BABATOMIWA ABDULAZEEZ OMONAYAJO

ADVANCEMENTS IN BIOMETRIC TECHNOLOGY

NEU 2021

ADVANCEMENTS IN BIOMETRIC TECHNOLOGY

A THESIS SUBMITTED TO THE INSTITUTE OF GRADUATE STUDIES OF NEAR EAST UNIVERSITY

By
BABATOMIWA ABDULAZEEZ OMONAYAJO

In Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Information Systems

NICOSIA, 2021

ADVANCEMENTS IN BIOMETRIC TECHNOLOGY

A THESIS SUBMITTED TO THE INSTITUTE OF GRADUATE STUDIES OF NEAR EAST UNIVERSITY

By
BABATOMIWA ABDULAZEEZ OMONAYAJO

In Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Information Systems

NICOSIA, 2021

Babatomiwa Abdulazeez OMONAYAJO: ADVANCEMENTS IN BIOMETRIC TECHNOLOGY

Approval of Director of the Institute of Graduate Studies

Prof. Dr. KEMAL HÜSNÜ CAN BAŞER

We certify this thesis is satisfactory for the award of the degree of Master of Science in Computer Information Systems

Examining Committee in Charge:

Assoc. Prof. Dr. Boran Şekeroğlu	Committee Chairperson, Department of Information Systems Engineering, NEU
Assist. Prof. Dr. Selin Üzelaltınbulat	Department of Computer Information Systems, NEU
Assist. Prof. Dr. Damla Karagözlü	Supervisor, Department of Computer Information Systems, NEU

I hereby declare that all information in this document has been obtained and presented under academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name: Babatomiwa Abdulazeez Omonayajo

Signature: 

Date: 27/07/2021

ACKNOWLEDGEMENTS

First and foremost, I will like to thank my supervisor, Assist. Prof. Dr. Damla Karagozlu, as well as all of my lecturers, Prof. Dr. Nadire Cavus, Assoc. Prof. Dr. Fezile Ozdamli, Assist. Prof. Dr. Seren Basaran, and Assist. Prof. Dr. Sahar Ebadinezhad, for their guidance and knowledge, imparted to me during my studies at Near East University.

In addition, I want to convey my gratefulness to my fellow students in the department of computer information systems for their unwavering support in helping me finish my master's degree.

Finally, I'd like to thank my family for their continuous support and encouragement that has helped me get to this point in my life.

To my Parents…

ABSTRACT

In recent years, biometric technology has advanced fast, particularly in terms of security and identification. User authentication has historically relied on security methods such as passwords, key cards, and pin codes. Theft, on the other hand, has become more prevalent as a result of these measures. This led to the development of biometric security, in which an individual's authentication is based on attributes obtained from physiological and behavioral characteristics of a human body utilizing biometric technology. As a result, an individual's unique identity may be authenticated. A significant amount of research on biometric technology, in general, was indicated. The purpose of this research is to look into advancements in biometric technology in both medical and engineering fields. Data were collected from twenty (20) participants at the Near East University of North Cyprus using an interview survey method (15 from the medical sector and 5 from the engineering sector). The study revealed the opinions and viewpoints of the participants, demonstrating the necessity for greater knowledge and integration of biometric technology to encourage its growth in the digital age. The study's findings have the potential to motivate individuals and organizations to better integrate biometric technologies to lessen the dangers to data and identity security.

Keywords: Biometric technology; security; identification; authentication; advancement.

ÖZET

Son yıllarda biyometrik teknoloji, özellikle güvenlik ve tanımlama açısından hızla ilerlemiştir. Kullanıcı kimlik doğrulaması geçmişte parolalar, anahtar kartlar ve pin kodları gibi güvenlik yöntemlerine dayanmıştır. Hırsızlık ise bu önlemler sonucunda daha yaygın hale geldi. Bu, bir bireyin kimlik doğrulamasının biyometrik teknolojiyi kullanan bir insan vücudunun fizyolojik ve davranışsal özelliklerinden elde edilen niteliklere dayandığı biyometrik güvenliğin geliştirilmesine yol açtı. Sonuç olarak, bir bireyin benzersiz kimliği doğrulanabilir. Genel olarak biyometrik teknoloji üzerine önemli miktarda araştırma yapıldı. Bu araştırmanın amacı, hem tıp hem de mühendislik alanlarında biyometrik teknolojideki gelişmeleri incelemektir. Veriler, Kuzey Kıbrıs Yakın Doğu Üniversitesi'ndeki yirmi (20) katılımcıdan görüşme anketi yöntemiyle (15'i tıp sektöründen ve 5'i mühendislik sektöründen) toplanmıştır. Çalışma, dijital çağda büyümesini teşvik etmek için biyometrik teknolojinin daha fazla bilgi ve entegrasyonunun gerekliliğini ortaya koyan katılımcıların görüş ve bakış açılarını ortaya koydu. Çalışmanın bulguları, veri ve kimlik güvenliğine yönelik tehlikeleri azaltmak için bireyleri ve kuruluşları biyometrik teknolojileri daha iyi entegre etmeye motive etme potansiyeline sahiptir.

Anahtar Kelimeler: Biyometrik teknoloji; güvenlik; Tanılama; kimlik doğrulama; ilerleme

TABLE OF CONTENTS

CHAPTER 3: METHODOLOGY

CHAPTER 4 RESULTS AND DISCUSSION

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

FBI:	Federal Bureau of Investigation
AI	Artificial Intelligence
DNA	Deoxyribonucleic Acid
MCS	Multiple Classifier Systems
MMI	Man-Machine Interface
ID	Identity
SEM	Structural Equation Modeling
PLS	Partial Least Squares
EEG	Electroencephalogram
LSTM	Long Short-Term Memory
GRU	Gated Recurrent Unit
RNN	Recurrent Neural Networks
BLSTM	Bidirectional Long Short-Term Memory
BGRU	Bidirectional Gated Recurrent Unit
NEU	Near East University
RFID	Radio Frequency Identification
NFC	Near Field Communication
Ph.D.	Doctor of Philosophy
M.Sc.	Masters of Science

CHAPTER 1
INTRODUCTION

The first chapter presents a general motive of biometric technology including the background, problem, aim, significance and limitations of the research topic.

1.1 Background of the Study

Human society has relied on the ability to recognize people and associate personal characteristics (e.g., name, nationality, etc.) by identifying one another based on body features such as face and voice, as well as other contextual information (Jain, Ross and Nandakumar, 2011). A person's identity is made up of a set of characteristics. People settled in small societies where they could easily identify one another in the early days of civilization. However, in today's society, rapid population growth combined with increased mobility has made the development of sophisticated identity management systems necessary and capable of effectively recording, maintaining, and erasing personal identities. The growing prevalence of identity theft, as well as increased national security concerns, has emphasized the importance of having a credible identity management system that has brought about biometric authentication (Prabhakar, Pankanti and Jain, 2003). In a variety of applications, identity management is crucial in managing border crossings, limiting physical access to important infrastructure such as power plants and airports, managing logical access to services and data, conducting virtual financial businesses and administering welfare privileges are examples of such applications. Identity theft has increased as a result of the propagation of web-based services and the deployment of decentralized customer solution centres (Hu, 2013).

As states by Asha and Chellappan (2012), biometrics is the oldest method of identification and authentication, dating back to 1882, when the Federal Bureau of Investigation (FBI) began using bertillon systems (invented by french criminologist alphonse bertillon in 1879) to take photographs of subjects, as well as their height, one-foot length, arm length, and index finger length. In the 1990s, interest in biometrics shifted from simple hand measurements to eye characteristics, and then to other emerging identification systems

focused on a broad range of biometric patterns (i.e. fingerprint, hand geometry, iris, and retina), as well as the advancement of speech, signature, palm print, and face recognition systems. As research continues, a few new innovative methods to biometric analysis are being explored, including shape of the human ear, deoxyribonucleic acid (DNA), keystroke (typing tempo) and body odour.

According to Harakannanavar, Renukamurthy and Raja (2019), biometric refers to a distinctive feature of a person, such as physiological or behavioural, that does not change over time, as opposed to the conventional method of identification (e.g. pin, passwords). The physiological characteristics include fingerprints, iris, palm prints, face, and so on, while the behavioural characteristics include handwritten signatures and voice. The terms "Biometrics" and "Biometry" are imitated from the words "bio" (which means "life") and "metric" (which means "measurement"), both of which have been in employed since twentieth century. Biometric system is a term used in information technology to describe systems that measure human behavioural and physical characteristics for identification and authentication motives (Jahankhani, 2007). The enrolment module and the identification module are the two components of a biometric system. The enrolment module is in charge of teaching the system how to recognize a particular person by scanning an individual's physiognomy and creating a digital format of them. This digital structure serves as a comparison sample. The module for recognition is in charge of identifying a specific individual by capturing their features and converting them into the same digital structure as the sample. The module for recognition consists of two stages: identification and verification. The system asks *"Who is Tommy?"* during the identification stage and tries to match *"Tommy"* with every structure or pattern in the database. The verification stage, on the other hand, requires the system to ensure that the user who professes to be *"Tommy"* provides an answer to the question *"Is this Tommy?"* (Galterio, Shavit and Hayajneh, 2018).

In global security systems, biometrics is a viable option to traditional identity (ID) cards, and passwords. This method has a high level of commonality, uniqueness, ease of acquisition, persistence, portability, and fakery resistance. Individuals' physical, biological, or behavioural traits like face, fingerprints, voice, signatures, palm prints, iris and retina

scans, hand geometry, and posture, are quantified using biometrics (Chan, Kuo, Cheng and Chen, 2018). With a growing need in many of today's security applications for secure access controls, traditional approaches such as pins, tokens or passwords are failing to meet the challenge of losing or stolen. Biometrics is based on "who" a user is or "how" he or she acts; on the other hand, represent a notable security advance in meeting these new challenges (Zhong and Deng, 2015). Hence, biometrics offers significant benefits that traditional methods such as tokens and passwords do not.

1.2 The Problem of Study

Biometric security is a rapidly growing field and has been the most effective means of authentication and identification. However, with the increased threats on information security, biometric has shown a reliable security level but still facing issues like the effect of a damp and wrinkled fingertip on biometric application performance is an issue that hasn't been well explored, contact lenses and watery eye in the case of iris recognition and so on (Dharavath, Talukdar and Laskar, 2013). The origin and degree of biometric trait distinctness and consistency across people are frequently questioned. According to Latonero and Hiatt (2019), there is insufficient diversity of interest in digital identification systems to provide sufficient benefits to social systems. Multiple classifier systems (MCS) and man-machine interface (MMI) require more diverse interests as they can provide a significant benefit in the design of robust biometric algorithms and improving biometrics usability and security (Fierrez, Morales, Vera-Rodriguez and Camacho ,2018; Singh,2019).

More innovation and funding should be recommended and allowed in the fight against terrorism and identity theft; More than one biometric means should be encouraged to achieve an optimal form of protection (Jahankhani, 2007). In a better space as discussed by Masayuki (2018), potential assessments of artificial intelligence (AI) technology with biometrics will support exponential growth in the future as biometric is a major aspect of AI technology. Biometric characteristics contain underlying statistical qualities, distinctness, and varying extent of stability under real physical circumstances and environmental obstacles, many of which are unknown and handled, particularly in a huge number, in a simple notion of saying, there is no known biometric trait that is completely constant and unique (Pato and Millett, 2010). To make matters even more complicated, the

basic biological characteristics and spread of biometric traits in a group are usually only visible with filters imposed by biometric feature selection and measuring techniques.

There are also some gaps in major biometric applications that need to be addressed in the medical and engineering sector to explore possibilities that can be realized from specific biometric technology applications, such as registered traveller operation, identity systems, authentication protocol, and payment systems in these sectors (Morosan, 2016). A good compromise between recognition and security accuracy has been a long-term area yet to be duly discussed as the relationship between these two can be of a great deal to biometrics enhancement to the medical and engineering sector (Yang, Wang, Hu, Zheng and Valli, 2019).

Biometrics is unique because it necessitates judgment under ambiguity on both automatic recognition software and the subjective translators of its results under barriers of accuracy, scale, security, and privacy which has been the major category of challenges facing biometrics (Jain, Pankanti, Prabhakar, Lin Hong and Ross, 2004). Biometric technology is used to improve the development of more diagnoses and security systems like personal digital bodyguard sensors to improve the rate of activities and operations undertaken in both the medical and engineering sectors (Faundez-Zanuy, Fierrez, Ferrer, Diaz, Tolosana and Plamondon, 2020).

1.3 The Aim of Study

The sole aim of this study is to examine the advancements in biometric technology in regards to medical and engineering views. This study will examine certain research-related questions in order to truly comprehend the study's objective.

- **RQ1:** What are the views of medical professionals regarding biometric technology?
- **RQ2:** What are the views of engineering professionals regarding biometric technology?

1.4 The Significance of Study

Many researchers are eager to fully comprehend the significance of biometric technology as the most successful means of data protection, and many individuals and organizations are worried about their privacy, which has become a major concern around the world, as a result of the consistent identity threats and attacks evolving against the security and safety of information globally. The low-tech identification is simple to forge. A national database containing names and ID numbers exists, but law enforcement officers have no way of knowing if the card or picture presented by a person is authentic (Phadke, 2013), with biometric instant identification and authentication of a genuine person, biometric instant identification and authentication of a genuine person will prevail.

