ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOCTORAL (PhD) THESIS

`

LAFEE ALSHAMAILEH

The use of biometric systems in critical infrastructures and their role in cybersecurity: Aviation industry focused

Supervisor: Prof. Dr. Kovacs Tibor and Prof. Dr. Rajnai Zoltan

`

DOCTORAL SCHOOL ON SAFETY AND SECURITY SCIENCES

Complex Exam Committee:
President:
Prof. Dr. László Pokorádi
Members:
Dr. habil. Tamás Berek
Dr. Endre Szűcs

Public Defence Committee:
President:
Prof. Dr. János Besenyő
Secretary:
Dr. habil. Andrea Tick
Members:
Dr. Nguyen Huu Phuoc Dai
Dr. Károly Fekete
Dr. Sándor Magyar
Reviewers:
Dr. Judit Lukács
Dr. András Tóth

Date of the Public Defense:
2023

CONTENTS

DECLARATION

I, Alshamaileh Lafee, am a student of Óbuda University, at Donát Bánki Faculty and the Doctoral School on Safety and Security Sciences. Hereby declare that I entirely wrote this PhD thesis, except where it is denoted in the references.

1 INTRODUCTION

What are the consequences of a biometric database breach? Is biometric a trustworthy option for vital infrastructures? In the future, may someone travel without a passport or other required documents? Overall, how will biometric technology enhance security and productivity? In the context of biometric solutions for critical infrastructures, these and other problems often arise. This dissertation investigates the security and privacy offered by biometric technologies in the context of critical infrastructures. The phrase "critical infrastructure" was first used in the October 1997 Report on the Protection of Critical Infrastructure by the United States Presidential Commission. The shaped substructures of society and the state are the channels required for these systems' existence. Infrastructures consist of the systems and questions utilized to provide transportation or fundamental requirements such as energy, health, water, food, job, and security. Airports, nuclear power plants, government institutions, the military-industrial base, primary communications and transportation networks, etc., are examples of key infrastructures. Paid shopping, transportation, energy, nuclear power, water, food-agriculture, chemistry, health, emergency services, reproduction-finance, public policies, industrial sector, services, and infrastructures become much more prominent. We must be recognized to pass a border, conduct financial transactions, and unlock our cellphones. This has led to the formation of a new technology field known as biometric recognition, or biometrics [1]. The fundamental objective of biometrics is to reliably and automatically distinguish between individuals based on one or more signals obtained from physical or behavioral traits, such as the face, fingerprint, iris, voice, hand, signature, etc. These qualities are sometimes referred to as biometric characteristics. Even though automated person identification has been studied for more than four decades [2], biometrics was not formed as a distinct scientific field until the past decade. As indicated by recent references, particular conferences [3], shared benchmark tools and assessments, worldwide cooperative initiatives, international consortia devoted exclusively to biometric identification, standardization efforts, and growing government and business interest.

Biometric technology offers various benefits over traditional security systems based on what you know (PIN, password, etc.) or what you have (key, card, etc.). These systems require the user to know complicated PIN numbers, which are often forgotten or to carry a key, which is easily lost or stolen. On the other hand, biometric recognition is founded on the enticing notion that "you are your own key, " which cannot be misplaced or forgotten. Moreover, typical recognition systems cannot distinguish between impostors who have unlawfully obtained access rights to a system and the true subject, nor can they fulfil negative claims of identification (e.g., I am not John Doe) [4]. Some large-scale efforts, such as the Indian Unique ID [5] and the Smart Borders package [6], have lately used biometrics as their identification technology for these reasons. In addition, biometric systems have lately been used in the banking industry [European Association of Biometrics (EAB), 2015], reaching our smartphones through applications for individual banks, generic payment apps such as ApplePay or LoopPay, and even Mastercard's payments.

Moreover, biometric ATMs are presently being implemented. Despite these benefits, biometric systems have some disadvantages [7], such as the lack of secrecy (e.g., everyone knows our face or could obtain our fingerprints) and the fact that biometric characteristics cannot be replaced - if we forget our password, we can easily generate a new one. However, if an impostor "steals" our fingerprint, we cannot generate a new one. Recently, a database storing the fingerprints and personal information of over one million government US workers was hacked. Such a breach will directly affect the lives of the impacted workers, who may seek "lifetime identity protection coverage" as a result.

For biometric systems to become a permanent part of the security market, it is important to develop new ways to protect templates and keep people's privacy. This will improve the security and privacy of this technology.

The protection of biometric data is necessary to prevent outside attacks that violate the subjects' right to privacy and make the most of the benefits these systems provide to the subjects who have volunteered their information. In order to accomplish this goal, hashes [8], cryptographic techniques, and fuzzy extractors have been applied to biometric templates; nevertheless, doing so has resulted in a decrease in the verification accuracy in the vast majority of circumstances. Concerning the standardization of such protection techniques, the International Organization for Standardization (ISO) did publish an international standard on the security evaluation of biometrics in 2009 (ISO/IEC JTC1 SC27 IT Security Techniques), but this does not apply to the standardization of such protection techniques. ISO/IEC 19792:2009 is a standard released in 2009 that evaluates the safety of biometric technologies [3], work on the creation of worldwide standards did not begin until the most recent few years of this century. The International Organization for Standardization (ISO) has just published the first standard for the security of biometric information, and it is now working to produce an international standard for testing template protection systems.

Despite these efforts, there is still a considerable distance to go until a standardized technique for the security of biometric systems is established and used as it is for other information technologies. This dissertation aims to shed light on the complex issue of strengthening the security and privacy of biometric systems by presenting effective study-cases that may limit the consequences of prospective assaults and raise the congruence of the subjects in this booming technology. In this approach, the experimental findings provided in this dissertation might contribute to the current standardization efforts to enhance biometric systems' security and efficacy.

1. I assume that the biometric system will gain significant ground with broader usage in the future

   Cyberattack on the smart power grid (under review)

   Alshamaileh Lafee 1, Kovacs Tibor2

2. I assume that installing a biometric system at critical infrastructures, especially in airports, will enhance safety and security

   L. Alshamaileh and A. Őszi, "Biometric system in the aviation industry (second part)," Biztonságtudományi Szemle, vol. 3, no. 1, pp. 25–33, 2021.

3. I assume that when institutions install biometric systems are not always considering the cost first but efficiency in usage

1.1 BIOMETRIC SYSTEMS AND MODALITIES

Biometric systems are basically pattern recognition systems that use biometric traits to identify persons. As stated before, the goal is to construct an identity based on who you are or what you create rather than what you own or know. This paradigm not only improves security but also eliminates the need for several passwords and various authentication tokens in recognition applications. Whom you are referring to is based on physiological traits, such as the face, iris, and fingerprint. What you generate refers to the learned behavioral patterns that define your identities, such as your walk, handwriting, and signature.

A biometric template is a digital model of a biometric identifier. The system database holds reference templates acquired during the enrollment or training method shown in the below mentioned Figure 1. Many current biometric systems use a centralized database, whereas others allow for decentralized access to the information (as in Match-on-Card systems where each subject carries the only copy of his template on a personal card). Two methods are available for carrying out the recognition process [4] once individuals have been entered into the system:

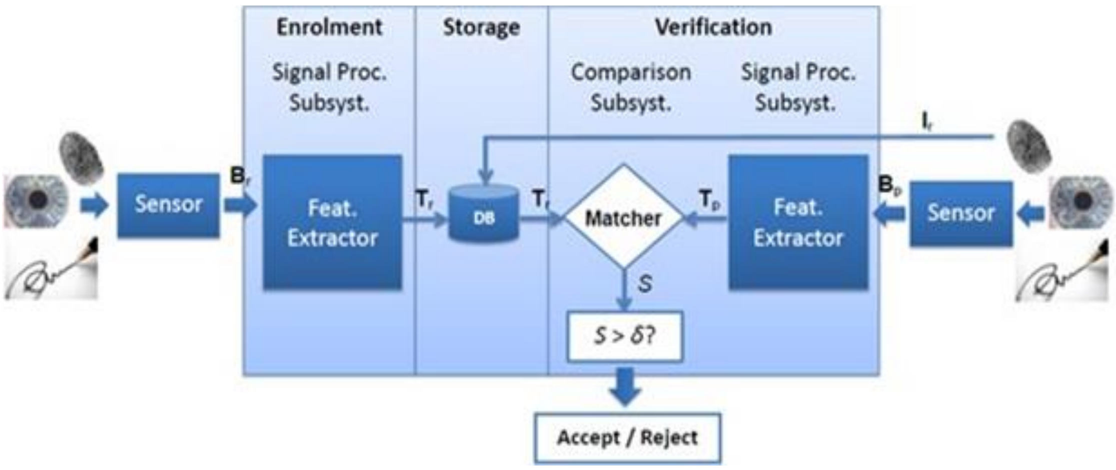

Figure 1 Diagram of the two processes involved in a verification system: enrolment (left) and verification (right). Both processes occur at different points in time, being enrolment always prior to verification [10]

- **Identification**: When operating in this mode, the system will pose the question, "Is this person already in the database?" The answer might be "no," which would indicate that the system does not recognize the person in question, or it could be one of the registered identities included in the database. As a consequence of this, the system has to carry out a one-to-many matching method in order to be able to compare the input sample to all of the templates that have been saved. When using the identification mode of operation, the system will typically return, in a ranked fashion, those identities that are more likely to be the searched person in a previously created database (i.e., those with a higher similarity score). Following this, a human expert will decide whether or not the subject is among this reduced group of individuals. [11] One of the most prevalent types of identification applications is the use of computerized fingerprint identification systems.

• **Verification:** In this particular situation, we are interested in identifying whether or not a person is who they say they are, and if not, why not. The users, or targets, are known to the system as a result of the registration process; however, the impostors might be from any global population (Fig. 1 left). The reference templates are acquired from the biometric input samples (Br) and then saved in a database throughout this stage.

To verify a given individual, however, the systems need two inputs (Fig. 1 right): the probing biometric sample (bp) and the claimed identity (Ir), which corresponds to one of the previously recorded templates in the database. The system compares the supplied biometric sample (particularly the template derived from this probe sample (Tp)) to the enrolled template (Tr) linked with the claimed identity, providing a score (S). This score is then compared to a specified verification threshold to decide whether the person is a client (the identity claim is approved, S > b) or an imposter (S b). Typical uses for authentication include network login, ATMs, physical access control, credit card transactions, and so on.

Several techniques and approaches proposed in this dissertation may be easily modified for identification systems. As stated before, several biometric traits have been presented and used in various applications [4]. In principle, any human trait that meets the following criteria may be used as a biometric identifier:

• **Universality** indicates to what extent a biometric is present in the world population

• **Distinctiveness** means that two persons should have sufficiently different biometrics.

• **Permanence** indicates that the biometric should have a compact representation invariant over a sufficiently large period.

- **Collectability** refers to the ease of the acquisition process and the ability to measure the biometric quantitatively. Other criteria required for practical applications include the following:

- **Performance** refers to the efficiency, accuracy, speed, robustness, and resource requirements of implementations based on biometrics.

- **Acceptability** refers to whether people are willing to use the biometric and in which terms.

- **Circumvention** reflects the difficulty of fooling a system based on a given characteristic by fraudulent methods.

The ideal biometric system should be capable of fulfilling every one of these objectives. Regrettably, there is not a single biometric feature that meets all of the criteria at the same time. Even while certain forms of biometric identification, such as fingerprints and irises, have a high degree of individuality, it is still extremely simple to circumvent the security procedures they use (e.g., using a gummy finger or an iris-printed photograph). On the other hand, some types of biometrics, such as human vein patterns, are very tough to get around, but they are also difficult to get a hold of. A multi-biometric system combines more than one kind of biometric identifier to compensate for the shortcomings of a single biometric system. This type of system is also known as an integrated biometric system. When employing multimodal biometric systems, the verification accuracy rises, the recognition system becomes more resistant to sensor or subsystem failures, and the number of cases in which the system cannot make a determination lowers. In addition to these benefits, multimodal biometric systems offer many additional advantages (e.g., bad quality biometric samples due to bad acquisition or deterioration).

1.1.1 Biometric efficiency in aviation

Biometrically linked identities – where, for instance, your face serves as your boarding card – are one of the essential technologies that will aid airlines and ports in restarting operations more effectively. This will also assist in boosting passenger trust and identification verification to satisfy conventional security demands while mitigating health threats. However, deploying biometric technology alone will provide only limited advantages to airports and airlines. The advantages are multiplied when biometric technology is integrated with other technologies to improve identity integration, traveler automation, and self-service [12].

Global airlines are in the middle of implementing biometric boarding as the next stage in boarding aircraft. No boarding permits are required, and the passport or identification card may stay in your pocket. Instead, a camera identifies the passenger and allows them to board the aircraft. Vision-Box, a solution provider operating at airports such as Amsterdam-Schiphol and Aruba, uses the term "Seamless Flow." In other nations, biometrics is already widespread. Biometric boarding is already in use in the United States, including on Lufthansa flights; the new Beijing airport is fully equipped with biometric systems, and similar systems are also in operation in New Zealand, the United Arab Emirates, France, and Finland.

The manufacturers have made great promises, but they can be summed up in one point: improved use of the current airport infrastructure. In a future scenario, the journey with biometrics begins early, even at home. The employees, visitors, and passengers then save face via the app, and that is all. According to the vision box, it will likely be another ten to fifteen years before this occurs.

Face recognition at an airport machine is already a reality. This information is subsequently used in the check-in line. Cameras identify the person, and the data is sent straight to the check-in employees. This strategy is also applicable when dropping off luggage at baggage machines. If local border security officials collaborate, a traveler may even pass through an exit while being observed by cameras. [13]

1.1.2 Problems and gains

I have named problems under the regulatory problems and efficiency as efficiency gains in below:

- **Regulatory problems**: There is a basic issue with the lack of global standards and the absence of comparable rules in many locations. Therefore, entrance and departure will likely continue to be handled manually for the foreseeable future. This inconsistency suggests that even passports with the ePassport emblem are not recognized in every nation. Typically, approvals are granted exclusively in certain nations. There is often a need for a specific residency status or a particular registration with the border authorities of each country. After departure, the frequent flyer proceeds to the lounge, where he or she recognizes and welcomes the passenger while the other biometrically recorded passengers amuse themselves at the boarding gate. Obviously, this does not substitute group or row-based boarding. The traveler is required to recall this information without a boarding card. According to the vision box, however, the group is projected from above in front of each Brazilian airport passenger. Therefore, the issue has been addressed in theory.

- **Efficiency gains:** As check-in, boarding, and other similar touchpoints are referred to by experts, biometric techniques are intended to boost efficiency at all of these touchpoints. For instance, there is no need to look for identification at the check-in desk, the border may be passed without a pause at the machines, and the makers guarantee time savings when boarding. There is savings potential for airlines and airports. Not necessarily with the workers since the procedures were already automated. Many travelers only interact with workers at the security checkpoint. Even at the entrance, there are increasing numbers of machines. The majority of the efficiency potentials in the presently prevalent instances relate to manual operations or wide-body aircraft entrance. In big airplanes with two aisles, for instance, a limit of five seats per aisle must be occupied. Typically, there are many entry doors, and entrance traffic jams are uncommon. If, on the other hand, you are familiar with boarding narrow-fuselage aircraft on short-haul routes with a 3-3 seat configuration, you already know that even with biometric boarding passes, you can hardly expect time savings, given that these aircraft are frequently filled with tariffs that generate more hand luggage, resulting in longer boarding times [14].

1.1.3 Acceptance factors and security goals

To provide a system based on a user-friendly biometric mechanism with a high degree of security, it is vital to comprehend the acceptability variables and the security objectives sought. Particularly challenging in the context of biometrics-based security architecture is the execution of the following requirements:

Security refers to the effort required to be acknowledged as a certain person by a biometric system without having access to the appropriate biometric feature. The objective of an assault on security is to forge identification documents and perhaps cheat security services based on their access control measures. There are technical-algorithmic and organizational components of security, which will be described here.

Protection of personally identifiable information: the specified protection objective refers to the effort necessary to get biometric data or derive it from the biometric system. An attacker who seeks to compromise personal data compromises the privacy and hence the personal rights of the affected individual and may potentially acquire unlawful access. For this reason, a successful assault is also a security breach in the form of identity theft. In addition, a breach is a severe issue since sharing biometric features is difficult, unlike with passwords.

This concept encompasses simple learnability, efficient and intuitive usage, and the avoidance of mistakes during use. Consequently, user-friendliness is a criterion that is orthogonal to or even in rivalry with the two preceding acceptance elements. When analyzing the user-friendliness of a system, the issue of which prospective users construct mental models - that is, what thoughts exist about the interaction with the system and how these concepts vary from the actual usage - emerges. As biometric methods are not yet extensively used, a period of familiarization might be anticipated. For IT security systems, another general usability element comes into play, which may be translated as a cognitive load: secure authentication based on knowledge, for example, may require the user to remember passwords of a certain length and complexity. Minimizing this cognitive burden without compromising security is, therefore, a significant task [15].

