Privacy Preservation of Biometrics Used for IoT Systems Security: Brief Review

Asma.Aounallah[1], Hakim.Bendjenna[1]and Abdallah.Meraoumia[1]

[1] *University of Larbi Tebessi, LAboratory of Mathematics, Informatics and Systems (LAMIS), Tebessa, Algeria*

Abstract

The security issue in the Internet-of-Things (IoT) environment becomes very essential with the big emergence of IoT technologies. Recently, various works and research have adopted a combination of two axes, IoT security, and biometric security, and as we know Biometrics plays an important role in securing emerging IoT devices, regarding its uniqueness and that it cannot be replaced, more protection is needed to store original biometrics away from invaders. The idea is to implement some techniques in a way that if the biometric template used is compromised it can be revoked and a new one will be generated. Various approaches adopted this concept of revocability in IoT-based systems. The idea of this paper is to give a review that gathers and classifies these approaches according to the general revocability approaches categories and minimize the threshold research in this field.

Keywords

Revocable Biometrics, IoT, Authentication, Security

1. Introduction

The Internet of Things (IoT) is a challenging research field [1, 2]. In an age when everything digital is connected and exchanging information, these devices are infiltrating every aspect of our daily lives including healthcare, offices control, home appliances control, doors and windows, professional devices, reception of information, and security systems, etc [3]. Considering how many devices are becoming connected to the internet exponentially, one of the biggest concerns is securing the devices so they can be accessed remotely because it is likely that more potential attackers will pay attention to your product as it becomes more successful. Whenever devices are connected, a secure communication system relies on authentication as the gateway.

Up until recently, two-factor authentication, such as a username and password, has traditionally been the means of securing the network between all our devices, but with today's development technologies have become insecure and replaced by biometric authentication [4]. Biometrics refers to automatically identifying people based on their biological and behavioral traits which are difficult to compromise and copy, such as the face [5], voice [6], iris [7], finger [8], palm [9, 10]. Biometrics-based systems work by capturing a biometric surface and analyzing it using a sensor for feature extraction and comparison, thus resulting in high matching speed and accuracy in addition to a moderate cost. Various works in the literature used biometrics for secure authentication concerns [11], especially for IoT cloud systems [12]. The two most crucial factors that must be taken into account when creating biometric authentication systems are security and recognition accuracy. The advanced technology of today's world makes it possible to create a loophole in it and make our biometrics suffers from privacy and security concerns. Although biometric authentication is intended primarily for security-enhancing, the biometric information storage in a database introduces new security and privacy risks [13], and unlike passwords, PINs, and access codes, biometric templates can never be substituted with a new one if they are compromised. The traditional biometric system stores original biometrics, unfortunately, without any encryption which needs to protect them as unique and irreplaceable personal characteristics against different attacks. To overcome the problem of stolen

SIoT-2022: International Workshop on Semantic IoT (SIoT-2022), Co-located with the KGSWC-2022, November 21-23, 2022, Madrid, Spain.

EMAIL: asma.aounallah@univ-tebessa.dz (A. 1); hakim.bendjenna@univ-tebessa.dz (A. 2); ameraoumia@univ-tebessa.dz (A. 3)

biometrics, several solutions are proposed in the literature under the concept of "Privacy by Design" to ensure the protection of biometric data against outside and inside attacks called biometric template protection schemes (BTPs) schemes introduced under the concept of Revocable Biometric which can preserve privacy and enhance template security in existing systems. The BTPs are generally divided into two main classes: Biometric Cryptosystems and feature transformation-based methods which are well explained in this paper.

Our contribution in this paper:

1. This paper presents a review of a specific area of enhanced biometric security methods called revocable biometrics used for IoT security, noting that there isn't a literature review paper of works that adopted the specification of revocability in IoT separately.
2. In this paper a classification of biometric methods used in preserving security concerns for IoT is presented and explained according to the two main revocable biometric varieties used; including the biometric-based cryptosystems and based feature transformation.

The rest of our paper is organized as follows: Section 2 presents attacks on IoT with the solution requirements mentioned in the literature in brief points. Next, Section 3 mentioned how biometrics could be used in IoT. In the next section, a description of revocability concept is well presented with its relation to the protection and privacy insurance of the biometric itself used in authentication based-systems under the concept of Biometric Template Protection schemes (BTPs). Section 5 aims to present works and research proposed in the literature to protect the biometrics enrolled in IoT systems. Finally, Section 6 provides the reached conclusions and future scopes.

