g., RAM)	Code size (e.g., Flash)
Class 0 (C0)	$<<$10 KiB	$<<$100 KiB
Class 1 (C1)	$\sim$10 KiB	$\sim$100 KiB
Class 2 (C2)	$\sim$50 KiB	$\sim$250 KiB

The scope of this work will be handling on-the-person sensors in a medical acquisition setting, and the accuracy of the ECG measurement is expected to be satisfactory. The noise-to-signal ratio is higher in this circumstance [Pinto et al. 2018], and thus the pre-processing accomplished the denoising part with simple bandpass filters, which do not require extensive computation. This work will focus on feature extraction and decision algorithm. For now, the acquisition of the signal and the denoising step from the pre-processing phase will be left out of the scope.

The final goal of the proposed system is to be employed in real-world scenarios. Therefore, it is desirable that the testing dataset would have a high degree of intra-subject variability as well as inter-subject variability, so the system can be tested to work properly even in circumstances in which the biometric signature of a subject is slightly altered.

3.2. Feature Set Selection

Fiducial approaches in biometric authentication systems require the detection of fiducial points in the ECG signal, such as the P, QRS, and T waveforms [Barros et al. 2020]. The noisier the input signal, the greater the difficulty in locating these features after filtering. However, the scenario of this work employs on-the-person sensors in medical acquisition settings, therefore making the fiducial feature detection and extraction attainable with less costly methods. Also, in this scenario, the medical equipment often produces the features for clinical diagnostic purposes, which could be reused in the authentication system.

A subset of the features used by Biel et al. [Biel et al. 2001] was selected for the evaluation of the system proposed in this work. This subset of features is related either to

the duration or to the amplitude of a fiducial event. These features are the duration of the P, R, S waves and QRS complex, the onset of the QRS complex, and the time interval of the whole PQRST segment. Features in the amplitude class are the T wave amplitude, the amplitude between the S and the T-peak, and the amplitude of the QRS complex.

3.3. Template-Matching Algorithm

One of the main goals of this work is to investigate an authentication algorithm as inexpensive as possible in terms of computational cost while maintaining acceptable accuracy. In authentication tasks, the system's goal is to accept or reject an identity claim from a user registered in the database. It is attainable with metric-based algorithms, which are less costly than the alternative machine learning classifiers employed in identification tasks, that must sort out the correct identity through a classification process [Pinto et al. 2018].

For use in this work, part of the authentication strategy proposed by Singh et al. [Singh and Singh 2012] and based on Euclidean distance was evaluated due to the similarity in the chosen feature set. The complete authentication algorithm employed in the proposed system works as follows.

A matrix $P_{(i)}$ of feature vectors for user i is populated with m vectors of d features (as shown in Equation 1). In a system with n users, there are n different template matrices in the user database, where i = 1, 2,..., n. A sample vector Q with d features f' is acquired from the test vectors list.

$$P^{(i)} = \begin{pmatrix} f_{1,1} & f_{1,2} & . & . & f_{1,d} \\ f_{2,1} & f_{2,2} & . & . & f_{2,d} \\ . & . & . & . & . \\ f_{m,1} & f_{m,2} & . & . & f_{m,d} \end{pmatrix} \tag{1}$$

The distance between sample vector Q and each jth vector of i user's matrix $P^{(i)}$ is then measured using the Euclidean distance formula, with j = 1, 2,..., m, as shown in Equation 2.

$$d(Q, j) = \sqrt{\sum_{k=1}^{d} (f_k - f'_k)^2} \tag{2}$$

Afterward, following the algorithm proposed by Singh et al. [Singh and Singh 2012], a final distance score between Q and the $P^{(i)}$ matrix is then generated by calculating the mean of all the m distance values. Following this algorithm, the smaller the value of the distance score between Q and $P^{(i)}$, the greater the probability of Q belonging to user i as well. The final step then compares the calculated distance score with a system threshold (T). The user will be successfully authenticated if the distance score is smaller than T and rejected otherwise. T is the relation between the allow as few as possible false acceptances while also keeping false rejections to a minimum.

