المجلة الإلكترونية الشاملة متعددة التخصصات
العدد الثالث والعشرون شهر (٤) ٢٠٢٠

BIOMETRIC AUTHENTICATION SYSTEMS TOWARDS SECURE AND PRIVACY IDENTIFICATION: A REVIEW

Ebtesam H Alharbi[1], Maryam M. Alahrbi[2]
Taibah University, College of Computer Science and Engineering, Department of Information Systems

Contact: tu4160203@taibahu.edu.sa[1], mamrai@taibahu.edu.sa[2]

***Abstract*:**
Biometrics uses techniques for body measurements and calculations, as they are measures related to human characteristics. Biometrics authentication is used in computer science as a form of identification and access control. It is also used to identify individuals in controlled groups.
Biometrics is a new anti-fraud feature within its mobile operating system, which makes biometric authentication mechanisms more secure than ever, as biometric authentication technologies improve the process of unlocking devices and applications by making them faster and safer.
This study came to show the big view of biometric authentication technology. This paper indicated that there are many types of biometric measurements such as fingerprints, iris reader or face recognition techniques, that biometric measurements have been used in many applications, in addition to studies that indicate that the future of biometric measurements is blooming because it will become more accurate and speed in the future.
Keywords: Biometrics authentication systems, fingerprints, face recognition, iris, application of biometric.

I. INTRODUCTION

There are innumerable our own traits that can make each of us a unique person, such as our physical traits, home address, birth date, our relationships, and our acquaintances. The uniqueness of our physical and personality traits is what we usually consider "our identity" [1].

In our current interconnected world in which computers are used in all fields, there are increasing benefits for properly connecting digital information to the individual and confirming our identity in a way that can communicate and be trusted. Our identity can be used simply to properly link some of our information which is useful for some purposes in the future (such as medical or financial records). But these types of records also enable us to demonstrate a historical pattern of behavior towards trust building, thereby imposing personal accountability [2].

Our personal names and numbers provide a relatively effective way to represent our identity and times have proven their efficiency as well. More importantly, it can be explained not only by people but also by computers to connect digital information and the attributes of trust or not trust us, which is clearly beneficial for many applications. For example, school record indicators, over speed receipt, and credit

history do this. But our names and numbers are only effective if they are unique, permanent, consistent and uniquely related to us. We know that names are not necessarily unique. Here, the importance of modern biometrics appears [3].

Biometrics are the physical (and behavioral) features that uniquely identify us, and which devices can feel practically and be interpreted by computers so that they can be used as a substitute for our physical bodies in the world of digital technology. In this way, we can link digital data to our identity permanently, consistently and unambiguously, and we can retrieve that data using computers in an automated and rapid manner [4].

The word Biometrics is taken from the Greek bios meaning life, and metron or metrikos means measurement and the old meaning of biometrics refers to the application of statistical and mathematical methods to data analysis in biological sciences. Now the term also refers to techniques for identifying individuals through biological features found in the body [or behavioral such as fingerprint, iris and retina, sound, and signature to distinguish a person from the rest of the people we may use biometrics consciously or unconsciously, sometimes describing someone as a "boy tall with brown hair "or" short girl with blond hair and blue eyes. Thus, we use biometrics to identify people based on their physical characteristics (Guruprasad) [5].

In view of the wide interest in biometrics and its importance in determining personal identity, this study aims to determine the current status of biometric authentication systems and techniques and what is the future and challenges of this technology.

Biometrics are techniques that determine the identity of individuals through the biological characteristics present in the body or behavioral to distinguish a person from the rest of the people, as the use of biometrics technology has existed since the beginning of the twentieth century but was focused only on criminal and military actors, and by the end of the century the private sector began and the rest Public sector agencies in realizing the advantages of using biometrics and its importance in maintaining information security, as this study came with the aim of determining the current status of biometric authentication systems and technologies and what is the future and challenges of this technology.

In order to achieve the study goals, it is necessary to answer the following questions:

1- What are the types of biometrics?
2- What are the applications of biometrics in the current days?
3- What is the future and challenges of biometrics?
4- What are the attacks of biometrics on biometrics authentication systems?