2 PROBLEM DESCRIPTION

Applying biometric technology to identify people in critical infrastructures and travelers across borders between countries has recently increased in important places and various international transit ports. Using biometrics can significantly help eliminate impersonation among travelers and prevent the entry of undesirable people into a particular country, preventing crimes and various terrorist acts. The main goal is to expose the infiltration of criminals and terrorists across the border and accelerate completing procedures inside the critical infrastructure buildings, which achieves travelers' satisfaction, saving time and cost together. The COVID-19 virus has brought a blow to all aspects of our lives. The aviation and travel industries are among the hardest hit and require a major redesign to rebuild and restore passenger confidence in safe and healthy air travel. Therefore, biometrics in aviation systems spread comfort and safety, as it does not require touching, only scanning the face from a distance. Biometric technology uses networks and clouds to transmit information. Also, it is directly engaged in IoT and clouds. Thus, the risk of a cyberattack on biometric databases is significantly dangerous and possible at any time. A biometric system should be built safely, from direct workers to hackers' cyber attacks.

2.1 OBJECTIVES

The main objectives of this study are:

- Examine how biometrics and occupational safety are effective in critical infrastructures, especially in airports.
- Provide a detailed description of what biometric applications in critical infrastructures are.
- Review the evaluation of biometrics in airports and questionnaires to be implemented.
- Extend the research about biometrics, cyber security attacks and their role in biometric.
- Perform experimental procedures detailing biometrics' importance and risk management's biometric role.
- Analyze the biometric efficiency data collected in the experimental case study to find an association between characteristics.
- Identify how biometric applications contribute to occupational safety and security.
- Unify efficiency in critical infrastructures, cost, and time factors

2.2 RESEARCH METHODS

The research methods used in this work consisted of the following elements:

- A comprehensive review of current scientific literature about topics such as biometrics, aviation safety, security, biometric applications, and cyber security.
- Preliminary research comprised a questionnaire about the biometric effect in the aviation industry. The target was random passengers and employees who interact with biometric systems daily.

- Preliminary research comprised a questionnaire about the biometric systems which are most used. The efficiency of these installed systems and the economic cost of them.
- Case study: The attack on the Ukrainian power grid
- The next chapter discusses the use of the biometric system in the aviation industry, provides deep insight into the term "risk management", and gives some examples of installing biometric technologies in critical infrastructures and aviation in general.

3 THE BIOMETRIC SYSTEM IN THE AVIATION INDUSTRY

Recently, biometric systems have been investigated and examined in many fields but have only lately entered the public consciousness because of high-profile applications, usage in several media and increased practice by the public in routine activities. The origins of biometrics are provided by the National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management; "biometrics" is derived from the Greek words "bio" (life) and "metrics" (to measure). Per Merriam-Webster dictionary, biometrics is defined as the measurement and analysis of unique physical or behavioral characteristics, especially to verify personal identity. Iris images, facial photographs, some types of voice patterns, palm prints, fingerprints and DNA are a small range of recent biological features, commonly referred to as modalities, used to classify individuals [16].

Considering their behavioral and organic qualities, biometrics is a method for the computerized identification of individuals. Face, fingerprints, hand geometry, iris, speech, signature, gait, and keystroke are the most common biometric modalities [17].

"Biometrics" is described as a process where detectable biological (anatomical and physiological) and behavioral characteristics are based on automated methods of recognizing an individual. At the beginning of civilization, humans used faces to recognize known (familiar) and unknown (unfamiliar) characters. Face recognition based on geometric characteristics is one of the most accepted methods for identification since facial features are unique to every human being. Biometric data must be reliable (safe and operating at a reasonable level of efficiency) and acceptable (non-invasive and socially tolerable). In addition, it must ensure universal, unique, permanent, and measurable features [155]. Human-to-human identification is also used in behavioral-predominant biometrics such as speaker recognition and gait recognition. Individuals use these traits, somewhat unintentionally, to identify recognized individuals daily [18]. This essential role has gradually become more stimulating as populations have grown.

The National Science and Technology Council acknowledged that automated biometric systems have only become possible over the last few decades because of substantial developments in the field of data processing. However, all these modern computerized systems are based on concepts initially formulated hundreds of years ago [18].

It is a way to ensure that one deals with individuals who are already established (or not known) and therefore fit into a category with certain privileges (or to a group denied certain treats). It depends on the fact that people have different physical and behavioral characteristics. The Airport Council International (ACI) rely on the importance of having a robust airport position on biometrics, and they published a position paper entitled “The Application of Biometrics at Airports” to give a general encouragement for the planning and application of biometrically enabled border control, passenger simplification and access control systems [19].

The pioneer biometric system used in Europe is called RAPID. Portugal used it for border control, as each passenger must use an electronic passport. Figure 2 shows a photo of Smart Gate (Facial and Fingerprint) Brisbane International Airport from Frontex, 2010 [156].

First, a photo of the traveler taken at the automated gate and current confirmation in the electronic passport with facial biometrics is processed. Subsequently, the automatic gate will open, allowing the traveler to enter.

Figure 2 Photo of Smart Gates (Facial and Fingerprint) Brisbane International Airport from Frontex, 2010 [20]

In the Netherlands, the Privium system is used as a voluntary option for frequent flyers, as described in Figure 3. This system is designed to speed up the passport control process of passengers, so in some busy airports or at other passport control points, it can be a nightmare to wait in a long queue, especially for people who are late for an appointment. It is worth mentioning that in order to benefit from the Privium system, a Privium card is needed, which can be obtained with a yearly fee [157].

Figure 3 Photo of Privium system in the Netherlands (Iris Scan) from Airport Business, 2009 [21]

Let us take Europe as a case. Both passengers entering or exiting the Netherlands are forwarded to a separate border control line where booths accept the Privium smart card as the traveler's biometric data is stored in a smart card, and the iris prototype is stored. Iris cameras are used to check a traveler's identification against an intelligent card. The software has been highly successful in the Netherlands [22].

Passenger classification may also facilitate the safety protocol in the aviation industry. Poole classified the traveler as the proposed risk-based method to affect the concentration on identifying hazardous persons to

(i) Low-risk passengers, of whom a great deal is known.

(ii) High-risk passengers, based either on lack of awareness or clear negative information; and

(iii) Ordinary passengers, mainly in-frequent travelers and leisure travelers [23].

Low-risk travelers have a current federal security clearance or have been admitted into the Approved Traveler Program. High-risk travelers are those who do not have a paper trail, so little is understood that the best thing to do is to presume the worst and to perform a comprehensive screening of both the individual and the luggage, and ordinary travelers are those in between the other two risk categories [23].

This measure would help to improve security monitoring in terminal lobby areas and outside the airport, in ramp areas and across the airport periphery. A different approach to both the screening of travelers and the screening of bags will apply to each category. There are several known biometric modalities, e.g. (face, hand geometry, iris, voice, etc.), see Figure 4, and it is worth mentioning here that there is no biometric modality suitable for all implementation as there are several aspects to take into consideration during the modality's selection and the biometric toll such as security risk, location, number of users and the available data. Moreover, it is significant to note that biometric modalities are subject to change in the phases of maturity.

Figure 4 Biometric Modalities [24]

On the other hand, the different sorts of biometric modalities do not all have the same level of consistency. Physiological measurements are usually considered to offer the benefit of remaining more constant during any person's life. Behavior-based identification may be affected by stress, which is not true for measurements based on physical features.

3.1 TECHNIQUES FOR BIOMETRIC DATA MANIPULATION

Several techniques for biometric data manipulation were listed in the literature, such as recognition, pattern categorization filtering, convolution, and Fourier transforms. It is favorable that an applied biometric method is the simplest possible. Some sophisticated decision-making algorithms that are also capable of making errors take the top place of the system, also having an important role in the relationship between a human and a machine. In this section, we consider verification and identification.

Biometrics is defined in two ways:

(i) Authentication in this system applies to one biometric and one biometric examination (1:1) to verify that the person is who he says he is.

(ii) Recognition relates one biometric to a biometric database (1:N) to find out who the individual is [25].

Biometric systems have sequences of crucial procedures that must be accomplished to

(i) Allows a person to use the system and

(ii) Verify or authenticate an individual's identity [19]. These vital processes contain:

- Enrollment – the capture of the raw biometric
- Development of a prototype – Preservation of the biometrics by using an algorithm to obtain a model from the input images, which will then enable the image to be matched to others using the same technique. Identification – takes new biometric samples and compares them to saved templates of all enrolled users.
- Verification – takes new biometric samples of a specific user and compares them to old samples taken from the same user.

A sequence of measures within a system as a multi-step process summarizes the concept of a biometric system. In other words, everyone shows several aspects of themselves;

after that, a sensor seizes this aspect and transforms it into an algorithm model. The registered model is then matched to the reference sample or baseline algorithms saved in the system database. The result of the comparison decides the next corresponding response, such as entry into a secure structure. Figure 5 shows a schematic diagram for a basic biometric system. The main component of the biometric system is a sensor in which data will be generated in the form of signals such as electromagnetic spectrum. Biometric data processing techniques in the second part involve different filtering, transformation, and pattern recognition algorithms. Therefore, decision-making mechanisms are used in many phases of the operation of biometric data. The third component is the hardware platform for the implementation of these techniques. Usually, a set of processors are used as a hardware platform for biometric devices and systems.

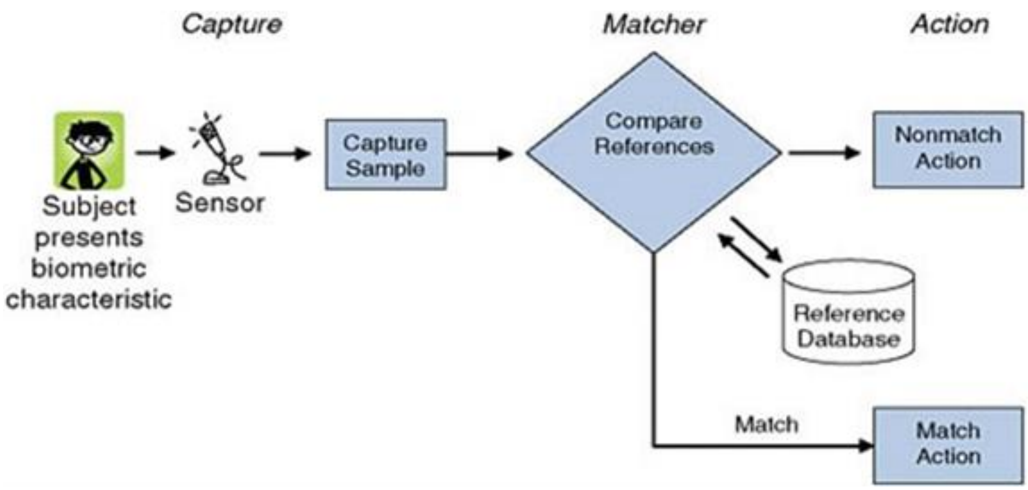

Figure 5 A Schematic Diagram for Basic Biometric System [26]

Verification or authentication technologies are basically one of the following:

(i) Things the person knows, like a password or

(ii) Something the individual has, such as a physical key or cards and

(iii) Something the individual is or does. Biometric systems can function without active input, user cooperation, or knowledge that the recognition is taking place. Thus, the last one is usually employed with biometric technologies. However, a biometric system does not store biometric data, as unprocessed or incomplete biometric data cannot be used to conduct biometric contests. The method whereby the user's biometric data is initially obtained, analyzed, treated, and saved in the form of a prototype is called enrollment [27]. So, identification follows three phase schemes: data acquisition, techniques, and computing platform. Creating a biometric system is the implementation of application-specific techniques (methods, algorithms, and programs) using some computing platform. Figure 6 describes how the biometric tolls generally work, so after the sensors receive a biometric character of the person, this data matches with his database from the data store. Finally, all the results about the subject person are saved or confirmed.

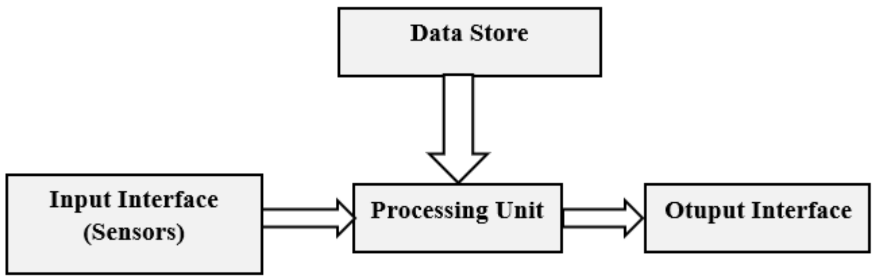

Figure 6 Biometric system is an application-specific computer system consisting of specific-purpose programs and computing platforms [27]

Biometrics can be used as biometric screening to multi-biometric systems. Biometric screening systems use a single source of biometric information, while multibiometric use several parameters. A multi-biometric system reported by Bartlow and Zekste is illustrated in Figure 7. The multi-biometric system depends on more than one basis of biometric feedback and can be used to cover lacks from one biometric signal. Debatably, such systems can also provide other sources, such as biographical, document-based travelling, etc. [28].

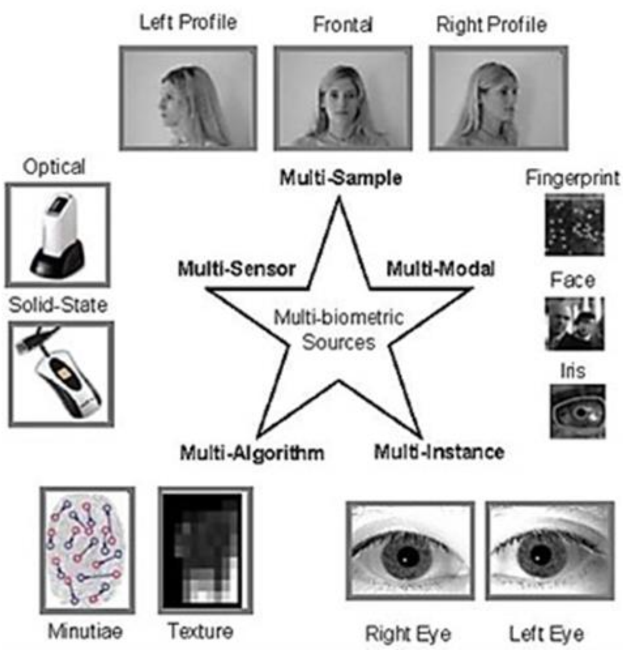

Figure 7 Multi-biometric system from Bartlow and Zekster [28]Figure 7

Another example of the integration of biometric data is the attack tree presented by Schneier, as he performed a qualitative method to present a security risk analysis [29]. In his model, several biometric approaches are created, as shown in Figure 8.

It is worth noting here that with the sophistication of the biometric authentication approach from (single/multi) factor monomodal to (single/multi) factor multimodal biometric authentication methods, a higher security advantage is produced [30]. Merging several biometric data is used to increase system precision.

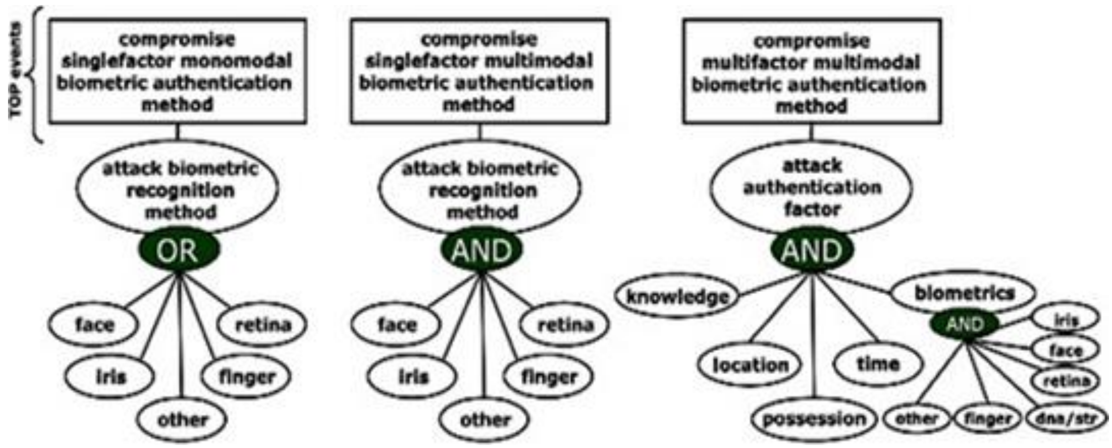

Figure 8 General attack trees for (single| multi) factor (mono |multi) modal biometric authentication methods [29]

3.2 POPULATION BASE, REDUCTION OF FAILURES TO ENROLL

In any biometric system, several issues should be considered in particular. Acceptability determines the degree to which individuals can accept the use of a specific biometric identifier (characteristic) in their everyday lives. Efficiency, which can relate to many factors:

(i) The accuracy and the speed of the recognition achieved.