4. Evaluation

This section focuses on the methodology and results to evalute the proposed heart-based biometric authentication system. We start by introducing the ECG-ID dataset from Phys-

ioBank [Goldberger et al. 2000], since it fitted the system requisites for variability and had denoised signals. Then, we present the further information about the development of the fiducial feature detector, the feature extractor, and the decision algorithm. We also introduce the experiments using the decision algorithm and the database of the user's features, evaluating both the accuracy and computational cost of the system. Finally, we discuss the obtained results, and some results are compared with the existing literature.

4.1. Dataset

The selected dataset for testing and evaluating the proposed system was the ECG-ID from PhysioNet [Goldberger et al. 2000]. While several of the available datasets focus on the study of cardiac conditions, the ECG-ID database is focused on the use of ECG for biometric recognition[1]. It contains 310 ECG recordings of about 20 seconds each from 90 subjects, acquired using limb-clamp electrodes from Lead I (the channel acquired from electrode placement on the wrists). The number of recordings per subject ranges from 2 to 20. The database provides original and filtered signals for each recording of 90 subjects. For this work, we selected the subjects from the ECD-ID database with at least four recordings to provide the desired degree of intra-subject variability.

Some of the selected records were found to be corrupted by noise peaks or measurement errors, which caused the feature detection to be unreliable. These recordings were either corrected by removing the corrupted length or removed. It led to a final set of 20 users, with four recordings of 20 seconds each, to be handed to the feature extraction phase.

4.2. Implementation

The QRS detection algorithm proposed by Pan and Tompkins [Berkaya et al. 2018] is still one of the most relevant fiducial feature detectors still used. Therefore, we rely on it for initial R-peak and waveform delimiters detection. The remaining necessary fiducial points, i.e., the Q and S peaks, are derived by analyzing the parts immediately before and after the appointed R-peaks for the lowest voltage values. We also set the onset and offset for the R wave, using the baseline value between the P, QRS, and T deflections as a reference. The P wave onset was considered the starting point of the heartbeat for feature calculation. Each set of fiducial points between a P wave onset and a T wave offset in a record generates a feature vector complete with all the discussed features.

The full list of feature vectors obtained from a record is then parsed to populate both the user database and the testing files. The subject's heart rate impacts the number of heartbeats detected in the 20 seconds segment and, consequently, the total of obtained feature vectors. This number ranges from 18 to 35 beats in different subjects. Each user's template matrix is populated with 30 vectors randomly chosen from 3 different subject records. Other 30 distinct vectors from all four subject records are selected to test legitimate authentication attempts. The illegitimate authentication testing is performed using 45 feature vectors from 15 different subjects.

After assembling the user database and the feature vectors for testing, to be used in place of data acquired from a sensor in real-time, the final step of the biometric authentication system is to decide if the sample vector matches the corresponding user's template.

[1]https://archive.physionet.org/pn3/ecgiddb/

The decision algorithm based on Euclidean distance is employed. The sample vector is considered legitimate if it scores lower than a system threshold and considers illegitimate otherwise.

4.3. Results

We evaluated the proposed system in terms of accuracy, computational cost, and authentication time. Specifically, the widely used Equal Error Rate (EER) metric is computed after testing for accuracy performance. The computational cost in memory usage is measured using the Massif heap profile tool from the Valgrind framework [Nethercote and Seward 2007]. All the tests are executed with an Ubuntu 20.04 LTS system with 15,5 GiB of RAM and a quad-core, 2.70GHz CPU.

4.3.1. Accuracy.

The analysis of the system's accuracy consists of selecting a reference threshold T to be applied to the distance score from the authentication algorithm in Subsection 3.3. The authentication attempt will be considered legitimate if the distance is lower than threshold T and rejected as illegitimate if the distance greater than T. The system's goal is to classify as few possible false attempts as illegitimate and as few as possible true attempts as legitimate.

