An Electrocardiogram-based Authentication Implementation Integrated with the Blockchain

Mateus Stürmer Pioner
Universidade do Vale do Rio dos Sinos
São Leopoldo, Brazil
Email: mspioner@hotmail.com

Luciano Ignaczak
Universidade do Vale do Rio dos Sinos
São Leopoldo, Brazil
Email: lignaczak@unisinos.br

Bruno L. Dalmazo
Federal University of Rio Grande do Sul
Porto Alegre, Brazil
Email: bldalmazo@inf.ufrgs.br

Elvandi da Silva Júnior
Federal University of Rio Grande do Sul
Porto Alegre, Brazil
Email: elvandi.junior@inf.ufrgs.br

Jéferson Campos Nobre
Federal University of Rio Grande do Sul
Porto Alegre, Brazil
Email: jcnobre@inf.ufrgs.br

***Abstract*—With the growth in the use of biometrics for authentication, a new approach has been growing in recent years. Cognitive biometrics has shown relevant results in the studies carried out. Likewise, in recent years, blockchain has been growing and expanding its use beyond cryptocurrencies and can be used in various market sectors. This work aims to analyze a new method for authentication on Electrocardiogram. It uses the Mean Squared Error formula and a private blockchain to store users' authentication samples. This work aims to analyze a new method for authentication in Electrocardiogram based on the Medium Quadratic Error formula and the storage of the samples for authentication of the users in a private blockchain, evaluating the feasibility of this approach. The results obtained prove that this method can be used for authentication through Electrocardiogram. Due to the level of correctness in relation to the comparison of the ECG of each user and distinction between them. In addition, the use of blockchain with its own resources presents an implementation comprising some security aspects related to the storage of information.**

***Index Terms*—Authentication; Blockchain; ECG; Electrocardiogram; MSE.**

I. Introduction

In the current authentication scenario, the use of biometrics, unlike the classic authentication methods, offers greater security and reliability to users [1]. This is due to the fact that it is not necessary for the user to remember a combination of letters and numbers or to have a physical object in his possession to authenticate himself. Unlike a password, biometrics are generally permanent and cannot be easily changed. In addition, biometrics cannot be shared with other parties because users have their own physical and behavioral characteristics [2].

As a way of increasing security in the authentication process, unlike the static process in which the user enters his credentials only at the time of login, through continuous authentication and its re-authentication process, it is possible to ensure that the user who initiated the session continues using the system and that it was not hijacked by an improper user [3]. According to the authors, one of the main requirements for the use of continuous authentication is that the input data for the process have enough information to distinguish different users, which makes the use of biometrics the best way to meet this requirement.

978-3-903176-32-4

Recently, the use of blockhain has been growing and has many advantages in several areas and sectors of the market [4]. One of the areas is portable electrocardiogram (ECG) monitors, which monitor arrhythmias and provide diagnostic accuracy at the cardiologist level [5]. Another area is identity management. With several projects developed by companies and governments, being a very broad context that offers numerous opportunities for the application of this technology [6]. With regard to the area of identity management, specifically a new approach has been evaluated for use in blockhain, it is the storage of biometrics for authentication.

This work aims to evaluate the use of the Mean Square Error (MSE) method for authentication based on Electrocardiogram (ECG) demonstrating in detail the procedures performed, integrated with a private blockchain using the biometrics references stored in the blockhain through of the proposed method for simulating authentication and evaluating the results obtained.

The article is organized as follows. Section 2 presents related works. Section 3 presents the proposed methodology. Section 4 presents the results obtained and, finally, Section 5 presents the final considerations of this article and perspectives for future works.