(ii) The specifications of the needed resources.

(iii) The organizational and environmental factors.

After contemplating the security risk of biometric verification strategies, scientists have come to more secure and dependable prototypical research arrangements like the one presented by Hong and Jain, with multimodal biometric strategies (biometric combination procedures) [31] and with multifaceted multimodal biometric validation techniques by Bromme and his co-worker [30]. An example of a High-Level Component and Process Model for Integrated Security Risk Analysis of Biometric

Authentication Technology was introduced by Eric P. Haas [30]. As shown in Figure 8, his model applies to several research and models, such as the one published by Schneier, as he presented attack trees. A general attack tree for different types of biometric methods can be constructed showing a security risk analysis in a qualitative way [29], and the one published by Leveson for the safety analysis technique of fault trees [32]. Figure 9 shows that the security attacks on biometric technology can be classified using three specific categories:

1. Sensor abuse (copy, falsification, similarity attacks)
2. Attacks on data exchange (replay attacks) and
3. Attacks on the servers (integrity attacks).

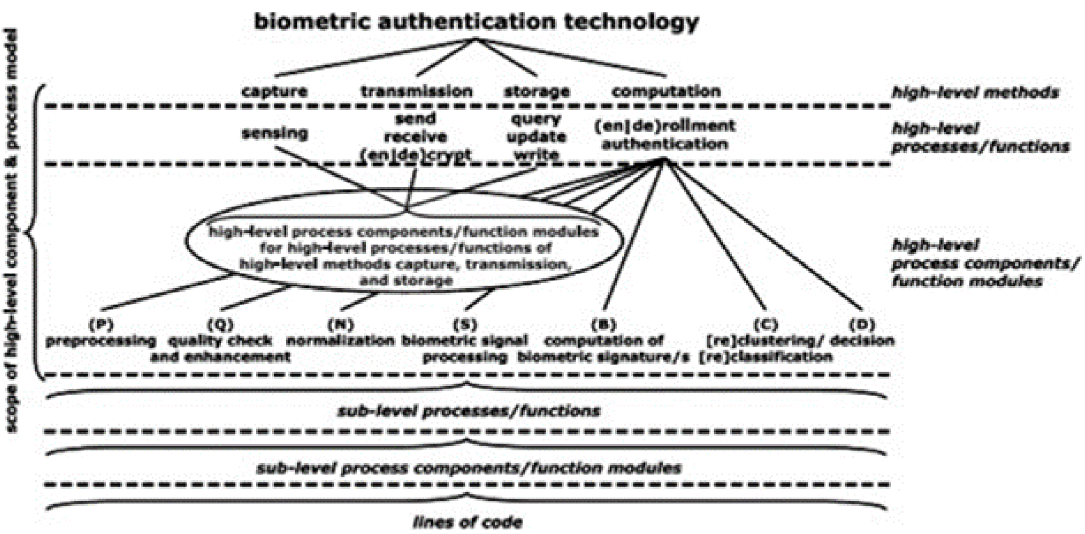

Figure 9 High-Level Component & Process Model for integrated Security Risk Analysis of Biometric Authentication Technology [30]

Software attacks and thus provides a clear understanding of the biometric processes used in bio-authentication technology [33].

3.3 BIOMETRIC IN AIRPORTS

The International Civil Aviation Organization (ICAO) asserts that biometric technology has the potential to provide a one-of-a-kind method for identifying persons based on one or more behavioral or physical features. In this scenario, it is very necessary to emphasize that the most recent recommendations for best practices are based on iris scans, fingerprints, and photographs of the face [68]. "Technology interface that permits clients to generate a benefit free of coordination benefit representative engagement" is how self-service technologies such as ABCs (Automated Border Control) are described (Meuter et al., 2000) [69]. E-gates, like any other kind of self-service system, need to have user-friendly and intuitive interfaces, be simple to recall, provide users with thorough advice, and provide universal access. The South African Social Security Agency Sasse makes the following observation: " We can evaluate usability based on three criteria: task performance, user happiness, and user cost" (Sassa 2007: 78). The user's ability to engage with the ABC gate effectively and efficiently is directly tied to the level of performance achieved in the task. When users can accomplish their objective and finish the job of having their passports scanned and their face pictures recorded effectively, the exchange is said to have been successful. If they can pass through the electronic gate in a reasonable amount of time, then the interaction with the gate is effective. The amount of mental or physical labor required by the user, in addition to other factors, might influence their degree of (subjective) pleasure. Last but not least, user cost considers how the interaction will affect the user in terms of their health and safety [70].

3.3.1 Airport’s characteristics

The airport’s characteristics refer to the internal features of the airport that may influence the expectation of using biometric technology for access control. According to Tornatzky and Fleischer (1990), organizational factors are considered when determining the predisposition to adopt an innovation [71].

Because of increased passenger and aviation activity, larger airports may be a higher priority target for terrorists. As a result, security requirements are more significant at larger airports and their related infrastructure. The location of the airport might affect the growth of biometric technology. Because of their proximity to more densely populated areas and increased passenger traffic and aviation activity, airports in urban areas are more likely to become a target for terrorists because of their proximity to higher populated areas and higher passenger traffic and aviation activity [72]. Airport classification is standard in air transport research, and previous research has demonstrated the necessity and appropriateness of grouping airports based on common characteristics. As of now, categories have been based primarily on airport size (including cargo tonnage), geographic location, overall functioning, nature of traffic, usage and technical characteristics, ownership, and network location [73].

3.3.2 Pre-Screening at the time of booking

The proposed new approach would compel travelers to provide personal information at the time-of-flight booking. Using the information given by the consumers, a risk rating will be assigned to each traveler. The traveler with the highest risk rating would be asked for further information. According to experts, this new development should not be considered an annoyance but a step in the right direction [74]. The new biometric security system would check the identification of travelers using biometric data. Due to its high level of dependability and user-friendliness, fingerprint access control is the most common airport security system. Nonetheless, alternative biometric security technologies, such as retinal scans and facial patterns, are gaining traction [75].

Due to the requirement for luggage checks, according to experts, this would result in longer wait times for passengers. In light of this, airports recommend that travelers come two to three hours early. However, sceptics argue that this would dissuade people from flying, signaling the end of the ailing aviation industry. However, its deployment is almost certain when homeland security is a factor [76].

3.4 RISK BASED SECURITY APPROACH

Modern risk analysis frameworks for bio-authentication technologies are limited to admission and identification/verification procedures, with bio-algorithms primarily considered to be running as part of the system with no clear indication of how they operate.

US-VISIT Program stated that the core of any biometric identification system is the database, which has all the previously stored biometric characteristics for base comparison. [16] Data base life cycle can be divided into four phases: collection, use, disclosure, processing, and retention-destruction [34].

Governments follow many protocols to keep these data at a high privacy level, as there are many arguments from civil libertarians regarding the accumulation of such personal data. Numerous citizens are anxious about the governmental intrusion, which can cause discomfort for the individual. For instance, the DHS Chief Privacy Officer claimed that “if the databases were combined, the government would enforce strict regulations on which agencies could use traveler information and how it could be accessed.” [35]

3.5 BIOMETRIC SYSTEM AND AIRPORT SECURITY

Air travel has become a standard in international travel between countries and even domestic flights between cities. Reducing air travel costs close to the costs of land travel made air travel preferable to land travel in terms of costs and reducing travel time, which causes airports to become more crowded. Citizens, diplomatic visitors, government officials, foreign and domestic tourists, and immigrants pass through airports to travel from one city to another. This makes airports vulnerable to provocation attempts and terrorist acts and creates security vulnerabilities in them.

Since terrorism has become a global threat, security weakness cannot be tolerated. However, it is impossible to fill this security gap by increasing the number of security personnel or resources allocated to security. Because of the congestion of airports, security personnel cannot pay attention to more than one problem or verify more than one situation simultaneously. There are inevitable gaps and blind spots in such an environment, so airport security must be handed over to flexible and scalable technology and systems. The People's Republic of China is one of the leading states in this field. Within the context of the social credit system, which was originally introduced in 2018, China may extensively monitor its residents [18]. This practice, considered Orwellian-style social engineering, is also criticized seriously for violating private life's privacy. The information screens at Chengdu Shuangliu Airport add a different dimension to the use of biometric data. The system provides this information by scanning the face of the passenger and matching it in the database. The most interesting aspect of this practice at Chengdu Shuangliu Airport is that the passenger does not need to have his / her face scanned at any point in the airport as per their request. To put it more clearly, even if the passenger made the check-in process using known methods (check-in counter, kiosk, mobile, internet, etc.) at the airport but somewhere in the city, the face of the passenger in question was scanned and entered the database of the relevant system. As a result, although there are opponents, it seems that using personal data in the electronic environment will become increasingly common. Thus, it seems that the „good" citizens will have a lot easier procedures on their travels. Several biometric systems were used at different facilities at airports. An illustration of the several locations where a biometric system might be installed is shown in the following diagram (Figure 10). Using several biometric technologies during the processing of passengers will make the movement of passengers through the airport more efficient. When it is possible to do so, airports and the investors that own them in one location should collaborate with airports and the stakeholders that own them in other locations to develop interoperable systems that will enable travelers to move freely between locations while using the same travel token. The following section will provide some examples of different types of biometric systems.

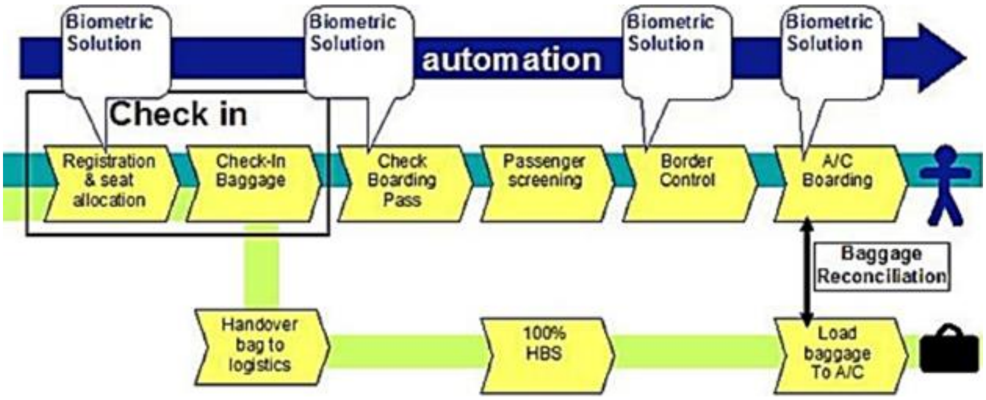

Figure 10 Diagram courtesy of Fraport; based on Simplifying Passenger Travel (SPT) Programme’s Ideal Process Flow [36]

3.6 CASE STUDIES IN THE USA

This section will discuss some case studies, showing their system engineering design of biometric systems and decision-making support in complex biometric-based systems.

Ross and Coworker reported in their work the digital biometric measurement process; data is collected, then transformed into a set of numbers or codes and stored in a database. Once the database is compiled, the measurements are compared to those previously stored in the database to determine if there is a match [17].

Since the terrorist attacks on the United States that took place on September 11, 2001, the federal government of the United States has established the Department of Homeland Security (DHS) and, within it, the Transportation Security Administration (TSA), which is in charge of ensuring the safety of passengers travelling through the country's numerous airports.

3.6.1 US-VISIT

As per the unveiled United States Visitor and Immigrant Status Indicator Technology (US-VISIT) and according to the Department of Homeland Security (DHS), new techniques, see Figure 11, were executed for all the visitors from nominated countries that pass in the United States at different ports of entry to be photographed and fingerprinted by customs officials [37]. As stated by DHS, using biometric identifiers will provide higher security than using name databases alone, particularly since persons will not be able to claim another's identity or fake travel documents. All the stored data will be safely stored, and it is only available for authorized and official usage to international travelers whom they say they are and do not threaten the United States.

Figure 11 US-VISIT's innovative biometric technology enables officers to verify efficiently [38]

3.6.2 Capps

The computer-Assisted Passenger Pre-screening System (often abbreviated as CAPPS) is a counter-terrorism system in place in the United States' air travel industry. "The United States Transportation Security Administration (TSA) preserves a watch list of individuals known to pose, or suspected of posing, a risk of air piracy or terrorism or a threat to airline or passenger safety" [158]. The list is used to preventively recognize terrorists trying to buy airline tickets, board aircraft travelling in the United States, and alleviate apparent threats. There are two versions in the USA of the program called CAPPS. The FBI and FAA managed the first version of CAAPS in the late 1990s. At that time, CAPPS I was implemented in response to the supposed threat of U.S. domestic and international terrorism.

The principle of CAPPS is to screen the selected passengers for additional screening of their checked baggage for explosives. CAPPS selectees did not undergo any additional screening at passenger security checkpoints [35]. The Office of National Risk Assessment (ONRA) proposed a second version of CAPPS (CAPPS II) with a list of necessities for replacing CAPPS I. Some of those requirements were:

- The government, not the airlines, would control and administer the system
- Every ticketed passenger would be screened, not just those who check bags
- Every airline and every airport would be covered by the system

In the summer of 2004, CAPPS II was cancelled by the TSA as the new version of CAPPS II is all dressed up in the language of privacy and concern for freedom, but it failed to address the core problems with the concept and continues to pose an enormous threat to American freedom and privacy.

Shortly after that, the TSA announced a successor program called Secure Flight that would work much the same way as CAPPS II. Secure Flight was implemented in August 2009.

3.6.3 Secure flight

This software checks the information provided by passengers against various watch lists kept by the federal authorities. The first phase of Secure Flight's deployment resulted in the transfer of all responsibility for matching passenger watch lists to those maintained by the Transportation Security Administration (TSA) from aircraft operators whose flights operate inside the United States [159].

After completing the second phase of Secure Flight, the Transportation Security Administration (TSA) will choose to match passenger watch lists for flights into, out of, and over the United States. Table 1 quickly compares Secure Flight and CAPPS II, highlighting the key differences. In contrast to CAPPS II, the new system will not attempt to identify anybody other than those who are already known to be terrorists or who are suspected of being terrorists. The installation of these technologies has resulted in improvements to both privacy and applicable legal rights [20].

Table 1 Comparison between CAPPSII and Secure flight (ACLU Conference) [25]

Program elements	CAPPS II	Secure flight
Provides no protection against terrorists with fake IDs	✓	✓
Provides no meaningful way for individuals to challenge their security designation	✓	✓
Centres around reliance on secret, inaccurate		✓

government terrorist watch lists		
Checks personal information against private databases	✓	✓
Requires a collection of personal information from travelers making reservations	✓	✓
Expands program beyond terrorists	✓	
Uses computer algorithms to rate individuals'" threat to aviation	✓	

3.7 NEW MODELS FOR AIRPORT SECURITY AND BIOMETRICS

Brömme, in his article, stated that biometric innovation ought to be accessible, for instance, with institutionalized information positions for biometric interchanging information and correspondence conventions. In addition, it should bring together programming interfaces for empowering the inter-operability of various biometric frameworks and parts in existing information and communication technology (ICT) infrastructures [23].

Improving airport security and immigration pain points with a risk-based approach is a new challenging trend. Smart security does not mean having to wait a long time in a queue, as many companies integrate devices and programs to enhance the airport layout to improve further ambience and passenger flows, e.g., IATA/ACI Smart Security program believed to be a catalyst for an important shift in the way certain passengers are screened [39].

Antoine Rostworowski, Director of Montréal Trudeau International Airport, stated that the industry is moving towards this approach where a single token process is feasible, which could make a difference. IATA, ACI, ICAO and others are having many discussions around this, and many believe biometrics is the way forward [19].

On March 2018, British Airways brought its biometric identification gates to three more US airports. Biometric identification gates were expanded to New York (JFK), Miami (MIA), and Orlando (MCO) airports. These "biometric e-Gates," which have been in trial at Los Angeles International Airport (LAX) since November 2017, use facial recognition to match flyers with their passport, visa, or immigration photos and can remove the need to show a boarding pass or identification when getting on a plane. Lufthansa has started using facial scans to permit passenger self-boarding at Los Angeles International [40]. Figure 12 shows how biometric face scans describe people`s identities. In critical infrastructures and some crowded public places, the biometric face scan method is widely used, especially nowadays, to find out the unallowed people and to prevent potential danger.