The accuracy performance was evaluated following the False Acceptance Rate (FAR) metric for analysis of the illegitimate authentication attempts, and the False Rejection Rate (FRR) metric for the legitimate attempts. These metrics take a number of trials previously labeled as legitimate or illegitimate and return the percentage of wrongly decided cases for a given threshold T [Pinto et al. 2018]. The Equal Error Rate (EER) can then be calculated, defined as the value of T in which both FAR and FRR are the same.

The data obtained from 600 legitimate tests and 900 illegitimate tests were analyzed. A simple histogram of the algorithm-computed threshold values for the legitimate trials can be found in Figure 1. The threshold values peaked highly in a short range between 25 and 45. The illegitimate attempts, however, despite varying in a broader range, still have an equally high occurrence in the same score values that would authenticate a user. It means that several impostors would have successfully authenticated to the system with an ECG signal that is not the same as the ones in the database. The system achieves an EER of 28%, as displayed in Figure 2.

Several factors may have increased the EER of the system, such as noise in the input signal and imprecision in the feature detection. Further discussion on these factors and the next steps for improving the accuracy results can be found in Section 4.4.

4.3.2. Computational Cost.

The performance in means of computational cost concerns the memory usage of the decision algorithm based on Euclidean distance. For this analysis, Valgrind's tool Massif [Nethercote and Seward 2007] was used to measure the total memory allocated by the application (both heap memory usage and the size of the program's stack).

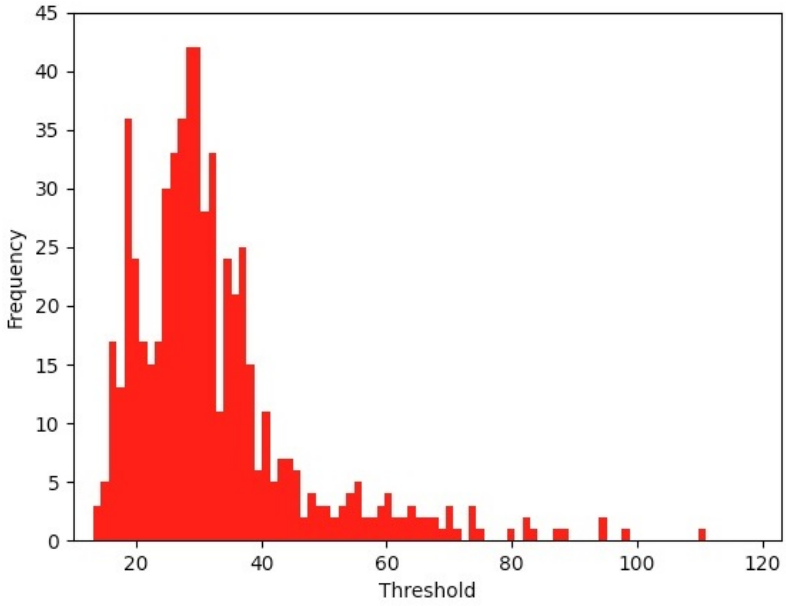

Figure 1. Legitimate authentication attempts.

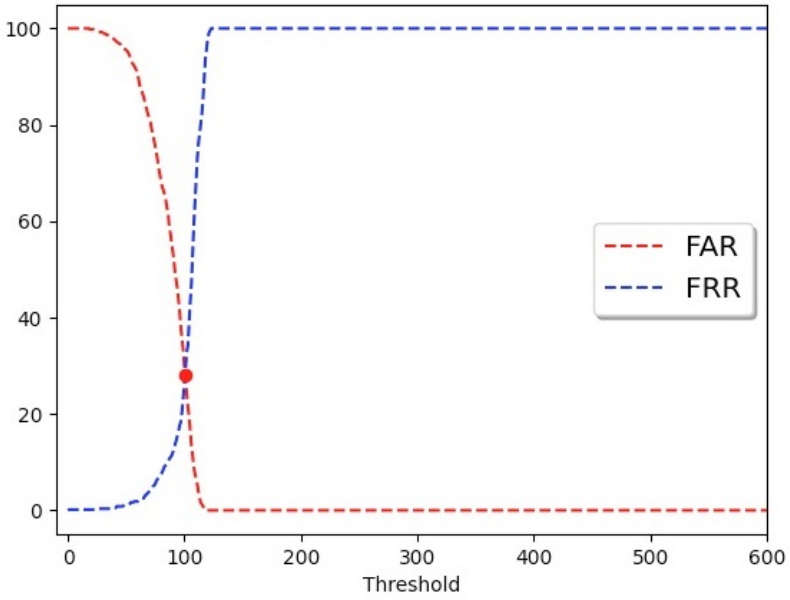

Figure 2. Equal error rate.