2. Attacks on IoT-based systems and security requirements

Today's IoT environment is susceptible to numerous types of attacks, lots of papers in the literature presented some types [14, 15]. Yang et al in [16] mentioned a list of possible attacks that could target the perception, network, and application layers of IoT systems with their security requirements. The attacks are listed for each layer separately as; Node Tampering, RF Interference, Node Jamming, Malicious Node Injection, Physical Damage and Malicious Code Injection for the perception layer, Traffic Analysis Attacks, RFID Spoofing, and Clonin, Man-in-the-middle Attacks, Routing Information Attacks, Denial of Service and Sybil Attacks for the network layer, and Phishing Attacks, Viruses, Worms, Trojan Horses and Denial of Service for the application layer. Sengupta et al. in [17] classified attacks on IoT into four types and each one targets one or more of the IoT layers including; application, processing, network and perception layers. In their paper attacks divided as follows: physical attack, software attack, network attack, and data attack,

In the other hand, several solution requirements for IoT security were proposed in the literature, the most mentioned are Authentication, Identification, Privacy, Confidentiality, Availability, Freshness, Forward and Backward Secrecy [18]. For an effective work of IoT objects, IoT security is crucial, because without it, any connected object in the IoT is vulnerable to dangers and threats.

3. Biometrics for IoT security

For biometric-based IoT systems, biometrics plays an important role in achieving and preserving enhanced security in IoT, various research papers adopted biometric technologies for this concern in different environments [19,20], and in different levels of IoT systems architecture. Ang et al. in [21] proposed a new architecture for IoT named BiometricIoT taking into account the specific requirements of biometrics-based security, multimedia content, and big data analytics. The proposed architecture consists of seven layers; Biometrics Identification Layer, Biometrics Object Layer, Biometrics Device Elements Layer, Biometrics Communication Layer, Biometrics Cloud Services Layer, Big Biometrics Data Computation Layer, and Biometrics Application Layer.

Despite how biometrics could be incorporated into IoT systems and the fact that biometrics is a reliable authentication and identity system, it cannot be trusted for security once it's compromised. The major problem of biometrics is piracy, and it is crucial to implement security and protection measures to mitigate attacks conducted against the biometrics itself.

4. Biometric template protection schemes (BTPs) and revocability

The main idea for template protection is to apply a transformation method to the original user biometric in such a way that the newly designed template does not affect negatively the system security and does not offer the possibility to recover the original one [22].

An ideal biometric template protection scheme should consist of the following four properties [23]:

1. Diversity: The same secured biometric template should used for one application and must not permit cross-matching between databases
2. Revocability: a stolen biometric template is simply revoked and reissued.
3. Security (Non-invertibility): unrecovered original biometric sample if the transformed sample got stolen.
4. Performance: The transformation does not deteriorate the system recognition performance.

The revocable - or cancellable - Biometric recognition process consists of two phases like any biometric system; Enrollment and Authentication, as it is shown in Figure 1. In the Enrollment phase, the features of the presented user biometric image to a biometric scanner are extracted and transformed later using a transformation technique to generate a revocable biometric template which will be stored later in the database to be matched later during the Authentication phase with another revocable template generated passing by the same steps as the first in the Enrollment phase.