Figure 12 Biometrics boom at the airport: Using fingerprints and facial scans to enter clubs and get on planes [41]

3.8 RISK MANAGEMENT

The phrase "risk management" was originally used in the 1950s before this one as a method for assessing the success associated with purchasing insurance. The study proposes a method for handling the security threats posed by airport biometric systems, with fingerprint readers taking center stage. Risk management aims to prevent unfavorable situations and reduce financial losses. In today's terminology, the risk is the potential for unfavorable results after an incident. On occasion, it is seen as having both positive and bad outcomes. Furthermore, such situations might be seen as either an opportunity (to acquire wealth and usefulness) or a risk (to get damage and loss) [42].

Recent news articles regarding network security breaches and identity theft show the necessity for trustworthy authentication. In recent years, biometric security has become the sole reliable technique for identifying a person. Fingerprints, faces, iris, strides, voices, and other behavioral and physical traits make up a person's unique biometric profile. Biometric security systems can verify identity with the highest level of accuracy and reliability because biometrics are unique characteristics of an individual. [160].

3.8.1 Security standards in biometric systems

For biometric recognition to be carried out efficiently, correctly, and securely, certain requirements must be met. Standards have been developed to fulfil these requirements, resolve issues that might occur during the creation and usage of biometric apps, and improve the system's security and utility. The standards also offer privacy, interoperability, flexibility, stability, and reliability. The development and usage of biometric systems can be considerably improved in terms of quality and safety by properly setting standards and using them [161].

The basic objective of biometric standards is to create low-cost and high-performance systems. National and international standards were looked at from this perspective. Groups provide international standards like the International Electrotechnical Commission (IEC) and the International Standards Organization (ISO). To operate in the field of information technologies, ISO and IEC organizations established science committees and created SC17, SC27, and SC37 standards under the designation of ISO/IEC JTC1. The SC37 is specifically working to standardize the biometric application interface, biometric data interchange formats, biometric data evaluation criteria, and biometric performance tests. On the other hand, the ISO/IEC 30107-1:2016 standard, which is related to the sensor level of biometric systems, tries to stop attacks on the sensor [146].

3.8.2 Threats to biometric system security

Although most of the issues with conventional authentication systems can be solved by biometric systems, their benefits can quickly be outweighed by their drawbacks if security standards are not considered when they are being designed. Concepts like vulnerability, attacker and threat should be accurately specified to establish the system security discussed here. Control mechanisms that stop attacks should also be identified, as should preventively actions. Even one component of a complex biometric system may be the target of several attacks, each of which may originate from different branches. The hierarchy of the assault is sometimes depicted in a directed graph known as the "attack tree" to help comprehend the relative threat levels in complicated biometric systems [42]. An exclusive attack is located at the summit of the tree. The requirements for this assault are all stated in the next step. The requirements that must be fulfilled for the previous item are provided in detail for each subsequent level. Basically, the attack tree is consisted of below [162]:

- Aimed at simplifying the analysis of vulnerabilities,
- Enabling the designer of defense mechanisms to understand how a system has been attacked,
- Facilitating the development of countermeasures to prevent attacks,
- A representation of an attack in which the target of the attack is the root node, a means of achieving this target is with the leaf nodes,
- Contains a set of rules on how to build an attack tree,
- Within these rules, attack targets, offensive collaborations, steps of attack, hierarchies among attackers, etc., help to evaluate the results from a holistic perspective thanks to the tree,

3.8.3 Eliminating the risks of biometric technology

All industries with essential infrastructure will be connected with end-to-end information technologies over the course of the next five years as 5G, blockchain, quantum computers, cloud systems, and IoT devices gain increasing traction. More data than is currently produced will be created. In order to connect at higher throughput, significantly higher capacity power, energy, infrastructure, security, and training will be required. Eighty billion gadgets are expected to have internet connections and be a part of our everyday lives after maintenance [149]. From this point on, it seems plausible that each individual has ten internet gadgets on average. However, data production will continue unabatedly from the earth to the sun, and the existing data universe will have two births every two years, causing it to grow quickly. Sectors with new technology will be greatly impacted by autonomous cars in the transportation sector, the expanding internet in business, 5G in telecoms, and blockchain in finance.

A critical infrastructure organization’s service to all institutions and organizations connected to its infrastructure may be out of order and result in millions of dollars in losses per second, regardless of whether the organization is in the public or private sector. It may be in danger if it is late in making the investments and breakthroughs listed above in accordance with today's needs [163]. Different factors, such as a data breach, a service outage, physical damage, or a shortage of raw materials and energy, might be to blame for this loss. The following aspects should be stressed in order for nations to maintain strong cyber capabilities in direct proportion to the evolving technology:

- Introducing the systems designed for security and privacy objectives by providing public training, expanding user knowledge and experience,
- Adding pertinent pieces of training to the curriculum so that the next generation of software engineers will be familiar with security concepts, facilitating the teaching of security principles in all computer science education programs,
- Increasing the use of AI in tandem with the pursuit of cyber security, promoting research into algorithms for cryptography and their usage, and fostering the development of new technological goods, including quantum and supercomputers,
- Creation of a novel method for evaluating the effects of dispersed, complex, interrelated systems. Secure, interoperable solutions should be developed by enabling integration and data sharing amongst crucial infrastructures.
- Patch management for information systems devices,
- Increasing security measures, identifying existing vulnerabilities and vulnerabilities with vulnerability management and finding solutions,
- Taking necessary measures as a result of the detection and analysis of cyber-attacks and threats, closing vulnerabilities,
- Performing vulnerabilities in institutions and organizations in phase time, reporting vulnerabilities and taking necessary security measures,
- Monitoring and mapping cyber-attacks and threats in real-time and providing centralized incident management support,
- Detection and prevention of unauthorized or unauthorized access to information and communication technologies, logging,
- Establishing a channel access management system
- Continuous monitoring and analysis of malicious software or unauthorized transactions that may occur in information and communication technologies, regulation of security authorizations of authorities,
- Establishing information and communication technologies infrastructures to create safe areas against physical attacks,
- Monitoring, investigating and evaluating not only the system it is in but also all vulnerabilities and vulnerabilities in cyberspace,

- Protection of information and communication technologies from electronic and directed energy attacks,
- Monitoring, detecting and preventing data leaks,
- Preventing the installation of malicious software, analyzing it in detail, detecting the movements of this software and evaluating possible threats,
- It helps to visualize the attack graphically rather than trying to digest the complexity of the attack mentally,

3.8.4 Examples of airports that utilize biometric technology

Some of the busiest airports` biometric technologies in use are given as examples below:

• Dubai International Airport: The passenger is registered for biometrics inside the UAE. This system is the same one used across the federation’s seven emirates: Abu Dhabi, Ras al-Khaimah, Ajman, Sharjah, Dubai, Fujairah and Umm al- Quwain. That can cause another queue at the airport, so more points should be added to improve the passenger experience. However, the launching of Apple’s new Face ID solution makes registration of mass biometric at the beginning of a passenger’s journey more possible than ever before. The passengers registered into a biometric system that was separate from the main infrastructure. For this trial, they implemented the MFlow system software from Human Recognition Systems (HRS), with hardware in the form of a handheld device from Tascent, which enables the efficient capture of iris, fingerprint, and face biometrics. The data was uploaded into the Cloud and accessed through a secure database in Dubai [43].

• Heathrow Airport: At Heathrow Airport and after a four-month trial period, air travelers in the UK gave their assent to a biometric security system. The trial used iris and fingerprint scans to screen more than 3000 passengers travelling from and to Hong Kong and Dubai. The goal of this trial was to test the system's feasibility, which would check the passenger’s details against various intelligence databases and watch lists before allowing them to embark on the flight. Before boarding the flight, the passenger must scan his or her passport and right finger at the self-service kiosk. Then the passenger’s biometric details will be compared, and if it is validated, access will be granted. The enrolment system collects two iris images, ten fingerprints and a facial scan, which is digitalized, and after that, it is stored in Radio Frequency Identification Card (RFID). This card was compatible with fingerprint readers installed at the immigration barriers at Heathrow, Dubai, and Hong Kong airports [44].

• Amsterdam Schiphol Airport: A biometric boarding trial has been started at Amsterdam Airport Schiphol and KLM. This trial will enable passengers to board their flight without the need to show their passport or boarding pass. Instead, passengers board the plane using a special gate that uses facial recognition technology. Passengers must register first in order to board using facial recognition. A special registration kiosk has been added in the waiting area near the gate. In addition, the KLM staff will be ready to offer all the possible help [45].

• Hong Kong airport: in Hong Kong International Airport (HKIA), travelers can use automated e-Security Gates, which depend on facial recognition technology. Eligible travelers can scan boarding passes and their documents using electronic gates. Then these documents will be verified by facial recognition technology using the gates' embedded cameras. However, this process is still done manually by the airport security staff [46].

• Orlando International Airport: Greater Orlando Aviation Authority (GOAA) is the first to deploy U.S. Customs & Border Protection fully. Biometric Entry and Exit Program. At the beginning of 2018, a cooperation between SITA, GOAA and British Airways and Customs & Border Protection (CBP) started incorporating the US biometric departure check for British Airways customers. The trial's success has prompted the airport-wide implementation of the technology. British Airways is said to have boarded flights of almost 240 passengers in around 15 minutes. The technology means passengers just need to look at the camera, removing the need to present boarding passes or passports at the gate. The system makes passenger boarding quicker and easier while it also incorporates the new secure biometric exit checks [47]

• Shannon Airport: Shannon Airport in Ireland has deployed biometric facial recognition technology to speed up its security screening process. Shannon Airport, which Shannon Airport Authority operates, is located on the west coast of Ireland, 24 km north of Limerick city. Last year, more than 1.75 million passengers passed through the airport. Using facial recognition technology, the security personnel at the airport verify passengers by matching them to the documents they are presenting [48]

- Ottawa Airport to enter Canada through the Ottawa International Airport, travelers will use biometric kiosks. Instead of the paper customs forms used previously, the kiosks will be used to process new arrivals to the country. After disembarking, travelers will use the kiosks to enter their details, and then the kiosks will scan their faces and compare the images against those in their passports. Besides, much of the process can be done on the plane by the visitors using a mobile app, proceeding to upload the data to the kiosks upon arrival [49]

- Atlanta airport In Atlanta's Hartsfield-Jackson International Airport, Delta Air Lines launched what it called America's first "biometric terminal". This technology was initially started to be used at boarding gates. On Nov 29, 2018, it opened the nation's first curb-to-gate biometric terminal, which is expected to improve aviation security and keep travelers moving faster, taking two seconds for screening. This program uses facial recognition technology to check in and pass-through board flights and security without having to scan boarding documents or a passport in all of the airport's international terminals. A camera-based system compares scans of travelers' faces to a database of verified ID photos curated by US Customs and Border Protection (CBP) with a 98% success rate. For the busiest airport in the world, like Atlanta, it saves 9 minutes for the boarding process, which is the time that the passengers will not be spending in lines waiting to board the aircraft. Besides saving time, it makes airports and air travel safer in an era when aviation is targeted by criminals and terrorists [50].

3.9 SUMMING UP

Biometric authentication is the process that is used to identify oneself through one's behavior, anatomy, physiology (for example, through fingerprint or iris), or even vocal patterns [51], To enable future use of one's biometric image, such image needs to be captured, encrypted, and stored [52]. According to research, fingerprints form 52% of the world's biometric systems [53]. This popularity of fingerprint biometrics is caused by the accuracy of fingerprint images [54]. An edge that the biometric authentication method has over other methods is its requirement for the presence of the actual use for the verification process to take place [55].

Biometrics is expected to grow rapidly in the 21st century, especially in countries such as India, South Africa, and Ghana [56]. These claims are supported by those who [54] purport that biometrics will be the ultimate authentication method. The growth in popularity of this technology may be attributed to its provision of better and more reliable access control compared to traditional systems. This assertion is also confirmed by those who state that biometrics improve security control and reduce fraud. Another reason for its growth could be the need to improve safety measures and curb acts of terrorism in public areas, such as airports [56]. For example, in Dubai, the airports have introduced an automatic identification system at their gates, which are e-Gates. The system scans facial and iris imprints to authenticate the passengers [43].

Malaysians are pioneers of biometric passports [11] (e-passports), which have curtailed the use of false travel passports in Malaysia [57]. Other use of biometric technology includes access to work or bank premises, network resources, and information protection [58]. The next chapter discusses the use of biometric technologies in smart cities and argues the term smart city, what it means and what it includes.

4 BIOMETRIC SYSTEM IN OTHER CRITICAL INFRASTRUCTURES

Despite the high amount of budget, advanced equipment, more control officers, and efforts put into airport security, threats to security and preventing illegal travelers keep troubling the border control agencies. Those unlawful entrants always try to innovate new ways to cross borders illegally [59]. From a safety and security point of view, air transport is considered as one of the most regulated means of transportation. Its size, impact, integration, and worldwide use expose it to threats. Over the years, the aviation environment has been subject to potential threats to flying, and those threats are expected to remain in the future. Criminals and terrorist organizations are rapidly becoming more sophisticated and imaginative with their strategies and methods [60][61].

However, identifying individuals at most border checkpoints, like airports, road checkpoints, seaports, etc., is still performed with traditional ID cards and documents. Biometric procedures gain more and more ground in the modern applications-oriented technical scene in both the private and the public security sectors [62].

Last year (2019), more than 3.5 billion people took to the air. Those figures are predicted to quadruple by the middle of the next decade, but airport capacity simply cannot keep up at a time when security, defense of national borders, and removal of threats demand increasingly strict screening of every passenger travelling through the system [63], getting you through the airport quicker and more effortlessly is necessary.

In commercial air travel, security hazards may come from many places than only passengers and their belongings. Some of the various procedures that aid an airport and its passengers and planes include maintenance, cleaning, booking, baggage handling, air traffic control, retail, food services, parking, auto rental, and others [64]. T.W.A. Flight 847 in 1985 was hijacked for 17 days, and during that time, members of the cleaning crew stowed weapons in the plane's restroom to help the hijackers (Gladwell, 2001). This means that even with flawless threat detection applied to travelers and their bags, security may still not be up to par [65]. Identification of passengers prior to boarding is essential for safety and risk mitigation; however, identification of airport staff offering a range of services to the airline firms is also necessary (SEA Milan Airports 2017). They use vehicles, including automobiles, wagons, and trucks, to cross the airport's land limits, including restricted technical areas. At the checkpoint, before entering the airport, security personnel verify their identification using a variety of methods [66].

Terrorist attempts in the aftermath of 9/11 led several airports to tighten security. Airport security inspections have become more comprehensive and time-consuming due to the constant vigilance required. As a result, the overall cost of airport security has gone up, which has significantly impacted airport activity and flight delays, necessitating adjustments to the financial model underlying airline terminal operations [67].

A smart city is a vast concept; it aims to organize and manage the whole city using embedded technology. These require the city to be able to watch and integrate the status of all its management, infrastructures, people, governance, education, natural environment, and health using information and communication technologies (ICT) [77]. The general idea of a smart city and its major components is shown in Figure 13. They are in order:

- Smart Commerce,
- Smart Environment,

- Smart Governance,
- Smart Mobility,
- Smart Connection.

Figure 13 Main majors of smart city

Highly advanced technologies are used in the design of the smart city. These technologies include electronics, sensors and networks linked with computerized systems, encompassing tracking, databases, and decision-making algorithms. The increase in urbanization makes the need to deal with social issues such as public sector problems, governance issues, environmental issues and the concern related to economic restructuring in a smarter approach. As the pace of change is becoming very big, modern cities' challenges are getting more complicated. This requires making changes in an organized way ensures using the latest technologies and internet connection. Therefore, the smart city will give smarter growth [78].

Besides, significant growth in the economic system could be achieved by developing city-systems using embedded technologies. Some cities are now considered smart cities, like Amsterdam, Barcelona and Masdar. Figure 14 shows smart cities around the world [79]. As we can see from this figure, the smart cities are mainly in Europe and US, with some well-developed cities, Dubai, Hong Kong and Singapore, due to being financial and economic centers.