The test consisted of a single authentication attempt from a legitimate user, as shown in Figure 3. The initial peak in memory consumption, reaching 7.2 KiB, represents the user's template matrix being loaded into memory. The following section of the graph shows the remaining Euclidean distance calculation between the test vector and each of the 30 vectors in the user's template. The memory usage in this program phase is at most 2 KiB.

It is possible to conclude from the tests that the program's total cost is suitable even for Class 0 devices. It is the most resource-constrained class defined in RFC7728, with less than 10 KiB of memory available for data (i.e., RAM size). Even if more calculations

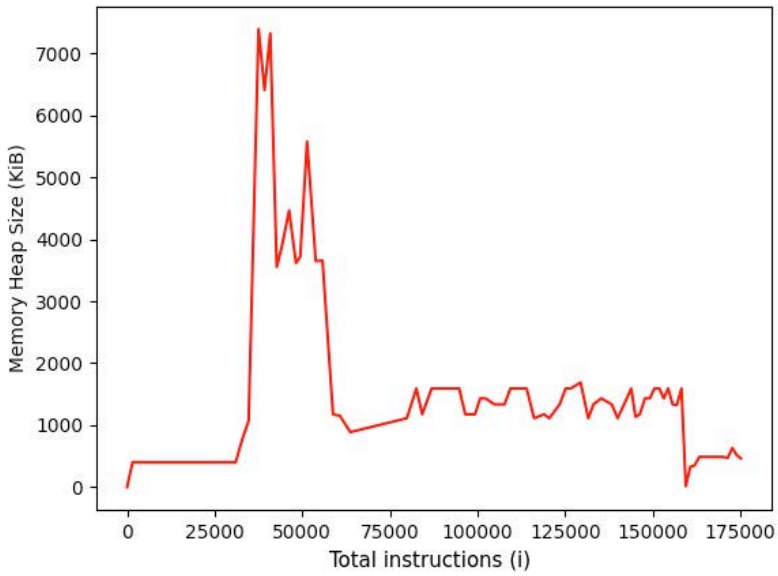

Figure 3. Memory usage for one authentication attempt.

are necessary for accuracy improvement, the system still needs to catch up in crossing the bounds of Class 2 devices and could easily increase memory usage. With this result, it is safe to conclude that the proposed system would be suitable for HIoT devices in terms of resource capabilities.

4.3.3. Authentication Time.

Authentication tasks in biometric systems, in which a system must either approve or reject a user claim, are usually faster than identification tasks, in which an acquisition module acquires the signal, and the system must select the corresponding user from an available database. The amount of time the system takes to perform all the computations described in Subsection 3.3 is negligible, as it often happens in the related literature. We completed the same tests as in Subsection 4.3.2, using the specific C functions for system time measuring and converting the results to milliseconds. The total time of operation of the tests performing one authentication attempt varies between 0.01 milliseconds and 0.018 milliseconds. Ten authentication attempts took between 0.084 milliseconds and 0.116 milliseconds. These results are similar to the ones found in the related works discussed in the following section.

4.4. Discussion

Several points have had a substantial impact on the performance of the proposed system in means of accuracy. First, while trying to guarantee high intra-variability from the ECG-ID database, some of the records used had more noise than average. It led to the loss of relevant signal features in the filtered versions and resulted in poor performance of the feature detector, which was only sometimes reliable in its accuracy. It often resulted in erroneous identification of structures such as the T wave. It caused an impact on the computation of important features, such as the PQRST segment, and caused the similarity between two feature vectors from signals that would otherwise be identical to decrease.