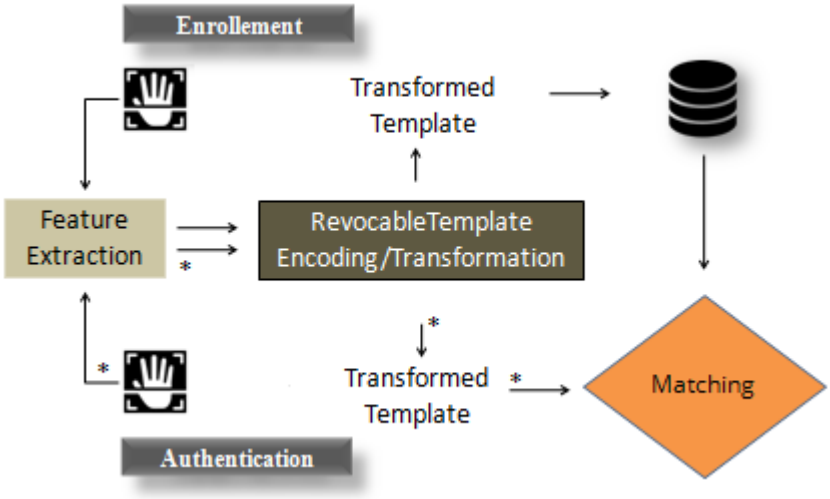

Figure 1: General revocable biometric system scheme

In recent decades, revocable biometric template generation has been a popular research area, in which multiple type of research has been suggested in the literature. Patel et al in [24] present a review of revocable approaches categorized according to two main classes: methods that can work with a special matcher/existing matchers, and the second level was divided into two categories: registration-free/registration needed base-methods. Finally, two categories are derived from each element of the last level including schemes that work with the signal/feature domain. The same paper proposed a classification of ten categories for revocable methods; Salting Methods, BioHashing Methods [25], Random Projections, Random Permutations [26], Bioconvolving, Non-invertible Geometric Transforms, Bloom Filters [27], Cancelable Biometric Filters, Knowledge Signatures, Hybrid Methods [28]. Whereas Kumar et al. in [29] presented a brief and well-discussed survey on revocable biometric techniques, in their work a new taxonomy was proposed in which these methods were divided into six categories. Cryptography-based, Transformation based, Filter base, Hybrid methods, Multimodal based, and other listed categories. In addition, the possible attack points in a revocable biometric system were well explained. But in general BTPs were divided into two categories; Biometric cryptosystems and the Transformation approaches.

4.1. Biometric cryptosystems

In biometric cryptosystems, by combining biometrics and cryptography according to the general principle, the biometric templates are generated based on the generation of cryptographic keys. The possibility to manage cryptographic keys securely and protect biometric templates is offered by using biometric cryptosystems. Depending on the data helper extraction method, biometric cryptosystem approaches can be divided into two categories (Figure 2): key-binding and key generation [30].

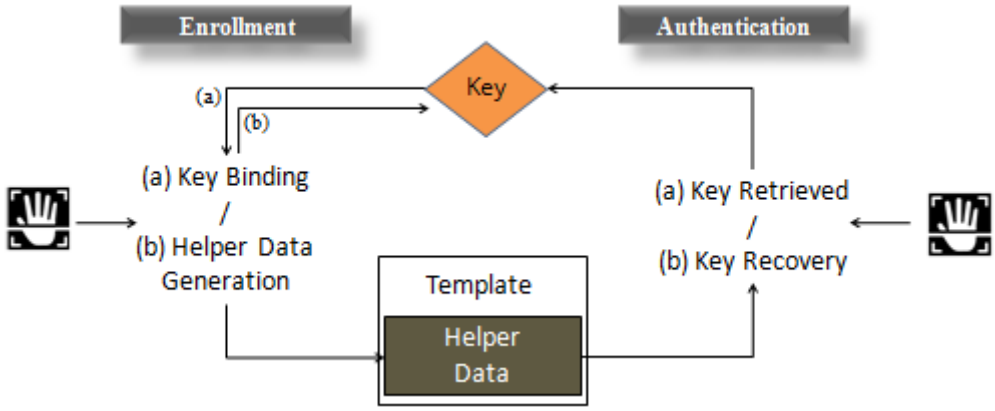

Figure 2: General key binding (a) and key generation (b) scheme

In the first category, a cryptographic key is used to bind the biometric template to create a so-called secure sketch that cannot be used to recover the biometric data or the key's origins. The well-known instances of key-binding schemes are fuzzy commitment [31] and fuzzy vault [32], which generates binary vectors and an unordered set of points respectively to encode the biometric templates. For the key generation cryptosystem, a direct cryptographic key generation from helper data and biometric features is applied.

4.2. Feature transformation approach

The general principle of feature transformation approaches is by using a specific function of transformation, the unprotected original biometric template is converted to another protected one using certain transformation parameters, which can be revoked and replaced if the transformed template is compromised [33]. These schemes can be further categorized into either invertible [34] or non-invertible transform [35] (Figure 3).