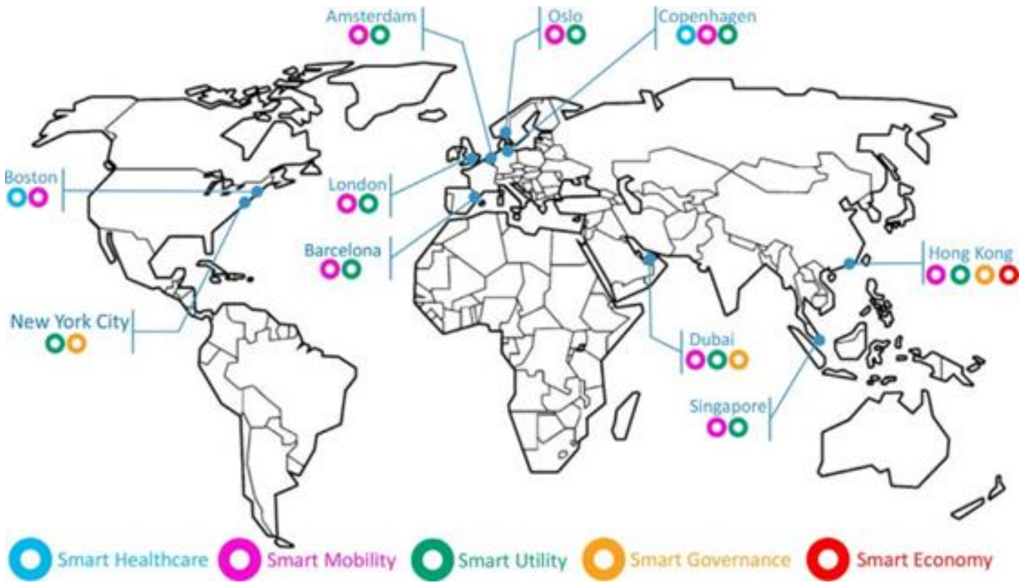

Figure 14 Smart cities around the world [80]

The residents of smart cities can experience a level of personalization on offer, and this experience can be lived in the city's workplace, homes or services. For example, in a smart workplace, the individual login and out will automatically be registered. The meeting room facilities can be set to the person's desired temperature or lighting style through a process called commercial building automation. A smart workplace is built to improve efficiency and productivity and help employees work comfortably and efficiently [81].

Here comes the vital role of biometrics. Biometrics is a branch of science that aims to recognize individuals through biological characteristics (e.g., fingerprint, face, voice, and iris) or unique behavioral (e.g., keystroke dynamics and gait). Biometric data in a smart city can be available using biometric sensors, surveillance videos, IoT devices, or social media uploads. Using biometrics in a smart city gives the ability to identify each user to provide him with a high personalization level of experience. Biometric ID with fingerprint or iris helps authenticate the user and gives him the ability to connect to any system based on personal data. In this way, we can understand the importance of biometrics in the context of a smart city [82].

On the other hand, biometric systems play a crucial role in the smart city in information security issues. This technology can secure many sections of the smart city and avoid fraud or malicious attacks. Biometrics can be used effectively in these sectors:

- Healthcare

- Education
- Transportation
- Utility
- Patrol and security

Figure 15 shows the smart city's infrastructure where biometrics can be used in the application layer, implementations and biometric backend levels.

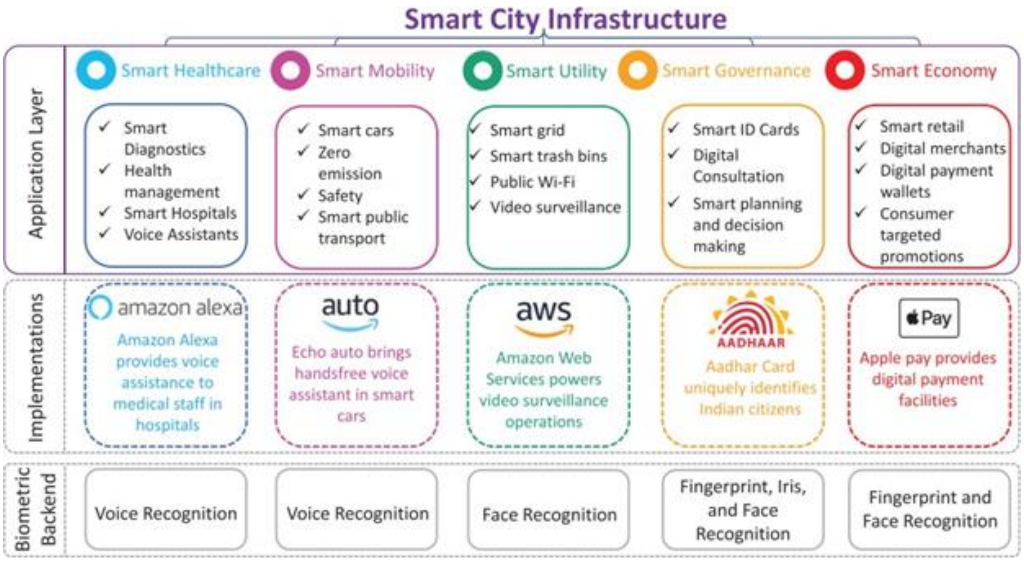

Figure 15 Integrating smart devices with biometrics in the infrastructure of a smart city [80]

In this section, the integration of biometrics with smart city sectors such as healthcare, education, and transportation will be discussed, and then a review of the connection between biometrics and the Internet of Things will be studied.

4.1 SMART HEALTHCARE

Using biometric systems in healthcare can enhance the secure storage, use, and exchange of patients' health information. It represents the future of identification in healthcare. There is a big gap in protecting patient information, which can create a problem for both patient and the provider [83]. In many cases, the patient can be a victim of stolen medical identity, and his/her records can contain erroneous data or other patient data. It might provide a fake medical record to support a kind of fraudulent claims. It is possible in these cases, the fraudsters use the patient's identity and provide a falsified claim [84].

Biometrics in healthcare is being used in Arizona's Children's Clinics. To access the clinic's resources, Arizona's Children's Clinics used a password and username. The staff includes about 40% part-time employees, who do not have a daily deal with patients. As a result, getting their passwords is common, leading to a significant delay for both patient and provider. That is why the clinic started to use the fingerprint reader, which helped to decrease the time needed to access health records. The clinic installed computers in patients' rooms, and now doctors can access the patients' data electronically. Besides, doctors can quickly log in by touching their fingers. Installing this biometric technology avoids reading the patient's record by the wrong person and increases the efficiency of the healthcare organization [85].

4.2 SMART EDUCATION

The traditional student card cannot verify the student's identity. It is not hard for the student if he/she wants to change his/her identity with another student, and identifying can be challenging. In the smart city, biometric student identification is used to verify students' identity when attending classes or exams and to access laboratories and libraries. In addition, it can be used to verify the identities of students who participate in seminars and when they are being charged for meals, in dormitories too, and when they enter or exit. That can be achieved by installing fingerprint scanners or cameras in the classroom [86] [87].

Moreover, biosensors such as surveillance cameras and infrared can be used to watch the students identify any behavioral problems and study student engagement. Observations related to the student's behavior, such as body language and eye contact, can indicate how they handle knowledge and class material. Using such information can attract attention when a learner loses interest or any distraction in the classroom. Furthermore, to protect the safety of pupils, biometric technology such as Radio-frequency identification (RFID) chips may be used to monitor their positions, ensuring that students, especially the young, arrive at school and return home safely [88][89].

This information may assist teachers in tailoring the program to each student's individual requirements. It is a useful approach for evaluating new educational technology's usefulness and informing instructors about the tactics most likely to ignite student involvement. However, there are ethical concerns with collecting Big Data in K-12 institutions [90].

On the other hand, the biometric system in schools and universities includes students, teachers, and staff. Using biometric identity for university staff can help verify their attendance and monitor schedules and classes. Besides, it can accelerate the payroll process by avoiding any errors that can happen [91].

Another aspect can the biometric system be used in schools is managing the visitors. It can ensure the security and safety of the schools. In the traditional id system, the identification of visitors is almost impossible. That is why using biometric identification fingerprint or iris to authenticate parents, or guardians' identity is vital for schools. In this way, when a suspicious individual tries to enter the school, scanners will prevent him from doing, and surveillance cameras will be able to recognize any unauthorized person who enters the school and engage lockdown protocol automatically [92].

4.3 SMART TRANSPORTATION

Using biometrics in the public transport sector is becoming increasingly popular, especially in protecting the traveler.

In air transport, biometric technology has mainly made inroads in international travel. However, adapting the biometric system in local commuting systems has been slower. Recently, the largest agency for municipal transit in North Texas, The Dallas Area Rapid Transit (DART), became one of the first companies to adopt cameras for facial recognition purposes in its train. This technology has many usages, and it can help control the train capacity in the case of medical emergencies [93]. Besides, it will give police a vital aid to track criminals or wanted persons when they take the train. However, security is not the only benefit of this technology. During the new lunar year holidays, facial recognition technology was installed in Beijing Train Station to improve passenger processing efficiency as the Chinese capital witnesses jam traffic during this time of year. For verification, the reading of the face scanner will be matched with the image of the ID. Therefore, the passengers had to have a smart ticket and smart ID card. Other developing countries follow suit, although their aims are different. In certain cities in India, train stations are planning to use passengers' biometric data to hold back the menace of touts [94].

The advantages of using biometric systems in transportation are clear. It provides the possibility for safer travel and makes the passenger management and ticketing process simpler. These advantages will encourage more companies to adopt biometric systems in the coming years [95].

4.4 INTERNET OF THINGS

For many years, biometric systems have been studied in the field of authentication and identification. The most prominent example is the fingerprint [96]. Due to its well-developed feature extraction approaches and low-cost implementation, fingerprints consider the most used biometric system (e.g., login to modern smartphones). On the other hand, the iris is acclaimed for its short verification time, high accuracy, and ability to give unique features, even in the case of identical twins. Face recognition is another biometric system. This system is more heavily used for surveillance purposes. Though they are commonly used, biometric systems are easy to circumvention [97].

Photoplethysmogram (PPG) and Electrocardiogram (ECG) are cardiovascular biometrics that is becoming better biometric systems choices. They are difficult to copy, circumvent and acquire without user approval. PPG detects changes in blood pressure and heart depolarizing. In comparison, the ECG signal gives information about heart muscle and depolarization and can be measured using cheap devices. Besides, biometrics can provide identification information related to demography, like sex and age and health-related information [98].

4.5 SMART POWER GRID

The classic power grid is facing a lack of robustness and flexibility to transfer electricity between the Generating stations and customers with one-way transmission; hence it is not possible to share information. In addition, the response to the disaster or problem on the transmission network is slow and cannot self-restore energy capability [129]. Figure 16 illustrates the main general components of electricity production. The order is in the right way from the market to the final user to show how the general process is going.

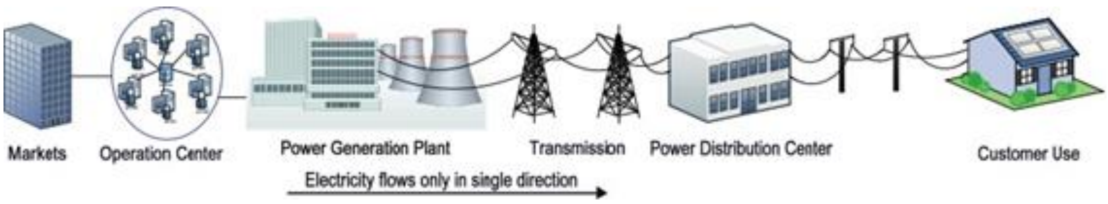

Figure 16 Classic power grid with one-direction connection [130]

On the other hand, the smart grid is an electrical grid integrated with various operational, innovative measurement and communication technology that efficiently controls energy production and electricity distribution. Below mentioned Figure 17 describes the smart grid chain and connection of facilities which are vital in terms of society's needs. As seen from this figure, how important is the smart power grid connection through these places? If these lines are broken, would there be hard consequences in the daily life of people?

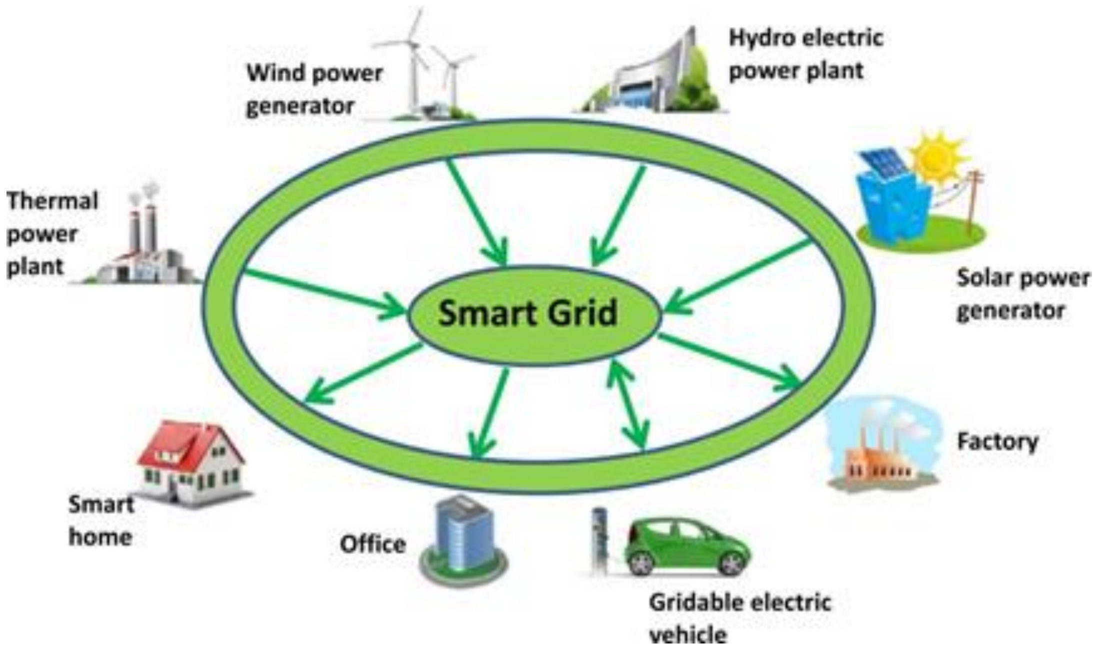

Figure 17 Smart power grade [131]

4.5.1 Architecture of smart grid

Stakeholders and multinational corporations are now developing multiple architectures. Therefore, the National Institute of Standards and Technology (NIST) and the smart grid interoperability panel (SGIP) established a standard guideline that every smart grid framework must meet. This worldwide standard offers several benefits. It accelerates development, promotes greater integration between equipment from various firms, gives additional advantages for the smart grid high-tech industry, and assures a high degree of security [132].

There are certain Architectural Objectives that every intelligent power grid must meet. [132]:

• Options: The architectural framework should enable a wide variety of high technology, be flexible enough to deal with old equipment, and embrace developing technologies in a standardized manner that eliminates unnecessary capital expenditure.

• Interoperability: Architectures must offer standard interfaces with other systems and manual processes and be compatible with third-party products and cybersecurity infrastructure.

• Upgradability: Architectures must allow the system's ability to be upgraded without difficulty and continue to function through partial system upgrades.

• Innovation: Architectures should facilitate and facilitate innovation. This includes the flexibility to accommodate innovation in legislation and policies, corporate processes and procedures, information processing, technological communications, and the incorporation of new, innovative energy systems.

• Scalability: Architectures should have architectural aspects that are suitable for the applications they contain. The designs must facilitate the construction of massively scalable, well-managed, and secure systems with lifespans ranging from 5 to 30 years, depending on the kind of system.

• Maintainability: Architectures should enable the system to be maintained safely, securely, and dependably throughout its life cycle.

• Older: Architectures should facilitate the integration and migration of legacy systems.

• Security: Architectures should provide the capacity to resist entry, access, or use of physical and cyber assets by unauthorized parties. This support must meet all of the system components' security criteria.

• Flexibility: an implementer should be able to select the kind and sequence of implementation based on the architecture. Flexibility also permits portions of implementation to diverge from the original plan without consequence.

• Governance: Architectures should foster a well-managed system of systems that is enabled by consistent policies over its full life cycle.

• Affordability: Architectures must fundamentally allow capital and life-cycle savings through standards-based operations and maintenance. They must facilitate the acquisition of interoperable smart grid equipment from many vendors via maturing national and international marketplaces.

4.5.2 Framework core

The core is a categorical list of intended cybersecurity actions and results that are aligned with Informative References. The framework's core is intended to be user-friendly and to function as a translation layer to facilitate communication across multidisciplinary teams using simple, non-technical language. The core has three components: functions, categories, and subcategories. The five high-level core tasks are identifying, protecting, detecting, reacting, and recovering. These five roles are relevant to general risk management and cybersecurity risk management [132].

4.5.3 Communication networks in smart grids

Figure 18 illustrates a standard communication network architecture of a smart grid, and we can see how it physically separates each section of the power grid, which provides more secure communication [133].

