جامعة
الملك سعود
King Saud University

Biometric Identification Impact on Privacy and Security

By

Taghreed M. Al-Hussan

Haya Al-Sulaiman

Haifa Al-Rayas

Yara Al-Fagih

Leena Al-Rajhi

Contents

Abstract

Biometrics plays an important role in identification and authenticating people such that a wide variety of systems uses biometrics as an authentication method, and since an individual's biometric data is personal and sensitive, issues and concerns related to biometric security and privacy have been raised. We conducted a survey to find out to what extent people's awareness about the biometric identification and its impact on privacy and security, and we found that people are partially aware of biometrics identification impact on privacy and security.

Introduction

Biometrics is the science of measuring physical and/or behavioral characteristics which are unique to each individual and they verify that an individual is who he or she claims to be. Many fields such as the e-government services, e-banking services, and e-commerce applications systems use biometric technology, and its increasingly becoming a basic element of authentication and identification systems. However, any human biometric characteristics are personal data that must be protected by privacy protection legislation, and there are many concerns and issues that arises about privacy and security impact due to the wide spread of biometrics use. In this research we will address people awareness of biometric identification impact on privacy and security.

Methodology

We used Quantitative methods (survey) to capture the extent of people awareness of biometric identification impact on privacy and security .The questionnaire had 11 questions combined multiple-choice questions predefined answers offering respondents, check box and linear scale questions with the possibility to choose grade on a “comfortable” to “uncomfortable” scale.

Survey sample:

To conduct the Survey, we questioned a universe of 207 ordinary people. Responses by gender; we found that 35.7% are males and 64.3% female. Responses by age; we found that 8.2% are less than 18, 67.6% are between 18 and 25, and 24.2% are more than 25. Responses by education level; we found that 41.1% are graduate from high school, 50.2% have bachelor's degree ,8.2% have master's degree, 2.9% have Doctoral degree (Ph.D.). Responses by his/her knowledge of computer science fields; we found that 78.3% have knowledge in computer science, and 21.7% have not knowledge in computer science.

Result

Question 1: "I prefer to use Face ID or Fingerprints over password on”

About 86.5% of the people chose finger prints over passwords to log in to their devices, 58% of the people chose Bank applications, 52.7% chose social media, and 38.6% chose online shopping Applications as shown in figure 1:

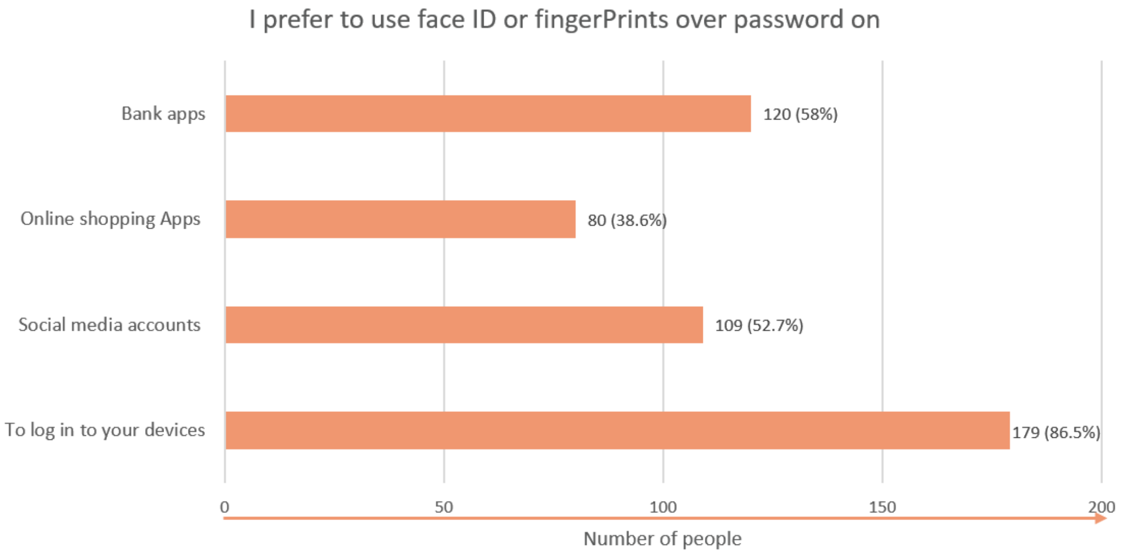

Fig. 1.