According to Ashok, Shivashankar and Mudiraj (2010), the need for more robust user authentication and thorough study as a result of the failure of conventional methods of identification and authentication has led to the idea of using human body parts or human mannerism as protection and authentication measures, and eventually to the advent of biometrics as a field. The research is vital for evaluating the performance of highly secure proof of identity and personal verification remedies in support of national security and fraud prevention, security infrastructures, user IDs, guarantee e-banking, investing, and other banking transactions, retail trade, public safety, and healthcare services.

Recently, more institutions and organizations across the world especially universities are conducting researches on how to improve biometric technology. Some educational institutions are using biometric for identification and authentication from getting access to a certain place to taking class attendance. However, biometric technology offers numerous functionalities based on the level of security it provides, having privacy to personal data and safety from false information can enhance the effectiveness of user's adaptation to the technology and improve the usage.

As a result of this, this study will contribute to the department of computer information systems and the Near East University as a whole by adding to the existing stock of knowledge in the areas of biometrics implementation and research. These studies will help understand the use of biometric technology. Specifically, the outcome of this study will

inform students and instructors more about the important features of biometric technology and the essence of acquiring more knowledge in that direction, students in the department and university will make use of this study as a guide for future research on biometrics. This study will serve as a reference for lecturers when it comes to lecturing students about the functionalities and importance of security and privacy of data.

1.5 Limitations of Study

For this study, there are various limitations faced that should be considered during future researches. The following constraints have been noted:

- During the study and data collection process, there was a time constraint. The study was conducted over up to 5 months.
- Language barriers when interviewing participants for data collections.
- Participants of this study were selected in Near East University resulting in geographic restriction.
- Due to the covid-19 pandemic, some of the interviews were carried out over the phone and online.

1.6 Overview of Thesis

This research conducts a descriptive study of the present and prospects of biometric technology, which is divided into five chapters.

Chapter one (1) introduces the subject under investigation and offers a brief context for it, as well as describing the problem statement, the goal, significance, limitations, and an overview of the following chapters.

Chapter two (2) offers an in-depth analysis of the report, concentrating on related research and the theoretical framework.

Chapter three (3) provides a detailed overview of the study's strategy, data collection procedure and data analysis techniques.

Chapter four (4) discusses the survey by providing research results, describing study differences, and addressing the outcomes.

The final chapter of the report, Chapter Five (5), contains the study's conclusion and recommendations for future studies.

CHAPTER TWO
THEORETICAL FRAMEWORK AND RELATED RESEARCH

This chapter focuses on relevant research, theoretical framework and provides an in-depth examination of the study.

2.1 Theoretical Framework

2.1.1 Biometric system

A biometric system is a means that identifies people by measuring their biological nature or specific behaviors of individuals and comparing them to biometric database prototypes of the same type (Jain, Ross and Prabhakar, 2004). As a result, it is classed as an identification or verification system and may be identified as a computerized technique of identifying or verifying human's identity based on particular biological / behavioral features (Dharavath, Talukdar and Laskar, 2013).

- Identification (one-to-many): The query *"Who is tommy?"* represents this approach. This query can be justified by comparing a biometric sample to a full archive of qualified samples of biometric.
- Verification (one-to-one): is a procedure of trying to confirm the identity of aan identified user. It is illustrated by the query *"Is tommy who he claims to be?"* and then be addressed by matching a biometric sample on the biometric samples claimed in the database.

The biometric identification system consists of two steps: registration and matching stage. Each phase includes the three sub-stages listed below: Obtaining biometric samples process and pre-process the input sample to create a template for reference, then match it to the database's reference template (Dharavath, Talukdar and Laskar, 2013).

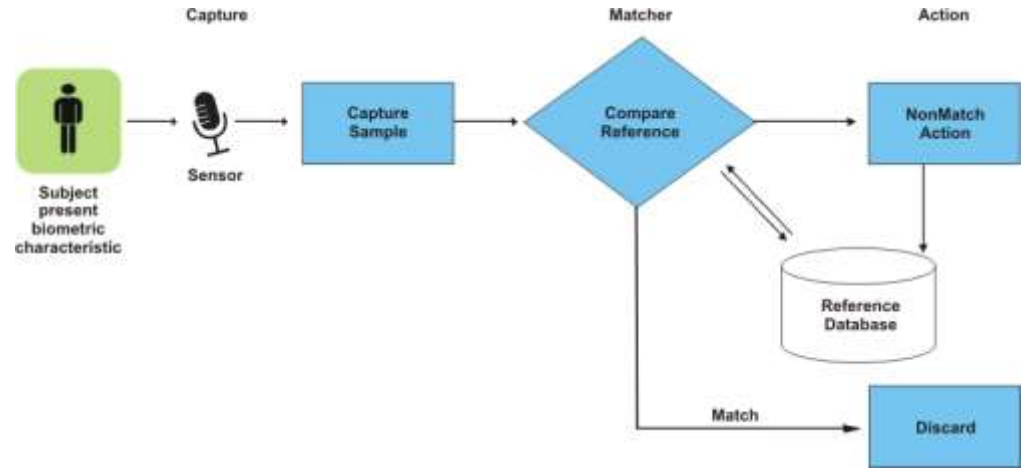


Figure 2.1: Enrolment/registration stage (Dharavath, Talukdar and Laskar, 2013)

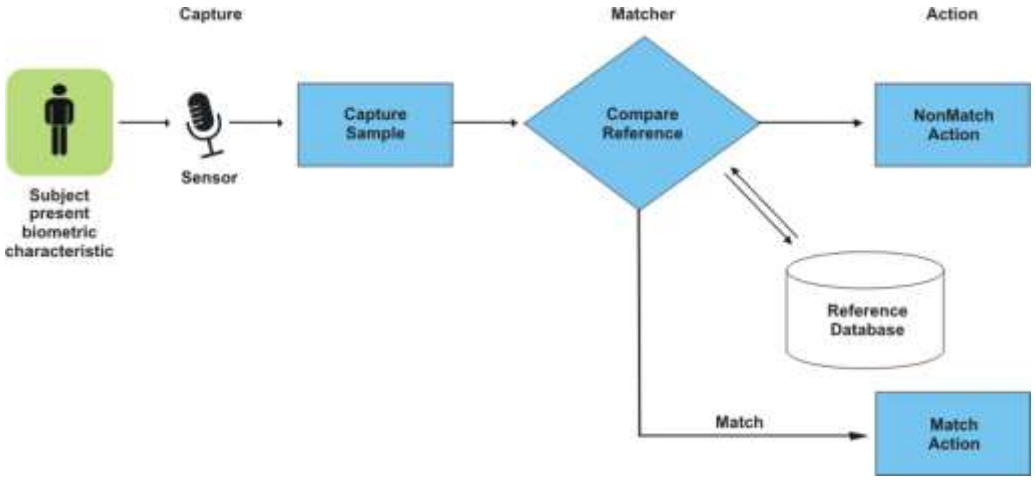


Figure 2.2: Authentication/matching stage (Dharavath, Talukdar and Laskar, 2013)

Figure 2.1 illustrates the stage at which each individual is required to enter their biometric feature into the database, which can be achieved whether it's regulated or unregulated. In a regulated scenario, the person must be ready to register and more cooperative during biometric registration, but in an unregulated scenario, the person may not be ready to register or cooperative. Any type of enrollment, however, necessitates the physical appearance of any individual in the presence of the biometric sensor.

The biometric scanner may collect a copy of the user's biometric characteristic, pre-processed the biometric sample and convert to a reference prototype, which is then compared to the biometric templates that have been saved (Pato and Millett, 2010).

Figure 2.2 illustrates the authentication procedure, which is similar to Figure 2.1 with the exception of the matching stage. Unlike in Figure 2.1, a person can only be authenticated for a permitted program if a match of the input template is discovered against the saved samples in the biometric archive; otherwise, the user would be denied.

When choosing a biometric, various aspects must be examined. Understanding the biometric needs and environment is critical. If a certain biometric is utilized for security reasons, it is also required to evaluate the degree of success (Anil, Hong, Jain and Pankanti, 1999). Nevertheless, no one biometric system performs well, thus many biometric approaches are utilized to provide maximum security. When establishing a biometric system, several elements must be considered, including tasks, user conditions, security threats, current data, number of users, etc. (Dharavath, Talukdar and Laskar, 2013). The below are the parameters to consider while selecting a biometric, which vary based on the application.

- **Universality:** The biometric feature must be present in all people (trait).
- **Permanence:** The characteristic must be time-invariant. Aging or any other ailment should have no effect on trait.
- **Acceptability:** The biometrics based on a certain attribute must be accepted by a broad number of related groups.
- **Reliability:** In order to attain maximum reliability, biometric technology based on a certain feature should not be conceal.
- **Avoidance:** The characteristic should not be reproduced in any other way.
- **Measurability:** The characteristic must be straightforward to be acquired in a short period of time, and the obtained data must be appropriate for additional process.
- **Individuality:** A persons personal attribute must be distinctive and have sufficiently diverse features to identify them from other people.

The importance of biometrics is well understood if you've misplaced the password on your computer or mobile phone. According to a 2007 report released by PBworks, Aside from logical usage, finger scan or other sort of technology determines if a person is given access to data or not. There is a growing demand to tackle user identification problems and reduce password administration expenses. Students find it difficult to remember passwords in

educational institutions, therefore they borrowed login credentials from other students and frequently abused them (Thakur, 2015). For these circumstances, biometric system is very important to the current state of security.

2.1.2 Biometric technologies and challenges

There are two biometric unique characteristics which are physiological and behavioral which don't change with time. The physiological features include the fingerprint, DNA, iris, hand, face etc., while the behavioral features are voice, signature and keystroke etc., as demonstrated in Figure 2.3 by Harakannanavar, Renukamurthy and Raja (2019) below.

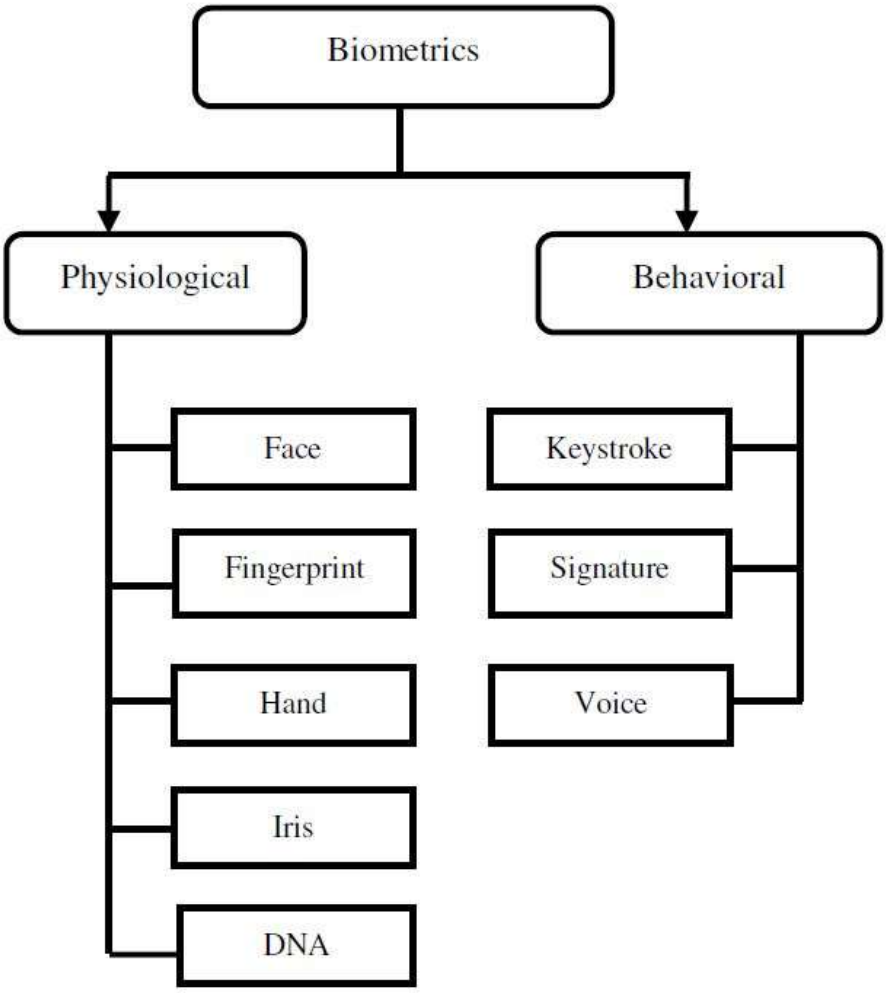


Figure 2.3: General block diagram of biometric systems (Harakannanavar, Renukamurthy and Raja, 2019)

2.1.2.1 Fingerprint recognition

Fingerprint-based identification is the earliest biometric approach that has been utilized effectively in a variety of industries. Fingerprints are acknowledged as being one-of-a-kind to each human. A fingerprint is a rough pattern on the finger's surface. The structure of rough surfaces, as well as the tiny spots, helps establish the uniqueness of a fingerprint (Thakur, 2015).

