DOI: http://dx.doi.org/10.26483/ijarcs.v13i3.6829

ISSN No. 0976-5697

Volume 13, No. 3, May-June 2022

International Journal of Advanced Research in Computer Science

SURVEY REPORT

Available Online at www.ijarcs.info

A BRIEF REVIEW ABOUT BIOMETRICS SYSTEMS IN MODERN CONTEXT

Héctor Caballero-Hernández
Computer Systems Department
TESJo,
Jocotitlan, Mexico

Leopoldo Gil-Antonio
Computer Systems Department
TESJo,
Jocotitlan, Mexico

Erika Lopez-Gonzalez
Computer Systems Department
TESJo,
Jocotitlan, Mexico

Juan Alberto Antonio-Velazquez
Computer Systems Department,
TESJo,
Jocotitlan, México

Abstract: Authentication systems employ various access mechanisms for the data validation process.Nowadays there are many proposals focused on solving the traditional problems that exist to validate the records of installations in public or private places. With the appearance of COVID-19, the use of technology has intensified to avoid contact with physical devices and achieve successful access. This article shows a compilation of work dedicated to methods and techniques for access to facilities by reading modern biometric systems.

Keywords: Biometric; Radio frequency; Validation; Authentication; Metrics

I. INTRODUCTION

Authentication systems based on biometric data acquisition, allow the recognition of individuals who intend to access facilities. Authentication systems can generally be by contact, such as fingerprint scanning, or contactless, generally based on taking a photograph of the face or iris. In times of the COVID-19 pandemic, authentication systems that require contact with devices are not advisable, because these devices expose people to contracting pathogens that are harmful to health [1] and [2].

The most recurrent systems used for biometric data validation are those based on face and iris detection analysis, because these systems are accessible and cheap, but require a series of validation elements to avoid being cheated [3]. Authentication systems based on the reading of biometric data allow the identity of a person to be determined to access a series of resources or specific sites. Generally, this type of data is classified into physiological and behavioral. The biometric data includes the following [4] and [5].

- Fingerprint.
- Palm of the hand.
- Iris
- Face

The most common behavioral-based biometrics are as follows.

- Autograph signature
- Voice
- Typing on keyboard
- Walking pace
- Electrocardiogram

Biometric data must maintain a series of characteristics that make them unique, which these are.

1. Universality. Every individual must have the same biometric trait.
2. Uniqueness. The same trait must be different between individuals.
3. Permanence. The biometric feature must not change over a period.
4. Acquisition. The ease with which biometric trait data can be measured, captured, and processed.
5. Performance. The recognition accuracy and the resources to achieve it must meet the specifications of the application.
6. Acceptability. The user population must be willing to submit their biometric trait to the system.
7. Circumvention. The ease with which it is possible to mimic a trait of an individual and therefore fool the biometric system.

Biometric systems generally present a series of elements that allow you to acquire the signals that have been sensed, some of the most important elements are the following.

1. Sensor module. Capture the biometric information of the individual in the form of images, audio, video, or some other signal.
2. Feature vector extraction module. The biometric information is processed to extract discriminant features that represent the captured trait.
3. Database module. In this module, the biometric information is stored after the stage known as enrollment, this information is processed and with it a pattern or model is created.
4. Comparison module. The extracted feature vectors are compared with patterns or models that represent the individuals registered in the biometric system, the result is a numerical qualification or score.
5. Decision making module. The results of the previous module are used to either validate an identity or identify an individual.

Biometric systems require validation processes on the input data these receive to validate the information from a biometric system, a series of metrics are generally applied to validate the information acquired.

II. METRICS TO BIOMETRICS SYSTEMS

Wherever Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts if possible. True-Type 1 or Open Type fonts are preferred. Please embed symbol fonts, as well, for math, etc.

Considering that a biometric system is used for the identification of certain characteristics of individuals that are considered unique and unalterable and aimed at correctly identifying approved users and rejecting those outside the system. For this reason, it is necessary that different biometric systems are applied to them different metrics that indicate their reliability to accept or reject accesses to the system. Below is a brief description of the metrics used in biometric systems [6], [7] and [8]: within these metrics we have, the False Acceptance Rate (FAR) which typically consists of measuring the samples or intruding users who accept the system, likewise the False Rejection Rate (FRR) which is also known as False Match (FM) or False Positive (FP) which measures the number of valid samples or users that the system rejects.