II. Related works

Biel et al. [7] evaluated the possibility of using the ECG as human identification. The heartbeat of a group of 20 people between 20 and 55 years of age, all at rest, was recorded. After analyzing the data obtained, the authors found a 100% accuracy rate in the unique identification. Lugovaya [8], complementing the work of Biel et al. [7], carried out a survey with 90 volunteers with the objective of developing an identification system based on the ECG. In the study, the

participants' heart rate and physical and mental states were not considered. This study suggested methods of interpretation and classification of data not used in previous studies, such as classification using the nearest average classifier, obtaining an 87% identification rate, the weighted average classifier, with a 94% success rate, and the discriminant linear analysis, the latter with a 96% identification rate among volunteers.

In relation to cognitive biometrics, the work of Revett [9] studied its use through vital signs as a way of identifying and authenticating users, specifically through ECG, EEG and EDR. The motivation for using these vital signs is in their potential for uniqueness, universality and their resistance to counterfeiting. The authors mention that some studies have achieved a 100% success rate in the classification of results. Israel et al. [10] analyzed the information obtained by reading the ECG and, from the points analyzed, stable characteristics were identified that demonstrate the uniqueness of an individual, demonstrating that the extracted resources are independent of the location of the sensor and invariant to the individual's state of anxiety.

In the work of Guennoun et al. [11], the authors developed a framework for the use of ECG in continuous authentication. Information was collected from 16 volunteers through a wireless cardiac monitoring sensor. In addition, the authors considered two scenarios: in the first, the user accessed the system and continued using it in the usual way. In the second, the user logged in and used the system for 5 minutes until he left the computer and his session remained active, with a new user taking possession of it. The results showed that all tests performed were successful and that all substitutions from one user to another were detected by the system based on the difference between the heartbeat of the first user to access and the second to take possession of the session.

Adrian Chan et al. [12] analyzed a dataset composed of 60 people in order to demonstrate that the ECG can be used as a biometric identification, obtaining the result of 100% correctness in the analyzed samples. The authors identified that the ECG has sufficient characteristics to distinguish between users, in addition to not having great variance over time. In this way, the authors demonstrated that the ECG is a precise method for use in biometric systems, either as the main biometry for authentication or in a multi-modal system, in which at least two biometric identifications are required to identify a user.

From the data obtained in the evaluated articles, only Guennoun et al. [11] presents the user identification process, using the Mahalanobis distance calculation. Following the methodology proposed by Guennoun et al. [11] and data selection suggested by Lugovaya [8], using the dataset developed by the same author, in the present work an alternative method for ECG comparison, known as Mean Square Error (MSE), will be used, according to with Wang and Bovik [13], this method is widely used to compare variable data and to identify the level of distinction between the two. In addition, the work will use a private blockchain where authentication data will be stored, an approach that, until the development of this work had not been presented. Metrics will be used to measure the accuracy in authentication between samples and the time for the authentication process, with the aim of verifying the technical feasibility of this type of implementation.

III. Methodology

This work proposed a method of authentication through ECG and storage integrated with blockchain, identifying which ECG data needs to be stored. For use in this work, research was carried out on the PhysioBank base, a set of databases of physiological signals for use in biomedical research. Among the datasets found, the ECG-ID dataset was selected. It is related to Lugovaya's master's dissertation [8], which was used to support.

Some steps will be followed: initially a sample of users will be extracted from the data set used. Then, the first sample of each user will be selected and a minimum amount of readings from this sample will be stored on a blockchain. Afterwards, it will be compared, by means of a mathematical formula, with the second sample of the user for authentication.

In addition to the authentication process of the users themselves for legitimate authentication, attempts at authentication in the system by illegitimate users will later be simulated in order to assess the acceptance and rejection rates of a person not authorized by the system. For this comparison, three other users will be selected at random, following the method used by Guennoun et al. [11].

To compare the biometric samples and their level of similarity, the Mean Square Error (MSE) formula was used in this work. MSE is dominant in the field of signal processing, providing a quantitative score that describes the degree of similarity or, conversely, the level of distortion between them [13]. According to the authors, the main advantages of the MSE are the need for little computational resources to perform its calculation and the precision of its results, presenting itself as a differential element for an authentication process.