Author	Authentication Task	Computation time (ms)
Huang et al. 2019	Computation of fiducial features from the acquired signal, and the Kullback-Leibler divergence between them and each sample in each signal channel in a template matrix	743.2
Peter et al. 2016	Hashing of the measured IPI value and comparison with the IPI form another sensor	0.16 (MD5), 0.29 (SHA256)
Our solution	Euclidean Distance between a sample vector of features and the user matrix of features	0.018 (one trial), 0.116 (ten trials)

Table 2. Execution time comparison of the related works.

The performance of the feature detector combined with the noisy records ultimately increased the system's overall threshold. The consequence of a high threshold is the high percentage of the EER value, shown in Figure 2 to be 28%. The performance by means of computational cost, in turn, was satisfactory. As shown in Figure 3, the total memory consumption was no higher than 10 KiB, which is suitable for Class 0 devices and even has room for increasing without crossing the resource boundaries of these devices. A necessary next step must evaluate if the accuracy can be improved only by the refinement of the input signal and feature vectors or if there is a need to reevaluate the Euclidean distance algorithm in exchange for greater memory usage.

The obtained authentication time is similar to the ones found in the related literature. For this comparison, we selected the work of Huang et al. [Huang et al. 2019], and Peter et al. [Peter et al. 2016] since their systems also perform authentication tasks similar to the one proposed in this work. Tan et al. [Tan and Perkowski 2017] and Choi et al. [Choi et al. 2016] while using similar techniques in the feature detection step of the biometric algorithm, are performing identification tasks. The decision algorithm in those works employs machine learning techniques and is bound to take more time than metric-based algorithms.

The authentication step compares the IPI values acquired by the different sensors [Peter et al. 2016]. This step uses several IPI samples to increase confidence in the positive or negative decision. The IPI value is hashed and sent to the other sensor for comparison. The hashing and comparison process has an overall small effect on the computation time of the protocol, taking only 0.16 milliseconds when using MD5 as the hash function and 0.29 when using SHA256.

Huang et al. [Huang et al. 2019] uses Kullback-Leibler divergence to measure the similarity between the features acquired from the ECG signal and each of the N samples from H channels stored in a template matrix. The Kullback-Leibler divergence takes a sum of logarithm operations. The overall divergence is then obtained by computing the average of all channels. In the end, the obtained value must be below a certain threshold to authenticate the subject successfully. The total computational time for the complete authentication phase is about 743.2 milliseconds. However, this time corresponds to extracting the fiducial features from the acquired signal and comparing them with the stored template.

Table 2 depicts the comparison between the execution time of our authentication

algorithm and the ones in the related works. As we can see, the computation of the Euclidean Distance between the sample features and the stored template can be performed faster than most methods.

5. Conclusion

In this paper, we introduce an ECG-based biometric authentication system, which employ a resource-friendly techniques. The algorithms had its performance analyzed using accuracy and computational cost. Besides, the implementation decisions were based on a review of related works in the existing literature proposing similar systems but with different requirements. While highly satisfactory in the computational cost analysis, the results have room to improve their accuracy. The total memory consumption of the template-matching program based on Euclidean distance was under 7.2 KiB, but the EER metric, widely used in the evaluation of the accuracy of this kind of system, was not yet acceptable for use in a real-life scenario, with a 28% equal error rate.

The next steps, will be focused on improving the quality of the feature extractor and better quality input signals. The goal is to reduce incorrect measurements in the feature vectors to a minimum. The focus will be on refining the features and the feature vectors. Improvements such as the normalization of time interval features and computing the mean of several heartbeats for assembling the feature vectors will be investigated, as well as the addition of angle-related features, such as the ST slope that may be more stable and consistent across different measurements. After adequate accuracy has been attained, we plan to expand the scope to use the same ECG signal to keep a previously authenticated user continuously logged into the system. The system will also go through a hardening process to work properly in situations where the subject's ECG signal is slightly altered, such as fatigue and heart conditions. There's also the possibility of expanding the system to work with real-time acquired data.