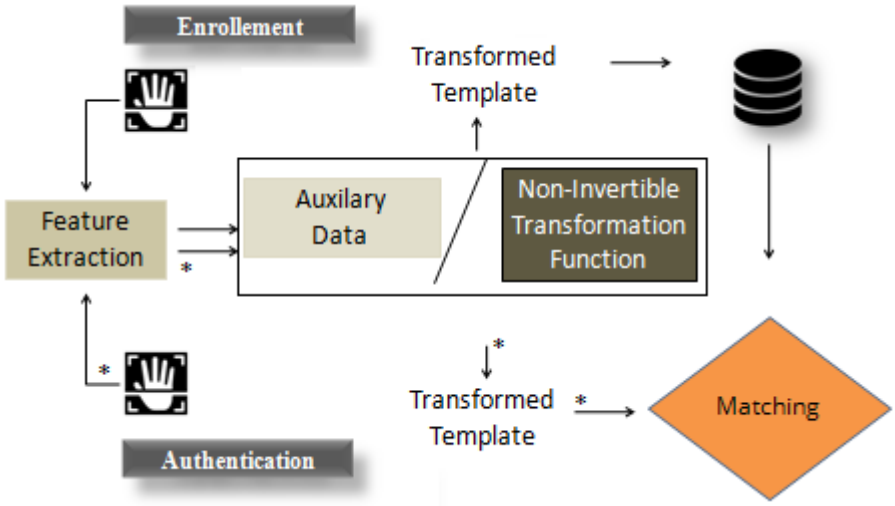

Figure 3: General biometric feature transformation scheme

In the invertible transform, the original biometric template can be recovered using a key. The top famous approach used in this type is Biohasing [36], which is generally adopted for fingerprint

minutiae to generate a revocable BioCode by first projecting the FingerCode on an orthogonal basis defined by the random seed. Whereas in non-invertible transform the key is one-way, which means that even if the key is known the original biometric template is not recovered. This approach type can effectively ensure revocability concerns.

5. Revocable biometrics in providing security for IoT

In recent years, Now that the Internet of Things has emerged, the demand for access control and data privacy on low-power ubiquitous devices is growing [37], which demand a high security level. Revocable biometrics is promising for IoT due to its convenient nature and lower susceptibility to attacks. In this context, several revocable biometrics protection schemes have been proposed in the literature that attempts to protect the privacy of original biometric templates used in IoT systems. The next section will present them according to two categories: Biometric cryptosystems and Feature transformation-based methods.

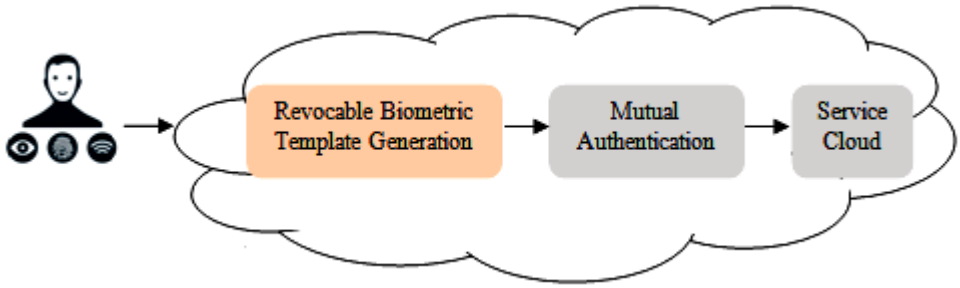

Figure 4: Example of IoT cloud authentication based on revocable biometrics used for a service cloud access control.

5.1. Biometric cryptosystems for IoT security

In this context, there have been a number of research efforts aimed at addressing the issues related to the implementation of biometric cryptosystems in IoT systems, all presented in Table 1, and the performance is given by the Equal Error Rate (EER) and/or False Acceptance Rate (FAR).

Guo et al. in [38] proposed a revocable secret keys method using Physically Unclonable Functions (PUFs) that can be implemented with the SRAMs of commercial Bluetooth Low Energy (BLE) chips. The method applied in the sensor node communication module, the user biometrics obfuscated with PUFs when the user biometrics is sensitive. The proposed method consists of two stages, Helper-Data generation and secret reconstruction, in their work revocability of the proposed method is achieved from new PUF responses. The method gives high performance with Error Equal Rate (ERR) equal to 0.02%.

A fuzzy commitment encryption method was performed well for securing IoT features. Bentahar et al. in [39] used the fuzzy commitment to present securing fingerprint biometric cryptosystem for IoT-based systems to protect the authentication information (user biometrics and things identifiers) and the data exchanging (after an accepted session). The proposed method defined on three main stages: human user to smart connected things authentication, human user to remote server identification and secure communication between things and remote system. Experimental results show improvements with performance of ERR=0.

Meraoumia et al. in [40] designed an e-security system for enterprise information exchange. The proposed system uses symmetric cryptographic and multi-factor authentication methods based on a card combined with a PIN code and a palmprint/palmvein biometric trait. In this work, after extracting the biometric features the Fuzzy commitment is used for biometric encryption which uses a random key (AES encryption to encrypt data of the enterprise then the key is binding in the biometric. In this experiment an ERR, FAR of 0 are obtained.