Question 2: “To what extent do you feel comfortable using biometric identification?”

About 39.1% answered (1), 23.2% answered (3), 22.2% answered (2), 10.6% answered (4), 4.8% answered (5) (where (1) refers to comfortable and (5) refers to uncomfortable) as shown in figure 2:

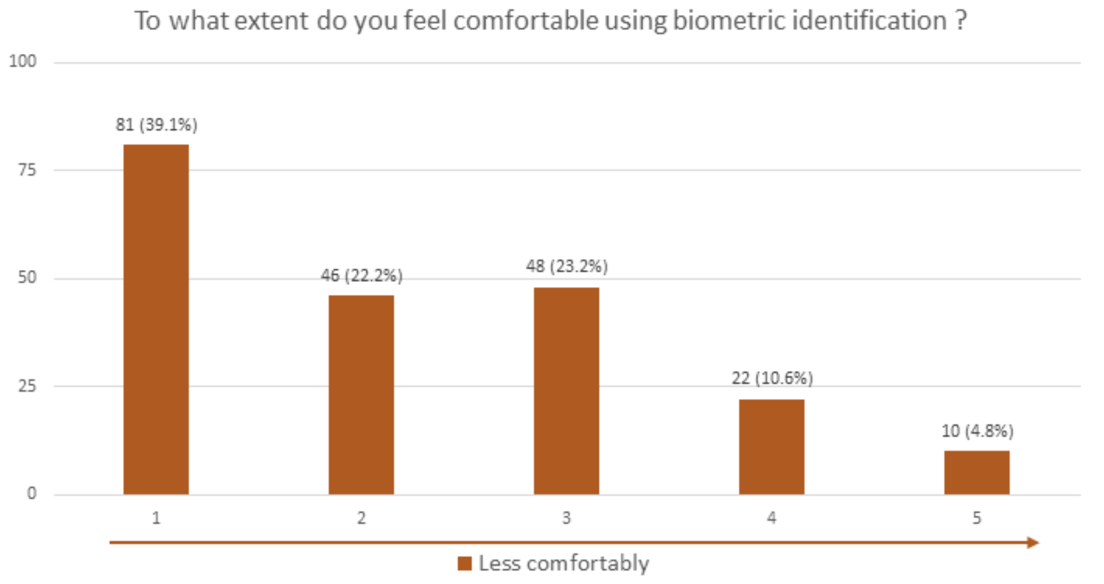

Fig. 2.

Question 3: “do you think using biometric identification is more secure than passwords?” About 56% people answered Yes, 29% answered No, 15% answered I don’t know, as shown in figure 3:

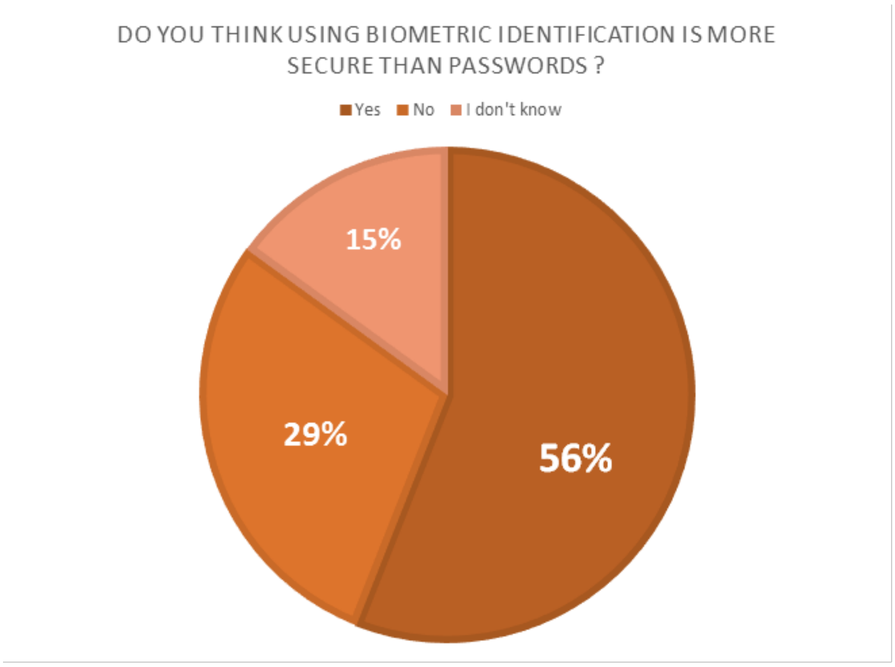

Fig. 3.

Question 4: “Do you think using biometric identification might affect your privacy?” About 44.4% of people answered Yes, 42% answered No, 13.5% answered I don’t know As shown in figure 4:

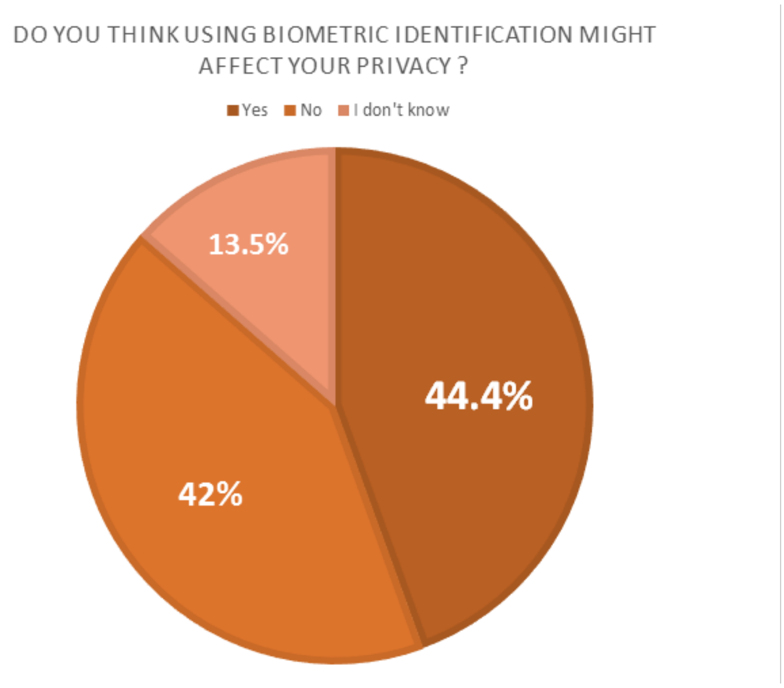

Fig. 4.

Question 5: “Do you think that biometric can be used without your knowledge?“
About 37.7% answered Yes and 41.5% answered No and 20.8% answered I don’t know as shown in the figure 5:

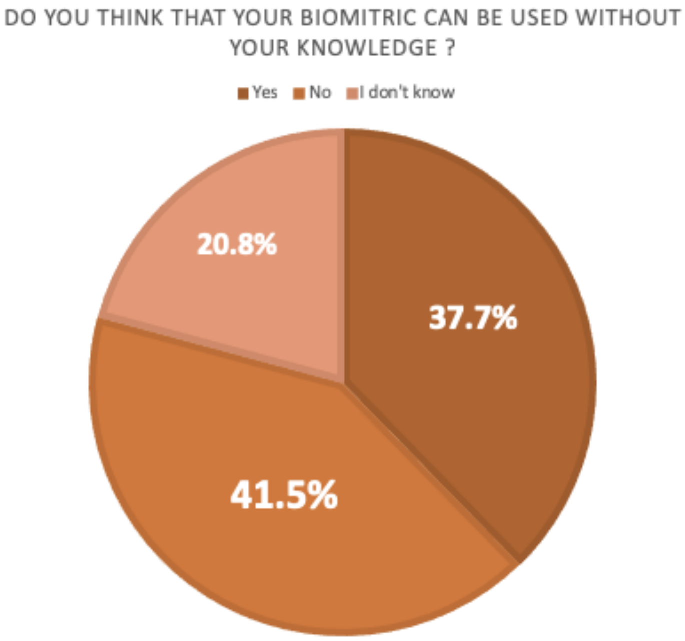

Fig. 5.