This paper is organized as follows: The literature Review of biometrics is presented in Section II. The methods of the biometric system are described in Section III. Section IV discusses the applications of biometrics authentication systems in currents days. Section V discusses the potential attacks for biometric authentication systems. Section VI discusses the future and challenges of biometrics. Section VII presents the conclusions.

II. LITERATURE REVIEW

The Biometric authentication technology is considered one of the most important applications for achieving reliability and safety, as this study came with the aim of building a model that has a high ability to determine the effectiveness of users' acceptance of biometric authentication, and its application to the electronic health system, and the descriptive and experimental approach was adopted to study the study goals, The descriptive approach was carried out by distributing the questionnaire to a sample of study members, to provide a comprehensive view of the ease of use of the system from the viewpoint of end users, and after building the model for the system[6].

The results showed that users benefited greatly from this system, as privacy concerns decreased, security concerns, and they were more motivating and positive towards the use of biometric reliability, it is an important and accurate tool that must be adopted in electronic health systems. Also, the results also indicated the need for users to understand the importance of this model, and to ensure the accuracy of the information to stimulate the use of biometric authentication, in addition to the need to use technologies that improve the system privacy and the quality of information [6].

They mentioned about the cells in the brain use low levels of electrical energy to communicate with each other. The electrocardiogram measures this electrical energy over time, as the electrical activity of the brain appears as wavy lines on a computer screen [7].

As the signals resulting from the electrocardiogram are linked to the headphone, as it is considered one of the most important challenges facing it and harming low generalization by users, as this study aimed to use biometric validation in the electrocardiogram planning that is done through the evaluation of tracking eye movement depending on Headphones, as a new model was built that uses these images of the eye,

Therefore, SVM technique was used with a linear nucleus, and after building the model more results were obtained than conventional and individual methods. It is noted that this study presented positive results.

Latest technology in the field of fingerprints is the AFIS automatic fingerprint system (AOUTOMATED FINGERPRINT IDENTIFICATION SYSTEM). Which is one of the most available and widespread techniques, and it has entered the system to achieve the human personality in the criminal and civil fields, it is the system that analyzes and compares the characteristics of fingerprints that differ from one person to another and through which the identity of the person can be identified. This research aims to use the automatic fingerprint system (AFIS) to identify the unidentified dead in Khartoum State. Where the following results were obtained [8]:

1. Fingerprints are a definitive and distinctive guide to the human personality and have become internationally the best way to identify people.

2. Fingerprints are one of the most important methods used to identify unidentified dead people.

3. AFIS is the ultimate fingerprint identification system.

4. AFIS is the system used to identify fingerprints in Sudan in the criminal and civil fields in both the General Department of Criminal Evidence and the General Administration of Civil Registry.

5. The fingerprints saved in the identity verification database are limited and insufficient to identify unidentified persons, as they only include the fingerprints of the accused and the courts.

6. More than 60% of the unidentified dead people in Sudan have identification documents and personal documents, which means that they can have national numbers and fingerprints stored in the civil registry system. More than 20% of them are homeless and anonymous who may have fingerprints saved in the personal identification database.

There is no complete crime in light of this progress and scientific development that if it entered all the judicial systems in the world, it would contribute to reducing crime and eliminating it. As this study came with the aim of shedding light on modern scientific evidence, and drawing attention to the importance of this modern evidence in achieving justice, and to avoid defects that may be attached to judicial decisions issued in this field, explaining the role of the genetic fingerprint of the biological evidence conclusive for the identification of human identity, in The Jordanian legal system has lost its court applications within the Hashemite Kingdom of Jordan. The researcher concluded that the genetic fingerprint is one of the modern scientific methods in forensic evidence, and it is not only a guide to conviction but also the innocence of the accused, and the evidence derived from the analysis of the genetic fingerprint has its value and evident strength established on scientific and technical grounds, the trends of the judiciary varied in the extent of acceptance of the fingerprint genetics as proof of proof, the direction of the Arab judiciary is based on considering the genetic fingerprint as an auxiliary guide that helps the judge to form his faith, unlike the foreign judiciary, which relies on the genetic fingerprint as evidence for evidence in judicial disputes regarding proof of filiation, and other issues[9].