According to Lugovaya [8], the dataset consists of a base with 310 ECG samples, obtained from 90 people. Each sample record occurred for a period of 20 seconds, scanned at the frequency 500 Hz. Records were obtained from 44 male volunteers and 46 female, between 13 and 75 years old. At least two ECG samples were recorded in the dataset for each volunteer, in order to use the first one for registration and the others for identification and comparison simulation.

Based on the dataset used, a sample of 20 people was selected, comparing each user's registration sample with their respective identification sample. In addition, the record samples from each of the volunteers were compared with three other samples of identification from three different volunteers selected at random, both tests in order to assess the TAR and FAR metrics related to the defined threshold level. This analysis of 20 volunteers does not have a statistical character, only the purpose of evaluating the proposed metrics. Table I presents a summary of the elements considered in the preparation of the evaluation of this work.

Element	Description
Total users evaluated	20 users
Legitimate authentication attempts	20 Attempts
Illegitimate authentication attempts	60 attempts (three per user)
Number of readings used per sample	1000 readings
Measured metrics	True acceptance rate (TAR), False acceptance rate (FAR)
Authentication method	Comparison of samples using the Mean Square Error (MSE) formula

TABLE I
ELEMENTS CONSIDERED IN THE DEVELOPMENT OF THE WORK.

The evaluation was organized in the following steps: pre-processing of information, environmental information for evaluation, selection of data for storage in the blockchain, authentication process and finally, the analysis of the implementation feasibility.

A. Pre-processing

In the pre-processing stage, dataset[1] was initially downloaded from the link provided in the work of Lugovaya [8]. After downloading this dataset, each person's ECG record files were read, in binary format, with the WFDB rdsamp tool (WaveFormDataBase)[2], a tool package made available by PhysioBank for reading and processing signals and automated analysis files from these databases [14].

Using the tool used to convert signal data into clear text, ECG samples containing 10,000 lines of readings and three columns were generated, as shown in Figure 1: the first with the identification number of the recorded reading, the second column with the reading of raw ECG signal containing low and high frequency noise and the third with the reading already filtered, without noise.

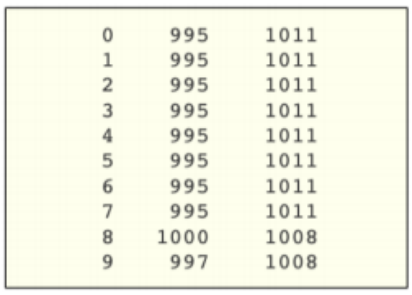

Fig. 1. Phases of Continuous Authentication, adapted from Goldberger et al. [14].

According to Lugovaya [8], the reading of the ECG is very noisy, and may contain distortions from various sources, such as the sensor that is reading the ECG and the means of transmission of the readings, and may omit essential information for the identification of users. Therefore, in this work, only the ECG information from the third column of the file was used, with the readings already filtered by the author of the dataset. After generating the clean readings, the ECG samples of each user were stored in new files with only two columns: the first containing the identification number of the reading and the second its respective value. Both columns were used to identify the ECG and served as the basis for storage on the blockchain.

B. Environment for evaluation

For the evaluation and implementation environment of the blockchain, the MultiChain[3] tool in version 2.0.2 was used. This free tool is used to implement private blockchains in a simple and fast way, and can be configured via API or command line. For its implementation, an environment composed of two virtual machines was created. The first one was created on Google Cloud Platform, Google's cloud services platform, with an Ubuntu Server operating system in version 18.04 LTS, with 10GB of storage, 2GB of RAM and 1vCPU. In addition, a local virtual machine was created with an Ubuntu Server system in version 18.04 LTS, with 10GB of storage, 2GB of RAM and 1vCPU in VirtualBox, Oracle's tool for virtualizing operating systems.

The installation and configuration of MultiChain took place on both servers for storage and sharing of ECG data for authentication. From the installation on the cloud server and the creation of the blockchain, a stream was created, a component which allows the blockchain to be used as a database for storing any type of data, providing a timestamp record, identification of the node that published the information and the immutability record, since this record cannot be changed [15]. After this configuration, access was granted through the cloud server to the local server for reading and writing on the blockchain and related stream, synchronizing the information between the servers and allowing the consultation and storage of ECG data also from the local node.