Question 6: “Do you use your biometric on daily basis?”
About 78.7% answered Yes and 11.6% answered No and 9.7% answered Sometimes shown in the figure 6:

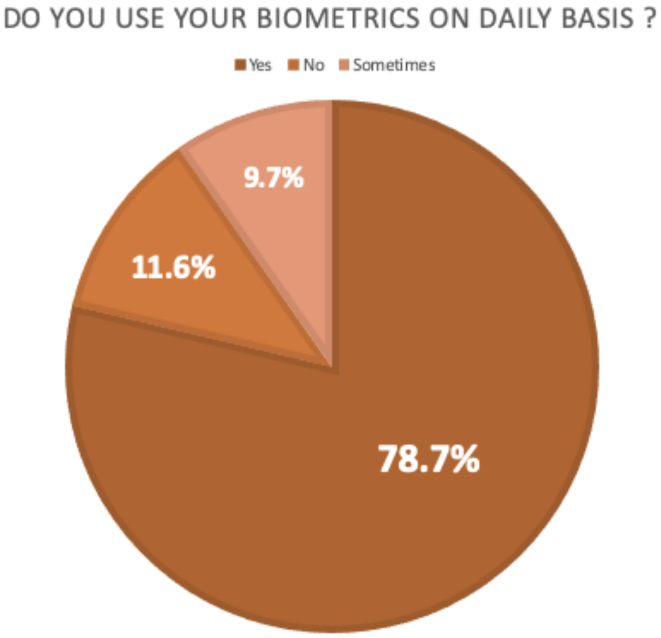

Fig. 6.

Question 7:" Is using biometric identification in your daily life necessary?"

About 52.7% answered Yes ,28.5% answered No, and 18.8% answered sometime as shown in figure 7:

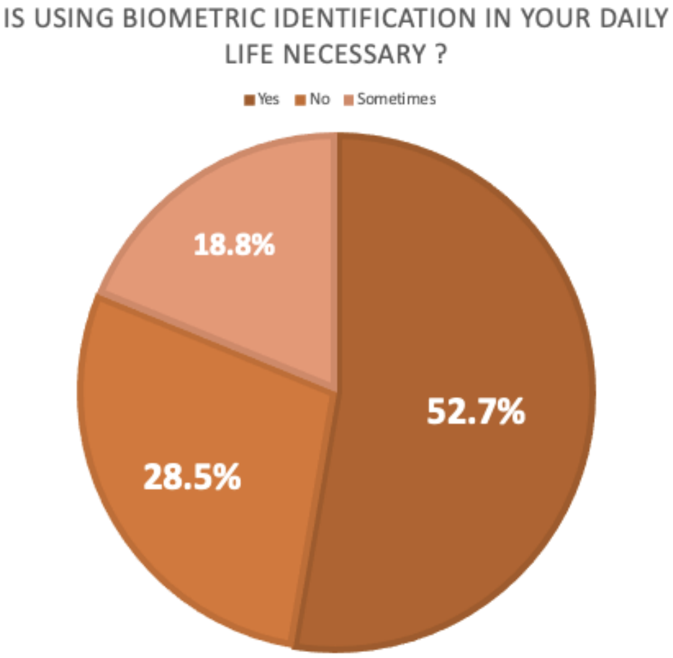

Fig. 7.

Question 8: " Do you think there is a possibility for an error to occur while identifying your biometrics?"