III. METHODS OF BIOMETRICS

There are a variety of biometrics that can be used to verify identity .Biometrics are considered as an automated way to get to know a person based on physiological which is based on the individual and unique static person characteristics such as fingerprint ,Face recognition ,iris and DNA and behavioral method which is based on dynamic characteristics such as stroke, voice recognition, handwriting ,mouse movement, lip motion and gait. Figure 1 shows the classification of biometric authentication methods.

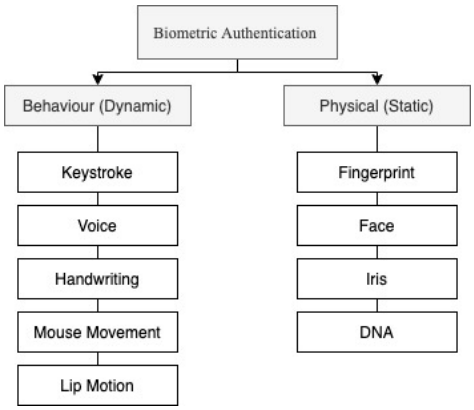

Figure 1: Biometrics authentication methods

The following are the most important of methods of physiological parameters:

A. Fingerprint

Figure 2: Fingerprints

Fingerprints are prominent bumps in the skin of the skin that are adjacent to depressions, making the process of holding things easier and everyone has a unique shape of their fingerprint. And it has been proven that the fingerprint can't be identical and identical in two people in the world even the identical twins that originate from one egg, and these lines leave their impact on every object they touch and on smooth surfaces in particular [10].

In general, there are 120 fingerprint recognition points that can be programmed within the computer, which will be used to match the fingerprint with the fingerprints stored in the database, the process of matching fingerprints does not take place throughout the fingerprint; because this requires high energy, and it will be easy to steal the printed data. In addition, the dirt or the process of deformation of the finger leads to a mismatch of two images of the same fingerprint, so it is an impractical method. Instead, most fingerprint systems do the comparison. Among the features of the fingerprint, this method is known as detail (minutiae.) The human and computer investigator focuses on the points at which the protrusion line

ends or when a protrusion separates into two (bifurcations). These distinct features are usually called typical [11][12].

The rapid technological development of mankind has produced many modern technologies that some people are still afraid to cause a direct or indirect impact on his health and safety, including the "fingerprint" technique, and because it is one of the methods that help governmental and private bodies and institutions in controlling the presence of The departure of its employees, those institutions have used finger technology as a basis for control systems to record attendance and leave from different workplaces [13].

B. Retina Recognition

The retina recognition is defined as the retina which is related to recording and analyzing the forms of blood veins in the nerve in the background of the eyeball, which treats the light inside through the human eye. The person should be very close to the lenses of the retinal scanning device, staring directly at the lenses, and remaining quiet during the passage of light inside the human being's eye, and any movement of the person may require re-operation from the beginning, and one of the most important advantages of defining the retina is that its forms are very distinct, and each eye has A unique shape of the blood vessels; even the eyes of identical twins are different [14][15].

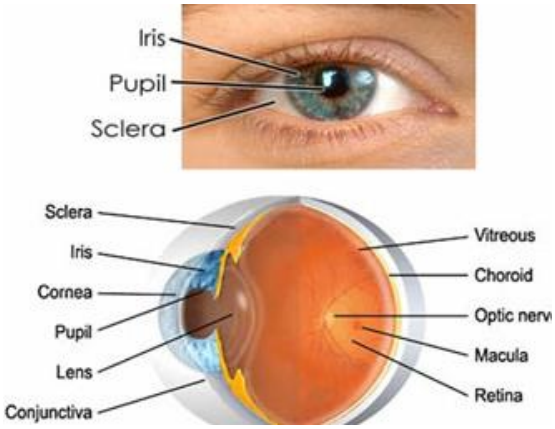

Figure 3: Fingerprints

C. Facial recognition

Facial recognition and [identification by image] are another widespread use of biometrics. This type of identification is used worldwide for important cases, such as international passports, and cases containing names [16].