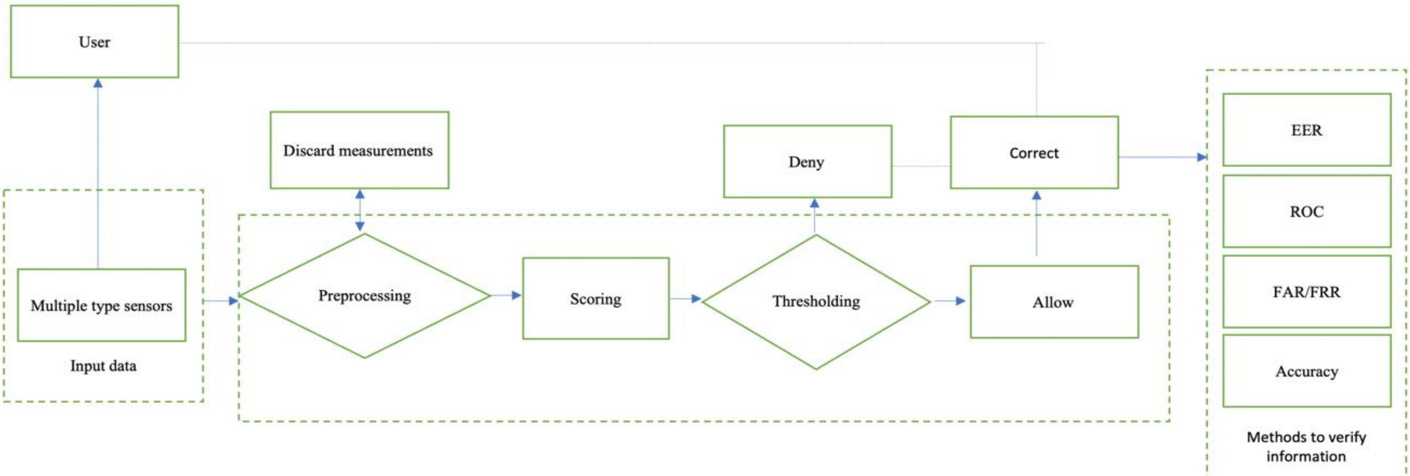

Fig. 1. General diagram of biometric system with methods to verify information

On the other hand, we have the Equal Error Rate (ERR) which is the error rate that is achieved by adjusting the detection threshold so that the FAR and FRR are equal, this metric describes the overall accuracy of the biometric system. Likewise, precision measures the fraction of users or samples that it accurately classifies without considering the two types of error. HTER is the target mean error rate which is the average between FAR and FRR considering a target threshold. On the other hand, the Receiver Operating Characteristics (ROC) curve is a metric which is a graph showing the dependence between FAR and FRR at the detection threshold of the system. Also, the area under the ROC Curve (AUROC) which varies from 0.5 to 1 and has the feature that observe the performance of the system in the threshold settings. On the other hand, the Confounding Matrix (CM) shows the fraction of samples accepted for each user. The CM shows each user's FRR and the FAR for users who are attacking the system. The detection rate is a measure that observes the number of users outside the system in an individual way.

There are also other types of metrics where the performance of biometric systems is observed, such as: Computational time considered the time it takes for a system to acquire, verify, and identify users who are accepted by the biometric system. Failure-to-enroll rate is representing the population that it is not possible to capture or extract biometric characteristics of system users. Likewise, the Failure-to-acquire consists of observing how incapable the system is of capturing the user's data.

In figure 1 its present the general structure of biometric system, taking into consideration the input data of the users, the process of data analysis and the analysis by metrics.

III. RELATED WORKS

The investigations of biometric systems present interesting proposals for the acquisition and treatment of the information obtained, among which is the work of [9] is a biometric authentication identification system is proposed using the palm, finger and iris impression using a Mapping of Minutiae (Minutiae), likewise the Discrete Wavelet Transformation (DWT) algorithm is used for the encryption and concealment of information and is tested in an e-business system.

On the other hand [10] proposes a biometric identification

encrypts and hides fingerprint and iris biometric information. In [14] proposes a multi-signature mapping approach that reduces the false acceptance rate without having to increase the false rejection rate in addition to eliminating the need to use a threshold that is empirically adjusted. On the other hand, in [15] a multimodal biometric identification system is proposed considering the iris, palm print, face, and signature using the discrete wavelet transform, thus obtaining integrated biometric features and eliminating the problems presented by unimodal biometric systems. In [16] a system is presented to securely store confidential documentation using a mobile device where a set of documents associated where the access policy is encrypted.Confidentiality is achieved through a biometric key binding scheme with facial recognition and the use of hardware-provided security primitives.