C. Data selection and storage

After the pre-processing and generation of the sample files for each volunteer, a bash script was developed to convert the samples containing the ECG readings to JSON (JavaScript Object Notation) format for later storage on the blockchain. This and other scripts developed for this work are available on the author's page on the Github[4] platform. JSON is a

[1]https://archive.physionet.org/pn3/ecgiddb/
[2]https://github.com/MIT-LCP/wfdb-python
[3]https://www.multichain.com/
[4]https://github.com/mspioner/scripts-ecg/

universal data structure, being able to order and organize data in the most diverse formats [16]. According to MultiChain requirements, using the JSON format it is possible to store the ECG reading information, containing the reading identification number and its respective value. By executing this script the data columns generated by rdsamp are converted into a single line for storage.

As a result of executing this script, the first 1000 readings of the file were selected, equivalent to 2 seconds of ECG recording, containing at least one set of PQRST waves for comparison and distinction between users in the authentication process, according to the work of Lugovaya [8]. Figure 2 exemplifies the PQRST wave of the ECG for heartbeat.

Fig. 2. Regular ECG pattern for heart rate, adapted from Lugovaya [8].

After selecting the minimum readings required for authentication, the samples were converted to JSON format for later storage on the blockchain. In addition to the premise of the information being in this format, MultiChain has a requirement to relate the data to a key, that is, all the information that is stored and consulted must be from an identifier composed of letters and / or numbers for blockchain location.

This key can be a CPF, RG number or some unique identification in hexadecimal format established according to the requirements of the implementation. In this work, in order to be an assessment environment and facilitate authentication tests, the key pattern “PersonXX” was used to identify readings on the blockchain, where “XX“ specifies the number of the volunteer with their respective sample stored record.

D. Authentication process

The authentication process took place using the MSE formula for comparison between the sample of records stored in the blockchain and the sample of user identification. As a result of this comparison, a similarity value was generated between the samples, where the value "0" represents the equality between the sample readings and, consequently, the higher the value of the result, the more divergent the samples and the values of their readings are representing the distinction between the ECG waves of each person. The data used for authentication were selected according to the work developed by Lugovaya [8], where the author selects an interval of 250 readings in relation to the peak of the R wave, with 80 readings before and 170 after this peak, including the R wave itself, as represented in the Figure 3. According to the work of Lugovaya [8], the interval of 250 readings in relation to peak R and the interval PQRST presents the best classification and distinction between the evaluated data, bringing better results in the identification of users.

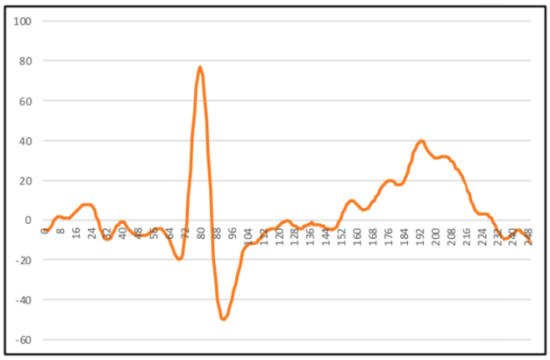

Fig. 3. Example of 250 readings with the peak of the R wave

The authentication process occurred through the execution of a Python script divided into three steps: in the first, the selection of the registration sample to be used in authentication, in the second step, the user identification sample was selected, and finally in the third stage, the MSE formula was applied, calculating the difference between the readings of each user sample. The MSE formula, described as:

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(yi - \bar{yi})^2 \quad (1)$$

Calculating the sum of the squares of the differences between two values, where each of the readings in their respective time is calculated to generate the general difference between the samples. The execution of this script took place on the local virtual machine, however the query for the blockchain was made on the Google Cloud Platform virtual machine, in order to evaluate the response time of this remote execution.