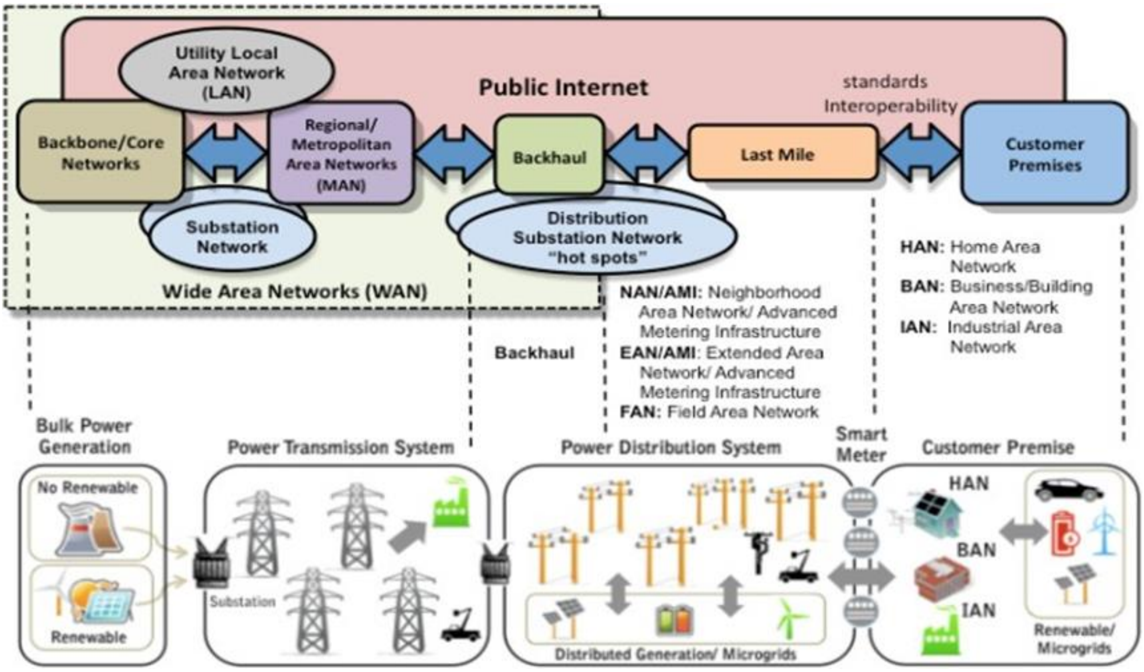

Figure 18 The communication network on the smart grid [134]

4.5.4 Smart grid cybersecurity challenges

The topic challenges can be summarized as follows [137]:

- Lack of expertise and budget limits
- A robust and resilient grid

- Data protection and secure data handling
- Raising awareness among manufacturers and operators
- Technical challenges
    - Proper integration of equipment and software in the system
    - Unauthorized access to systems or devices
    - Availability of traffic analyzers, communications monitoring, and application log monitoring
- Incomplete or inexistent regulations

4.5.5 Common vulnerabilities and risk factors in smart grid communication networks

The weak sides of smart grid networks and possible risk factors can be written as follows:

- Vulnerable consumers: The intelligent devices of the smart power grids can handle huge amounts of information and data of the customer and power demand and then send this information and data to the service provider by a bi-directional communication line. Therefore, protecting private consumer data and consumption habits is particularly necessary to prevent unauthorized disclosure of information [138].
- The massive number of devices: The massive number of devices leads the system to several networks connected between them, which provide a communication line to manage the demands and supply electricity with many features covered by the power grid. There- fore, the system will be complicated to manage. On the other hand, the vulnerabilities could result in intelligent devices or networks being used as entry attack points to the network [139].
- Coexistence of old and new devices: The integration of smart grid technologies is a significant obstacle in the process of creating and implementing smart grids, particularly in terms of ensuring compatibility between them without causing any faults. This cohabitation might lead to potential incompatibilities at both the physical and protocol levels and vulnerabilities and threats resulting from potential interdependencies between devices and networks [140].

- Implicit trust: M2M is the default setting for many devices, and many of them employ implicit trust in their Machine to Machine (M2M) connections. The interdependency with the other machine has led to the emergence of new vulnerabilities, which makes this a serious flaw that needs to be addressed immediately. An attacker can transmit inaccurate data to the first computer or get personal and private information if they acquire control of the other machine involved and pretend to be it. In control systems, Device-to-Device communication is vulnerable to an attack known as Data Spoofing. Even more, attackers may take advantage of this implicit confidence to carry out Man-in-the-Middle attacks, compromising the network connections between the devices in question and the remainder of the network [138].
- Commercial hardware and software: Commercial hardware and software are often built-in isolation from the operator's grid, which may lead to issues of incompatibility between various pieces of hardware and a potential inability to build a security protocol or communication system. Therefore, using commercially available software and hardware results in the introduction of inherent vulnerabilities. These vulnerabilities might take the form of a backdoor or a sudden breakdown and pose a significant threat to the system [141].
- Communication protocols: Communications between devices in the smart grid are improved via wireless protocols, such as Bluetooth, Zig-Bee, Infrared, WiMAX, Wi-Fi, LTE, UMTS, or GPRS; nevertheless, this is also a source of vulnerabilities and is well-known by those who would want to exploit it [141].
- Human Considerations: Even if cyberattacks from outside sources are becoming more sophisticated, human error is still the most important factor in the majority of data mishaps and losses. Software, rather than people, is relied on by the operators to safeguard data and information from assaults because the software provides a higher level of security and integrity. However, we are able to avoid errors caused by humans by training employees to receive and the security actions taken by organizations, particularly concerning the use of network communications and the management and configuration of the smart grid assets to ensure that their communications are carried out securely and reliably [139].

4.6 THE USE OF BIOMETRICS IN FINANCE

Biometric technology is becoming more commonplace in financial institutions, payment systems, retail chains, cafés, and other types of businesses. On the one hand, this makes it more difficult for dishonest individuals to steal money from clients since cracking double or triple biometric identification codes is far more difficult than just memorizing a PIN. On the other side, it makes it easier to conduct financial activities, such as making purchases, transferring money, or paying for services quickly and simply [99].

In addition, biometrics protect in case of emergencies. For example, in Japan, after the devastating earthquake and tsunami in March 2011, many people lost their bankcards and their documents. They had to go through long and tedious identification procedures to withdraw money from their accounts. After that, a unified biometric system was created in the country, excluding such a problem.

4.6.1 Biometric payments

The introduction of payment systems like Apple Pay, Samsung Pay, and Android Raw, which authenticate customers by their fingerprints and are accessed via their smartphones, was a game-changer. In addition, in 2016, a facial identification function was launched in the mobile application of the Chinese payment system Ali- pay [98].

On the eve of the 2020 Olympic Games in Japan, they have already begun testing a new payment system for goods and services for foreigners. It will allow them to pay in hotels, shops, and restaurants by simply placing their finger on the reader. In addition, guests can take fingerprints and link them to a bankcard account immediately upon arrival - at ports and airports.

Companies in the financial sector and those in the technology industry are collaborating to create some very unique biometric solutions. For instance, one of the international financial institutions demonstrated a prototype of a contactless payment wristband that determines the user's identity based on their heart rate.

Biometrics is also used in Russia. Sometimes, you can already pay just by looking at the camera at the checkout. For the system to recognize a person, you need to download a particular application in advance, link a bank card, and upload your portrait. Special software installed on cameras near cash registers recognizes a person and automatically debits money from his account.

4.6.2 Money transfers

Some banks use face recognition technology for money transfers. You download a special application to your smartphone and choose “translation by photo”. Then find the recipient’s photo in the gallery. The image is sent to the bank’s face recognition system. The masked number of the recipient’s card is displayed on the screen. You just must confirm the sending of money.

4.6.3 Loans and deposits online

Biometric identification in banks is already widely used. For example, large banks use voice technologies in call centers, face recognition technologies when a client repeatedly contacts a bank branch to obtain a loan, and fingerprint scanning to enter a mobile application and access safe deposit boxes.

The remote identification mechanism in Russia allows you to open deposits and accounts and receive many other services online. To do this, the client only needs to come to the bank with the documents once and go through the initial identification - to record a voice and video. After that, the bank sends this data to the Unified Biometric System. Then a person can remotely receive the services of any bank, having passed double identity confirmation: through the Unified State System of Identification and Authentication (Portal of Public Services) and the Unified Biometric System. The whole procedure will take a few minutes.

Is it safe to use biometric data? How are they protected from scammers?

PIN codes and text messages from a bank are two forms of financial security, but biometrics is a far more complex and sophisticated method. Scammers cannot imitate your voice or steal your fingerprints or face [100]. Additionally, biometric systems are constantly and thoroughly secured against hackers, theft, and data fabrication.

- Information is held in closed systems with restricted access. Biometric data used for remote identification, for instance, is encrypted and maintained impersonally.

- The collecting of biometric data is only permitted with the individual's agreement. At the Visa Application Center, for instance, you will be required to sign the related application. The same holds true for financial services.

- In the financial industry, multifactor authentication is most often used to provide security, that is, authentication based on several criteria, such as a PIN or one-time password and biometric data. The user must pronounce a unique sequence of digits, preventing attackers from forging the client's video. The customer must first leave a reference voice recording at the bank to utilize the system.

Shopping in a cafe briefly, transfers literally with one finger, loans and deposits without leaving the couch have already become available, but not everywhere yet. It will certainly take some time before biometric technologies are used, even in the smallest stores in all regions. At the very least, you need to have the Internet throughout the country.

4.7 OTHER APPLICATIONS

Using biometrics can improve security in the smart city. Biometrics can be used in age, and sex identification, parental control, and better penalization, in applications that need identity verification. Using biometric systems can end the need for traditional kind of logins and passwords. Using biometrics-based login control, smartphones, implanted medical devices, personal laptops, etc., will be able to distinguish their owners and operate only in their hands. Biometric systems like PPG and ECG can provide information about the sex and age of the person. That can automatically restrict inappropriate content based on age on TVs or smart computing devices. Besides, such health information, which can be obtained using PPG and ECG, could also help by alerting the users of some health problems. For protecting user information, using a biometric system can be efficient; the user’s sensitive data can be encrypted to ensure it can be decrypted only by the authorized person [100].

On the other hand, biometric systems can give demographic information. This information can be used to improve marketing by organizations. Organizations can use this information to characterize the sex and age distributions of consumers. In the same way, retailers can use this kind of biometrics to collect such information from customers. In the smart city, using biometrics can avoid long ones [101]. By automatically reading user biometrics and RFID tags in products, customers will be charged when they leave the store with any product. In the same way, it can be used this information to watch the patients. Using biometrics and RFID makes it possible to make sure that the patients take the dose appropriately.

Biometrics can be useful when they are used in the domain of public safety. An example is access control for schools, buildings, companies, etc. The door can be controlled by biometrics. They can also help avoid disaster-related gun violence by using automated tracking and surveillance at entrances based on biometric systems. Moreover, biometric can be used to identify individuals who are violent or suicidal in a way that prevents these kinds of crises [102].

4.8 CHALLENGES

Though the applications that have been mentioned above are promising, there are still some challenges in integrating biometrics with IoT.

- Reliability: in physiological biometrics, stress, health and exercises can reduce the identification’s accuracy.

- Privacy: biometrics can be used in a way that can invade the privacy of the user. Protection and Revocability: if a password is hacked, it is easy to replace it. However, it is not the same situation for biometrics. Biometrics are permanent, and it is very difficult to revoke if compromised.

- Feature extraction: there is a need for algorithms that are able to extract reliable and unique features from biometric systems for identification purposes [97].

5 CYBERSECURITY

Using computers, the Internet of Things (IoT), networks, and data sharing in infrastructure technologies significantly advance this sector. However, nothing comes without a price. Using IoT and other smart technologies makes infrastructure systems vulnerable and exposed to the risk of cyberattacks and electronic sabotage. These attacks can be for stealing data, changing the setting, or even controlling the whole system [164].

The smart power grid infrastructure allows the power system to be managed smartly. It includes a verity of energy measures and operations, such as:

- Demand Response (DR): this technology provides monitoring and controlling of the system depending on the load and the power supply information in real-time, even collecting the data of consumption and production of the electrical power over a year in a way that allows expecting the behavior of the power grid and makes a balance between the production and the consumption [125].

- Advanced Metering Infrastructure (AMI): This technology is responsible for improving the efficiency of electrical power meters and providing monitor and control capabilities. This technology allows the grid operators to disconnect the service on customers remotely or add new control paths, which can affect the customer's behavior in a way that grid operators have not experienced [126].

New technology brings a new level of risk. Security is a challenge in the smart grid. AMI network gives access to functions that control the whole grid, which may affect the integrity of the system or the availability of data in case of unauthorized person can get the right to access this network. This can have a significant risk to human safety and the privacy of the consumer's data. Therefore, protecting the system and mitigating the risk of cyberattacks are vital in this technology [127].

Recently, market penetration and cyber threat increased for criminal or cyberwarfare reasons, and attackers are learning and developing malware, viruses…etc., so they should improve and fix gaps in all types of infrastructure. For instance, smart meters can be hacked to cut power bills, as happened in Spain in 2014 or due to a Distributed Denial of Service (DDoS) attack or malware infection. Moreover, these attacks maybe give the attackers access to the communication and control of the system network, causing damage or a halt on energy production and effective on several systems, for instance, the cyberattack on the Ukrainian Power Grid on December 23, 2015 [128].

This chapter highlights the main security challenges, demonstrates how to protect, and mitigate the risk of cyberattacks on smart grid systems, and investigates the cyberattack on the Ukrainian power grid as an example of threatened.

5.1 BIOMETRIC ATTACK MODELS AND TYPES

If proper inspection procedures are not used to verify biometric systems throughout the development phase, they are open to assaults. Regulated access to these systems, controlled entry and leave, authorization, etc. It is well known that the incentive needed by attackers to compromise the systems is extremely strong, given that it is employed in vital sectors. Problems occur because biometric data, unique to each individual and employed in these systems, cannot be readily modified, unlike knowledge-based encryption schemes. It is important to protect the privacy, integrity, and accessibility of the biometric system in order to assess its dependability. Before creating a safe environment for biometric systems, it is important to explicitly outline potential issues and identify any dangers that require attention [165]. Attack models have been created due to evaluate biometric systems' dependability. With many assessment metrics and viewpoints employed in these models, it is intended to create highly reliable platforms.

5.1.1 Biometric attack models

A biometric system's component design and system integration should undergo a typical security analysis, and threat models and situations where potential security flaws may appear should be taken into account. By analyzing the biometric system's intended use, the environment in which it is used, and its users, a threat model that is appropriate for the system's components should be constructed. Before modelling such a system, it is vital to assess the resources attackers can employ, previous attack patterns, and potential scenarios.

Ratha suggested the first attack model identify biometric system security flaws. This model found weak points in the system, and new solutions were generated to completely or partially eliminate these weak links after the merits and disadvantages of biometrics-based authentication were discussed. Spurious biometrics are defined as repetitive sending, disabling feature extraction, changing the feature vector, disabling the matcher, unauthorized access to the templates stored in the database, altering the template data, and changing the matcher result [147]. These are eight critical points where the attack can happen in the model.

Wayman provided a framework, arguing that the system components should be evaluated from a macro viewpoint and the sub-modules inside the components from a micro perspective to comprehend biometric systems' functioning processes. In this framework, in addition to the sensor module, feature extraction module, matching module, and decision module, which are defined as the components of the biometric system, the communications of these models are also defined as a component in order to carry out a more thorough analysis of potential attack vectors. This model tests the dependability of the technical devices used by the system and simulates the relationships between the system's component parts [147].

The Bartlow and Cukic Model is an attack model that incorporates biometric system components and sub-components, analyzes Ratha's method of detecting vulnerabilities for biometric systems with more crucial levels of information, and is influenced by Wayman's framework. The Bartlow and Cukic Model treated administrative and environmental characteristics as subsystems while describing each component in order to adhere to Wayman's logic architecture. While the Wayman model suggests an architecture to identify the biometric system and its sub-components merely, the Bartlow and Cukic model defines twenty possible attack locations and twenty-two weaknesses.

The Fishbone Model was developed with a different viewpoint than the models used to examine potential attacks on biometric systems generally, and it is intended to find the weak points in biometric systems. According to this approach, internal design flaws and outside threats put biometric systems in danger. Internal errors are characterized as mistakes made during the data collection, feature extraction, and matching stages, whereas assaults are defined as deliberate actions taken by people or organizations who have specialized expertise [166].

The biometric system is vulnerable to several harmful assaults that numerous threats may carry out. A biometric machine is vulnerable to malicious assaults, which compromise system performance. The biometric system has many drawbacks, including interclass variances, noisy sensor data, spoof assaults, and interclass resemblance.

5.1.2 Biometric attack types

Any biometric system that is being examined must consider the high attacks, and countermeasures must be considered while building the biometric system. The following list includes the many biometrics system attacks:

- Fake biometric: Hackers increasingly use phony biometric samples to fool sensors in order to access biometric systems, thanks to the development of new technology. Examples of such malicious attacks on the sensor include fake face masks, silicon fingerprints that are not real, iris lenses, and others.
- Attack through replay: In this attack, the biometric system's data stream is inserted between the sensor and the processing system. Two to three stages can be included in a repeat attack. It initially duplicates or intercepts the sensor transmission, adjusts the data, and then replays the information.
- Spoofing of Data: Spoofing of data refers to replacing the feature set with false or changed features. These kinds of spoofing attacks are frequently used to infiltrate other networks, disseminate malware, and steal sensitive data.