Fingerprints are often collected using a scanner, that produces a picture of the fingerprint. The picture of a fingerprint can then be enlisted and compared using algorithms like hybrid, minutia-based or pattern-based (Boukhonine, Krotov and Rupert, 2005). Fingerprint identification has comparatively exceptional characteristics such as permanence, universality, accuracy, uniqueness and low cost, making it the most popular and dependable approach as well as the leading biometric technology (Tiwari, Chourasia and Chourasia, 2015). They are popular in forensic units, in-network entry, access control entry setup, and financial organizations.

Challenges: When the finger is moist and wrinkled, the biometric profile's recognition rate decreases. The effect of a damp and wrinkled finger on the functioning of a biometric device has yet to be adequately addressed. Also, the research conducted by Tiwari, Chourasia and Chourasia (2015) stated that fingerprints may be reproduced in latex using a person-touched object and that noisy data may lead in dust film formation on a sensor or from ambient circumstances.

2.1.2.2 Hand recognition

For authentication, the human palm can be utilized as a biometric trait given that Its layout includes spatial geometry with varying dimensions for each user and cannot be amended. According to Harakannanavar, Renukamurthy and Raja (2019), To identify a user, two or three fingers of the subject must be measured as it usually demands little storage capacity. The palm prints of an individual's hand are captured using an powerful sensor module (optical reader) and saved as a template for matching and differentiating people; nevertheless, the enormous amount of the recorded data limits its practical application. (Dharavath, Talukdar and Laskar, 2013).

To detect someone's identity, an scanning equipment scans the tri geometry of the hand, creating a arithmetic representation that can subsequently be compared to an image recorded in a archive, and measurements of the person's hand are obtained (Jahankhani, 2007). It indicates a bright future for moderate security systems.

Because of its simplicity of acquisition, large user acceptability, and reliability, hand recognition-based authentication has swiftly entered the biometric group. Data sources based on digital cameras, digital scanners and video cameras involve less work for system development and are used in office settings. Because the human hand is bigger than a finger, palm prints are believed to be more accurate than fingerprints. Palm print pictures can be captured using low-resolution cameras and scanners while still retaining enough data to identify high identification rates, and they are resistant to aging (Tiwari, Chourasia and Chourasia, 2015).

Challenges: Pictures may be difficult to detect if the quality of the digital and video cameras used in the capture of palm vein photographs is inadequate, and gathering images in an unregulated setting with lighting fluctuations and distortions due to hand movement is also a concern. The influence of moist and wrinkled palms on identification rate has to be explored further (Harakannanavar, Renukamurthy and Raja, 2019; Tiwari, Chourasia and Chourasia, 2015).

2.1.2.3 Iris recognition

Every person's iris has numerous distinguishing features that can be used to identify them. The major visible feature of the iris is tissue, which is produced continuously in each human being at the age of eight (8) months (Daugman, 2004). The iris is a tinted muscular circle around the center of the eye that comprises the pupillary region and the ciliary region, and the iris resides between both the cornea and the lens of the eyeball, so in terms of the user authentication, the iris pictures are captured by the sensor and the iris structures are analyzed using numerous iris database systems such as UPOL, MMU, IITD and others (Harakannanavar, Renukamurthy and Raja, 2019). There is no hereditary influence on it throughout formation; a process known as chaotic morphogenetic happens in the seventh month of pregnancy and aids iris formation, allowing even twins to have distinct irises (Dharavath, Talukdar and Laskar, 2013).

Tiwari, Chourasia and Chourasia (2015) further explain that iris identification utilizes camera technology and modest infrared illumination to capture photos of the iris's complex, detail-rich structures without harming or distressing the person. The identification of a person or someone claiming to be that person is possible thanks to digital templates encoded from these patterns by mathematical and statistical algorithms. Because it is an internal organ, the iris is stable. From the first year following birth until death, this mode does not vary with time.

Challenges: Changes in illumination can have an impact on scanner accuracy and various facial expressions captured by the scanner. Contact lenses, watery eyes, and other variables might all have an effect on iris recognition (Boukhonine, Krotov and Rupert, 2005). Optical scanners are considerably more costly than other types of biometrics.

2.1.2.4 DNA recognition

DNA is specific to each person and stays stable throughout life. Because the human body is made up of about 60 trillion cells, deoxyribonucleic acid (DNA) is the most dependable kind of biometric personal identification method. DNA, which may be thought of as the template for the construction of the human body, is wrapped inside the nucleus of each cell and does not alter throughout or after a person's life (Hashiyada, 2011). DNA identification is a time-consuming technique of authentication that requires a specimen of saliva, blood, sperm, hair, or tissue for validation (Srivastava, 2013; Dharavath, Talukdar and Laskar, 2013).

When obtaining identifications is challenging, especially in the aftermath of a violent conflict, it may be theoretically viable to begin a DNA-led identification. DNA may be examined to provide a profile which can be compared to other patterns with confidence. DNA is inherently digital and unchanging throughout a person's life and after death. It is the framework that determines who we are physically and cognitively; unless a person is an identical twin, no other person is suppose to have same collection of DNA (Tiwari, Chourasia and Chourasia, 2015).

Challenges: The DNA recognition approach is not precise and test substance must me upgraded. The most severe issue is that DNA testing takes time. No real-time applications

are conceivable since DNA match necessitates sophisticated chemical processes that require specialist knowledge (Harakannanavar, Renukamurthy and Raja, 2019).

2.1.2.5 Face recognition

The human face is unique to every person, which is also a universal truth, It may be used to secure authentications as a biometric. Face recognition systems are based on the notion of utilizing the face as a measure for authentication (Phillips, Flynn, Scruggs, Bowyer, Chang, Hoffman, Marques, Min and Worek, 2005). With the use of good cameras, a face is captured as an image and used as a framework for comparison. Then, the framework is compared using different approaches for pattern matching to identify or verify an individual identity (Dharavath, Talukdar and Laskar, 2013). The rates are calculated using several face databases such as ORL, JAFFE, Yale, Multi Pie, AR database, FERET database and so on (Harakannanavar, Renukamurthy and Raja, 2019). Face recognition has become one of the most popular biometrics due to its ease of use and lack of interference; it can be performed using still photos, video sequences, stereo, and range images, among other things. Facial recognition under well-controlled collection circumstances is more precise and delivers excellent identification rates even though there are a huge number of samples in the gallery (Tolba, El-Baz and El-Harby, 2006). Some face recognition algorithms take landmarks or characteristics from a subject's face picture to detect facial traits. An algorithm could look at the relative location, size, and/or form of eyes, noses, cheekbones, and jaws, for example. These characteristics are then utilized to find another picture with similar characteristics. By using 3D facial recognition, a new trend claims to facilitate maximum levels of accuracy (Asha, Vipul, Singh, Bhavesh, Subramanian and Student, 2018). The picture is captured with or without the subject's consent. Individuals may be identified in crowds using well-designed devices deployed at airports, multiplexes, and other public areas. Securing mobile devices with facial recognition technology is also becoming more common (Tiwari, Chourasia and Chourasia, 2015). The mobile phone industry is experimenting with face recognition and incorporating it into its products.

Challenges: Unregulated illumination, changes in face expression, age, and a considerable drop in recognition rate are among issues that biometrics may encounter. The face, as a changing social organ capable of exhibiting a wide range of expressions, poses a

significant difficulty (Dessimoz, Richiardi, Champod, and Drygajlo, 2007). In addition, Face recognition encounters problems such as face rotation (position variation), lighting circumstances (illumination difficulty), individuals wearing collusions such as hats, scraps, eyeglasses, etc., and varied facial emotions, all of which decrease the system's performance. To build a strong and reliable identification system, research must be more focused on all of these difficulties.

2.1.2.6 Voice recognition

Rather than attempting to identify words, this form of biometric concentrates on the tone of the voice. This is not the same as technology that detects language and responds to orders. The words "speaker recognition, verification and identification" are used to prevent misunderstanding (Jahankhani, 2007). The underlying idea behind voice authentication is that each human speech is distinct enough in pitch, tone, and volume to be recognized individually. An essential technological challenge in Human-Computer Interaction is a comfortable and user-friendly interface. People assume speech contact with computers since spoken languages dominate verbal speech (Tiwari, Chourasia and Chourasia, 2015). In order for voice recognition to work, a person must say a previous phrase in front of the sensor. The sensor will transform the acoustic data into a unique digital code called template, which will then be analyzed to identify the person. Resonance in the larynx produces the sound of a human voice. The sound measured by this technique is affected by the length of the larynx as well as the shape of the nasal and oral cavities (Dharavath, Talukdar and Laskar, 2013). This biometric technique is applicable to telephone applications. However, rear noise in the environment and telephone network interference can degrade the performance of these devices.

Challenges: Due to old age, physical problems, and mental reactions, a person's speech recognition varies with time. Sometimes, sickness may affect the sound of the voice, it may not identify the user well enough i.e. voice identification is not stable (Tiwari, Chourasia and Chourasia, 2015). A technology must also be develop in order to reduce the amount of space required to store the unique digital code (Harakannanavar, Renukamurthy and Raja, 2019). And also, when a person's voice changes, the accuracy decreases.

2.1.2.7 Signature recognition

Signature recognition is catergorized under the behavioral feature of humans. This system dynamically collects data-based motion, speed, writing intensity, and signature form using physical traits that an individual provides when signing (Dharavath, Talukdar and Laskar, 2013). Individual signatures are regarded as the "seal of approval" and the most natural means of validating a person's identity. Individual signatures, on the other hand, may be treated as a picture and identified with the help of machine learning and neural network algorithms (Tiwari, Chourasia and Chourasia, 2015). Signature sensor arrays checks both the final signature and the traits that were utilized to produce it. The inclusion of behavioral features prevents forgeries and improves the accuracy of this biometric technique (Jahankhani, 2007). People are more likely to switch from the conventional pen-and-paper signing to one in which the handwriting signature is collected and confirmed digitally, therefore rapid algorithms for signature verification validation to establish if it is authentic or counterfeit are needed with current computers.

Challenges: Non-linear alterations with scale changes and sensitivity to energy and time, e.g., a person's signature slowly changes with time or a person's signature varies from time to time (Tiwari, Chourasia and Chourasia, 2015).

2.1.2.8 Keystroke dynamics recognition

This form of biometrics is a method for determining an individual's behaviour when typing on the keyboard based on a pattern. The algorithms in this technology are continuously being improved to increase robustness and distinctness. This system measures speed and pressure, as well as the overall time spent inputting a password and the time a user spends between keystrokes on the keyboard. Computer access might be a beneficial use, as this biometric could be used to continually check the identification of the computer user (Thakur, 2015). Compared to the other biometric technologies investigated, keystroke recognition operates in a unique way. It's definitely one of the simplest to set up and manage. This is due to the fact that keystroke dynamics is currently a software-based solution. All it requires is for the user to use his or her present computer and keyboard (Jahankhani, 2007). It is most likely the only biometric technology that does not necessitate the use of any extra, sophisticated gear; software-based solution and can be integrated easily with existing authentication processes (Jain, Ross and Prabhakar, 2004).

However, keystroke dynamics, like other biometric systems, is still a new technology that hasn't been tested in large-scale deployments.

Challenges: Regardless, keystroke dynamics facilitate a simple way for computer and phone security controls and access protection. The biometric technique still needs standard keystroke dynamics archive for the research communities and has to be enhances to increase the effectiveness of the technology (Zhong and Deng, 2015).

2.1.3 Biometrics law and privacy

Confidentiality is an important civil right, and in today's modern society, it is the foundation that protects who we are and encourages our continuing battle to retain our independence in the face of growing governmental authority. Today's "new technical realities" oblige us to consider these rights in terms of legislation and policy, in order to protect the public interest and provide correct outcomes for society. Businesses, a variety of government entities, law enforcement, and other commercial and public entities are increasingly relying on biometric scanning technologies, which must balance biometric privacy with a variety of conflicting needs, including the desires of others and civilization as a whole (Woodward, 1996).

Because data is gathered wherever we turn, and with improvements in telecommunications, databases, and data gathering, it is virtually simple to disseminate private information to anybody that is willing, it is impossible to retain the levels of privacy individuals knew in the past (Jahankhani, 2007). Biometrics could provide a fast and accurate form of identification, therefore improving safety and confidentiality, for example, by supporting a person in maintaining control over his or her data and lowering the possibility of fraudulent activity. However, the use of biometric data poses challenges about a person's capacity to handle the data about himself/herself that he/she is prepared to share with those around, which might inevitably influence his/her confidentiality. Several security issues raised by biometrics fall into two categories: individual rights (worries about the destruction of human identity and physical autonomy) and data confidentiality (fears about the misuse of data) (Christopher, Amujo, Oluwasegun and Silas, 2019). The use of biometrics for identity verification may pose a lower degree of data privacy if the validation program uses the individual intentionally trying to exercise a choice to

participate in a system, the system does not require the validating body to retain vast volumes of data about an individual other than that which is designed to prove that the individual is legit.