The facial recognition system depends on recognizing the structure of the face, the distances between the eye, nose, mouth, ... etc are unique in a person and the opportunity to repeat them in another person is very rare. Facial recognition is a mapping of a person's face and reminds the basic data about the

circumference of the face and the distances between its components and when scanning an attempt is made to search for the closest matching, and there are more than 80 points in the structure of the face that can be used to define the face unambiguously. Different systems usually do not use all of these points, but they analyze a small number of them by analyzing the distances between the points. Facial imaging is affected by many factors, including lighting, angle of shooting, the distance between the imaging device and the person, and the quality of the imaging device [16].

Years ago, Apple relied on the iPhone and iPad fingerprint protection feature, this feature that ensured great protection for users 'devices, but the new, Apple introduced a new feature, which is the face recognition feature, or what it called the Face ID, of course it is safe, and this is an example One, like the owner of the device is asleep, can anyone carry the device and put the owner's finger to open it. In short, this feature comes to depend on the face fingerprint to determine the identity of the owner of the device, and protect the device from any use without its owner, but the Face ID feature prevents this, as no one can open the device except its owner, and the eyes must be open, so this example gives us how capable This feature protects the device *[16]*.

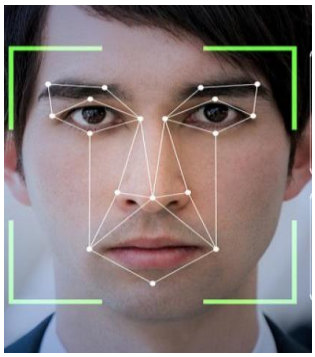

Figure 4: Facial recognition

D. DNA

DNA is most effective static techniques to identify the individual identity. For reasons of computation time it can't be used for access control and because the individual would not be prepared to take a little blood to perform the identification. Hence, the choice of the modality depends on the application being used. The fact is that biometrics is the protection industry's future and is rapidly being accepted as the market's most reliable identity technology. User behavioral properties usually show continuity in the time domain. Extraction of attributes is a crucial stage in verification for the collection in behavioral data gathered. The following are the most important of methods of behavioral parameters [17].

E. Keystroke Recognition

Keystroke patterns in behavioral features move through certain constraints that authenticate apps by calculating and assessing app timing typing on physical platforms such as cell phones or machine keyboards [18].

The typing functionality can be reached simply by inputting the personal password without any extra hardware, making it incredibly simple to install and can be built into the standard password-only authentication framework to improve its protection.[18].

Keystroke dynamics has drawn many researchers in this area today, due to the benefits of low-cost, easy-to-integrate and high-security work.

F. Voice recognition

Each individual in the world has a specific voice pattern, even if the variations are subtle and barely visible to the human ear. At the other side, for unique speech recognition technology, certain moments of difference in each person's voice may be observed, heard and verified to enable access to an entity with a sound pitch that is right and at the same time a volume standard. Surprisingly, it can be successful in differentiating two individuals who have nearly similar voice habits [19].

G. Handwriting

Handwriting verification may be achieved with digital products such as pen tablet or touch screens. In fact, a handwriting signature has developed into an IT-devices symbol. Nowadays, finger movement is simple to catch as touch panels are becoming common and inexpensive.

One such example is a handwriting sign. Personal identification, frequency, and pressure characteristics are used in this system for personal recognition, which are biometric details. Those characteristics *c*an't be modified when the same individual writes the same message [20].

H. Mouse Movement

Another important part of biometric security is the nature of the device, which is great for intrusion prevention, in addition to access control. Mouse Dynamics Signature or MDS uses the factors, a specific set of values which characterize the behavior of the user over the monitoring period. Many considerations combine in the measurement of the average speed against the distance travelled or in the measurement of the average speed against the direction of movement. A total of seven factors exhibiting high stability and uniqueness are recorded.

Many network threats against mechanisms such as stealing of sensitive documents, insider net misuse and unauthorized access are among the top 5 losses. The number of compromised systems has risen to the point that such exposure is not really known and there is a need to find methods of defending networks other than passwords. Biometric study has been extensive, but no progress has been produced. The Research with Multimodal Biometrics reveals identification principles use specific characteristics. Two

biometrics styles which are both physiological and behavioral. Physiological evidence is fingerprint, and human keystroke dynamics. Two of the security access techniques *c*an't be left behind by the users [21].