About 55.6% answered Yes ,34.3% answered No, and 10.1% answered Sometimes as shown in figure 8:

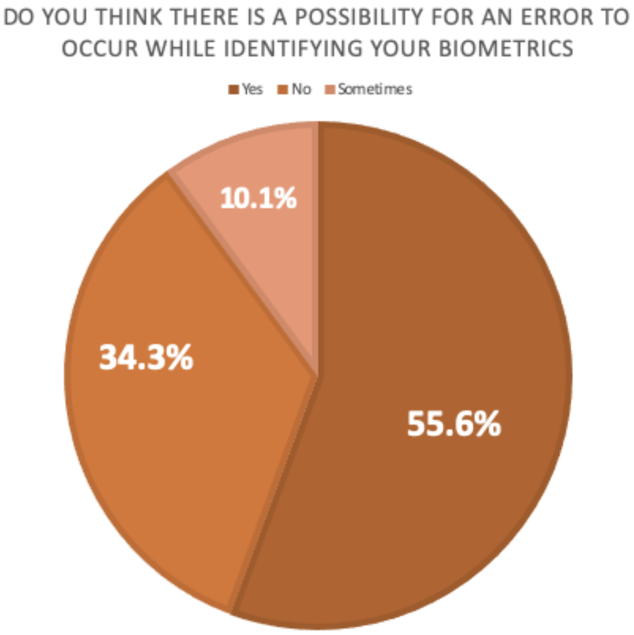

Fig. 8.

Question 9: “Do you allow using your biometrics for identification to big companies or small companies?"

About 90.3% of people would allow Big/ popular companies to use their biometrics, and 28.5% of the people would allow small/ unpopular companies to use their biometrics as shown in figure 9:

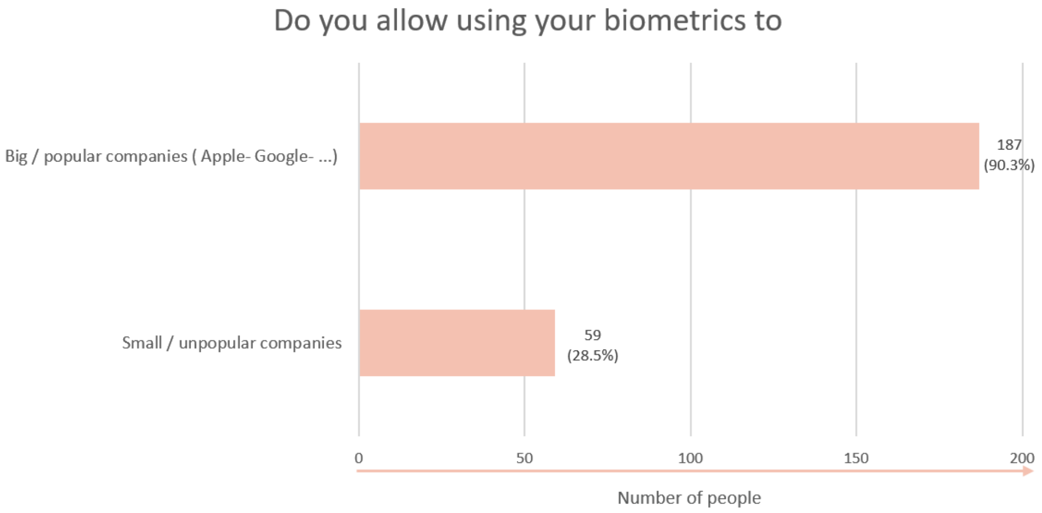

Fig. 9.

Question 10: “Do you think biometric identification will be used as your national ID in the future?”

About 86.8% of people answered Yes, 6.3% answered No , 6.9% answered I don't know as shown in figure 10:

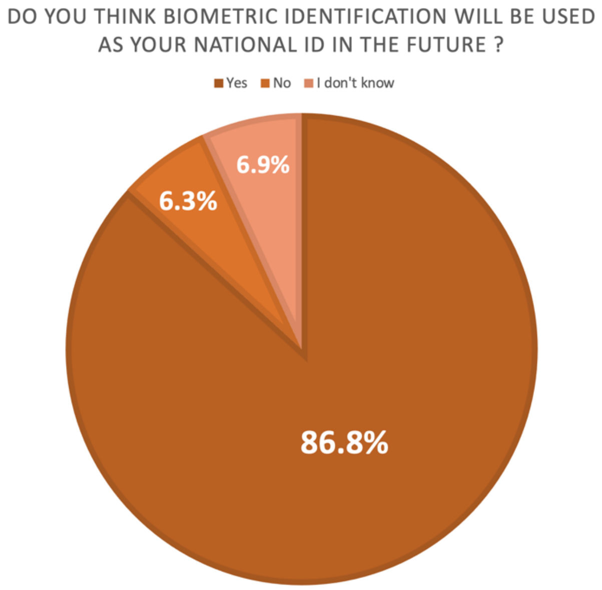

Fig. 10.

Question 11: “Does the future of biometric identification concern you in terms of privacy ?” About 41.1% of people answered Yes, 43.5% answered No, 15.5% answered I don't care as shown in figure 11:

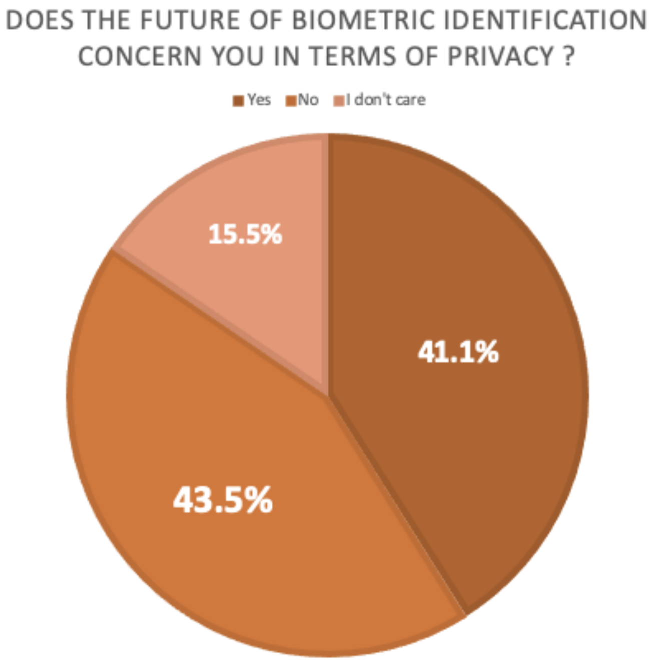

Fig. 11.

Discussion

The majority of the sample prefer to use their biometrics to log in to their devices , the result might be influenced by the fact that the usage of mobile devices like smartphones, tablet PCs, laptops, and other portable devices are increasing and its used by the users on their daily basis, such devices enforce users to use biometric methods such as fingerprint recognition and face recognition since these methods are embedded in mobile phones and electronics. Biometric identification technology is easy to use and it saves the users time, it has many advantages such that its more secure than other identification methods, since it cannot be lost and forgotten, thus it indicates the reason why the majority of the sample feels comfortable using biometric identification.