In [17] analyze the design of a non-intrusive continuous biometric authentication approach using results from cognitive psychology considering different behaviors to validate the results using a usability scale system. In [18] present an analysis of the existing problems Cloud Computing, Internet of Things and Cloud of Things, observing the different risk factors as well as the trends to avoid the intrusions and vulnerabilities of the systems. In the same way, these carry out an analysis of current and future trends related to the technologies, describing, and indicating concepts related with them. In [19] propose a system for the control of medication application using Near-field Communication (NFC) technology and protocol that, according to the authors, complies with International Organization for Standardization (ISO) security and communication standards that guarantee patient safety. For implementation, different devices that are available in the market can be used. Likewise, the authors consider that the developed system has greater safety and efficiency. On the other hand, in [20] present a work for the authentication of users considering the biometric behavior based on the calculator theorem, which seeks to give the user the necessary attempts to authenticate. Likewise, the authors carry out an investigation where the dynamics of pressing on the keys is observed for a better precision in the authentication of the system users. In [21] presents a work for the biometric identification for remote users between IoT devices or applications. The proposed method is based on feature extraction based on sparse coding, proving that the proposed scheme accurately extracts biometric features and is robust against different noise levels. Alternatively, [22] propose a dual system with the Radio Frequency Identification (RFID) biometrics that is used to lock or unlock bank vaults. Where three levels of security are proposed. Lock control uses RFID via NFC, biometrics via a web portal, and Bluetooth for authentication. Also, the authors consider that their security system provides intelligent digital procedures and low cost. On the other hand, [23] perform an analysis of different techniques that are applied in biometric authentication is considering different aspects such as: security, precision, deficiencies, attacks on biometric systems and measures to protect systems from this type of attack.The proposed method is based on feature extraction based on sparse coding; the scheme accurately extracts biometric features. [24] propose a dual system with RFID biometrics that is used to lock or unlock bank vaults. Where three levels of security are proposed. Lock control uses NFC in biometrics via a web portal, and Bluetooth for authentication. Also, the authors consider that their security system provides intelligent digital procedures and low cost. On the other hand, [25] perform an analysis of different techniques that are applied in biometric authentication is considering different aspects such as: security, precision, deficiencies, attacks on biometric systems and measures to protect systems from this type of attack. The authors propose a possible methodology to solve the problems and make a general description of biometric authentication systems.

In [26] an extensive work on a hybrid encryption system is presented and complemented with the use of hash in a decentralized way to uses an algorithmic version, while the hybrid encryption is implemented by means of a symmetric key, and asymmetric encryption for key generation. The proposed encryption scheme works through a multifactor verification that is based on mutual data segmented between nodes. The evaluation of the security scheme was based on its integration in a fingerprint and iris recognition type biometric interface, generating encryption without affecting data processing, and being immune to brute force attacks. The proposal requires a client server scheme. [27] present an investigation where the concept of fingerprint is analyzed with biometric authentication methods based on 2D and 3D. In this study, the authors developed a different Android application for each form of authentication, in the work was used 6 volunteers in the preliminary evaluation. In the work, the accuracy of fingerprint authentication and biometric authentication of behavior through 2D and 3D gestures was compared through an application developed for Android, as an observation it is necessary to collect more exhaustive data and an analysis of data in depth get better response in biometrics system.

In [28] present a security scheme for remote authentication of users based on biometrics, the authors propose a scheme to overcome attacks such as specific temporary information attack, reply attack, forward secrecy, man-in-middle attack, user anonymity and others. In the work of [29] propose a system for user authentication through a dynamic online signature, the analysis that authors did is based on determining the threshold of the signature taking into account characteristics such as shape, size and speed relative in the recording of signatures, for each comparison error count is also shown, this proposal indicates that the signature of an individual generally changes over time and this threshold is taken into account, took into account a base of 100 signatures.

Fingerprint registration is one of the best known processes in the recognition of biometric data, in the work of [30], where did an experiment with FAR where it has been shown that fingerprints have better performance than biometric systems of facial features and voice features, because the acceptance of impostors is much lower in the fingerprint biometric system, in the second experiment fingerprint biometric system shows the best performance of FRR compared to the biometric system of facial and voice features, obtained that a smaller number of users genuine ones are rejected by the fingerprint biometric system. In a third experiment, the fingerprint biometric system shows the best Failure to Capture (FTC) performance compared to the facial and voice biometric system, therefore identified that a lower number of identification failures in the fingerprint biometric system.