In the first step, the user is asked to enter his key so that his stored sample is located on the blockchain and starts the authentication process. The script then accesses the blockchain on cloud machine, identifies the desired key and returns the data in JSON format with the related readings. Then, the Script selects in the information stored in this key, the interval of 250 readings in relation to peak R for use in the MSE formula.

In the second step, the user is asked to insert the identification sample, in this case, a file in the same format as the sample stored in the blockchain generated by a bash script, containing the 1000 readings in JSON format. After the user enters his sample, the authentication script will select the interval of 250 readings for comparison. In the third step, using the MSE formula, the 250 readings of the sample registered in the blockchain are compared with the 250 readings of the sample entered by the user in the authentication process. If the final value of the MSE is located between the defined threshold, the user will be successful in its authentication, otherwise, access will be denied.

Based on the information presented in the work of e De Luca et al. [17], the threshold was developed from the calculation of the standard deviation between the compared samples and added to the average of each result. From these

calculations, the threshold was established in order to obtain the lowest possible false acceptance rate, adding and subtracting the standard deviation of the result from the average obtained. Table II presents the results of the average of some users, their standard deviation σ and the defined thresholds.

User	Average	σ	Threshold
06	76,24	0,78	$75{,}46 \leq T \leq 77{,}02$
26	16,43	0,67	$15{,}76 \leq T \leq 17{,}10$
16	50,85	0,59	$750{,}26 \leq T \leq 51{,}44$
31	84,15	0,83	$83{,}32 \leq T \leq 84{,}98$
10	87,55	0,73	$86{,}82 \leq T \leq 88{,}28$
36	1573,12	0,99	$1572{,}13 \leq T \leq 1574{,}11$
12	38,11	0,44	$37{,}67 \leq T \leq 38{,}55$
50	64,98	0,61	$64{,}37 \leq T \leq 65{,}59$
80	26,00	0,49	$25{,}51 \leq T \leq 26{,}49$
69	159,73	0,50	$159{,}23 \leq T \leq 160{,}23$

TABLE II
DEFINED THRESHOLD RESULTS.

The choice of 20 users was made randomly using the Microsoft Excel tool with the RANDBETWEEN function, used to generate random numbers, performed 20 times from the range of 1 and 90 according to the number of people in the dataset used. For validation of the authentication process, the samples stored in the blockchain of each of the 20 selected users, identified as "Legitimate", were compared with their respective identification samples to assess the TAR rate of this process. In addition, three other possible illegitimate users, identified as "Impostor", were randomly selected from the 90 people in the dataset to assess the level of FAR in the authentication process.

E. Analysis of implementation feasibility

The stage of analysis of the feasibility of implementing this work was established in two ways: in the first stage, the analysis of the authentication response time in relation to the blockchain used and, in the second stage, the analysis of the threshold defined for the authentication process. To define the acceptable response time for the user authentication process, the work developed by Nielsen [18] was used, where the author establishes that this response time is directly linked to user satisfaction in relation to the system used. Nielsen [18] defines the response time as follows:

• 0.1 second: is the time limit for the user to feel that the system is reacting instantly, just waiting for the result to be displayed.

• 1.0 second: it is the limit for the user's thought flow to remain uninterrupted, even if the user perceives the delay. In this way, the user loses the feeling of direct access to data.

• 10 seconds: this is the limit to keep the user's attention focused on the process, so users should receive feedback from the system indicating that they are executing the process, otherwise users will not know what to expect.

IV. RESULTS

In this section, the results obtained in this work from the authentication process performed are presented and analyzed. This process took place with a sample of 20 people for legitimate authentication and threshold development and 60 people for illegitimate authentication attempts. For the analysis of legitimate attempts, the true acceptance rate (TAR) was used and for the analysis of illegitimate attempts, the false acceptance rate (FAR) was used, identifying the probability of the system correctly accepting the access of an authorized person and the probability of the system. incorrectly accepting the access of an unauthorized person, respectively.