Most of the sample sees that biometric identification is more secure than passwords, which indicates that people are aware of the consequences of using passwords to secure personal data, since passwords can be forgotten, shared or observed easily in contrast biometric identification is more secure since it's based on human characteristics which cannot be forgotten, shared or observed. Organizations and companies can share or sell peoples biometrics to third parties since we cannot guarantee that the organization and companies will follow the customer privacy policy, thus there is a possibility of having an impact on your privacy by using your biometrics. The result shows that part of the sample think that using biometric identification might affect their privacy, and it shows that they are aware of the possible impact of biometrics on their privacy, also the result shows that the majority of the sample think that their biometrics cannot be used without their knowledge, since any organization or company can use your biometrics to gain money by selling it to third parties, thus it shows that the majority of the sample are not aware of the possibility of using their biometrics without their knowledge. Mobile phones have become a necessity for many people, because they allow users to store data . Pictures, text and audio can be stored on many mobile phones .This enables users to carry their files around wherever they go, ensuring that they are always with their important documents for work or their personal life, with all these advantages, people use their mobile phones on their daily basis and since mobile phones contain biometrics features such as fingerprint recognition and face ID recognition, we conclude that this what makes the majority of the sample use their biometrics on their daily life and why they think it is necessary to use biometric identification on their daily basis. The result shows that the majority of the sample think that there is a possibility for an error to occur while using their biometrics, since every technology that has a biometric identification system installed in it, can make two kinds of errors which are the false accept, in which the device accepts an unauthorized person, and the false reject, in which the device falsely rejects an authorized person, we conclude that the majority of the sample are aware of the accuracy issue in biometric identification technologies. Majority of the sample allow using their biometrics in popular companies over unpopular companies. Many people hesitate to provide their biometrics to unauthorized or small/unpopular companies because they don’t trust them enough or they don’t think they have strong system that protects their biometrics, unlike big/popular companies where people feel more safe and comfortable knowing they are a trustworthy companies, which indicates why majority of the sample chose big companies over small companies. Most of the sample think that biometric identification will be used as their national ID in the future, since many countries are now “modernizing” their ID databases to include biometric identifiers that authenticate or verify identity based on physical characteristics such as fingerprints, iris, face and palm prints, gait, voice and DNA, to use the biometrics rather than the national id in the future, which indicates that the majority of the sample are aware of the biometric identification role in the future. The result indicates that the majority of the sample has not any concerns about the future of biometrics in terms of privacy, since biometrics are hard to get lost, compromised or shared people tend to feel more secure which is why most of the majority don’t have any concerns in terms of privacy in the future. Although biometrics are hard to get lost, compromised or shared, the consequences of stealing or using your biometrics without your consent is possible and very dangerous since we can't change our biometrics.

Literature review

"Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioral attributes of the person." [1] .

Biometric identification technology is a system that has four main modules:

a sensor module, a quality assessment and feature extraction module, a matching module, and a database module. The sensor module is a technology like camera is used to read or scan the raw biometric data of an individual. The quality assessment assesses the biometric data that has been scanned or read by sensor to determine its suitability for further processing. The matching module are features that compared against the templates to generate match scores. The database module the database acts as the repository of biometric information, during the enrollment process, the feature set extracted from the raw biometric sample is stored in the database [1] .

Types of biometrics:

A biometric identifier is one that is related to intrinsic human characteristics. They fall roughly into two categories: physical identifiers and behavioral identifiers.

1)Physical identifiers are:

-Chemical composition of body odor.

- Facial features and thermal emissions.

-Features of the eye.

-Retina and iris.

- Fingerprints.

-Hand geometry.

-Skin pores.

-Wrist/Hand veins.

2)Personal traits:

- Handwritten signature.

-Keystrokes or typing.

-Voiceprint.

[2], [3], [4], [5] .

Of these, only three of the physical characteristics and personal traits currently used for biometrics are considered truly unique: the retina, the iris, and fingerprints [6] .

Biometric Applications:

There are numerous applications for the use of Biometric Technology, "The influence of biometric technology has spread to all continents on the globe” [7]. the most common ones are as follows:

1) Commercial applications such as computer network login, electronic data security, e-commerce, Internet access, ATM or credit card use, physical access control, mobile phone, PDA, medical records management, distance learning, etc.

2) Government applications such as national ID card, managing inmates in a correctional facility, driver’s license, social security, welfare-disbursement, border control, passport control, etc.

3) Forensic applications such as corpse identification, criminal investigation, parenthood determination, etc. [1]

Privacy Concerns:

-Biometric information (especially raw images) can expose sensitive information such as information about one’s health, racial or ethnic origin and this information can then provide a basis for unjustified discrimination of the individual data subjects [8].

-Biometric data are unique identifiers but are not secret: fingerprint is leaved on everything we touch, faces can be easily acquired, and voice can be simply recorded. Hence, the potential collection and use of biometric data without knowledge of its owner, without his/her consent or personal control make this information very sensitive [9].

- The linkage problem which means the possibility to cross matched data across different services or applications by comparing biometric references is another privacy concern. The uniqueness of biometric characteristics allows an intruder to link users between different databases, enabling violations as tracking and profiling individuals.