- Attack on Template Modification: A template is a set of distinguishing characteristics that summarizes a person's biometric information (signal). Whatever image is submitted to the system, the templates can be altered to achieve a high verification score. The templates that are kept in the database are susceptible to replacement, theft, and even modification. Consequently, the system will suffer since real users' scores will be low.
- Overriding Answer: Yes or No Your biometric systems have an inherent flaw in always returning a binary response, Yes/No (i.e., either match or no match). In other words, there is still a fundamental mismatch between the applications and the biometric, which leaves the system vulnerable to intrusion [147].

5.2 CYBERATTACKS ON CRITICAL INFRASTRUCTURES

Although the definition varies from nation to nation, critical infrastructure is defined as infrastructure that, when compromised in terms of accessibility, confidentiality, or structure, poses a risk to human life, significant economic harm, vulnerabilities to national security, or disruption of the peace. We might cite the transportation and energy sectors as examples of crucial infrastructures. Infrastructures for nuclear and chemical research, space exploration, and the food industry are all regarded as important infrastructures in nations that make up the European Union [167]. In the USA, vital infrastructure covers a far wider range of industries. In addition to the infrastructures listed above are dams, the defense industry, essential manufacturing, and the material and chemical industries. Please see two major critical infrastructure examples below, which highlight the importance of cybersecurity:

a) Baku-Tbilisi-Ceyhan Pipeline (2008): An explosion happened in Turkey's natural gas pipeline in 2008. The attackers breached the network via a flaw in wireless security cameras. The attackers contacted the field staff after they gained access to the control network through the integrated camera network. The field-based error and leak detection alarm systems have been deactivated. The pipeline's pressure was raised, which led to the explosion. The sight of flames discovered an explosion due to sirens being turned off [147].

b) Wiper (2012): Wiper is malware that infected government agencies, oil and gas firms, and energy corporations in Iran in 2012. The first half of the disk was the target of this attack. It started by deleting crucial files required for the system's proper operation. Important files were deleted, and the system crashed. To avoid being discovered, the assailants attempted a variety of strategies. They restricted the system to BIOS functions by prohibiting the operating system from booting [147].

In terms of the power grid, the traditional grid power is upgraded to a smart power grid depending on two-way digital communication, which supports much other technology such as intelligent monitoring and measurement, which provide more efficient power management and raise the depending on renewable energy. However, the complex system comes with many vulnerabilities in communication technology, software, and devices that work in a smart power grid, so providing security for all components and communication lines from cyberattacks or sudden malfunctions is not easy [135]. Hence, the smart power grid creates new types of problems. Some problems we cannot well-understood and need to study the case and analyze the situation and potential vulnerabilities, and then we solve it, also some problem we have a good background about it, but it needs a com- plex solution. The security case is a complex problem, especially when related to a consumer's privacy data and information, so we need to develop legal and regulatory regimes that respect consumer privacy and promote consumer access to information from third-party companies [136]. In the next several years, smart power grid security will face some problems in securing processes and identifying the gaps in systems and organization tasks.

5.3 CYBER SECURITY IN AVIATION SYSTEMS

There have long been investigations into how to protect vital facilities. At the state level, information security has been recognized as a high-risk problem since 1997. Since 2003, the security of information systems supporting vital infrastructures, such as avionics systems, has been elevated to the status of a priority problem. If avionics systems are attacked, it is obvious that if they malfunction, it would negatively affect important sectors like the national economy and maybe passenger safety. Because of this, aviation systems were developed as closed, autonomous systems with rigorous security controls. However, with the project called NextGen (Next Generation Air Transportation System) launched in the USA in 2005 and the SESAR (Single European Sky ATM Research) project [1], which is the European leg of this project, aviation infrastructure systems have begun to be replaced with new systems. These projects aim to design highly efficient, less costly, reliable and safe systems. In the last 15 years, with the studies and systems offered in this area, processes have been automated in many areas, and therefore more interdependent systems have been used. Interdependent systems, while more efficient, introduce different vulnerabilities. It also appears to face challenges in areas such as protecting air traffic control information systems, protecting avionics systems, and clarifying cybersecurity roles/responsibilities. For this reason, studies have been started on these issues to increase avionic systems' safety, reliability and sustainability.

The security of avionics systems against attacks and possibly the prevention of attacks is a very important and critical field of study. For a system to be called secure, The system must ensure confidentiality, authentication, integrity and non-repudiation. However, completely preventing security breaches is not a realistic approach. Therefore, various measures are taken to detect intrusions and repair damages. Secure systems must detect possible attacks and identify the risks of attacks. In this way, it will be much easier to identify events with an acceptable risk level and to take precautions against events with a high-risk level. Different risk management mechanisms are used here. For example, the US Federal Aviation Administration (FAA) presented a tool for risk management in flight safety and mentioned the risk components and consequences in its report [148]. With flying systems becoming more interconnected, the internet idea entering our life, and the growth of the accessibility concept, cyber assaults have grown over time in numerous industries [168]. Given the history of cyberattacks in the aviation sector, it is clear that this is one of the most significant and crucial industries where security risk has grown. There are a few examples of major attacks on the aviation industry:

- The virus infecting the Electronic Flight Bag (EFB) in Taylan caused an error (2007).
- A truck carrying a Global Positioning System (GPS) jammer accidentally disrupted Newark Liberty Airport's ground station systems (2009).
- 750GB of sensitive data was leaked from a New York airport, including device passwords and employee social security numbers (2017).
- Millions of data from Malaysia Airlines, including passengers' passport information, addresses, and phone numbers, were leaked and shared on the internet (2019).

5.3.1 Aviation system vulnerabilities

Avionics designs were created as large point-to-point systems that took up room and had nearly independent analogue processors and powerful power supplies. With the development of technology, the Flight Management System (FMS) has emerged as the first central architectural strategy capable of providing a more comprehensive presentation to the flight crew while remaining autonomous. This has been enhanced with the aviation information management system, and data has started to be gathered in a single location and delivered from there. On the other hand, the integrated modular avionics architecture advanced this system and gave avionic systems a far more centralized and software-based architecture [140]. Although a comprehensive system is shown in this design, the danger from the core structure is also reduced because software and resources are segregated from one another. This stops harmful software from spreading to other areas of the system after finding one area.

Thanks to the integrated modular avionics architecture, Avionics systems now have a more centralized, software-based architecture. Because of this, investigations in this field have risen. It has been projected that those systems may be susceptible to different cyberattacks. It is important to assess the system's dependability and vulnerabilities caused by internal threats such as software bugs, power outages, human mistakes, and external threats coming from attackers or other systems. Threat regions and their extent should be investigated first in order to offer cyber awareness and discover system weaknesses such as:

- Networks: Air Traffic Management (ATM) with Internet Protocol addresses.
- Electronics: Sensors supporting battery power and motor control.
- Software: Integrated Modular Avionics (IMA).
- Analytics: Compatibility and entitlements for GPS and Automatic Dependent Surveillance–Broadcast (ADS-B).
- Communication: The navigation signals required to coordinate the flight.
- Data: System Wide Information Management (SWIM) feature for real-time support for collision avoidance.

5.4 CASE STUDY: THE ATTACK ON THE UKRAINIAN POWER GRID

The cyberattacks in Ukraine are considered the first incidents to result in power outages. It is important to study the effect of this attack on customers and operators. However, the operators rate these incidents as highly important because they can measure the system's reliability. Moreover, it is important to understand the vulnerabilities and develop a defense system which provides mitigation strategy concepts related to the attack. This attack demonstrated varying tactics and techniques to match the defenses and environment of the three impacted targets [142].

The following list summarizes the technical components used by the attackers [128]:

- Spear-phishing to access the business networks of the oblenergos
- Identification of Black Energy 3 at each one of the impacted oblenergos
- Theft of credentials from the business networks
- Using virtual private networks (VPNs) to enter the ICS network
- Using the existing remote access tools within the environment or issuing commands from a remote station which is similar to an operator HMI.
- Serial-to-ethernet communications devices impacted at a firmware level.
- Using a modified Kill Disk to delete the master boot record of impacted organization systems.
- Using UPS systems to affect connected load with a planned service outage

5.4.1 Opportunities

In addition, the firewall enabled the attacker to remotely administer the system from outside the environment by using a remote access capability already present on the computers. In addition, there did not seem to be any resident capacity to monitor the ICS network continuously and look for irregularities and threats via active defensive measures such as network security monitoring, according to reports from the media. Because of these weaknesses, an attacker would have had the opportunity to remain inside the environment for a period of more than six months, during which time they could have conducted reconnaissance on the environment and subsequently carried out the attack [143].

5.4.2 ICS Cyber kill chain mapping

- Reconnaissance: This is the first phase of an attack before selecting a target and formulating an attack strategy. During this phase, attackers gather information from various sources to better comprehend their target, discovering susceptible and insecure software. However, there are no indications of any suspicious network activity before targeting energy businesses. However, the assault and targeting strategy were closely coordinated, indicating that reconnaissance and studies of the impacted system were conducted prior to the strike, allowing the remote triggering of breakers in many substations [128].
- Weaponization: In the second phase, attackers penetrate the network and transfer malware to susceptible systems and individuals, sometimes without the user's knowledge. In this assault, access to specialized infrastructure is not required. Instead, the attackers included BlackEnergy3 in Microsoft Office documents (Excel and Word) [128].
- Delivery, Exploitation, and Installation: For Delivery, the malicious office document was sent to employees of businesses. Exploit, when these documents were opened, the user was prompted to enable macro documents through a pop-up window. This malicious macro document enables the macro-office to install the malicious application BlackEnergy3 on the victim's computer [128].

Following installation, the BlackEnergy3 malware connected with the IP command and control system to facilitate communication between the attacker and compromised computers. The attackers then collect credentials, elevate their privileges, and spread laterally across the environment (e.g., target directory service infrastructure to manipulate and control the authorization and authentication system directly). At this phase, the attackers have accomplished all operations required to gain permanent target access. With this information, enemies could locate VPN connections and entry points into the ICS network. Using native commands and connections, attackers may find the remaining systems and obtain the required data to create a strategy [128].

Using the compromised credentials, the attacker might pivot into network segments, including supervisory control and data acquisition (SCADA) dispatch workstations and servers. The opponents' behaviors upon entering the network were similar in the topic but varied in technical specifics. The attackers then located a UPS-connected network and changed it. The attackers would have had to undertake network reconnaissance on these systems before identifying particular targets for their coordinated assault [128]. The available evidence reveals that the malicious firmware was consistent across devices and published to many sites quickly, indicating that the malicious firmware uploads were likely designed before the assault for predictable execution [128]. Throughout the ICS Attack Phase, the adversaries employed native software to enter the environment and interface directly with the ICS components. They accomplished this utilizing remote administration tools already installed on the operator desktops. The threat actors continued to access the IT environment through VPN [128]. During the same period, the attackers used a remote telephonic denial of service on the energy company's contact center by flooding it with thousands of phone calls to prevent affected consumers from reporting outages [128][144].

5.5 PROTECT AND RECOMMENDATION

Emerging cyberthreats aimed at power systems underscore the need to integrate modern security to safeguard vital assets without interfering with operations. Therefore, should action be taken to defend cybersecurity:

1. Foster awareness-raising and training initiatives for staff: Beginning with recommending end-user awareness training and continuous phishing testing. Services providers and end consumers should be trained on fraud prevention, privacy, etc. [145][140]. Manufacturers should receive training on how to create secure devices and applications. Grid operators should receive training on the threats and risks affecting the resiliency and security of the grid. Because of the role of social engineering in cyberattacks, namely directed email and easily available cyber assets on the internet. Since these regions are not to be trusted, it is important to regulate, partition strictly, and monitor any interactions with them [145].
2. Improve the regulatory and policy framework: Policies and regulations should at least look for [145]:
   A. Taking into account privacy and cybersecurity as two subjects that are inherently dependent on one another,
   B. Outlining security measures that should be addressed in existing smart grid installations (for example, rollouts of smart meters); c. requiring grid operators to conduct mandated risk assessments,

C. Demanding grid operators for mandatory risk assessments,
D. Mandating that grid operators, manufacturers, integrators, and service providers all conform with various security certifications,
E. Imposing regulatory pressures (such as penalties) for enterprises that do not comply with regulations making public the results of compliance checks,
F. Requires operators to disclose cybersecurity issues to a national or international organization.

3. Develop a minimum set of reference standards and guidelines [145][140].
4. Promote the development of security certification schemes for products and organizational security [128].
5. Foster the creation of testbeds and security assessments [140].
6. Foster research in smart grid cybersecurity leveraging existing research programs [145].
7. Using the YARA tool and antimalware can search, detect, and remove malware from infected systems [128].
8. Monitor the users’ behavior on the network and communication throughout the environment and should be focused on the directory (e.g., Active Directory, Domain, eDirectory, and LDAP) [128] [140]
9. Disable remote management of field devices when they are not required [128].

6 THE IMPLEMENTATION OF BIOMETRIC IDENTIFICATION AND ELECTRONIC DATA STORAGE IN MACHINE-READABLE TRAVEL DOCUMENTS

Electronic machine-readable travel documents (eMRTDs) are equipped with biometric data that is internationally compatible and can be used as inputs for face recognition systems, as well as optionally for iris or fingerprint identification systems. The biometric data must be stored as high-resolution images on a high-capacity contactless integrated circuit (IC) along with an encoded replica of the machine-readable zone (MRZ) data. In addition, the requirements allow for the optional storage of certain data at the discretion of the issuing state or organization. These standards apply to all MRTD formats with electrical features, though the variations in eMRTD formats pertain to the MRZ and affect the storage of the MRZ on the contactless IC [103].

6.1 BIOMETRIC IDENTIFICATION

Biometric identification refers to the use of computerized methods to identify an individual based on their physical or behavioral characteristics. A biometric template is a machine code representation of these characteristics that is generated by a software algorithm. It allows for comparisons to be made in order to determine the likelihood that records of characteristics created separately identify the same individual. In general, biometric templates are relatively small in terms of data size, but each biometric system has its own template format, and templates cannot be shared across systems. In order to use a biometric system effectively, the data must be stored in a format that allows the system to generate a template from it. This typically requires the storage of biometric data as one or more images.

6.1.1 ICAO's vision for biometrics

The ICAO has a vision for the use of biometric technology in the following ways:

- Identifying a primary, interoperable type of biometric technology to be used at border control points for verification and watchlist checks by carriers and document issuers and by specifying supplementary agreed-upon biometric technologies.
- Providing specifications for biometric technology usage by document issuers for identification, verification, and watchlist checks.; • Ensuring the capacity to store data for a maximum of 10 years, the acceptable validity term for a travel document.
- The lack of proprietary aspects protects governments or organizations investing in biometrics against changes in infrastructure or suppliers [104].
- Doc 9303 only allows for three different kinds of biometric identification systems. The issuing state or organization MUST conform with the appropriate international standard [105] when storing biometrics in the contactless IC of an eMRTD. There are three types of biometric identification that can be used: facial recognition (which is required), fingerprint recognition (which is optional), and iris recognition (which is also optional)
- ISO / IEC 39794 is the new international standard for encoding biometric data, replacing ISO / IEC 19794: 2005. The transition timeline outlined below has been established [106]:

- By 01/01/2025, passport-reading equipment shall be able to handle ISO/IEC 39794 data after a five-year preparatory period beginning 01/01/2020.
- Passport issuers may utilize the data formats provided in ISO / IEC 19794-X: 2005 or ISO / IEC 39794-X during a five-year transition period between 2025 and 2030. During this moment of change, interoperability and compliance testing will be essential.
- Beginning on 01-01-2030, passport issuers MUST encode biometric data using the ISO / IEC 39794- X standard.

The transition from ISO / IEC 19794: 2005 to ISO / IEC 39794 is outlined in ISO / IEC 49794.

The following terms are used in biometric identification [107]:

- "verify" refers to a one-to-one comparison of provided biometric data, which was collected from the holder of an eMRTD at the time the data was submitted, and a biometric template made when the holder registered for the system;
- "identify" refers to a one-to-many (1: N) search between the biometric information that has been supplied and a collection of templates that represent each individual that has signed up for the system.

In order to improve the accuracy of the background check conducted as part of the application process for a passport, visa, or another travel document, biometrics can be used in the identification function. They can also be used to create a strong correlation between the travel document and the person presenting it. The concepts and meanings of the biometric vocabulary listed in ISO / IEC 2382-37: 2017 are applicable for the purposes of this section [108].

6.1.2 Essential considerations

The following essential considerations should be considered in the specification of biometric applications for eMRTD [109]:

• Global interoperability: the key requirement for specifying a globally compatible deployment system.

• Uniformity: the requirement to reduce, to the greatest degree feasible, discrepancies between the various solutions that may be implemented by issuing States or issuing organizations by defining particular standards.