A. Authentication attempts - TAR and FAR

After comparing the registration samples of the legitimate users with their respective identification samples and with the samples of the imposter users, some results were obtained. From the threshold defined based on the standard deviation and in the average of the samples used, users whose result of the comparison reached the determined threshold value would have their authentication performed successfully, otherwise, the user's access would be denied.

After analyzing the data obtained from the 20 attempts of legitimate authentication, 20 successful attempts were obtained, reaching a TAR value of 100%. Due to the similarity of the peak waves R of the legitimate users themselves, the analysis from other identification samples shows satisfactory results in the authentication, as for example, the user "Person64". In its legitimate authentication, the result of the MSE obtained was "25.43", exactly the maximum value of the calculated threshold. In comparison with the second sample of identification of this user, the result obtained was "23.89", a value that is also inserted in the defined threshold, authenticating the user again successfully.

Regarding the login attempts of illegitimate users, none of the 60 attempts were successful in authentication, with the FAR metric with zero result. These results, specifically due to the great discrepancy between some values, demonstrate the relevant difference between the heartbeat and its waves from person to person, being distinct among them specifically for physiological reasons, guaranteeing the distinction of this type of evaluated biometrics. As it is a small sample of users, the similarities between the volunteers evaluated were not identified in the tests performed, and may possibly appear in a larger sample.

B. Performance

For the performance analysis of the authentication process proposed in this work, the time elapsed between the moment after the user inserted the key for location on the blockchain and the moment when the result of the calculation of the MSE for the same was presented, thus ending the process. This counter was inserted directly into the authentication script, seeking to obtain the highest possible accuracy. From the obtained authentication times, the general average of these results was calculated to identify and evaluate this metric.

The overall result obtained between the processes was 4.08 seconds, with the shortest authentication time being 3.73 seconds and the longest with 4.93 seconds, considering the users' complete authentication time. The overall average time obtained is close to 5 seconds, half the time limit mentioned by Nielsen [18] in his work. In this way, the time is satisfactory for this authentication process in relation to the user's satisfaction with the response time. In addition, according to the data provided by Lugovaya [8], the frequency used for ECG recording considered 500 readings per second, so it is possible to perform the authentication procedure and the user identification reading while the registration sample is located on the blockchain with the key inserted by the user. Regarding the general time obtained for the authentication process, it is likely that it will vary in each implementation environment, since, as the current work uses a small environment and for tests, changes in other larger environments may occur due to bandwidth and speed. of internet used, cloud infrastructure in which the tool is installed, among other factors.

V. Final considerations

The objective of this work was to evaluate the application of the method based on the MSE formula for authentication through Electrocardiogram and to analyze the feasibility of implementing a private blockchain infrastructure for storing information in this scenario. The results of the tests using the MSE as a formula for authentication demonstrated that this formula may be relevant to an authentication system due to the results obtained, especially since there were no successful authentications by imposter users in this evaluated sample, and may undergo changes with a quantity bigger.

Regarding the authentication time obtained in the evaluation of this work, it is less than 5 seconds, half the limit value defined by Nielsen [18] for the level of user satisfaction, thus presenting a satisfactory result for the tests performed and expected results.

Thus, in relation to the contributions cited in the present work, the feasibility of using the MSE for authentication and the use of a private blockchain infrastructure for data storage has been proven. It can also be said that the response time of the authentication process was satisfactory and can be improved in new implementations. The feasibility analysis of this work did not take into account data injection attacks forging ECG measures for illegitimate authentication attempts, being limited only to tests of the feasibility of the authentication procedure and its results.

As future work, it is proposed to carry out tests with more samples of the same dataset used or with a new dataset and evaluate possible attacks on this authentication scenario. In addition, it is suggested to analyze samples with possible changes in users' emotions well defined, evaluating if there are significant changes in the process of authentication and identification of them.

Acknowledgements

This work was carried out with partial support from CNPq, National Council for Scientific and Technological Development - Brazil.