Jiang et al. in [41] proposed a cancelable biometric modality based on high-density surface electromyogram (HD-sEMG) encoded by hand gesture password. During user authentication, biometric token formed when the user used the required gesture password with the acquired HD-sEMG signals of the right forearm muscles. The ability to cancel is validated when the user changes muscle activations after exposing the biometric token. Experiments showed the effectiveness and security enhancing of HD-sEMG against attacks, and showed a high performance with ERR=0.003%.

A lightweight bio-cryptosystem is developed for DNA encoding in [42] for security insurance of biometric templates when store and transmit them, they begin by adopting 2D_Logistic Sine Map for random key generation, then, a hexadecimal-based conversion of fractional chaotic keys to applicable integer forms is executed. next, for obtaining a confused image, chaotic key series used for confusing images(ODD and EVEN images) separately and then merged them for encoding using random keys.

Soliman et al. in [43] applied Discrete Cosine Transform (DCT) for the introduced biometric, and then presented a revocable biometric scheme to generate a revoked template. The original biometric is blurred with two co-prime operators. Hence, it can be recovered as the Greatest Common Divisor (GCD) between its two blurred versions. Experiments show good system performance with EER = 0.04%.

A revocable multimodal biometric verification system for IoT environments based on watermarking and encryption algorithms is presented in [44]. Both voice print and facial images are used as individual biometrics. Double Random Phase Encoding (DRPE) is used for face encryption and The SVs matrix of the voice images is chosen as a stable matrix to hide the encrypted face images. Finally, the watermarked voice image is encrypted by a chaotic Baker map.

Table 1
A summary of works used biometric cryptosystems for IoT security

Year(Ref)	Revocable Method	Modality	Best Performance
2018[38]	Physically Unclonable Functions (PUFs)	Fingerprint	EER=0.22
2018[39]	Fuzzy Commitment	Fingerprint	EER=0
2019[40]	Fuzzy Commitment	Palmprint Palmvein	EER =0 FAR=0
2021 [41]	HD-sEMG-based Biometric	Hand Gesture	EER=0.003
2021[42]	2D logistic sine map	Fingerprint	/
2021[43]	Blurring+ GCD-based method	Palmprint Face Fingerprint Iris Palmprint	EER=0.04
2022[44]	Double Random Phase Encoding (DRPE) and chaotic Baker map	Voice Face	/

5.2. Transformation approaches for IoT security

In this section a number of research efforts aimed at addressing the issues related to biometric-based transformation approaches are presented. Thus, Table 2 summarizes some important works in this area of research. In this table, the performance is given by one of the following metrics; Equal Error Rate (EER) and False Acceptance Rate (FAR), False Rejection Rate (FRR), Recognition Rate (RR), and Area under the Receiver Operator Characteristic Curve (AROC).

Table 2
A summary of works used biometric based feature transformation for IoT security

Year(Ref)	Revocable Method	Modality	Best Performance
2019[45]	Random Projection + Steganography	Iris	EER=1.66
2019[46]	Partial DCT Transformation	Fingerprint	EER=1.32
2020[47]	3D Chaotic maps	Face Fingerprint	AROC=99.98 FAR/FRR= 1.8895×10^{-15} / 2.0234×10^{-12}
2022[48]	Random vectors for index generation+ Element Wise Average	Fingerprint	EER=0.04
2022[49]	Chaos AES Key generation + Projection Matrix	Palmprint Palmvein	RR=99.895
2022[50]	Partial-Cancelable Feature Generation + Encoding-nested-difference XOR scheme	Fingerprint	EER=2.29

A cancelable iris and steganography-based mechanism for hiding user-specific keys in an authentication system for IoT networks is proposed by [45]. First, feature quantization and shifting is applied on the original iris, then a random projection-based feature transformation is used to generate a revoked iris template. Finally, steganography is used to hide user-specific keys.

Punithavathi et al. in [46] proposed a cloud-based cancelable biometric system. For an authenticate user access control in the system, after the extraction of DCT matrix from the original fingerprint image, and to obtain a revocable biometric for storing it in the CTD in the cloud, a random generation of key transformation is applied to perform a partial DCT transformation.