The IoT devices is highly used for the registration of biometric data, because allow a large number of actions to be carried out to process data, in [31] used a Raspberry Pi as a remote authentication and registration node. , the enrollment is successful and the captured data is sent to the cloud, The fingerprint and face capture sensors along with the Wi-Fi adapter are successfully connected to the Raspberry Pi, the captured data is sent to a biometric service Based on Microsoft Azure, the service extracts features as feature vectors are stored in a vector database. The system that the authors propose allows control through the capture of biometric data, which is scalable. In [32] use a Raspberry Pi for user authentication through biometric data, the proposed work the collection of 6 samples of the same person footprint and 6 samples of fingerprints, in the data acquired performed the steps of Image Acquisition, Image Enhancement, Binarization, Thinning and Feature Extraction, the images that enter the are subjected to a preprocessing stage followed by the pattern matching stage, finally proceeding to a decision-making based on the match score if the given input is authenticated or not. The IoT system uses a version of Linux NOOBS and image recognition is done using OpenCV. The data recognition algorithm implemented for fingerprints is SIFT for feature extraction, a fold pattern orientation flow and fingerprint orientation normalization using the centroid rule.

In [33] developed a work for access to vehicles through biometric data, this work used a system implemented in a Raspberry Pi sensor to acquire fingerprints, the process consists of capturing the thumb to recognize if the registered fingerprint matches that of the base, all the car doors will automatically unlock, otherwise the car will not be unlocked. The system uses a Global System for Mobile Communication (GSM) module to communicate to the owner about access events or access attempts. In [33] propose the implementation of an Arduino Uno connected to a GSM module and an NFC reader and implement in Arduino Mini connected with a fingerprint sensor and an NFC card. The fingerprint detection algorithm is SmartFinger 3.0. At work use authentication when a verification occurs, the system sends the user an SMS with the telephone number of the guest who wishes to enter to give access authorization, the NFC band allows to acquire fingerprints and will allow access when it coincides with registration on the device. In [34] present an interesting work on the registration of biometric data with EGC analysis, firstly filter the ECG signal, by eliminating noise with linear or non-linear methods, propose an adaptive wavelet decomposition (AWD). However, the AWD has a high demand on Signal Noise to Ratio (SNR) when reconstructing signals, furthermore, for this reason the authors add the Singular Vector Decomposition (SVD) to efficiently extract compressed features from the based on the reading of Electrocardiogram (ECG) signal and then recover a clean ECG signal from the noisy one. The authors highlight that the algorithms can be implemented in IoT devices using Python 2.7, to filter out noise, allowing effective user authentication as well as data assurance. In [35] carry out an advanced study on the authentication and identification systems that are implemented in the current IoT technology, in which the Bayesian network algorithms, the radial based SVM in the kernel function and the dynamic time warping stand out. distance, while the identification systems are based on algorithms such as Radial Basis Function Network, Sparce Approximation Classification, Artificial Neural Network among others, this investigation gives as a result the identification and authentication systems are still in an improvement process in which mathematical processes are still subject to challenge by attacks and hardware limitations. In [36] develop an authentication scheme based on multiple factors and the generation of secret keys using entropy sources ECG, HRV, and SRAM PUF values. The basis of the work is ECG and Photoplethysmogram (PPG), to achieve multifactorial safety. The authors developed a hardware security engine with ECG entropy sources, Heart Rate Variability (HRV) and SRAM-based Physical Unclonable Function (PUF) to perform real time authentication, thus proposing hybrid signatures that vary from person to person, and from device to device, for the generation of random secret keys. The chip proposed is a manufactured in LP CMOS of 65 nanometers, the database used for the data obtained from the ECG is 741 people. The hardware was tested by ERR, and the 256-bit keys that were generated were tested by NIST randomness tests.