I. Lip motion

Lip motions require complex muscle and bone synchronization during speaking period. When creating specific vowels in voice, the upper and lower lips develop various forms, as shown in Fig. 5. When talking the lip formation varies, resulting in motion of the mouth. The composition of the lip-related muscles and bones depends on the individual, contributing to slight variations between lip-shaped individuals. In addition, individuals' special, speaking ways often produce various forms of lip movement. The unique features of lip motions may therefore be used as the biometrics for user authentication.

Multimodal biometrics verification on devices, which addresses the deficiencies of the initial schemes by incorporating the benefits of lip and speech gestures. At the same moment, Multimodal biometrics verification detects these two biometrics on smartphones with the built-in audio tools and fuses them to data point. The secure and efficient authentication features are then extracted from the fused data [22].
Lip is one of those biometric features with strong universality, reliability, longevity, and measurability, and its efficiency and acceptability as a biometric feature should improve as more and more work is being carried out in the area.

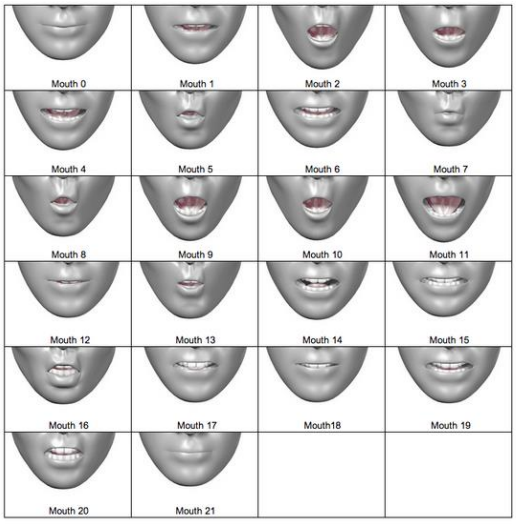

Figure 5: lip motion

IV. APPLICATIONS OF BIOMETRICS

A. Airport Security

Thousands of people travel through the airport terminals, so it can be very difficult to distinguish these travelers. Biometric equipment to check the identification of travelers is already being utilized in many airports across the world.

The best option for immigration control is iris recognition at several airports and to apply to utilize iris recognition, passengers must first get their iris and face recorded by a camera in a registration process.

Such records are collected and include special information that are preserved in a global database. The database is also used for the identity checking of travelers at entry and exit locations. The validation is first achieved by enabling the camera to record the iris and then use a software system to fit what's contained in the database.

Employment monitoring has been a concern in companies with thousands of workers and the usage of biometrics has been implemented to reliably measure the hours spent employed as well as the performance of the staff. A biometric time and attendance system are implemented in this scenario and offers an automatic mechanism for identifying workers based on both physiological and behavioral features. Different characteristics may be included, but ears, fingerprints, finger veins, palm veins, irises and speech patterns are the most important types used for employee recognition. Verification is achieved by requiring an individual to attempt biological character recognition, instead a biometric hardware tool to match the current catch or check to the established one in the database. Recently, government agencies and organizations are beginning to adopt this type of biometrics to ensure prompt staff attendance as well as payroll estimates [23].

B. Law Enforcement

Organizations such as the Federal Bureau of Police (FBI) often utilize biometrics. It may be used to classify offenders. It is also commonly used by goal and correctional administration because it offers a mechanism that can handle inmate identities efficiently and securely [23].

C. Access Control

Access control is one other field that may be incorporated with biometrics. Indeed, the primary explanation behind enterprise as well as employees is the introduction of biometric technologies primarily for access control as well as Single Sign On (SSO) is attributed to the reality and awareness that passwords are inadequate for personal recognition. The result of this is that password is merely evidence of information or truth. In the case of biometrics, it provides a special benefit simply by focusing on person being known by who they are and not just by whom you know. Home Access Protection, Cell Phone Connection, and Vehicle Access Security demonstrate the impact of this [23].

D. Banking

International banking has expanded globally and most of the finance companies are digitally focused. The result of this is that banks are introducing biometric technologies to further enhance control of client

and employee identification. The purpose for this was to help reduce theft as well as improve the protection of purchases through various networks and also improve customer experience [23].