Currently, the laws and privacy guarding biometric technology does not widely use and considered which poses a big challenge. So, in order to meet such legislative and policy problems, existing initiatives have offered some hints for building the legislative structure that will regulate biometric future technology. Nevertheless, Mindful of the regulatory gap, recommendations suggested according to Liu (2008) are stated due to the fact different types of personal data cannot be properly eliminated from the biometrics user authentication, biometrics pattern, and biometrics picture in general.

2.1.4 Benefits and applications of biometric systems

The primary benefit of biometric systems is security and identification, people cannot simply transfer their biometric feature to other people as they do with their password which makes biometrics more reliable and secure. Because biometric features are not concealed, the existence of a person's fingerprint or iris scan does not compromise security in the same way that the disclosure of the passcode would (Matyáš and Říha, 2002). Biometrics offer consumers more confidence by confirming a concrete, real-world attribute as both something the user has and something the user is (Mitek, 2020). Benefits and applications of biometric technology generally vary between civilian, commercial, or law enforcement applications (Thakur, 2015).

- Criminal justice (investigation, surveillance and terrorism prevention and so on).
- Citizen biometric applications, such as National ID, photo id, voting and ballot access, social payout, controlled immigration and so on.
- Business (Workstation access, physical intrusion detection, attendance management, secure transactions, cctv, credit Check).
- Banking and Financial services.
- Border security and immigration (for example, entrance and departure points at the airports, passport and visa issuing, and refugee situations).
- Social assistance (for example, in welfare programs, theft control).
- Medical care (for example, confidentiality precautions for hospital data).

- Controlling physical access (for example, Educational, administrative, and domestic).
- Timekeeping and attendance (for example replacing a timestamp).
- Computer safety (for example, computer and network access and encryption).
- Information and communication technologies (for example, mobile phones, televised shopping).

2.2 Related Research

With a look into past research on biometric technology, one can think that the main reason for applying biometric solutions is security. Biometrics, in general, relate to the use of data to enable people due to biological measures or physical attributes like fingerprint tracing, face detection, and retinal and eyeball scanning etc.

2.2.1 Previous Studies on biometrics

Delgado-Mohatar, Fierrez, Tolosana, and Vera-Rodriguez (2020) address opportunities and obstacles for the integration of blockchain with biometrics and focused on storage and security of biometric templates. This study was carried out using an experimental method with a random hypothesis to determine the integration of biometrics in the blockchain set up with the results showing that the biometric integration process would given a fully certified plug of secured operation in blockchain and demonstrates the need for new ways to conduct biometric alignment and associated activities in blockchain.

The research by Thomas and Zhang (2020) attempted to explain how automated systems are used to spread the ID2020 conspiracy. It focuses on the conspiracy behind the ID2020 alliance, which was spearheaded by Bill Gates, a billionaire philanthropist who has been connected to a scheme to implant microchips into people as a way of global digital identification using vaccines as a pretext. Since it is a conspiracy theory, the report made no significant findings.

Mohsin, Jalood, Baqer, Alamoodi, Almahdi, Albahri, Alsalem, Mohammed, Ameen, Garfan, Zaidan, Zaidan, Albahri, Bin Ariffin, Alemran, Enaizan, Shareefand Jasim, (2020) want to support the system-based software and hardware-based digital vector verification

components development. Only 61 final publications were found after a systematic review and meta-analysis that yielded 492 results from science direct (297), IEEEXplore (92), and WoS (103) filters with parameters (year, full text, titles, and abstracts), leaving only 492 total. Researchers should use more taxonomy to identify gaps in the digital biometric authentication process, according to the results of the quest, which were graded under software and hardware-based development design that suggests and concludes that researchers should use more taxonomy to identify gaps in the digital biometric authentication method.

The use and trends of electronic handwriting (signature) biometrics in e-health and e-security were investigated by Faundez-Zanuy et al. (2020). Researchers have compiled a summary of the state of the art and application of handwriting signals, as well as the key achievements and challenges that the scientific community should address to provide direction for future research. Contrary to other biometric features, handwriting signals are essential for e-security and e-health, according to the findings.

Singh (2019) examined the use of MMI (man-machine interface) by speech technology, including automated speech and natural language processing, and what it has to offer, to determine whether MMI based on voice technology could replace the keyboard and mouse. Human-computer interaction will be enhanced in the future with the use of MMI technology so that communicating with computers will be much easier and rewarding no matter who you are or what language you speak as the review was concluded by the author.

Delgado-Mohatar, Fierrez, Tolosana, and Vera-Rodriguez (2019) discussed the value of the blockchain for biometrics, analyzing how the two systems would support each other. In the short term, full integration of blockchain with the biometrics process appears to be very difficult, but there are some exciting areas of research recommended for future research that could significantly help to maximize frequency band, or the creation of new knowledge proofs that would allow users to be validated via biometric identification without any party knowing the individual.

Harakannanavar, Renukamurthy and Raja (2019) conducted a systematic analysis of the current biometric methodologies, their use, and drawbacks used in real-time situations. The authors also present the inspiration for the adaptation of biometrics to current conditions in an attempt to talk about technology and security problems relevant to biometric systems. They also made it feasible for individual features to be replaced in the future by multi-factor validation, and biometrics would assess candidates and assist users in re-identifying themselves.

Yang et al. (2019) carried out a systematic literature review to shed light on the latest developments in the fingerprint biometry study, covering two areas, to enhance device protection and recognition accuracy. A total of 42 papers in the field of biometric protection have been studied and discussed. Analysis problems and potential directions have also been provided to researchers to consider a good compromise between recognition and security accuracy in the future.

Latonero and Hiatt (2019) attempt to revise the notion that biometric technology would not offer simple solutions to migration and refugee situations by using Italy as a case study. A qualitative interview, with 25 migrants and refugees, was conducted with 25 workers and representatives from 16 organizations'. The results of this research have shown that there is a wide range of socio-technical mechanisms that have consequences for the identification of migrants and refugees. The author suggests that there should be a greater diversity of interest through digital identification systems to help migrants integrate into the social system with sufficient benefits.

Fierrez et al. (2018) address the developments and challenges in biometric technology's multiple classifiers systems (MCS) and how MCS can help overcome those challenges. MCS will act a major function in the design of robust biometric algorithms, integration with end applications, and understanding and enhancing biometric usability and security in the future, according to the authors.

Galterio, Shavit and Hayajneh (2018) examined the scientific backdrop for why face biometry has now become a reliable method of identification, a user-friendly procedure, and an examination of the safety of smart phone apps available for Android and iOS

systems. After conducting a facial recognition test on both systems using printed images, electronic images, and video, the authors found that iOS facial identification is more safe than the applications provided in Google Play Store for Android and concluded that the use of passcode and biometrics is not sufficient, but using all forms of validation in every individual identification will keep peoples data more safe and private.

Masayuki (2018) discusses potential assessments of the AI technology biometrics and how biometrics will support exponential growth in the future. It was concluded, according to the author, biometrics is a key element of AI technologies and plays a major role in exponential development, a feature of both the industrial and the information revolutions.

Tolosana, Vera-Rodriguez, Fierrez and Ortega-Garcia (2018) proposed a platform for investigating recurrent neural networks (RNNs) for online handwritten signature biometrics employing both Gated Recurrent Unit (GRU) and Long Short-Term Memory (LSTM) programs focus on Siamese structure and bidirectional techniques (i.e. BLSTM and BGRU). The experimental work in the study involved 400 participants who provided a total of 11,200 signatures throughout four collection periods. The proposed BLSTM is then shown to be the most effective compared to other proposed schemes, leading to the conclusion that future research should focus on input system interoperability in terms of signature and mixed writing tools.

By surveying to review and analyze 93 cutting-edge papers on their suggested techniques, signal databases, and publicly available data accessible electrocardiogram acquisition, Ribeiro Pinto, Cardoso and Lourenco (2018) hope to uncover existing benefits as well as encourage and direct future studies in electrocardiogram. The survey results show that some challenges in electrocardiogram-based biometrics remain unresolved, especially in the areas of acquisition, deep learning, multimodal biometrics, public data, spoofing, and data protection. Future research should focus on open issues that are becoming increasingly competitive and relevant to electrocardiogram biometrics. systems based on the vulnerability of attacks in the biometric systems and algorithms.

The aim of Chan et al. (2018) is to better understand the problems and potential prospects of EEG-based biometrics. The article examines the various systems proposed in recent

years with a particular emphasis on the flaws that have protected widespread adoption, such as seasonal consistency, psychological and physiological fluctuations and performance appraisal are all important considerations. A study of the literature indicates that EEG-based biometrics are different from other biometrics and cannot be misplaced by individuals.

Normalini and Ramayah (2017) proposed an extension to the technology acceptance model to allow researchers to comprehend the critical elements that directly impact the desire to maintain utilizing online banking, the report's objective is to provide substantial insight into the possible efficacy of biometric technology in the context of online banking in alleviating privacy and security concerns while also increasing trust among Malaysian clients. A sample of 413 internet banking users was evaluated using a questionnaire. The model developed was evaluated through the structural equation modeling (SEM) approach using partial least squares (PLS) utilizing SmartPLS 3.0 software, indicating that, while there was no significant link between perceived privacy and trust, perceived biometrics efficacy had a substantial impact on the strength of both perceived privacy and perceived security with trust.

Quadri, Kazim and Aditya (2017) analyze the biometrics and cloud computing aspects that have been applied as biometric authentication as a service, and the authors have gone deeply into biometrics and cloud computing to finally understand that these can be integrated to create a potential authentication scheme. Later, it concluded that biometrics can be shown to be the best way to authenticate any person in countries or organizations with a visible population.

Syazana-Itqan, Syafeeza, Saad, Hamid and Bin Mohd Saad (2016) aim to determine the potential course of biometric systems using a machine-language framework to illustrate and analyze methods taken from other pre-processing research for the recognition of individual identity. The researchers have evaluated a large number of papers covering the current approaches to the identification of finger veins, showing that the biometric traits are not adaptively modeled by the machine learning algorithm because the similarity of machine learning is applied to the device classifier instead of using machine learning as a feature extraction technique.

Zhong and Deng (2015) conducted a literature survey aimed at reviewing recent developments and emerging patterns in keystroke dynamic biometry. Keystroke dynamics have been said to have unmatched versatility and immense potential for cybersecurity applications, leading to the fact that the merger of keystroke biometry with other biometry would provide the ultimate comprehensive and reliable authentication solution both now and in the future.

Thakur (2015) summarized opinions on the usefulness of biometrics system, various methods, their pros and cons and potential capabilities. The author came to the conclusion that conventional authentication methods can be modified and interchanged, but that physiological features cannot be interchanged, making biometric authentication technology the best safety mechanism yet to be used.

Tiwari, Chourasia and Chourasia (2015) assess the effectiveness of biometric identification system, their kind and working theory, application areas, tools available, benefits, limitations, and major recent advancements. Biometric programs are beneficial for human identification and authentication at various stages of implementation, are hard to replicate, and may be protected by combining more than one biometric feature that can be identified as multimodal biometric systems, according to the author.

Revett and de Magalhães (2010) seek to review and address the potential future problems of cognitive biometrics, a novel approach to user authentication/identification. The findings of this peer-reviewed analysis show that there is an equal rate of heritability scores in line with cognitive bio-signal biometry challenges intended to improve the information quality of the acquired data.

Jahankhani (2007) summarized statistics, advancements, benefits, and drawbacks of the use of biometric technology in criminal justice today and in the future. The authors' analysis has shown that there is a clear need to use and include biometric technology in the future from the point of view of current developments in the fight against terrorism and concerns regarding identity theft, the use of a single biometric means is probably not an optimal type of protection. The level of innovation and funding for biometric technology would also help to ensure its accuracy and reduce the level of error.

Wieslaw (2006) attempts to predict the future of biometric technology and application. After a thorough explanation, the author concluded that further advancements in biometric technology would dramatically alter the environment in such a way that it can be used for purposes other than identification.

Boukhonine, Krotov and Rupert (2005) address the benefits and disadvantages of biometric and conventional safety methods, existing and potential applications of biometric, performance measurement of biometric systems, and privacy concerns related to modern technology. After a thorough explanation of the pros and cons between biometrics and traditional safety approaches, it was concluded that biometrics are more accurate than traditional safety approaches.

Previous research has focused on the differences between conventional and modern security (biometrics and pin), the use of MMI (man-machine interface) as biometrics, the use of Gated Recurrent Unit (GRU) and Long Short-Term Memory (LSTM) systems according to Recurrent Neural Networks (RNNs), electroencephalogram (EEG) based biometrics, and biometric technology's multiple classifiers systems (MCS). Furthermore, some research focused on the future benefits of combining blockchain with biometrics, while other inconclusive research was conducted on the ID2020 conspiracy theory. All of these studies have a common goal: to explore what biometrics could become in the future if allowed to achieve its full potential.

CHAPTER 3
RESEARCH METHODOLOGY

This chapter discusses the research methodology. It comprises of the research strategy, volunteers, collecting data, and data analysis.

3.1 Research Strategy

To assess the aim of the study, the qualitative research method, which is a systematic investigation of social processes in natural settings (Teherani, Martimianakis, Stenfors-Hayes, Wadhwa, and Varpio, 2015), was used in this study to explore what biometric technology means to the participants. Before engaging in the qualitative approach, existing studies were examined to determine how much further the current state of biometric technology can be advanced. Participants' point of view on biometric technology were examined using semi-structured interview, which were also used to obtain data from participants of this research.