In [37] proposed a DSA for a Biometric Authentication System (EBA) based on ECG, one of the contributions is that the authors managed to reduce the vulnerabilities of the EBA when time-based attacks were applied, reducing the latency of the system. The authors tested their system with attacks on a convolutional neural accelerator based on FPGA to recover the captured energy traces, being this work in verifying countermeasures to side channel attacks in EBA systems based on system times, without interfering in running system applications when authentication execution is not being enforced. In [38] conducted research on Match-on-Card (MOC) authentication for mobile devices using models for offline machine learning. The model used by the authors was calculated by simplifying the SC of the mobile devices, registering the users, and storing the data in vectors so as not to retrain the model, comparing the characteristics obtained by deriving a binary authentication decision. The authors point out that the advantage of their model is that it can be applied to different biometrics. The software used by the authors was Java Card in a 16/32-bit version for face detection. For the experiments used 8 face images from a template and 4 recently registered facial images. The ERR results were between 2.4 and 5.4. %. Authentication times are on the order of 1 second.

In [39] developed a biometric authentication system for automobiles based on EEG, the recordings collected are transformed to create unique biometric identifiers based on the acquisition of unrepeatable physiological characteristics, the system is implemented in mobile devices, the work is based on obtaining data from brain waves, which are read by the system and measure the stability of the subject, if the subject is in an altered state the system does not allow the user to enter, due because it would be in a disturbed state and it would not be possible to establish the correct state with which the system was trained, although author's work has the defect that in a disturbed state of the user in which their security is not compromised it would not be possible to access the system.

Table 1 presents a summary of the most relevant works of this research.

Table 1: Compilation of signal biometric and methods used in the analyzed investigations

Author	Biometric	Method
Govindraj, 2020	Fingerprint	SmartFinger 3.0
Cherupally (2020)	ECG	No mentioned
Cordeiro (2020)	ECG	EBA
Findling (2018)	No mentioned	On match-on-card
Klonovs (2013)	EEG	Neruohead Emotive COPD
Shah (2015)	Fingerprint	Microsoft Azure
Huang (2017)	Face	No mentioned
Sujatha and Chilambuchelvan (2018)	Iris, palm print, face, and signature	FAR, FRR, EER
Wójtowicz (2016)	Voice, face, and fingerprints	FAR, FRR
Kang (2017)	Face	No mentioned

As can be seen in the analyzed investigations, the signals captured by biometric systems can be classified into two parts, the signals that are acquired with contact such as fingerprints, palm of the hand and signature, on the other hand, those that do not require contact such as voice capture, face, iris, among others. Innovative applications have been found such as the use of EEG and ECG signals to guarantee the authenticity of the acquired data. The data acquired without contact ensures that users who use biometric devices are not put at risk, although it depends on a more reliable mechanism to validate the information acquired.

IV. Future directions

According to the analysis carried out in the present investigation is possible to determine the direction to take, which is focused on developing a biometric system that captures data without the need for contact and supported by an acquisition of multiple biometric signals with additional radio validation. frequency to avoid false positives or false negatives, without neglecting a data encryption mechanism that guarantees the privacy of the information.

V. Conclusion

The development of biometric systems for access control to different systems has undergone many changes to provide more secure access and to prevent system access violations. For this reason, such systems have progressed due to the need for secure authentication and to deal with attacks from different systems.

According to the analyzed data, it is possible to observe that biometric systems depend on the accuracy of the sensors to collect information from users and on computational techniques that allow validating the identity of the user. The efficiency of an authentication system is based on the ability to determine that the biometric signal comes from an individual, without false positives, in addition to the correct use of validation metrics such as FAR, FRR, ROC, among others.

Currently, the biometric data obtained allow the generation of secure cryptosystems to prevent malicious agents from obtaining information, therefore, the information obtained from EGC and EEG allows the generation of highly secure cryptosystems, because the information obtained contains many patterns that it encodes. the information securely.

The biometric data that are commonly acquired are those from fingerprints, face, and voice, because these are easily obtained and processed, but these need a strict and reliable validation process to guarantee the authenticity of the data entered in the system.

VI. Acknowledgment

We thank the Technological Institute of Higher Studies of Jocotitlan for the support provided in carrying out this research.

VII. References

[1] K. Okereafor, I. Ekong, I. Markson and K. Enwere. “Fingerprint Biometric System Hygiene and the Risk of COVID-19 Transmission”, in JMIR Biomedical Engineering. 5. 1-15. 10.2196/19623, 2020

[15] E. Sujatha and A. Chilambuchelvan.“Multimodal biometric authentication algorithm using iris, palm print, face and signature with encoded DWT”, in Wireless Personal Communications, vol. 99, no. 1, pp. 23–34, 2018.