V. ATTACKS ON BIOMETRICS AUTHENTICATION SYSTEM

Biometric applications are exposed to multiple potential attacks and can be executed in various threats. There is no evidence that a malware attack on biometric systems poses a major security risk which may result in a major reduction in system performance. Here, therefore, you identify and differentiate many attack points in the biometric authentication system, and take countermeasures in developing the biometric method and deter different attacks in the biometrics system, and the types of attacks identified are as follows:

A. Faking the sensor:

Sensor counterfeiting with the implementation of new technologies, today different hackers have provided fake biometric sensor samples to access biometric applications such as false iris face picture or fake silicone fingerprints, fake individual voices, etc. Unlike conventional network systems, biometric authentication systems are more vulnerable to these attacks by changing actual biometric features [24].

B. Masquerade attack

Composite images have been shown to be from fingerprint templates to provide the matching method. The object may look like a real image. This attack thus poses a significant challenge to remote authentication systems. It saves a lot of hackers and makes their job easier. They don't have to trouble with accurate biometric samples. Access to models saved on the remote server is what they require [24].

C. Resend biometric signals

This form of attack will override the sensor and restart the device signals that have already been registered. Data between the sensor and the processing system or application is injected or into the biometrics system. This occurs in three steps, This will begin registration and authentication details, and can network eavesdropping to steal biometric information Instead, after reaching the second stage, the attacker can reload the biometric information on the next authentication to complete the biometric reload attack on the next authentication which generates the third stage with the restart threat [24].

D. Simulation feature set

The code spoofing is named replacing a feature set with a falsified or updated one. Typically, such forms of plagiarism attacks are used to target different networks and distribute programs that rely on sensitive information [24].

E. Template attacks

Templates reflect a collection of influential functions that describe biometric details (signals) of individuals. If fraudsters deal safely with databases through inserting fresh templates, removing established templates or changing templates to get a higher degree of authentication irrespective of the picture shown on the server. Database templates may be substituted, robbed or even changed .Therefore, by minimizing the output of two program users, the number of systems is decreased, but this is because the design is covered by automated structures (such as watermarks, secret data, etc.), it is not easy to target the program database as it needs certain knowledge of the system's internal activity [24].

F. Trojan attack

The function extractor itself can be substituted in a Trojan attack by rendering the necessary features and such features back to the current database. Fraudulent identification technology has been an integral aspect of biometric recognition systems and with people growing involved in protection it is crucial to recognize, track and minimize biometric attacks [24].

After examining these attack points, the analyst found that much of the time the attacker targets the models to be contained in the database. Through inserting additional templates to the database, changing current templates in the database, and deleting old templates from the database, these templates that are stored in the database can be changed.[24][25].

VI. FUTURE OF BIOMETRICS

Standards allow the effective development of biometrics systems to establish common rules and set guidelines for protecting confidentiality. Reaching agreements on data format and application software will help reduce systems development costs. Moreover, setting standards for the application of biometrics and testing their accuracy will contribute to clarifying vulnerabilities and lead the search for countermeasures for penetration.

The characteristics of biometrics are comprehensive and unique, they should also be reasonably sustainable and easy to collect and measure. The biometrics system should provide accurate results in varying environmental conditions, and it should be difficult to defraud and deceive. Perhaps the most critical aspect of the biometrics system is the general public's acceptance of it. For obvious reasons, non-intrusive methods are more acceptable than intrusive techniques. Although genetic fingerprinting is the primary and final method for identifying a person (except for cases of identical twins), DNA fingerprint matching is too complex to be widely applied to verification and verification. As for the method based on measuring the temperature of the blood that passes in the blood vessels and is emitted from the skin of the face, although it does not involve breaking into the privacy of the individual, it is very expensive. Among the biometrics considered for future use are pulse velocity, body odor, skin composition, fingernails, walking style and ear shape. Further research is required to ensure the proper use of any of these features in biometrics [23][24].

In addition, business operations will be affected by biometrics, which will really affect the future. But we find that in recent years, business operations depend on specific steps in particular, all of which require validation or Verifications, we mention it here in a brief way, verifications of this information may be made at arrival or tracking usage, even log in or out. By fully integrating biometric technology with business operations, the workload can be greatly simplified. This effect is saved at the time of implementation, which saves operating costs.

Today, it can be used as fingerprint cell phones or face recognition. In the soon of future it may turn to speech recognition entirely on the mobile phone and it is only accessible when the real owner talks to the phone. This is because two people can't have the same voice, this also increases personal safety.