References

[1] M. Mohammedi, M. Omar, W. Aitabdelmalek, A. Mansouri, and A. Bouabdallah, "Secure and lightweight biometric-based remote patient authentication scheme for home healthcare systems," *International Symposium on Programming and Systems*, vol. 13, pp. 1–6, 2018.

[2] M. Boatwright and X. Luo, "What do we know about biometrics authentication?" Available at http://portal.acm.org/citation.cfm?doid=1409908.1409942, accessed on 2020/12/31.

[3] K. Revett, "Continuous authentication using biometrics: Data, models, and metrics," *IGI Global*, vol. 1, 2011.

[4] M. Mettler, "Blockchain technology in healthcare - the revolution starts here," *IEEE International Conference on e-Health Networking, Applications and Services*, vol. 18, pp. 16–18, 2016.

[5] K. Chayakrit, R. Albert, J, A. Mehmet, C. Edward, J. Kipp, W, W. Zhen, and N. Sanjiv, M, "Integrating blockchain technology with artificial intelligence for cardiovascular medicine," *Nature reviews – CardIology*, vol. 17, 2020.

[6] O. Jacobovitz, "Blockchain for identity management," Available at https://www.cs.bgu.ac.il/frankel/TechnicalReports/2016/16-02.pdf>, accessed on 2020/12/31.

[7] L. Biel, O. Pettersson, L. Philipson, and P. Wide, "Ecg analysis : A new approach in human identification," *IEEE transactions on instrumentation and measurement*, vol. 50(3), pp. 1–4, 2001.

[8] T. S. Lugovaya, "Biometric human identification based on ecg," *Faculty of Computing Technologies and Informatics, Electrotechnical University "LETI"*, 2005.

[9] K. Revett, F. Deravi, and K. Sirlantzis, "Biosignals for user authentication - towards cognitive biometrics?" *International Conference on Emerging Security Technologies, ROBOSEC 2010 - Robots and Security, LABRS 2010 - Learning and Adaptive Behavior in Robotic Systems*, vol. 2010), pp. 71–76, 2010.

[10] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold, and B. K. Wiederhold, "Continuous authentication by electrocardiogram data," *Pattern Recognition*, vol. 38(1), pp. 133–142, 2004.

[11] M. Guennoun, N. Abbad, J. Talom, S. M. M. Rahman, and K. El-Khatib, "Continuous authentication by electrocardiogram data," *IEEE Toronto International Conference - Science and Technology for Humanity*, vol. 09, pp. 40–42, 2009.

[12] A. D. Chan, M. M. Hamdy, A. Badre, and V. Badee, "Person identification using electrocardiograms," *Canadian Conference on Electrical and Computer Engineering*, vol. May, pp. 1–4, 2007.

[13] Z. WANG and A. C. BOVIK, "Mse: Love it or leave it?" *IEEE Signal Processing Magazine*, vol. January, pp. 98–117, 2009.

[14] A. L. Goldberger, L. A. N. Amaral, L. Glass, J. M. Hausdor, P. C. Ivanov, R. G. Mark, J. E. Mietus, G. Moody, C. K. Peng, and H. E. Stanley, "Physiobank, physiotoolkit, and physionet," Available at https://www.ahajournals.org/doi/abs/10.1161/01.CIR.101.23.e215, accessed on 2020/12/31.

[15] MultiChain, "Multichain private blockchain - white paper," Available at https://www.multichain.com/download/MultiChainWhite-Paper.pdf>, accessed on 2020/12/31.

[16] D. Crockford, "Introducing json," Available at https://www.json.org>, accessed on 2020/12/31.

[17] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and i know it's you!: Implicit authentication based on touch screen patterns," Available at http://doi.acm.org/10.1145/2207676.2208544, accessed on 2020/12/31.

[18] J. Nielsen, "Usability engineering," *Morgan Kaufmann Publishers Inc, San Francisco, CA, USA.*, 1993.