[2] Y. Guo.“Impact on Biometric Identification Systems of COVID-19”, in Scientific Programming. 2021. 1-7. 10.1155/2021/3225687, 2021.

[3] R. Gupta and P. Sehgal.“A survey of attacks on iris biometric systems”, in International Journal of Biometrics, 8. 145. 10.1504/IJBM.2016.077833, 2016.

[4] A. S. Zimik and C. Keishing.“A Study on the Performance of Biometric Devices with Reference to Employee Interface”, in Indian Journal of Management and Language. 1. 8-12. 10.54105/ijml.C2039.041322, 2020.

[5] I. Buciu and A. Gacsadi.“Biometrics Systems and Technologies: A survey”, in International Journal of Computers Communications & Control. 11. 315. 10.15837/ijccc.2016.3.2556, 2016.

[6] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic. (2017) “Evaluatingbehavioral biometrics for continuous authentication: Challenges andmetrics”, in Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, pp. 386–399, 2017.

[7] F.Cherifi, B. Hemery, R. Giot, M. Pasquet, and C. Rosenberger. “Performance evaluation of behavioral biometric systems”, in Behavioral biometrics for human identification: Intelligent applications, pp. 57–74, IGI Global, 2010.

[8] S. Neware.“Biometrics System an Overview”, in International Journal of Computer Sciences and Engineering. 6. 313-319. 10.26438/ijcse/v6i1.313319, 2018.

[9] R. Malathi et al. “An integrated approach of physical biometric authentication system”, in Procedia Computer Science, vol. 85, pp. 820–826, 2016.

[10] A. Wójtowicz and K. Joachimiak. “Model for adaptable context-based biometric authentication for mobile devices”, in Personal and Ubiquitous Computing, vol. 20, no. 2, pp. 195–207, 2016.

[11] P.-C. Huang, C.-C. Chang, Y.-H. Li, and Y. Liu.“Efficient access control system based on aesthetic QR code”, in Personal and Ubiquitous Computing, vol. 22, no. 1, pp. 81–91, 2018.

[12] H. Kang, K.-H. Lee, and G.-J. Kim. “Safe and convenient personal authentication method using moiré 3d authentication based on biometric authentication”, in Cluster Computing, vol. 22, no. 1, pp. 2017–2026, 2019.

[13] E. B. Tarif, S. Wibowo, S. Wasimi and A. Tareef. “A hybrid encryption/hiding method for secure transmission of biometric data in multimodal authentication system”, in Multimedia Tools and Applications, vol. 77, no. 2, pp. 2485–2503, 2018.

[14] E. R. Isaac, S. Elias, S. Rajagopalan, and K. Easwarakumar.“Gait verification system through multiperson signature matching for unobtrusive biometric authentication”, in Journal of Signal Processing Systems, vol. 91, no. 2, pp. 147–161, 201

[16] L. Catuogno, C. Galdi and D. Riccio.“Off-line enterprise rights management leveraging biometric key binding and secure hardware”, in Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 7, pp. 2883–2894, 2019.

[17] D. M. Kaburu, J. Sansa-Otim, K. Mayanja, D. P. Mirembe, and T. Bulega.“A usability-based approach to designing continuous user biometric authentication system”. Quality and User Experience, vol. 3, no. 1, pp. 1–14, 2018.

[18] S. Sahmim and H. Gharsellaoui.“Privacy and security in internet-based computing: cloud computing, internet of things, cloud of things: a review”, in Procedia computer science, vol. 112, pp. 1516–1522, 2017.

[19] M. H. Ozcanhan, G. Dalkilic, and S. Utku. “Criptographically supported NFC Tags in medication for better inpatient safety”, in Journal of medical systems, vol. 38, no. 8, pp. 1-15, 2014.

[20] K.Chatterjee et al.“Biometric re-authentication: An approach towars achieving transparency in user authentication”. Multimedia Tools and Applications, vol 78, no. 6, pp. 6679-6700, 2019.

[21] H. Amintoosi an A. J. Taresh.“Sparce coding-based feature extraction for a biometric remote authentication in inter of things”.SN Applied Sciences, vol. 1, no. 9, pp 1-5, 2019.

[22] S. D. Kaul and D. Hatzinakos. “Intelligent RFID biometric enables dual security lock in the banking environment”, in Jornal of Banking aFinancial Technology, vol. 4, no. 2, pp. 159-173, 2020.