Ibrahim et al. in [47] proposed a one-way cancellable biometric method for face and fingerprint. the proposed system usign 3D chaotic maps encryption has been applied to FPGA model and showed a high security for the biometric templates with an EER =1.32%, AROC = 99.98% , and FAR and FRR equal to 1.8895×10-15 and 2.0234×10-12 respectively.

A non-invertible transformation approach is proposed in [48], by generating two random vectors with a same length, the first vector used to extract elements from vector T whose indices are of the same values as entries in it to generate vector v_1. The remaining elements of v_1 are extracted using the second vector, the same thing, its indices are of the same values as entries in the first and generated a vector v_2, then, they obtained the element-wise average of vectors x and y.

Amroune et al. in [49] proposed a secure cloud-based IoT framework to secure the interaction of the person with his own objects. To generate AES encryption keys used for user messages encryption, the Chaos system was adopted, on the other hand projection matrices were used to encrypt biometric templates. The experiment is performed on two hand modalities, palmprint and palmvein, and show that the proposed method is well performed with Recognition Rate (RR) equal to 99.895%.

Yang et al. in [50] proposed a cancelable template consisting of two components to accommodate privacy-preserving authentication systems and resource-constrained Internet of Things applications. Firstly, using a designed re-indexing scheme, they generate length-flexible partial-cancelable features. Second, to ensure non-invertibility, using a designed encoding-nested difference-XOR scheme, revocable biometric templates were generated by passing by three operations: the nested difference operation, the encoding operation, and the bitwise XOR Boolean operation.

6. Conclusion

Unfortunately, biometric systems, despite their effectiveness in ensuring authentication in IoT systems, these systems may be exposed to new security and privacy risks. This paper presents a brief review of biometric template protection schemes used to protect the biometric trait itself. Also in this paper, we diminished the threshold of existing revocable biometric methods presented in the literature and adopted them to protect the biometric used for example for authentication, access control, or protect messages exchanged in IoT. Therefore, our future work should focus on using new revocable techniques not implemented in the literature for IoT system security, in different IoT environments for the privacy preservation of the biometric template adopted for IoT systems security and therefore achieving enhanced security in IoT systems.

7. Acknowledgements

The authors are grateful to the anonymous referees for their valuable and helpful comments. This research has been carried out within the PRFU project (Grant: A01L08UN120120180001) of the Department of Electrical Engineering, University of Larbi Tebessi, Tebessa. The authors thank the staff of LAMIS laboratory for the helpful comments and suggestions.

8. References

[1] Ali, Z., Ghani, A., Khan, I., Chaudhry, S. A., Islam, S. H., & Giri, D. A robust authentication and access control protocol for securing wireless healthcare sensor networks. Journal of Information Security and Applications, 52, 102502. (2020).

[2] Khan, A. A., Kumar, V., & Ahmad, M. An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach. Journal of King Saud University-Computer and Information Sciences. (2019).

[3] M, Gaurav. C, Sarika. Biometric authentication in internet of things: A conceptual view. Journal of Statistics and Management Systems. 22. (2019), 643-652. 10.1080/09720510.2019.1609722.

[4] Rui, Z., & Yan, Z. A survey on biometric authentication: Toward secure and privacy-preserving identification. IEEE access, 7, (2018), 5994-6009.

[5] Baqeel, H., & Saeed, S. Face detection authentication on smartphones: End users usability assessment experiences. In 2019 International Conference on Computer and Information Sciences (ICCIS), IEEE, (2019), (1-6).

[6] Zhang, X., Xiong, Q., Dai, Y., & Xu, X. Voice biometric identity authentication system based on android smart phone. In 2018 IEEE 4th International Conference on Computer and Communications (ICCC), IEEE, (2018), 1440-1444.

[7] Morampudi, M. K., Veldandi, S., Prasad, M. V., & Raju, U. S. N. Multi-instance iris remote authentication using private multi-class perceptron on malicious cloud server. Applied Intelligence, 50(9), (2020), 2848-2866.

[8] Tan, T. N., & Lee, H. High-secure fingerprint authentication system using ring-LWE cryptography. IEEE Access, 7, (2019), 23379-23387.

[9] A. Meraoumia, S. Chitroub and A. Bouridane, "Fusion of Multispectral Palmprint Images For Automatic Person Identification", International Conference on Electronics, Communications and Photonics-SIECPC, Saudi arabi, (2011), 1-6.

[10] Aounallah, A., Bradji, L., & Bendjenna, H. Is There Still Confidence In Hand-Crafted Feature Extraction Techniques To Use Them In Biometric Systems?. In 2021 International Conference on Recent Advances in Mathematics and Informatics (ICRAMI), IEEE, (2021), 1-5.