3.2 Research Participants

The purposeful sampling method was used to select participants who could give in-depth and thorough details on the topic under research. Purposeful sampling is widely used in qualitative research to identify and choose relevant data instances related to the phenomena of interest. Its objective is to get detailed information from the appropriate respondents (Palinkas, 2013). Only participants with a doctor of philosophy (Ph.D.) and masters of science (M.Sc.) degree from the medical and engineering departments of Near East University are chosen specifically as criteria that each participant must meet to be considered for the study. These participants were chosen among students and instructors of the medical and engineering departments. A total of twenty (20) participants were recruited for this research.

3.2.1. Demographic information of participants

The participants of this research span within variables of gender, age group, profession, educational level and the sector as shown in Table 3.1 below.

Table 3.1: Participants' demographic information

Demographic Variable		Frequency	Percentage (%)
Gender	Male	13	65%
	Female	7	35%
Age Group	Below 35	17	85%
	Above 35	3	15%
Profession	Students	17	85%
	Instructors	3	15%
Educational level	Masters	13	65%
	PhD	7	35%
Sector	Medical	15	75%
	engineering	5	25%

The gender results to 65% of males and 35% of females, the age group ranges below and above 35 which appears that 85% of the participants are below 35 years old and 15% are above 35. The majority of the participants are 85% students and 15% instructors. There are a low percentage of Ph.D. holders of 35% and a high percentage of master's degree holders of 65% as shown in table 3.2 below. More rate of participants from the medical sector is easier to recruit at a high rate of 75% because of the covid-19 which has made the medical professionals present in the school premise to probably carry out test and researches on the covid-19 situation than every other department like engineering sector with a low rate of 25%.

3.3 Data Collection Tools

Following the categorical selection of research participants, two different semi-structured interviews were prepared, suitable to collect participants' views on biometric technology. The semi-structured interview included a mix of closed and open-ended questions through selecting participants, writing and validating interview questions, and conducting the interview (Adams, 2015). The content validity during the compilation of the interview questions was ensured through literature review and expert views. Two experts were approached for the clarity and appropriateness of the prepared interview questions and required changes were made in respect to the feedback received to complete the questions.

Validity of content is the scope to ensure that a data collection sample covers the domain to be measured (Taherdoost, 2016).

After finalizing the contents of the interview questions, twenty (20) voluntary participants including students and instructors were approached and briefed about the essence of the study and its aim with the option of face-to-face or online interview. The following are the steps involved in data collection:

- A suitable environment with less distraction was chosen.
- Researcher explains the purpose of the interview to the participants to give them more idea about the topic.
- The terms of confidentiality and ethical consideration was addressed with participants to gain their trust and confidence.
- The format of the interview was explained to the participants so that they can understand the process of the interview.
- Researcher indicates the duration of the interview.
- The participants were allowed to clarify any doubts about the interview.
- Participants' responses were recorded as they were being questioned, and notes were collected.

3.4 Data Analysis Methods

The data obtained from the semi-structured interviews with participants were analysed using descriptive analysis within the context of qualitative data analysis. Descriptive analysis was chosen because it serves the same function as qualitative data analysis in describing a scenario and identifying characteristics, frequencies, themes, and categories (McCombes, 2019). Following the collection of the data, the five steps of conducting a descriptive analysis were observed: identifying a framework; sorting data into the framework; analysing the data; describing the findings and interpreting the findings (Loeb, Morris, Dynarski, Reardon, Mcfarland and Reber, 2017).

Throughout each interview, notes of participants response were recorded, organized, saved, and labelled in a way participants' confidentiality agreements was respected at the interview stage. Significant response themes obtained in the interview and research

questions were used to create a conceptual framework. The responses from the participants were then organized in a significant sense under the topics, with direct quotations chosen. Lastly, direct quotes from the response obtained were used to describe the structured data and the findings were interpreted by the researcher.

3.5 Procedure

Step-by-step procedures for conducting the study are listed below:

i. Previous studies on the chosen research topic were reviewed to gain a better understanding of the study.
ii. A summary of the research topic was submitted for review to the department of computer information systems.
iii. The ethical committee application was submitted for approval.
iv. For ethics committee approval (see Appendix 1).
v. Following approval, an interview was conducted to obtain participants' views on the research topic.
vi. Response obtained from the participants were analysed.
vii. Report was prepared and submitted to the supervisor for review and corrections.

3.6 Research Schedule

For effective time and resource management, every research follows a study plan or schedule. The research for this study began in February 2021 and ended in July 2021. To ensure proper thesis planning, each stage of the research was assigned a completion time. The thesis's timeline is listed in Table 3.2 below:

Table 3.2: Research timeline

Schedule	Duration (Weeks)
Review of previous studies	4
Thesis proposal	3
Proposal submission and feedback	2
Data collection	3
Analysis of data collected	4
Concluding chapter compilation	5

Last review by the thesis supervisor	1
Corrections and amendments	1
Jury and final correction	2
Total	25

CHAPTER 4
RESULTS AND DISCUSSION

This chapter summarizes the study's findings on advancements in biometric technology. Research questions are explained and response obtained from participants is presented in this chapter.

4.1 Medical Professionals' View on Biometric Technology

4.1.1 The current state of biometrics in the medical sector

The aim of understanding participants' view about the current state of biometric technology in the medical sector was created under three themes along with the frequency and percentage which are presented in Table 4.1 below:

Table 4.1: Participants' view on the current state of biometrics in the medical sector

Themes	Frequency	Percentage
Strong	0	0
Limited state	2	13.33
Weak	13	86.67

As seen in Table 4.1 above, most of the participants stated that the current state of biometrics is low in the medical sector of Near East University. Below is some participants' expression to this question.

"*It is increasingly advanced right now, generally but I am not sure the university hospital is using any biometric means right now. I have not seen any personally"* (Participant 1).

"Maybe other department uses biometrics but we don't use in the medical. There is no usage of biometrics in this department" (Participants 5 and 6).

While two participants claim that the current state of biometrics in the medical sector is limited to simply attendance tracking of specific personnel. The following expression was obtained:

"I think it's not that fully developed but I think It has a future in medical science. I know some staff sign-in using fingerprint here in the hospital" (Participant 7).

"Scaling the usage of biometrics between patients and staffs, maybe some staffs use it as attendance but I don't think it is used as a means of identification for patience yet at the hospital" (Participant 12).

Whereas no response claims that the usage of biometric technology in the NEU's medical sector is high. The response in this section demonstrates that biometric technology is not incorporated into NEU's medical sector.

4.1.2 Participants' personal biometrics experience in professional life

This section aims to determine participants' biometrics experience in their professional lives. Two themes were obtained to investigate the participants' professional experiences in biometric technology, as shown in Table 4.2 below:

Table 4.2: Participants' personal biometrics experience in professional life

Themes	Frequency	Percentage
Yes	1	6.7
No	14	93.3

As shown in Table 4.2 above, a large number of participants as no experience of biometric technology in their professional lives. Participants' expressions obtained were short answers such as "no", "not at all".

While one of the participants who is an instructor in the medical sector claims to have studied research that involves biometrics. The following statement was obtained:

"We have some studies to diagnose parasites and bacteria through deep learning" (Participant 5).

Due to the low use of biometrics in the medical sector of the Near East University, almost all participants have no professional life experience with biometric technology, except for one participant who has worked and read on research in the sector on deep learning methods to diagnose parasites and bacteria.

4.1.3 Role of biometrics in medical science

The purpose of this section is to ascertain the participants' understanding of the role of biometrics in the medical sector. From the participants' point of view, a single theme emerged: "identification." The responses of the participants to the interview question are shown below.

"Generally, I think it has help hospitals to identify a particular patience and also clarify which patient has insurance or not" (Participant 3).

"From my point of view, it improves the way we manage patient files, by keeping track of patients, from the time they come to the hospital to the time they leave." (Participant 4).

"Well, for example in forensic medicine, I think it has played an important role in recognition of patients who have been involved in a situation or accident where their body is not fully recognized. Biometric analysis can be used to identify them". (Participant 7).

Biometric technology is said to have played numerous important roles in medical science, including determining the authenticity of staff and patients, as well as in forensics. All participants agreed that biometrics' primary role in the medical sector is identification.

4.1.4 Biometrics opportunity and challenges in medical science

Participants were asked about both the opportunity and challenges of biometrics in medical science to acquire participants' view of understanding of the opportunity and challenges biometric technology provides. Table 4.3 below shows themes obtained, which are categorized under opportunities and challenges to get a clear view of participants' responses.

Table 4.3: Biometrics opportunity and challenges in medical science

Themes		Frequency
Opportunities	Identification	9
	privacy	3
	Career boost	1
Challenges	adaptation	2

As seen in Table 4.3 above, most participants have more to about the opportunities of biometrics. The following are some of the participants' notable statements about the possibilities of biometric technology in the medical field.

"It has helped in reducing fraudulent acts, for example, in cases where a person is trying to get treatment under a different name. So biometrics has given opportunities to medical sector in terms of unique identification" (Participant 3).

"Well, I don't have much knowledge about that but I think if a person has a prior knowledge about this biometrics, it will be a great opportunity for such person to stand out among practitioners" (Participant 7).

"It has improved privacy of staffs and patient data unlike writing down names and phone number and signature which anyone can have access to. So biometrics has improved privacy" (Participant 8).

While few of the participants have something to say on the challenges facing the use of biometric technology. Expressions obtained from these participants are stated below:

"Here in the hospital, I think biometrics has not been fully integrated, that is a challenge I think we are facing here because with fully integrating biometrics in the medical field, we cannot know how far we can go with the technology and improve on it" (Participant 7).

"The challenge I can think of is adaptation. Adapting to the use of biometric technology in the medical sector and depends on the part of the world you are in. Some countries adapt fast to technologies like this while some countries have difficulties adapting as well" (Participant 4).

When participants in the medical sector were asked about the opportunities and challenges of biometrics in their industry. Many of the participants are more open about the opportunities that biometrics has provided than they are about the challenges, which most have identified as data security and individual identification. Few participants responded to the challenges of biometric technology.

4.1.5 Health risk of using biometrics in the medical sector

This section aims to understand the health risk of using biometric technology. Participants were asked the question with an explanation to direct their understanding of this interview question. The explanation is based on the two categories of biometric technology that were used to create a theme along with their frequency as shown in Table 4.4 below.

Table 4.4: Health risk of using biometrics in the medical sector

Themes		Frequency
Contactless	No infection	13
	Radiation risk	2
Contact	Direct infection	14
	Accuracy risk	1

As shown in Table 4.4 above, following the explanation given to participants, the majority believe that biometric technology has no health risk when it comes to contactless biometrics and there are more chances of infection risk when it comes to contact biometrics. Below are some expressions obtained from participants.

"Based on this explanation I have a clearer view, the contact biometrics you explained, For example, Here in near east university, there is this kind of biometrics used to sign in personnel when the resume work, to record the time they came in and the time they go out. So you see, so many people use this kind of biometrics, so there is a risk of bacterial contamination, if care isn't taken, anyone can get infected" (Participant 7).

"For the contact biometrics, I think there might be health risk especially during this covid-19 time but for the contactless, I don't think there is any health risk because even with its scans the face for an instant, it uses cameras and digital recognition" (Participant 11).

While few participants believed biometric technology can present radiation and accuracy risk. Below are some expressions of participants on the health risk presented.

"In terms of iris biometrics, I think it can be harmful to the human eye in the long run because it uses some kind of light to scan the eye. But it depends on the individual" (Participant 1).

"Biometrics itself doesn't involve any risk but the accuracy of measures taken involves risk because when it comes to the simple parameter like blood pressure in a patient if that parameter is not taken with accuracy, it can affect the diagnoses of the patient." (Participant 4).

"The retinal scan, I don't think there are enough studies on it but I believe studies are still going on. Maybe it might have some health risk due to the energy it uses" (Participant 7).

"The truth is most of these technologies have radiation which we all know regardless of being contact or contactless, so we can't ignore the fact that there can't be even the smallest amount of radiation that can affect our health. We cannot say the damages those radiations might cause in a long run. But I believe any biometric devices that are powered by electricity are emitting a form of radiation" (Participant 12).

The majority of participants believe biometrics poses no risk, however after some explanation about contact and contactless biometric technology; they began to notice a tiny variation in risk. Then, many participants feel that touching an infected biometric surface poses a direct health risk, and that, despite the low risk in contactless biometrics, it can still pose a risk to human health due to radiation and a lack of reliable measures.

4.1.6 Negative outcomes of using biometric technology

The participants' view on the negative outcome of using biometric technology is aimed to find out more on the negative possibilities involving biometric technology. Two themes were obtained with their frequency and percentage is shown in Table 4.5 below:

Table 4.5: Negative outcomes of using biometric technology

Themes	Frequency	Percentage
No	14	93.3
Yes	1	6.7

As seen in Table 4.5 above, many participants in the medical sector state that biometric technology has no negative outcomes. Some of the participants' statement that has something to say to this question other than the expressions obtained in short answer "*no"* are stated below.