Biometrics technology can now be used to access the engine and start it. For example, if a car owner must use voice commands to access his vehicle's operation, a small change in tone is not enough to start and control the vehicle.

Thanks to this biometric technology, the owner can only start the engine with the user's personal settings. This may include temperature control, chair position, direction of wheel, and motivation operate specific radio station and type of music being played.

On the other hand, due to privacy issues and personal data violations, users are concerned about the safety of their mobile devices. The cost of authentication should be taken into account in a limited-source computing device, we find that most mobile devices have limited resources in terms of storage space, electricity, computing power, etc.

Therefore, biometric authentication of advanced methods and algorithms that can be implemented in computing devices must be studied.

Because most users store a lot of important data on them, including biometric data settings. This means that computing power must improve compared to the storage space for mobile devices (especially smartphones). These improvement and development requirements refer to the highest levels of safety for mobile phones, especially smartphones.

However, the ability to use mobile devices should not be neglected because the added security features are often complex and difficult to use, and given the fact that the maximum number of mobile device security features needs to be expanded, this has also led to problems in improving usability that also requires reducing the effort required by users to turn on security features.

shortly, it is necessary to focus on research and improve the usability of mobile devices and ensure their accuracy, which is very important because it will ensure a high degree of acceptance and adoption on a large scale among technology users as it is another focus of research and development through the design of user interfaces for interaction between the user and the device, methods data collection, design of identity verification protocols, development of biometric data processing, and appropriate algorithms. More research should be done on advanced algorithms as they also play an important role in supporting ease of use and accuracy while also taking into account privacy and security.

It can be seen from an extensive literature review conducted earlier that most research focuses on maximizing the security functions of mobile devices (especially smart devices), while ignoring the assessment of their usability in practical use.

So, it became important to focus on such few studies that are concerned with improving safety and ease of use together [25][26].

VII. CONCLUSIONS

Biometric determinants are the distinctive and measurable properties used to classify and describe individuals. Biometric properties are related to body shape. Examples include fingerprints, palm veins, facial recognition, DNA, palm print, hand geometry, iris recognition, retina, and scent. Multimedia biometrics systems use multiple sensors or biometrics to overcome the limitations of traditional multimedia biometric systems, authentication through biometric verification has become increasingly common in corporate systems, public security, consumer electronics, and point of sale applications.

As this study came to achieve three goals, which are to indicate the types of biometric measurements, to show the methods and applications in which biometric measurements are used, and to explain what the attacks and future of these measurements is.

The results indicated that there are many biometrics measurements and three types have been displayed, namely facial recognition, fingerprint and iris, as the applications are used in many different fields, and the study also indicated that there is a great demand for biometric measurements because of their positive impact in applications and accuracy in the results.

REFERENCES

[1] Vivian, "Identity: personal AND social," *Sussex Research Online : Sussex Research Online*, 15-Mar-2017. [Online]. Available: http://sro.sussex.ac.uk/id/eprint/68102/. [Accessed: 16-Apr-2020].

[2] Chang, W. H., & Liu, C. Y. "Information apparatus for playing digital content that is received from a digital content service provided over the internet." U.S. Patent Application 16/215,506. 2019.

[3] J. He and N. Jiang, "Biometric From Surface Electromyogram (sEMG): Feasibility of User Verification and Identification Based on Gesture Recognition," *Frontiers in Bioengineering and Biotechnology*, vol. 8, 2020.

[4] Giesing, Ilse (Compiler), "Biometrics", University of Pretoria.- pp. (49-76). 2003.

[5] P. Hitchcock, "Biometrics and Revolution," *Biotheory*, pp. 248–264, 2020.

[6] L. Kwao, R. Millham, and E. Opanin, "An Integrated Success Model for Adopting Biometric Authentication Technique for District Health Information Management System 2, Ghana," *International Journal of Computer Applications*, vol. 177, no. 40, pp. 1–16, 2020.

[7] "Handbook of Research on Intrusion Detection Systems," *Google*. [Online]. Available: https://books.google.com.sa/books?hl=ar&lr=&id=y8jYDwAAQBAJ&oi=fnd&pg=PA237&ots=yVnR97XWvP&sig=nquii4J5kY1kxuUv1XhtHLynYyI&redir_esc=y#v=onepage&q&f=false. [Accessed: 16-Apr-2020].