[11] Bibi, K., Naz, S., & Rehman, A. Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities. Multimedia Tools and Applications, 79(1), (2020), 289-340.

[12] Yadav, B. P., Prasad, C. S. S., Padmaja, C., Korra, S. N., & Sudarshan, E. A Coherent and Privacy-Protecting Biometric Authentication Strategy in Cloud Computing. In IOP Conference Series: Materials Science and Engineering, Vol. 981, No. 2, p. 022043. IOP Publishing. (2020).
[13] Sarkar, A., & Singh, B. K. A Review on Security Attacks in Biometric Authentication Systems. International Research Journal of Engineering and Technology, 5(12), (2018).
[14] Obaidat, M. S., Rana, S. P., & Maitra, T. Biometric Security and Internet of Things (IoT) Chapter 19 Biometric Security and Internet of Things (IoT). (2018).
[15] Deogirikar, J.; Vidhate, A. Security attacks in IoT: A survey. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 32–37
[16] Yang, W., Wang, S., Sahri, N.M., Karie, N.M., Ahmed, M., & Valli, C. Biometrics for Internet-of-Things Security: A Review. *Sensors (Basel, Switzerland), 21*. (2021).
[17] Sengupta, J.; Ruj, S.; Bit, S.D. A Comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J. Netw. Comput. Appl. (2020), 149, 102481.
[18] A. Bentahar, A. Meraoumia, H. Bendjenna and A. Zeroual, "IoT Securing System using Fuzzy Commitment for DCT-based Fingerprint Recognition," 2018 3rd International Conference on Pattern Analysis and Intelligent Systems (PAIS), (2018), 1-5, doi: 10.1109/PAIS.2018.8598511.6
[19] Ross, A., Banerjee, S., & Chowdhury, A. Security in smart cities: A brief review of digital forensic schemes for biometric data. Pattern Recognition Letters, 138, (2020), 346-354.
[20] Farid, F., Elkhodr, M., Sabrina, F., Ahamed, F., & Gide, E. A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services. Sensors, 21(2), (2021), 552.
[21] Ang, K. L. M., & Seng, K. P. Biometrics-based Internet of Things and Big data design framework. Mathematical Biosciences and Engineering, 18(4), (2021), 4461-4476.
[22] Sarkar, A., & Singh, B. K. A review on performance, security and various biometric template protection schemes for biometric authentication systems. Multimedia Tools and Applications, 79(37), (2020), 27721-27776.
[23] Maltoni, D., Maio, D., Jain, K., and Prabhakar, S. Handbook of Fingerprint Recognition. Berlin, Germany: Springer. (2003).
[24] V. M. Patel, N. K. Ratha and R. Chellappa, "Cancelable Biometrics: A review," in IEEE Signal Processing Magazine, vol. 32, no. 5, (2015) ,54-65, doi: 10.1109/MSP.2015.2434151.
[25] Belguechi, R., Cherrier, E., Rosenberger, C., & Ait-Aoudia, S. Operational bio-hash to preserve privacy of fingerprint minutiae templates. IET biometrics, 2(2), (2013), 76-84.
[26] Kumar, N., & Rawat, M. RP-LPP: a random permutation based locality preserving projection for cancelable biometric recognition. Multimedia Tools and Applications, 79(3), (2020), 2363-2381.
[27] You, L., & Li, X. A Cancelable multi-biometric template generation algorithm based on bloom filter. In International Conference on Algorithms and Architectures for Parallel Processing, Springer, Cham, (2018), 547-559.
[28] Helmy, M., El-Shafai, W., El-Rabaie, E. S. M., El-Dokany, I. M., & Abd El-Samie, F. E. A hybrid encryption framework based on Rubik's cube for cancelable biometric cyber security applications. Optik, 258, 168773, (2022).
[29] N, Kumar. Cancelable biometrics: a comprehensive survey. Artificial Intelligence Review, 53(5), (2020), 3403-3446.
[30] Tantubay, N., & Bharti, J. A Survey of Biometric Key-Binding Biocrypto-System using different Techniques. International Journal on Emerging Technologies, 11(1), (2020), 421-432.
[31] A. Juels, M. Wattenberg, A fuzzy commitment scheme, in: Proceedings of the 6th ACM Conference on Computer and Communications Security (CCS), (1999), 28–36 .
[32] A. Juels, M. Sudan, A fuzzy vault scheme, in: Proceedings IEEE International Symposium on Information Theory, (2002).
[33] R, Christian, Uhl, Andreas. A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security. (2011). 10.1186/1687-417X-2011-3.
[34] M. Ram and K. R. Radhika, "Biohashing application using fingerprint cancelable features," *15th International Conference on Industrial and Information Systems (ICIIS)*,IEEE, (2020), 214-218.
[35] Belguechi, R., Rosenberger, C., & Ait-Aoudia, S. Biohashing for securing minutiae template. 20th International Conference on Pattern Recognition, IEEE, (2010), 1168-1171.