"From my perspective, I can't come up with any negative outcomes of biometrics. There might be but to the best of my knowledge, I don't think there are any negative outcomes to the use of this technology" (Participant 4).

"Well, in all aspects of life, there are always positive and negative outcomes. But I think it is much more important to look at the positive side of it. For example, in medicine, when we give patients drugs, it doesn't mean that the drugs don't have side effects but we try to minimize these side effects to the lowest level. So with biometrics, I don't see any side effects" (Participant 7).

While one participant has some different to say about the negative outcomes of biometric technology. Participant expression is stated below.

"As I said before, radiation can be the negative outcome of using biometric technology" (Participant 12).

When questioned about the negative outcomes of using biometric technology, the majority of the participants stated that there are none, whereas one participant believes that radiation may be involved in the use of biometric technology.

4.1.7 Point of view on the ID2020 alliance conspiracy

The ID2020 alliance is a sustainable development goal that aims to provide legal identity to every individual. The concept of this idea is to implant a chip into the human body as a means of identification and authentication. This section aims to know participants' view on the new biometric technology conspiracy. Table 4.6 below shows the themes that were obtained with their frequency and percentage based on whether participants "Agree", "Disagree" or "Indifferent" about this idea of biometrics.

Table 4.6: Participants' point of view on the ID2020 Alliance conspiracy

Themes	Frequency	Percentage
Disagree	10	66.7
Indifferent	3	20
Agree	2	13.3

As noted above, the majority of participants in the medical sector disagree with the idea as they think of it as very harmful to the human body and a form of privacy invasion. Below, some of the participants' expressions on this question.

"From a microbiology point of view, I think this can cause a lot of infection long term. So I don't agree with this kind of technology" (Participant 1).

"First, we have to consider the health implications of nanobots. Now nanobots are technologies that can be controlled once they are in the human body system. So that means you can be controlled by this kind of technology. This is not the kind of technology that should be allowed" (Participant 3).

"Maybe it is helpful, reduces a lot of workloads but right now is thinking of the risk. The lack of privacy, so for me I won't accept this technology. Time changes though, so maybe in the future, I can accept it if I fully understand the measures. But right now, I won't" (Participant 7).

"Well, it's a good thing to find ways to make life easier but we never know the effect of these technologies until in a long run, everyone's body system is different, 100 people might get it and be perfectly fine with it but 101 people can get it and have a serious reaction to it. Also, it means if it can identify, then it has a form of charge in it which is transmitting constant radiation through the body system. So try and picture this technology in a child and elderly person. So without a doubt, it will have some serious side effects" (Participant 12).

While some of the participants are unsure if it is a good idea or not, they are in a state of uncertainty. The expressions obtained are listed below.

"The main question we should be asking ourselves is if this technology is ethical or not. So it can be ethical to some extent but beyond that, it is unethical because it doesn't respect human rights. Some people are already living with implanted devices in their body to help them survive, so if those devices can be accepted, definitely this technology also can be accepted to an extent but it all depends on ethics" (Participant 4).

"I heard some time that implanted devices like this are used for concurrent diagnose but here in near east hospital, we don't use that. We don't have much research on this kind of technology so I can't say if it is a good or bad idea" (Participant 5).

"I know this is a conspiracy theory to the best of my knowledge. So maybe it can be used for data mismanagement. So I am not sure if it is a good or bad development but sometimes it can be harmful and if it is used correctly for the right reasons, it can be very helpful to the development of biometric technology and it should be considered if it is good for people or not" (Participant 6).

Few participants agree with the idea since they see things from a different view. The expressions obtained are listed below.

"It's a good and a bad idea because if it only uses for identification and authentication, then it is the next level of biometrics. There is no need to carry your documents around but at the same time, can you be sure that's the only purpose it will be used for and it also depends on what data it holds. I agree to it one hundred percent if it's only for identification purposes" (Participant 10).

"Generally I think it makes the whole means of identification easier and faster, for example in airports, there will be lesser queue and delays and in terms of privacy, I don't see any difference from our mobile phones cause any individual can still be tracked by using a mobile phone. Even if it will be used for any other purpose, it will probably be in terms of security, maybe to find criminals. If you think about it, if the whole population has this kind of device, there is no point tracking every one of them" (Participant 11).

All participants in the medical sector claim they have never heard of this kind of biometric technology, thus an explanation was given to them to gather their thoughts on the matter. Ten (10) participants disagree with this idea, while three (3) are indifferent about it and two (2) agree to it.

4.1.8 Future expectations of biometrics in the medical sector

Participants were asked about their thoughts on how big they think biometrics will become in the future (in the next 10 years), to gain insight into their view on the future of biometrics. The following are some of the participants' thoughts on the subject.

"It will go more than its current stage like now we have voice recognition in cars, mobile devices. If all this happened 10 years ago, imagine where it will be now, maybe by now, cars might even sense the presence of their owner and just open. Science is constantly improving, so definitely I will be huge in future" (Participant 12).

"10 years from now, I feel everything we do will be based on Biometrics. Like AI, maybe we will have robots by then" (Participant 13).

"if am to scale 1-10 the rate at which biometrics will go 10 years from now, I will say 7 because technology is one of the fastest things humans adapt to" (participant 7).

"It will grow very large actually." (Participant 4).

"In some countries, I think it is moving very fast but in north Cyprus, at the scale of 1-10. I will say 5 because it depends on the area of application and how mandatory it will be" (Participant 1).

With no doubt, biometric has a bright future in the medical sector. Biometric technology, according to all participants, will be very big in the future because it is already being adopted in different fields.

4.1.9 Manipulation of biometric technology

Traditional security methods like passwords and pins can be easily manipulated but biometric technology has been said to be the modern form of security that involves human characteristics compared to the traditional ways. The response obtained from participants were used to create two themes with their frequency and percentage rate as seen in Table 4.7 below.

Table 4.7: Participants' view on biometric technology manipulation

Themes	Frequency	Percentage

Yes	2	13.3
No	13	86.7

As shown in Table 4.7 above, majorities of the participants say biometric technology cannot be manipulated easily except extreme steps are taken. Below are a few of the expressions obtained.

"Am not sure how that is possible, but it cannot be as easy as the pin and password hacks" (Participant 3).

"Compare to the password and all, I will say biometric is safer and cannot be manipulated unless an individual is been forced. But without that, it will be extremely hard" (Participant 12).

Two (2) participants gave a clear explanation of how biometrics can be manipulated. Below is what they have to say.

"Yes, everything that is human-made, can be manipulated. We already have DNA rearrangements, DNA manipulation in labs. So as far as we have that, we can hack other forms of biometrics" (Participant 4).

"It can be manipulated but it has to be through organized crime. For example, if before it takes just looking at someone's password to manipulate their privacy, you know desperate times attract desperate measures, so if the criminal is fully committed to stealing data, they can go to the extent of cloning fingerprints or cutting off the fingers maybe, so yes it can be manipulated" (Participant 7).

The majority of participants from the medical sector agree that biometric technology cannot be manipulated, whereas two participants feel that biometric technology can be manipulated if greater attention is paid to it.

4.1.10 Ethical rules and policies governing biometric technology

Rules and policies are expected to be followed in the development and adaptation of any technological devices to prevent human privacy and rights. There are committees assigned to evaluate these ethical rules and policies. Participants were asked if they are aware of any

rules, policies, or regulations governing the use of biometric technology. The following are some of the responses received from participants when asked this question.

"No, am not aware of any" (Participant 4).

"Data in biometrics should follow certain guidelines, I don't know if there are any rules. If there isn't then there should be to protect human rights" (Participant 10).

"Can't say I know any policies actually" (Participant 12).

"No, I don't" (Participant 2).

"I have no idea" (Participant 1).

All participants in the medical sector have no idea of any rules surrounding the use of biometric technology. The most response is "*no*".

4.2 Engineering Professionals' View on Biometric Technology

4.2.1 The current state of biometrics in the engineering sector

As part of this study, the aim of understanding participants' view about the current state of biometric technology in the engineering sector was obtained. All participants gave a response which is presented in Table 4.8 below under three themes with frequency and percentage rate.

Table 4.8: Participants' view on the current state of biometrics in the engineering sector

Themes	Frequency	Percentage
Strong	5	100
Limited state	0	0
Weak	0	0

As shown in Table 4.8 above, All participants gave a positive response, some of the responses obtained are presented below.

"With recent technology and likes of apple for an instant, biometrics has gone beyond what it used to be in terms of RFID (Radio Frequency Identification) biometrics that uses

tags and pin. It now involved unique identifiers like fingerprint and face IDs. So I will say it is fast trending" (Participant 1).

"Currently, biometrics has become very popular and advanced, there is a lot of research and it is moving into mainstream unlike before when it used to be a complex technology but as of now, we use it daily in our phones to access applications and all. And there is another kind of biometrics coming into mainstreams which are not popular yet" (Participant 3).

"It's pretty much advanced at the moment, I mean; it's been integrated into many things" (Participant 4).

From various views, participants in the engineering sector all gave a significant responses. This demonstrates that biometric technology is advancing in the engineering sector.

4.2.2 Participants' personal biometrics experience in professional life

Understanding participants' professional life experience with biometric technology aims to give more insight into their experience with biometric technology. Participants were asked the question, creating two themes alongside their frequency and percentage as shown in Table 4.9 below.

Table 4.9: Participants' personal biometrics experience in professional life

Themes	Frequency	Percentage
Yes	5	100
No	0	0

As shown in Table 4.9 above, all of the participants have significant experience with biometric technology. Below are some expressions from participants' view.

"I use it daily, to have access to my phone and laptop (Lenovo). In the past, I made use of RFID which is radio frequency identification, so that was integrated with some locks to control doors, so that way a user can only gain access via a card/tag or pin a pin-like I said earlier" (Participant 1).

"I had a project in 2016 that involves using biometrics to capture student's fingerprints for attendance since it is a unique feature in the human body" (Participant 2).

"I have been involved in some research that is biometrically related" (Participant 3).

"I read some researches on face recognition that reads patterns of user's face to extract some particular features" (Participant 5).

There were no participants with a *"no"* response, indicating that engineering participants are more familiar with biometric technology.

4.2.3 Contribution of biometric technology in the engineering world

Participants were asked about their opinions on the impact biometrics has made on the engineering sector intending to understand this question from their view. Participants' response is collected under two themes. The frequencies of these themes are presented in Table 4.10 below.

Table 4.10: Participants' view on biometrics contribution

Themes	Frequency
Security	5
Identification	5

As seen in Table 4.10 above, all participants gave opinions on the contribution of biometrics in the engineering sector. Below are some expressions obtained.

"So far, it has been a good development for technology and the world at large, in the sense that security has been enhanced, so with the help of biometrics, you can't have easy access to a system unlike the old way of brute force attack of passwords because this time around it deals with unique identifier" (Participant 1).

"it has contributed security-wise, most time its use to identify individuals. so it has contributed a lot in terms of security" (Participant 2).

"It has contributed a lot especially when it comes to security, most of the applications we see involving biometric are mainly for security like the safety of data. And also, for identifying individuals, the government use most times" (Participant 3).

"It has made a lot easier, more insecurity and identification" (Participant 4).

Security and identification were mentioned by all of the participants as benefits of biometric technology in the engineering sector.

4.2.4 Technical factors and challenges faced in biometrics development

The goal of this section was to find out what participants thought about the technical factors and challenges that are encountered during the biometric technology development. Themes generated from the responses are shown in Table 4.11 below.

Table 4.11: Participants' view on factors and challenges that are faced during the development of biometric technology

Themes	Frequency
Tools for development	2
Compatibility	2
Unique identifiers	1

As seen in Table 4.11 above, Participants gave a different point of view when asked the technical factors and challenges that are encountered during the biometric technology development. Two participant stated that tools to be used in the development of the technology should be considered. Below are expressions of participants that gave points on the tools used for the development of biometric technology.

"I think few of the factors to be considered for example in voice recognition which uses natural language processing in Artificial intelligence is to ensure that the system is smart enough to recognize a voice at different age stage so the user doesn't have to update it frequently and this is also a challenge, to match the pitch of a user's voice at different age stage" (Participant 1).

"Using three-dimensional cameras should be considered as a factor to avoid future manipulation and identify individuals" (Participant 5).

While some other participants feel compatibility is a major factor that should be considered. One of the participants' expressions is presented below.

"Most times, compatibility issues are a big challenge. There are software development kits that are not compatible with certain computers, sometimes, your code is right but then it's not just working because there are certain compatibility issues involved with the system being used" (Participant 2).

Then one participant stated that unique identifiers should be considered to avoid problems at the end of the development. The expression obtained is presented below:

"When it comes to biometrics, the key thing is to look for a way to uniquely identify individuals, so first of all, you need to look for features that are unique to individuals e.g. finger, and eye, etc. and the system needs to be very sophisticated. In terms of challenges, I will say the availability of data, which is one of the most difficult challenges faced by developers" (Participant 3).

The technical factors and challenges faced during the development of biometric technology seem to be an essential aspect of biometrics. To avoid inadequate results in the development of biometric technologies, certain factors like compatibility, unique identifier and tools should be considered.