[8] O. Abdul Rahim, "The role of the automated fingerprint system (AFIS) in identifying Faceless Case study," *The National Rabat University*, 2017.

[9] Hassan. Amal." The role of modern scientific evidences in proven ". Master's degree in public law. Middle East University. law School. Department of Public Law.2012

[10] Harris, H. A., & Lee, H. C. Fingerprints and other personal identification patterns. In Introduction to Forensic Science and Criminalistics, Second Edition (pp. 117-142). CRC Press. 2019

[11] Ling, L., Huang, L., Guo, K., & Huang, H. Detection of latent fingerprints on papers. In 14th National Conference on Laser Technology and Optoelectronics (LTO 2019) (Vol. 11170, p. 111703B). International Society for Optics and Photonics. 2019

[12] F. Sadikoglu and S. Uzelaltinbulat, "Biometric Retina Identification Based on Neural Network," *2th International Conference on Application of Fuzzy Systems and Soft Computing, ICAFS 2016*, 2016.

[13] Singh, N. S., Hariharan, S., & Gupta, M. Facial Recognition Using Deep Learning. In Advances in Data Sciences, Security and Applications (pp. 375-382). Springer, Singapore. 2020. [Online] Available: https://books.google.com.sa/books?hl=ar&lr=&id=FV_BDwAAQBAJ&oi=fnd&pg=PA375&ots=A4D2-9UQKz&sig=SfLkFB0rXIc4xg0mqSpCYvebGvQ&redir_esc=y#v=onepage&q&f=false

[14] K. A. Gates, "Our biometric future: facial recognition technology and the culture of surveillance," in *Our biometric future: facial recognition technology and the culture of surveillance*, 2011.

[15] S. Wilkinson, "Artificial intelligence, facial recognition technology and data privacy," *HSTalks*. [Online]. Available: https://hstalks.com/article/5408/artificial-intelligence-facial-recognition-technol/. [Accessed: 16-Apr-2020].

[16] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, 2000, paper 11.3.4, p. 109.

[17] Himanshu Srivastva, "A Comparison Based Study on Biometrics for Human Recognition", International Journal of Computer Engineering, vol.15, pp. 22-29, 2013.

[18] K. Lv, J. Liu, and P. Tang, "'Keystroke Biometrics for Freely Typed Text Based on CNN model,'" *Site*, 2018. [Online]. Available: https://aisel.aisnet.org/pacis2018/291. [Accessed: 16-Apr-2020].

[19] K. CH, "Various Biometric Authentication Techniques: A Review," *Journal of Biometrics & Biostatistics*, 2017.

[20] S. Kamaishi and R. Uda, "Biometric Authentication by Handwriting Using Leap Motion," *Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication - IMCOM 16*, 2016.

[21] J. Handa, S. Singh and S. Saraswat, "A comparative study of Mouse and Keystroke Based Authentication," *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, 2019, pp. 670-674.

[22] L. Wu, J. Yang, M. Zhou, Y. Chen and Q. Wang, "LVID: A Multimodal Biometrics Authentication System on Smartphones," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1572-1585, 2020.

[23] A. A. Ahmed, "Future Effects and Impacts of Biometrics Integrations on Everyday Living," *Al-Mustansiriyah Journal of Science*, vol. 29, no. 3, p. 139, Oct. 2019.

[24] Z. Rui and Z. Yan, "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification," in *IEEE Access*, vol. 7, pp. 5994-6009, 2019.

[25] "Biometrics System Attacks and Security - Javatpoint," www.javatpoint.com. [Online]. Available: https://www.javatpoint.com/biometric-system-security-and-attacks. [Accessed: 15-Apr-2020].

[26] T. M. Ibrahim, S. M. Abdulhamid, A. A. Alarood, H. Chiroma, M. A. Al-Garadi, N. Rana, A. N. Muhammad, A. Abubakar, K. Haruna, and L. A. Gabralla, "Recent advances in mobile touch screen security authentication methods: A systematic literature review," Computers & Security, vol. 85, pp. 1–24, 2019