[23] Sarkar and B. K. Singh.“A review on performance, security and various biometric template protection schemes for a biometric authentication system”. Multimedia Tools and Applications, vol. 79, no. 37, pp. 27721-27776, 2020.

[24] B. Meden, P. Rot, P. Terhorst, N. Damer, A Kuijper, W. J. Scheirer, A Ross, P. Peer and V. Struc.“Privacy-enhancing face biometrics: A compressive survey”, in IEEE Transactions on Information Forensics and Security, 2021.

[25] M. Obaidat, J. Brown, S. Obeidat and M. Rawashdeh.“A Hybrid Dynamic Encryption Scheme for Multi-Factor Verification: A Novel Paradigm for Remote Authentication”, in MDPI, Sensors, 20, pp. 1-32, 2020.

[26] D. Anguiano-Cervantes’ G. Saaduddin, Y. Li. and M. Xie. (2016) “Comparison between Fingerprint and Behavioral Biometric Authentication Using 2D and 3D Gestures”, in 2016 IEEE Conference on Communications and Network Security (CNS): IEEE CNS 2016, 2016.

[27] Doshi, N. Patel, C.“A Novel Approach for Biometric Based Remote User Authentication Scheme using Smart Card” in 2018 IEEE, conference paper, 2018

[28] P. Baraki and V. Ramaswamy. “Biometric Authentication of a User using Online Dynamic Signature”. IEEE, 2016

[29] B. Naidu, K. V. L. Bhavani, C. Rao and P. V. G. D. Reddy.“Comparative Analysis of Three Single Trait Biometric Authentication Models”. 0956-0959. 10.1109/ICCSP.2019.8698041, 2019.

[30] D. Shah, V. Bharadi, V. Kaul, and S. Amrutia.“End-to-End Encryption Based Biometric SaaS: Using Raspberry Pi as a Remote Authentication Node”. 52-59. 10.1109/ICCUBEA.2015.19, 2015.

[31] S. Sivaranjani, and S. Sumathi.“Implementation of fingerprint and newborn footprint feature extraction on Raspberry Pi”. 10. 1-6. 10.1109/ICIIECS.2015.7193087, 2015.

[32] Nagamma, N.N. & Lakshmaiah, Mv & Narmada, T.“Raspberry Pi based biometric authentication vehicle door locking system”. 2348-2351. 10.1109/ICPCSI.2017.8392138, 2017.

[33] V. Govindraj, P. V., Yashwanth, S. Bhat, and T. K. Ramesh.“Smart Door Using Biometric NFC Band and OTP Based Methods”. 1-4. 10.1109/INCET49848.2020.9153970, 2020.

[34] P. Huang, L. Guo, M. Li and Y. Fang.“Practical Privacy-Preserving ECG-Based Authentication for IoT-Based Healthcare”, inIEEE Internet of Things Journal. 10.1109/JIOT.2019.2929087, 2019.

[35] Y. Liang, S. Samtani, B. Guo, and Z. Yu.“Behavioral Biometrics for Continuous Authentication in the Internet of Things Era: An Artificial Intelligence Perspective”, in IEEE Internet of Things Journal. PP. 1-1. 10.1109/JIOT.2020.3004077, 2020.

[36] S. Cherupally, S. Yin, D. Kadetotad, C. Bae, S. Kim, and J. Seo.“A Smart Hardware Security Engine Combining Entropy Sources of ECG, HRV, and SRAM PUF for Authentication and Secret Key Generation”, in IEEE Journal of Solid-State Circuits. 55. 1-1. 10.1109/JSSC.2020.3010705, 2020.

[37] R. Cordeiro, D. Gajaria, A. Limaye, T. Adegbija, N. Karimian and F. Tehranipoor.“ECG-Based Authentication Using Timing-Aware Domain-Specific Architecture”, in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 39. 3373-3384. 10.1109/TCAD.2020.3012169, 2020.

[38] R. D. Findling, M. Hölzl, and R. Mayrhofer.“Mobile Match-on-Card Authentication Using Offline-Simplified Models with Gait and Face Biometrics”, in IEEE Transactions on Mobile Computing. PP. 1-1. 10.1109/TMC.2018.2812883, 2018.

[39] J. Klonovs, C. Petersena H. Olesen, A. Hammershoj.“ID Proof on the Go: Development of a Mobile EEG-Based Biometric Authentication System”, in Vehicular Technology Magazine, IEEE. 8. 81-89. 10.1109/MVT.2012.2234056, 2013.