4.2.5 Participants' view on ID2020 conspiracy

ID2020 alliance being a sustainable development goal that aims to provide legal identity to every individual and a concept of implanting a chip into the human body as a means of identification and authentication. This section aims to gain an insight into participants' view on the new biometric technology conspiracy. Table 4.12 below shows the themes that were obtained with their frequency and percentage based on whether participants "Agree", or "Disagree" about this idea of biometric technology.

Table 4.12: Participants' point of view on the ID2020 Alliance conspiracy

Themes	Frequency	Percentage
Disagree	5	100
Agree	0	0

As noted above, all participants in the engineering sector disagree with the idea. Below, some of the participants' expressions on this question.

"No, I don't buy the idea. Simply because we are dealing with microchips here and the human body has its consistency, so putting metal into it could lead to damages to the human body and more so, I think the world is becoming a smart village, where everyone uses a smartphone which uses NFC (near field communication), so NFC can be used in terms of microchips and apple is developing something called a smart tag compare to the bill which seems to want to destroy humans for some reasons" (Participant 1).

"No, I don't support this idea because most people don't know what it involves and I believe it is much more complicated than what they show to the public" (Participant 2).

"First of all, we have to look at this from a different perspective. If we are thinking of the damages, I think people who developed this technology would have that into consideration. If we look at it regarding privacy, it's not a good idea. So in my opinion, it's not the best idea. " (Participant 3).

"It's unnecessary. We already know every individual has something unique. So this idea is not necessary" (Participant 4).

"This idea is not good, to me; it takes right to privacy away from people" (Participant 5).

No participant agrees with this idea. All participants believes the technology is not necessary as there are alternative technologies that poses no harm to human life and privacy.

4.2.6 Future expectations of biometrics in the field of engineering

To obtain insight into participants' ideas on the future of biometrics, they were asked how big they anticipate biometrics would grow in the future (in the next 10 years). The following are some of the opinions expressed by the participants on the topic.

"It will be huge because most industries now integrate AI and almost every part of human lives. So with AI in collaboration with Biometrics, it will grow big fast than expected. And I think one of the advantages of that will be response time will be really fast." (Participant 1).

"Right now, I feel many people don't know about this technology, so let say in 10 years with proper awareness people will understand what it is and adapt to it" (Participant 2).

"I feel it will be into a lot of things, here at the university, I have started seeing students researching biometrics. So it will go into a lot of mainstream things in future" (Participant 3).

"Biometrics has vital importance for any human identification. Deep learning in artificial intelligence is the future of biometrics" (Participant 5).

According to participants, the future of biometrics is positive with the use of AI and deep learning, and it will become increasingly important since it has improved approaches for identification, authentication, and security.

4.2.7 Manipulation of biometric technology

When compared to traditional security systems, biometric technology provides a superior level of protection. Traditional security measures such as passwords and pins can be effortlessly manipulated, but biometric technology is regarded to be the safest option. Participants' responses were used to produce two themes, each with a frequency and percentage rate, as shown in Table 4.13 below.

Table 4.13: Participants' view on biometric technology manipulation

Themes	Frequency	Percentage
Yes	5	100
No	0	0

As indicated in Table 4.13 above, Participants agree that biometric technology can be exploited, but only with extreme measures. Expressions obtained are listed below.

"It cannot be easily manipulated but at the same time, it could be manipulated which will take a lot of expertise to manipulate biometrics and it just has to do with studying the owner of the device to see where the user has touched and all to extract what is needed to carry out the manipulation" (Participant 1).

"I don't know how it's done but I know fingerprints can be stolen and use it to carry out whatever intentions it's planned for" (Participant 2).

"Well of course there are ways in terms of faking fingerprints and taking pictures to manipulate facial recognition" (Participant 3).

"To manipulate biometrics will be difficult" (Participant 4).

"I read about Samsung phones face recognition and putting someone picture in front of the camera which unlocks the phone. But now I think it has been improved. So these are ways biometrics can be manipulated" (Participant 5).

Biometrics can be altered, according to engineering participants, but it will take a lot of effort. Participants believe that modern biometric technology can be exploited because all technology has a backdoor, but that this technology will be difficult to manipulate compared to traditional techniques of identification.

4.2.8 Ethical rules and policies governing biometric technology

To protect human privacy and rights, rules and laws must be observed in the development and application of any modern technology. Committees have been formed to assess these ethical standards and practices. Participants were asked if they were aware of any biometrics-related guidelines, policies, or regulations. Some of the participants' responses were as follows:

"I have not done any research into the ethical aspects of biometrics but I can vouch that the likes of BCS (British Computer Society) will have certain rules in place in regards to biometrics" (Participant 1).

"No, I can't remember any rules" (Participant 2).

"I don't know of rules. I haven't looked into it" (Participant 3).

"No, I don't know of a particular rule or committee." (Participant 4).

"I don't know any ethical rules on biometrics" (Participant 5).

Participants in the engineering sector all responded with a resounding *"no"*, It appears that the participants has no knowledge of the rules and policies surrounding biometric technology.

4.3 Discussion

Biometric technology is a technology that measures human physiological or behavioral characteristics for identification, authentication, and security. The biometrics aspect in this study is about the advancements in biometric technology. According to the data collected from the medical and engineering participants, it has appeared that the majority of participants in the medical sector are not aware of biometrics as a word but are more conscious after a few explanations that they can relate to while participants in the engineering sector seem to have more knowledge about biometric technology. This could be because the majority of the engineering participants have either worked on biometric technology development or conducted research on the topic, and/or biometrics is closely tied to the technological world than the medical world. As a result, engineering participants have greater knowledge and expertise with the topic than medical participants.

The majority of participants from both sectors indicate that biometric technology is rapidly advancing in the sectors. The finding reveals that biometric technology has proven to be more efficient and accurate for identification and data security, which has given the technology more attention in the medical and engineering sector, and also, the world in general. Nevertheless, few medical participants feel that biometric technology poses a danger to human health, particularly for those with specific health problems. These hazards, according to the participants, cannot be eliminated, but must be controlled if biometric technology is to be utilized in the sectors. Biometrics has more positives than negatives, according to participants from the medical and engineering sectors, because it is less hazardous and gives better security.

CHAPTER 5
CONCLUSION AND RECOMMENDATIONS

This chapter presents the conclusion and recommendations of the study based on the results of the research conducted.

5.1 Conclusion

The use of biometrics in our daily and professional activities seems to be regular but very unmindful when it comes to what biometrics is all about. Biometrics which has provided a unique means of identification and authentication for the security and privacy of data has been proven based on results to be difficult to bridge. Biometrics involvement with deep learning and artificial intelligence is concluded to be the future of biometric technology. This study aims to investigate the advancements in biometric technology from the medical and engineering views. The research has examined the data collection through different point of views in the aspect of what biometrics is about, what surrounds the technology, and what it has to offer in the future.

Based on qualitative data analysis, the results of the response obtained from participants show that the majority of participants (especially participants from the medical sector) have little knowledge of biometrics even though they use it in its simplest form on daily basis. This simply proves the point that many people use technology for its usefulness and ease of use than they understand the damages and advantages of technology before use. Participants from the medical sector understood more of the risk biometrics may present to human life while the participants from the engineering sector understood the technicalities of biometric technology than its relationship to human health but the common understanding between the two sectors is the basic security and identification purpose of biometric technology.

The findings of this study demonstrate the potential for biometric technology to flourish when properly studied and integrated. Biometrics has great prospects, but lack of expertise and opportunity in the medical and engineering sectors has hampered its expansion possibilities. This research shows a review and expectation of biometric technology based

on data collected from the medical and engineering sectors as a whole. Further research into biometric technology is planned as a follow-up to this study.

5.2 Recommendations

Biometric technology has contributed to the improvement of data security and identification methods. However, there are still some gaps in the study of biometric technology that requires attention. The following recommendations have been made for future studies in biometric technology.

- Courses on biometrics should be thought in classes to allow students to understand the full advantage of biometrics and also to increase awareness on biometric technology.
- Adaptation to biometric technology should be increased by integrating more biometric technologies in offices and classes for the purpose of identification.
- Research on biometric technology should be encouraged so that researchers can obtain a better understanding of the scope of biometric technology.

REFERENCES

Adams, W. C. (2015). Conducting Semi-Structured Interviews. *Handbook of Practical Program Evaluation*, *1*(4), 492–505. https://doi.org/10.1002/9781119171386.ch19 *Advantages and disadvantages of biometrics | Mitek*. (2020, April 6). Www.miteksystems.com. https://www.miteksystems.com/blog/advantages-and-disadvantages-of-biometrics

Anil, L. H., Hong, L., Jain, A., and Pankanti, S. (1999). *Can Multibiometrics Improve Performance?* CiteSeer. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.3.7621

Asha, M., Vipul, M., Singh, K., Bhavesh, M., Mr, S., Subramanian T, and Student. (2018). *Face Recognition Using Principle Component Analysis*. Retrieved May 19, 2021, from http://www.iaetsdjaras.org/gallery/5-april-638.pdf

Asha, S., and Chellappan, C. (2012). Biometrics: An Overview of the Technology, Issues and Applications. *International Journal of Computer Applications*, *39*(10), 35–52. https://doi.org/10.5120/4859-7134

Ashok, J., Shivashankar, V., and Mudiraj, P. V. G. S. (2010). An overview of biometrics. *International Journal on Computer Science and Engineering*, *2*(7), 2402-2408. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.301.2569&rep=rep1&type=pdf

Boukhonine, S., Krotov, V., and Rupert, B. (2005). Future Security Approaches and Biometrics. *Communications of the Association for Information Systems*, *16*. https://doi.org/10.17705/1cais.01648

Chan, H.-L., Kuo, P.-C., Cheng, C.-Y., and Chen, Y.-S. (2018). Challenges and Future Perspectives on Electroencephalogram-Based Biometrics in Person Recognition. *Frontiers in Neuroinformatics*, *12*. https://doi.org/10.3389/fninf.2018.00066

Christopher, U. E., Amujo O. E., Oluwasegun A., and Silas, F. (2019, July). *Privacy Concerns in Biometrics*. ResearchGate; unknown.

https://www.researchgate.net/publication/338395600_Privacy_Concerns_in_Biometrics

Daugman, J. (2004). How Iris Recognition Works. *IEEE Transactions on Circuits and Systems for Video Technology*, *14*(1), 21–30. https://doi.org/10.1109/tcsvt.2003.818350

Delgado-Mohatar, O., Fierrez, J., Tolosana, R., and Vera-Rodriguez, R. (2020). Blockchain meets Biometrics: Concepts, Application to Template Protection, and Trends. *ArXiv:2003.09262 [Cs]*. https://arxiv.org/abs/2003.09262

Delgado-Mohatar, O., Fierrez, J., Tolosana, R., and Vera-Rodriguez, R. (2019). Blockchain and Biometrics: A First Look into Opportunities and Challenges. *ArXiv:1903.05496 [Cs]*. https://arxiv.org/abs/1903.05496

Dessimoz, D., Richiardi, J., Champod, C., and Drygajlo, A. (2007). Multimodal biometrics for identity documents (). *Forensic Science International*, *167*(2-3), 154–159. https://doi.org/10.1016/j.forsciint.2006.06.037

Dharavath, K., Talukdar, F. A., and Laskar, R. H. (2013, December 1). *Study on biometric authentication systems, challenges and future trends: A review*. IEEE Xplore. https://doi.org/10.1109/ICCIC.2013.6724278

Faundez-Zanuy, M., Fierrez, J., Ferrer, M. A., Diaz, M., Tolosana, R., and Plamondon, R. (2020). Handwriting Biometrics: Applications and Future Trends in e-Security and e-Health. *Cognitive Computation*, *12*(5), 940–953. https://doi.org/10.1007/s12559-020-09755-z

Fierrez, J., Morales, A., Vera-Rodriguez, R., and Camacho, D. (2018). Multiple classifiers in biometrics. Part 2: Trends and challenges. *Information Fusion*, *44*, 103–112. https://doi.org/10.1016/j.inffus.2017.12.005

Galterio, M., Shavit, S., and Hayajneh, T. (2018). A Review of Facial Biometrics Security for Smart Devices. *Computers*, *7*(3), 37. https://doi.org/10.3390/computers7030037

Harakannanavar, S. S., Renukamurthy, P. C., and Raja, K. B. (2019). Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends. *International Journal of Advanced Networking and Applications*, *10*(4), 3958–3968. https://doi.org/10.35444/ijana.2019.10048

Hashiyada, M. (2011). DNA biometrics. *Biometrics*. https://doi.org/10.5772/18139

Hu, M. (2013). Biometric ID Cybersurveillance. *Indiana Law Journal*, *88*, 1475. https://heinonline.org/HOL/LandingPage?handle=hein.journals/indana88&div=48&id=&page=

Jahankhani, H. (2007). *A review on Biometrics in the Past, Present and Future*. Repository.uel.ac.uk. https://repository.uel.ac.uk/item/866q8

Jain, A. K., Pankanti, S., Prabhakar, S., Lin Hong, and Ross, A. (2004, August 1). *Biometrics: a grand challenge*. IEEE Xplore. https://doi.org/10.1109/ICPR.2004.1334413