[36] Kaur, H., & Khanna, P. Gaussian random projection based non-invertible cancelable biometric templates. Procedia Computer Science, 54, (2015), 661-670.
[37] L. Guo, Y. Mao and Y. Guo, "Non-invertible fingerprint template protection with polar transformations," *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, (2016), 730-735, doi: 10.1109/PST.2016.7906990.
[38] Arjona López, M. R., Prada Delgado, M. Á., Arcenegui, J., & Baturone Castillo, M. I. A PUF- and Biometric-Based Lightweight Hardware Solution to Increase Security at Sensor Nodes. Sensors, 18 (8), (2018), 1-25.
[39] A. Bentahar, A. Meraoumia, H. Bendjenna, S. Chitroub and A. Zeroual, "Biometric Cryptosystem Scheme for Internet of Things using Fuzzy Commitment principle," 2018 International Conference on Signal, Image, Vision and their Applications (SIVA), (2018), 1-6, doi: 10.1109/SIVA.2018.8660993.
[40] Meraoumia, A., Bendjenna, H., Dris, Y., & Amroune, M. Enhancing Security and Privacy in Enterprises Network by Using Biometrics Technologies. In Digital Business, Springer, Cham. (2019), 175-197.
[41] X. Jiang *et al*., "Enhancing IoT Security via Cancelable HD-sEMG-Based Biometric Authentication Password, Encoded by Gesture," in *IEEE Internet of Things Journal*, vol. 8, no. 22, (2021), 16535-16547, doi: 10.1109/JIOT.2021.3074952.
[42] Sujarani, R., Manivannan, D., Manikandan, R., & Vidhyacharan, B. Lightweight bio-chaos crypt to enhance the security of biometric images in internet of things applications. Wireless Personal Communications, 119(3), (2021), 2517-2537.
[43] Soliman, N. F., Algarni, A. D., El-Shafai, W., Abd El-Samie, F. E., & El Banby, G. M. An Efficient GCD-Based Cancelable Biometric Algorithm for Single and Multiple Biometrics. Computers Materials and Contiua, 69(2), (2021), 1571-1595.
[44] Salama, G. M., El-Gazar, S., Omar, B., Nassar, R. M., Khalaf, A. A., El-banby, G. M., ... & Abd el-samie, F. E. Cancelable biometric system for IoT applications based on optical double random phase encoding. Optics Express, 30(21), (2022), 37816-37832.
[45] Yang, W., Wang, S., Hu, J., Ibrahim, A., Zheng, G., Macedo, M. J., ... & Valli, C. A cancelable iris and steganography-based user authentication system for the internet of things. Sensors, 19(13), 2985. (2019)
[46] Punithavathi, P., Geetha, S. Partial DCT-based cancelable biometric authentication with security and privacy preservation for IoT applications. Multimed Tools Appl 78, (2019), 25487–25514.
[47] Ibrahim, S., Egila, M. G., Shawkey, H., Elsaid, M. K., El-Shafai, W., & Abd El-Samie, F. E. Hardware implementation of cancellable biometric systems. Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), IEEE, 2020, 1145-1152).
[48] Bedari, A., Wang, S., Yang, W. A Secure Online Fingerprint Authentication System for Industrial IoT Devices over 5G Networks. Sensors (2022), 22, 7609.
[49] Amroune, M., Meraoumia, A., Laimeche, L., & Bendjenna, H. Biometric Cryptosystem to Secure Smart Object Communications in the Internet of Things. Kuwait Journal of Science, 49(2), (2022).
[50] X. Yin, S. Wang, Y. Zhu and J. Hu, "A Novel Length-Flexible Lightweight Cancelable Fingerprint Template for Privacy-Preserving Authentication Systems in Resource-Constrained IoT Applications," in *IEEE Internet of Things Journal*, (2022),