Acknowledgements

This work was funded by process nº 2020/05155-6 of the project entitled "PROJETO MAYA - Innovative and disruptive technologies to prescribe, encourage and evaluate the practice of physical activity" of the Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP).

References

Barros, A., Resque, P., Almeida, J., Mota, R., Oliveira, H., Rosário, D., and Cerqueira, E. (2020). Data improvement model based on ecg biometric for user authentication and identification. *Sensors*, 20(10):2920.

Bastos, L., Cremonezi, B., Tavares, T., Rosário, D., Cerqueira, E., and Santos, A. (2021). Smart human identification system based on ppg and ecg signals in wearable devices. In *2021 International Wireless Communications and Mobile Computing (IWCMC)*, pages 347–352. IEEE.

Bastos, L., Martins, B., Medeiros, I., Neto, A., Zeadally, S., Rosário, D., and Cerqueira, E. (2022). Ensemble learning method for human identification in wearable devices. In *2022 International Wireless Communications and Mobile Computing (IWCMC)*, pages 1052–1057. IEEE.

Berkaya, S. K., Uysal, A. K., Gunal, E. S., Ergin, S., Gunal, S., and Gulmezoglu, M. B. (2018). A survey on ecg analysis. *Biomedical Signal Processing and Control*, 43:216–235.

Biel, L., Pettersson, O., Philipson, L., and Wide, P. (2001). Ecg analysis: a new approach in human identification. *IEEE Transactions on Instrumentation and Measurement*, 50(3):808–812.

Bormann, C., Ersue, M., and Keranen, A. (2014). Terminology for constrained-node networks. RFC 7228.

Choi, H.-S., Lee, B., and Yoon, S. (2016). Biometric authentication using noisy electrocardiograms acquired by mobile sensors. *IEEE Access*, 4:1266–1273.

Goldberger, A. L., Amaral, L. A., Glass, L., Hausdorff, J. M., Ivanov, P. C., Mark, R. G., Mietus, J. E., Moody, G. B., Peng, C.-K., and Stanley, H. E. (2000). Physiobank, physiotoolkit, and physionet: components of a new research resource for complex physiologic signals. *circulation*, 101(23):e215–e220.

Huang, P., Guo, L., Li, M., and Fang, Y. (2019). Practical privacy-preserving ecg-based authentication for iot-based healthcare. *IEEE Internet of Things Journal*, 6(5):9200–9210.

Matni, N., Moraes, J., Pacheco, L., Rosário, D., Oliveira, H., Cerqueira, E., and Neto, A. (2020). Experimenting long range wide area network in an e-health environment: Discussion and future directions. In *2020 International Wireless Communications and Mobile Computing (IWCMC)*, pages 758–763. IEEE.

Nethercote, N. and Seward, J. (2007). Valgrind: a framework for heavyweight dynamic binary instrumentation. *ACM Sigplan notices*, 42(6):89–100.

Peter, S., Pratap Reddy, B., Momtaz, F., and Givargis, T. (2016). Design of secure ecg-based biometric authentication in body area sensor networks. *Sensors*, 16(4):570.

Pinto, J. R., Cardoso, J. S., and Lourenço, A. (2018). Evolution, current challenges, and future possibilities in ecg biometrics. *IEEE Access*, 6:34746–34776.

Seepers, R. M., Strydis, C., Sourdis, I., and De Zeeuw, C. I. (2015). Enhancing heartbeat-based security for mhealth applications. *IEEE journal of biomedical and health informatics*, 21(1):254–262.

Singh, Y. N. and Singh, S. K. (2012). Evaluation of electrocardiogram for biometric authentication. *Journal of Information Security*, 3(1):39–48.

Tan, R. and Perkowski, M. (2017). Toward improving electrocardiogram (ecg) biometric verification using mobile sensors: A two-stage classifier approach. *Sensors*, 17(2):410.

Wang, Z. (2018). A privacy-preserving and accountable authentication protocol for iot end-devices with weaker identity. *Future Generation Computer Systems*, 82:342–348.