Jain, A. K., Ross, A. A., and Nandakumar, K. (2011). Introduction. Introduction to Biometrics, 1–49. https://doi.org/10.1007/978-0-387-77326-1_1

Jain, A. K., Ross, A., and Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, *14*(1), 4–20. https://doi.org/10.1109/tcsvt.2003.818349

Latonero, M., and Hiatt, K. (2019, April 15). *Digital Identity in the Migration and Refugee Context*. Data and Society. https://datasociety.net/library/digital-identity-in-the-migration-refugee-context/

Liu, Y. (2008). Identifying Legal Concerns in the Biometric Context. *Journal of International Commercial Law and Technology*, *3*, 1. https://media.neliti.com/media/publications/28661-EN-identifying-legal-concerns-in-the-biometric-context.pdf

Loeb, S., Morris, P., Dynarski, S., Reardon, S., Mcfarland, D., and Reber, S. (2017). *Descriptive analysis in education: A guide for researchers*. https://files.eric.ed.gov/fulltext/ED573325.pdf

Masayuki, M. (2018). *Special Issue on Social Value Creation Using Biometrics The Future Evolution and Development of Biometrics Studies*. Retrieved March 7, 2021, from https://www.nec.com/en/global/techrep/journal/g18/n02/pdf/180204.pdf

Matyáš, V., and Říha, Z. (2002). Biometric Authentication — Security and Usability. *Advanced Communications and Multimedia Security*, 227–239. https://doi.org/10.1007/978-0-387-35612-9_17

McCombes, S. (2019, May 15). *Descriptive Research Design | Definition, Methods and Examples*. Scribbr. https://www.scribbr.com/methodology/descriptive-research/

Mohsin, A. H., Jalood, N. S., Baqer, M. J., Alamoodi, A. H., Almahdi, E. M., Albahri, A. S., Alsalem, M. A., Mohammed, K. I., Ameen, H. A., Garfan, S., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Bin Ariffin, S. A., Alemran, A., Enaizan, O., Shareef, A. H., and Jasim, A. N. (2020). Finger Vein Biometrics: Taxonomy Analysis, Open Challenges, Future Directions, and Recommended Solution for Decentralised Network Architectures. *IEEE Access*, *8*, 9821–9845. https://doi.org/10.1109/access.2020.2964788

Morosan, C. (2016). Opportunities and Challenges for Biometric Systems in Travel: a Review. *Travel and Tourism Research Association: Advancing Tourism Research Globally*. https://scholarworks.umass.edu/ttra/2011/Oral/61/

Normalini, M.K., and Ramayah, T. (2017). Trust in Internet Banking in Malaysia and the Moderating Influence of Perceived Effectiveness of Biometrics Technology on Perceived Privacy and Security. *Journal of Management Sciences*, *4*(1), 3–26. https://doi.org/10.20547/jms.2014.1704101

Palinkas, L. A. (2013). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. Administration and Policy in Mental

Health and Mental Health Services Research, 42(5), 533–544. https://doi.org/10.1007/s10488-013-0528-y

Pato, J., and Millett, L. (2010.). *Visit the National Academies Press online and register for... Biometric Recognition: Challenges and Opportunities*. https://dataprivacylab.org/TIP/2011sept/Biometric.pdf

Phadke, S. (2013). The Importance of a Biometric Authentication System. *The SIJ Transactions on Computer Science Engineering & Its Applications (CSEA)*, *01*(04), 18–22. https://doi.org/10.9756/sijcsea/v1i4/0104550402

Phillips, P. J., Flynn, P. J., Scruggs, T., Bowyer, K. W., Chang, J., Hoffman, K., Marques, J., Min, J., and Worek, W. (2005). *Overview of the Face Recognition Grand Challenge*. CiteSeer. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.85.4375ss

Prabhakar, S., Pankanti, S., and Jain, A. K. (2003). Biometric recognition: security and privacy concerns. *IEEE Security & Privacy Magazine*, *1*(2), 33–42. https://doi.org/10.1109/msecp.2003.1193209

Quadri, S. L., Kazim, A., and Aditya, A. (2017). Cloud and Biometrics: The Future of Authentication. *International Journal of Advanced Research in Computer Science*, *8*(2). https://doi.org/10.26483/ijarcs.v8i2.2936

Revett, K., and de Magalhães, S. T. (2010). Cognitive Biometrics: Challenges for the Future. *Global Security, Safety, and Sustainability*, 79–86. https://doi.org/10.1007/978-3-642-15717-2_10

Ribeiro Pinto, J., Cardoso, J. S., and Lourenco, A. (2018). Evolution, Current Challenges, and Future Possibilities in ECG Biometrics. *IEEE Access*, *6*, 34746–34776. https://doi.org/10.1109/access.2018.2849870

Singh, S. (2019). The role of speech technology in biometrics, forensics and man-machine interface. *International Journal of Electrical and Computer Engineering (IJECE)*, *9*(1), 281. https://doi.org/10.11591/ijece.v9i1.pp281-288

Srivastava, H. (2013). A Comparison Based Study on Biometrics for Human Recognition. *IOSR Journal of Computer Engineering*, *15*(1), 22–29. https://doi.org/10.9790/0661-1512229

Syazana-Itqan, K., Syafeeza, A. R., Saad, N. M., Hamid, N. A., and Bin Mohd Saad, W. H. (2016). A Review of Finger-Vein Biometrics Identification Approaches. *Indian Journal of Science and Technology*, *9*(32). https://doi.org/10.17485/ijst/2016/v9i32/99276

Taherdoost, H. (2016). Validity and Reliability of the Research Instrument; How to Test the Validation of a Questionnaire/Survey in a Research. SSRN Electronic Journal, 5(3). https://doi.org/10.2139/ssrn.3205040

Teherani, A., Martimianakis, T., Stenfors-Hayes, T., Wadhwa, A., and Varpio, L. (2015). Choosing a Qualitative Research Approach. *Journal of Graduate Medical Education*, *7*(4), 669–670. https://doi.org/10.4300/jgme-d-15-00414.1

Thakur, R. K. (2015). Biometric Authentication System: Techniques and Future. *International Journal*, *3*(6). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1047.4731&rep=rep1&type=pdf

Thomas, E., and Zhang, A. (2020). *ID2020, Bill Gates and the Mark of the Beast:: how Covid-19 catalyses existing online conspiracy movements*. JSTOR. https://www.jstor.org/stable/resrep25082

Tiwari, S., Chourasia, V., and Chourasia. (2015). A Review of Advancements in Biometric Systems. *International Journal of Innovative Research in Advanced Engineering (IJIRAE) Issue, 1*. https://www.ijirae.com/volumes/Vol2/iss1/30.JAEC10091.pdf

Tolba, A. S., El-Baz, A. H., and El-Harby, A. A. (2006). Face recognition: A literature review. *International Journal of Signal Processing*, *2*(2), 88-103.

Tolosana, R., Vera-Rodriguez, R., Fierrez, J., and Ortega-Garcia, J. (2018). Exploring Recurrent Neural Networks for On-Line Handwritten Signature Biometrics. *IEEE Access*, *6*, 5128–5138. https://doi.org/10.1109/access.2018.2793966

Wieslaw B., (2006). *Future of biometrics*. Retrieved March 7, 2021, from https://www.optel.eu/uploads/PDF%20ENG/future%20of%20biometrics.pdf

Woodward, J. D. (1996). Biometrics: Identifying Law and Policy Concerns. *Biometrics*, 385–405. https://doi.org/10.1007/0-306-47044-6_19

Yang, W., Wang, S., Hu, J., Zheng, G., and Valli, C. (2019). Security and Accuracy of Fingerprint-Based Biometrics: A Review. Symmetry, 11(2), 141. https://doi.org/10.3390/sym11020141

Zhong, Y., and Deng, Y. (2015). A Survey on Keystroke Dynamics Biometrics: Approaches, Advances, and Evaluations. *Gate to Computer Science and Research*, 1–22. https://doi.org/10.15579/gcsr.vol2.ch1

APPENDICES

APPENDIX 1

YAKIN DOĞU ÜNİVERSİTESİ

BİLİMSEL ARAŞTIRMALAR ETİK KURULU

16.03.2021

Dear Omonayajo Babatomiwa A

Your application titled **"Future Advancement in Biometric Technology"** with the application number NEU/AS/2021/116 has been evaluated by the Scientific Research Ethics Committee and granted approval. You can start your research on the condition that you will abide by the information provided in your application form.

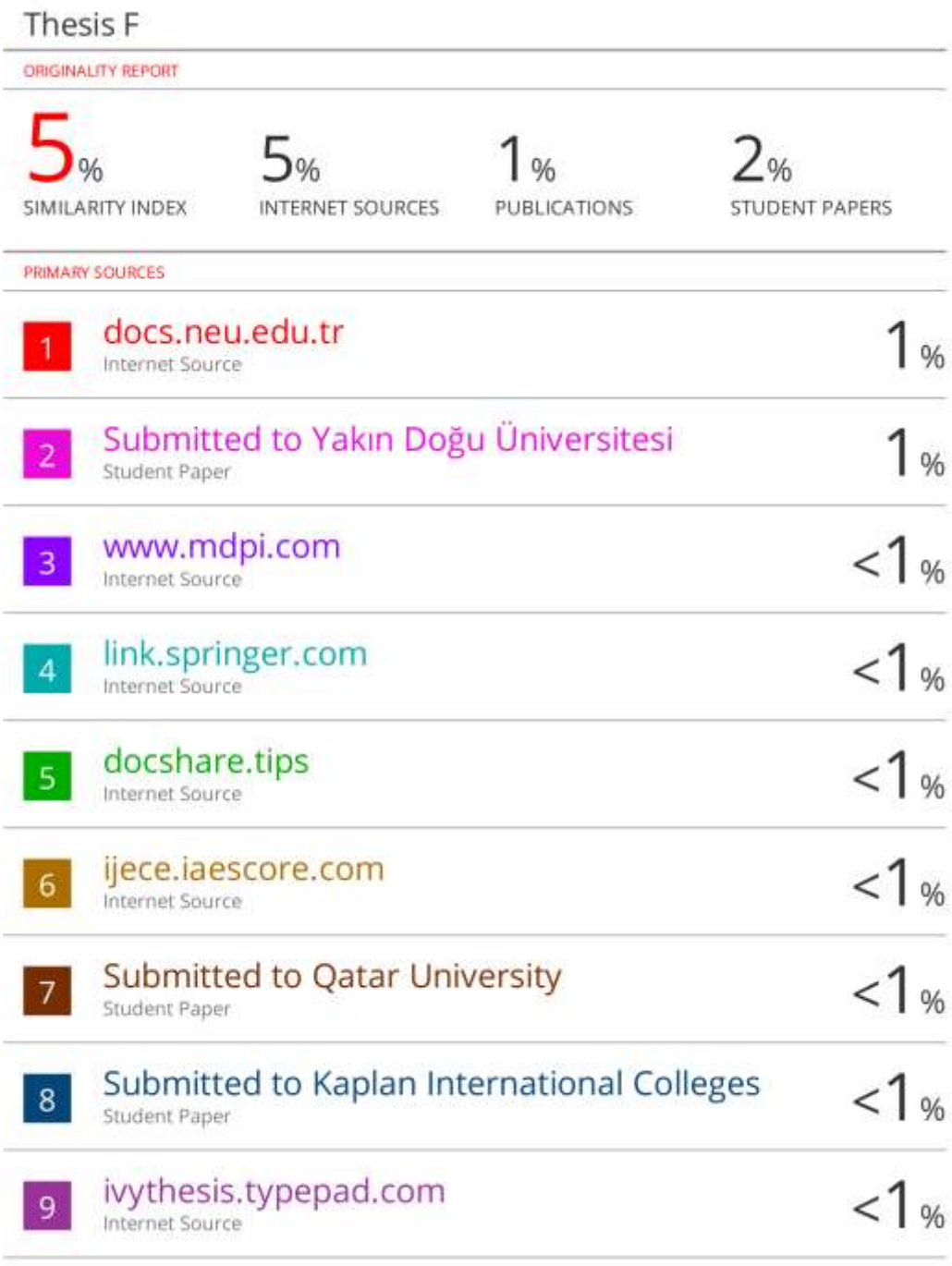
Assoc. Prof. Dr. Direnç Kanol

Rapporteur of theScientificResearchEthicsCommittee

Direnc Kanol

Note: If you need to provide an official letter to an institution with the signature of the Head of NEU Scientific Research Ethics Committee, please apply to the secretariat of the ethics committee by showing this document.

SIMILARTITY REPORT



Thesis F

ORIGINALITY REPORT

5%	5%	1%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	docs.neu.edu.tr Internet Source	1%
2	Submitted to Yakın Doğu Üniversitesi Student Paper	1%
3	www.mdpi.com Internet Source	<1%
4	link.springer.com Internet Source	<1%
5	docshare.tips Internet Source	<1%
6	ijece.iaescore.com Internet Source	<1%
7	Submitted to Qatar University Student Paper	<1%
8	Submitted to Kaplan International Colleges Student Paper	<1%
9	ivythesis.typepad.com Internet Source	<1%