- The inherent irrevocability of biometric features in case of data misuse like database compromise or identity theft makes biometrics very sensitive [10].

- Information obtained: it is possible that some biometrics might capture more than just mere identification information. Information about a person’s health and medical history might also be incidentally obtained. Recent scientific research suggests that fingerprints and finger imaging might disclose medical information about a person [11].

Security of Biometric:

Biometric security devices have a lot of patterns the iris or retina, fingerprint and voice pattern. With biometrics, it can be more difficult to the hackers to reach to the information. Security currently is much better and stronger than the old security which is wasn't strong enough to protect our information, so it was much easier to be hacked [12]. Usually a PC consist of processing hardware and special hardware, the special hardware part consists of a sensor, which is connected to the processing hardware. The two pieces cause the danger of an attack. We can use encrypt methods from biometric attribute with a different private cryptographic key [13]. When the information of our biometric have been attacked we can't change it is stable information, when your biometric is stolen or lost everyone can use it also your biometric is not secret since the fingerprint could be left on the table for example. In contrast you can change your password, but you can't change your biometric [14].

Conclusion

The results shows that the sample is partially aware of the biometrics impact on privacy and security , since most of the sample sees that using biometrics is more secure than using passwords , it indicates that the sample is aware of biometric effect on security, also the sample thinks that using their biometrics as an identification method might affect their privacy ،which indicates that the sample is aware of biometrics impact on their privacy. The result also shows that the majority of the sample thinks that while using their biometrics there is a possibility of errors to occur which indicates that the sample is aware of some possible security and privacy risks that biometrics can cause to an individual. We found that part of the sample is not aware of possible security and privacy interventions since they think that their biometrics can't be used without their knowledge.

References

[1] A. K. Jain, P. Flynn and A. A. Ross, Handbook of Biometrics, New York: Springer Science+Business Media, 2008.

[2] R. Chandrasekaran, "Brave new whorl: ID systems using the human body are here, but privacy issues persist,," *Washington Post,* 30 Mar 1997.

[3] F. James, "Body scans could make ID process truly personal,," *Chicago Tribune,* 4 June 1997.

[4] B. Miller, "Everything you need to know about automated biometric identification,," *Security Technol. Design,* Apr 1997.

[5] B. Carter, "Biometric technologies, what they are and how they work,," Proc. CTST'97, Orlando, FL, 1997.

[6] D. R. Richards, "Rules of thumb for biometric systems,," *Security Manage.,* 1 Oct 1995.

[7] G. Roethenbaugh, "Biometrics: A global perspective,," Proc. BiometriCon'97 Conf., Arlington, VA, 1997.

[8] E. Mordini and S. Massari, "Body, biometrics and identity," *Blackwell,* 14 Oct 2008.

[9] B. Schneier, "Biometrics: Uses and Abuses," Communications of the ACM, Aug 1999. [Online]. Available: https://www.schneier.com/essays/archives/1999/08/biometrics_uses_and.html. [Accessed 27 Nov 2019].

[10] R. Belguechi, E. Cherrier, V. Alimi, C. Rosenberger and P. Lacharme, "An Overview on Privacy Preserving Biometrics," in *Recent Application in Biometrics*, France, IntechOpen, 2011.

[11] J. D. WOODWARD, "Biometrics: Privacy's Foe or Privacy's Friend?," *Proceedings of the IEEE,* vol. 85, no. 9, pp. 1480 - 1492, 1997.

[12] S. Guennouni, A. Mansouri and A. Ahaitouf, "Biometric Systems and Their Applications," 1 Mar 2019. [Online]. Available: https://www.intechopen.com/online-first/biometric-systems-and-their-applications. [Accessed 27 Nov 2019].

[13] F. Orság and M. Drahanský, "Biometric Security Systems: Fingerprint and Speech Technology," in *Indian International Conference on Artificial Intelligence*, Czech Republic, 2003.

[14] W. Yang , S. Wang , J. Hu , G. Zheng and C. Valli, "Security and Accuracy of Fingerprint-Based Biometrics: A Review," *Symmetry,* 2019.