• Ensuring technical reliability: It is necessary to establish guidelines and parameters to ensure that issuing states or organizations use proven technologies that provide a high level of confidence in identity confirmation. This will assure states or organizations reading data encoded by other issuing states or organizations that the data provided to them is of sufficient quality and integrity to allow for accurate verification in their own systems.

• Functionality: the need that the suggested standards be operational and implemented by governments or organizations without requiring the introduction of a slew of diverse systems and equipment to accommodate all potential variances and interpretations of standards.

6.1.3 Key processes in biometrics

The main processes of a biometric system include the following [110]:

- Establishing identity: Ensuring that the identity of the enrolled individual is known without any doubt.
- Capture: Acquiring a raw biometric sample.
- Extract: Converting the data from the raw biometric sample into an intermediate form.
- Creating a template: Converting intermediate data into a template.
- Comparison: Comparing the information contained in the reference template stored in memory.

These processes are structured as follows:

- The enrollment procedure is based on collecting a raw biometric sample, is utilized for each new individual (possible eMRTD holder) and includes the collection of biometric image samples that will be saved. The automated collection of the biometric element utilizing a device such as a fingerprint scanner, a picture scanner, a digital camera for live capture, or a zoom camera for capture is called the capture process. Each of these devices necessitates the definition of particular criteria and processes for the capture process, such as a standard attitude in front of the camera for image capture for face recognition, the capture of flat or unrolled fingerprints, and eyes wide open to capture the iris. The generated picture is compressed and saved for future identification verification.

- The template production procedure maintains the unique and reproducible biometric properties from the collected biometric picture and often extracts a template from the stored image using a proprietary software technique. When identity confirmation is necessary, the picture is designated to be compared to another acquired image, and a comparison score is obtained. This method incorporates quality control through a sample quality rating system. Quality requirements should be as high as feasible since all subsequent tests depend on the original picture quality. The operation should be repeated if the capture quality is unsatisfactory [105].
- The identification procedure compares the template from the new sample to stored templates of registered users to establish if the user has previously enlisted in the system and, if so, whether they are using the same identity [105].
- The verification method compares a fresh sample from an eMRTD holder to a template from that holder's stored image to verify whether the holder is the same [109].

6.1.4 Examples of how biometric solutions can be applied

The essential application of biometric techniques is identity verification, which establishes the relationship between the holder of an eMRTD and the eMRTD holder of which the holder is the holder.

Several common biometric applications occur throughout the enrollment procedure required in applying for an eMRTD.

The biometric data collected during the enrollment process can be used to search one or more biometric databases (identification) to determine if the user is known to any of the corresponding systems (e.g., as an eMRTD holder with a different identity, as having a criminal record, or as an eMRTD holder from another state or organization) [111].

Users' biometric data may be gathered again and confirmed against the biometric data taken originally if they have the eMRTD (or show up for one of the phases in the issuance procedure after submitting the first application and collecting the biometric data).

The enlisting agents' identities may be confirmed to ensure they can complete the duties allocated to them. Furthermore, biometric authentication may be used to begin a digital signature of audit logs from various stages of the issuance process, allowing biometrics to connect agents to actions for which they are accountable [112].

There are numerous common uses for border biometrics. When a traveler (i.e., an eMRTD holder) arrives or exits a state, their identification may be checked against the picture produced during the travel document's issuance. This improves the efficiency of any advance passenger information (API) system by ensuring that the bearer of a document is the genuine holder to whom it was issued. Furthermore, an issuing state or issuing organization may find it useful to retain the biometric template (s) on the travel document with the picture so that a traveler's identification may be validated at sites inside the nation where the issuer controls the biometric system.

Two-Factor Verification - To validate that the travel document has not been tampered with, compare the current biometric image data acquired on the traveler with the biometric data from their travel document (or a central database) (if appropriate by generating biometric templates of each) [111].

Three-Factor Verification - To confirm that the travel document has not been tampered with, compare the current biometric image data captured on the traveler, the biometric data in their travel document, and the biometric data stored in a central database (if applicable, by constructing biometric templates of each). This approach provides a link between the individual, their eMRTD, and the database where the data was recorded in this eMRTD when it was granted saved [112].

Four-Factor Verification - A fourth, non-electronic confirmatory verification is the visual comparison of the three-factor verification findings with the scanned picture that appears on the traveler's eMRTD [109].

In addition to the use of biometrics in enrollment and border checks, which are utilized in the comparisons of 1: 1 and 1: N, states or organizations should additionally take into consideration the following characteristics and create their own criteria for them [113]:

• The precision of the biometric comparison functions that are included in the system. According to the requirements of the SDL, issuing states or organizations are required to encode the face image on the eMRTD, and they also have the option of encoding one or more biometrics on the fingerprint or the iris. (Biometric information may also be maintained in a database to which the receiving organization or state has access.) The ICAO is responsible for standardizing the biometric picture, but it is the duty of the nations or entities that are receiving the images. Pick their biometric verification software and choose their thresholds for the acceptance scores of identity verification and the rejection scores of imposter attempts.

• The throughput of the biometric system or the border control system refers to the number of passengers who pass through it each minute.

• Whether or not a certain biometric technology (facial recognition, fingerprinting, or iris scanning) is suitable for use in border controls.

6.1.5 Constraints related to biometric technologies

It is common knowledge that the maturation of most biometric technologies is a prerequisite for their widespread use. Because of the quick pace at which technological progress occurs, it is necessary for all specifications, including those outlined in this document, to take into account both the current state of affairs and the future shifts that advancements in technology will bring about.

The laws of the issuing state or the issuing organization on data protection and privacy protection must be complied with to save biometric information on travel documents.

6.2 SELECTION OF BIOMETRIC ELEMENTS APPLICABLE TO ELECTRONIC MACHINE-READABLE TRAVEL DOCUMENTS

It has been known for a very long time that a person's name and reputation are not sufficient characteristics to ensure that the person to whom a travel document (eMRTD) has been issued by the issuing state or organization is the same person who claims to be the same holder in a receiving state or receiving organization. This is something that has been known for a very long time.

The only method that allows a person to be linked incontestably to their travel document is to associate in a tamper-proof manner a physical characteristic, also known as a biometric element, of that person with their travel document [114]. This is the only method for a person to be linked to their travel document.

6.2.1 Main biometric element: facial image

One of the most important information carriers linking this document to its owner is the picture printed on the MRTD, which complies with ICAO regulations. This portrait is a vital component of this document and an essential aspect of the MRTD itself. In addition, having a standardized picture of a high-quality helps issuing agencies authenticate identities, allowing border agencies to review travel documents either physically or via automated processing [115].

6.2.2 Additional optional biometric elements

Issuing states or issuing organizations can add additional data to their identity verification processes (as well as those of other states) by including multiple biometric elements in their travel documents, such as a combination of a traveler's face, fingerprints, and/or iris. This can be done by including multiple biometric elements in travel documents. These additional elements are particularly useful in situations where states or organizations already possess databases of fingerprints or eye-prints, which they can use to verify the biometric elements that are presented to them, for instance, as part of a system for issuing identification cards [116].

An optional component of biometric identification is the fingerprint, which can be used in one of three different types of fingerprint-based biometric technologies. These include systems that recognize fingerprints based on finger images, systems that recognize fingerprint minutiae and systems that recognize fingerprints based on the shape of the finger. There are standards in place to make most computer systems compatible with their respective categories. However, this is not the case. Image data storage, minutiae data storage, and shape data storage are the three standards that have emerged as a direct consequence of the development of fingerprint interoperability. When an issuing state or issuing organization decides to include fingerprint data in its eMRTD, storage of the fingerprint image is required to ensure worldwide interoperability across classes. This is the case even if the fingerprint data is not being used. Whether or not to save an associated template rests solely with the state or entity that is issuing the certificate [114].

An optional iris biometric element: If an issuing state or issuing organization chooses to offer iris data in their eMRTD, then it is required to save an image of the iris to facilitate worldwide interoperability. An optional fingerprint biometric element The decision of whether or not to save an associated template rests solely with the state or entity that is issuing the certificate [116].

7 EFFICIENCIES IN BIOMETRIC SYSTEMS

Biometrics has entered the stage of mass industrial application, and in this regard, the assessment of the effectiveness of biometric systems is coming to the fore: customers, manufacturers and investors are interested in it. However, this task is essential and complicated and attempts to establish the effectiveness of any IT solution [117].

The efficiency of the information system is determined by the ratio of resources expended and results. Moreover, despite how easy it is to establish the cost of the resources spent on implementing a biometric system, it is not easy to determine the results of this implementation. What are the results - increased security, reduced labor costs for employees and customers, reduced or eliminated the cost of material identifiers (cards, keys, etc.)? Moreover, how to measure results if the ultimate implementation goal is formulated in quantitative and qualitative terms? [118]

In other words, first, you need to decide on the interpretation of the term “efficiency”. It should also be noted that performance assessment is a process that takes place in several stages. And finally, it is essential to identify various and multidirectional factors in the vector of their action, which directly or indirectly affects the efficiency of the biometric system [117]

7.1 APPROACHES TO THE DEFINITION OF EFFICIENCY

Various interpretations of the term under consideration reflect the breadth of its content, and their comparative analysis allows us to choose promising directions for assessing effectiveness.

Efficiency = quality: It is possible to understand the supporters of this point of view: any biometric identification technology is probabilistic and does not guarantee one hundred per cent recognition accuracy. Here, the indicators of FAR-coefficients of false admission (False Acceptance Rate) come to the fore, at which the biometric system opens access to a user who is not registered in it (“stranger”). It is generally recognized that the highest quality (lowest FAR) is characteristic of DNA identification systems, but it is not easy to imagine the functioning of these systems in practice, for example, in access control or time tracking [119].

Efficiency = productivity: This approach is closer to reality and reflects the key requirements for mass identification systems. While maintaining high requirements for FAR indicators, the analyzed approach is not limited to them. Also, particular importance is attached to the comfort and speed of identification. The identification rate is primarily determined by the FRR (False Rejection Rate), the probability that the biometric system will not recognize “its”, that is, the user registered in it. As a result, the user will have to repass identification, directly affecting both its speed and comfort [120].

Analyzing the system for compliance with these indicators also affects individual biometric identifiers' internal, essential characteristics. So, for the user, the most convenient recognition technologies are without direct contact with the scanner (for example, by the eye's iris) and at a distance (usually, this direction is associated with face recognition). However, with all the attractiveness of the latter of the technologies mentioned today, it does not provide the necessary levels of FAR and FRR (for example, when trying to identify a person by face by isolating him from the general video stream, and not by comparing a passport photo with photographs of wanted people).

Another issue is related to the processability of the identifier. For example, it is often mentioned that it is difficult to scan fingerprints in elderly people or those who use aggressive substances (detergents, chemicals, etc.). However, similar difficulties arise when working with other identifiers: for example, recognition by the iris is impossible in the presence of diseases affecting the eyeball, and it does not always pass without problems among representatives of the Scandinavian peoples [118].

Efficiency = efficiency and benefit: This approach develops a line aimed at carefully considering the internal characteristics of biometric systems and their external manifestations, most clearly revealing the advantages of biometrics compared with other identification technologies. The list of these advantages is known recognition of a person, and not a password or material medium; the impossibility of refusal from actions confirmed by the presentation of biometric identifiers; the fact that identifiers are inseparable from a specific person and cannot be lost, stolen, or exchanged. And so that this enumeration does not remain a declaration, let us consider a specific example of what consequences the use of other technologies can have [120].

An analysis of the activities of Jerome Kerviel, who caused the bank Societe Generale five billion euros in damage, revealed that this trader borrowed the passwords of his colleagues and, under their names, participated in trading, manipulated the banking information system, deleting information about the transactions, and then restoring them. Of course, these actions do not exhaust the list of Kerviel's offences, but the above is enough to conclude the severe shortcomings of the system for identifying users and managing their access to information resources.

However, in addition to the fundamental aspects, business customers are also interested in the economic return from introducing biometric systems, which should be expressed in specific indicators. To determine them, methods are often used based on the analysis of ROI (Return on Investment - return on investment), and calculations are already being carried out concerning biometrics.

Nucleus Research, an IT ROI consulting firm, estimates that introducing a biometric time tracking system saves 800$ per employee annually. Several factors ensure these savings: suppression of attempts at buddy punching (situations when one employee notes for himself and his colleagues coming to work or leaving), increasing the reliability of reporting information, eliminating overpayments for not worked hours, etc.

Another way to determine ROI is to establish a calculated effect, expressed in a decrease in operating costs, an increase in the number of customers and an increase in traffic, etc. For example, analyzing the activities of biometric payment systems, experts found (according to information from CNN money) that the use of biometrics halves the operating costs of servicing payments and increases traffic by 15% to stores with biometric terminals operating at the checkout [118].

You can also interpret ROI indicators in terms of the effect of saving time and increasing labor productivity. For example, summarizing the results of a survey of its customers, Lenovo found that up to 50% of support calls are caused by problems with passwords (employees simply forget them or lock their account by repeatedly entering the wrong password); in turn, according to Kompulenta, the cost of executing one call to the support service ranges from 20$ to 50$ [121].

7.2 EVALUATION OF EFFECTIVENESS AS A PROCESS

Determining the effectiveness of a biometric system is not a one-time act; appropriate conclusions should be made at all stages of its life cycle. This “defragmentation” makes it easier to tackle this complex problem and reveals ways to improve efficiency [122] further.

This stage is often not considered, although strategic decisions are made at this stage. In addition, it should be borne in mind that the time the customer’s employees engaged in selecting and analysing suppliers’ proposals is also measured in monetary terms.

The completeness of the presentation of the system on the manufacturer’s website, its information openness (including access to information about prices, various forms of feedback, the speed of response to customer requests), the availability of reviews and a portfolio of successful implementations, the rating of the websites of the vendor and its suppliers in search engines - all this data is into a large extent, they save the mentioned time costs and make it possible to formulate the first predictive estimates of the effectiveness of the selected solution [122].

7.2.1 Installation and deployment phase

Here, the key performance criteria are:

- The possibility of centralized installation of the system software.
- Ease and simplicity of registration of biometric identifiers.
- The degree of integrability of biometric technologies into the existing organizational and IT infrastructure.

The introduction of biometrics, as a rule, does not start from a blank slate: for example, with the existing access control and management system for biometric access control terminals, options for full support of Ethernet, Wiegand, and RS interfaces are essential. However, their installation will not lead to the need for significant modification or even more elimination of the existing system. No less important is the ability of the biometric system to combine centralized installation with mechanisms for distributed registration of identifiers when employees of territorially remote branches do not need to visit the head office for this purpose, but it is possible to carry out this registration remotely. The de facto standard is the integration of biometric technologies with such “classic” components of the IT environment as the 1C platform (for time tracking solutions) or Microsoft Active Directory (for identification systems for users of corporate information systems) [123]. Moreover, it is vital to ensure that the biometric system fully matches the specifics of the business processes of the customer company. So, for a significant number of time-tracking solutions, compatibility with 1C is valid only within the framework of the standard configurations of this platform. The efficiency of the biometric system will increase if it can also support information exchange with 1C when changing the mentioned configurations. The IT service, accounting and personnel departments will be relieved of the need to manually enter the biometric system of information about employees already in 1C to display hours worked from the time tracking system.

7.2.2 Industrial operation stage

At this stage, the requirements for ensuring the continuity of the serviced business processes, balancing the load during peak hours (beginning and end of the working day), stable operation in case of external failures, and the ability of individual elements of the system to function in an autonomous mode come to the fore [124].

No less important is the system's scalability, which manifests itself in the absence of restrictions on the number of users and in an uncritical change in the main parameters of its functioning (for example, the time of user identification) with the growth of this number. The functions of centralized management are becoming increasingly popular, which in some cases, are integrated into the general mechanisms of IT management. This trend is most clearly manifested in the field of information security: the stand-alone interfaces for registering biometric identifiers have been replaced by additional tabs in the Active Directory Users and Computers console, which is familiar to administrators [123].

Another argument in favor of the effectiveness of the biometric system is its maximum user-friendliness and the presence of various ways of informing about the identification results: using sound signals or voice messages, displaying the corresponding information in Russian on display, and color indication. In addition, the biometric system should include self-protection elements - signaling in case of attempts to the unauthorized dismantling of access control terminals and providing identification event logs with the ability to customize the levels of detail of information and notify the administrator about emergencies, etc. [124].

7.3 FACTORS AFFECTING THE EFFECTIVENESS OF BIOMETRIC SYSTEMS

1. Biometric identifier properties:

A. Immutability.

B. Informativeness.

C. Convenience of presentation.

D. The maximum possible number of identifiers (per user).

2. Identification algorithm:

A. FAR / FRR indicators.

B. High-speed performance.

C. Recognition support in" one-to-one" and "one-to-many" modes.

D. Volume of files with digital models of identifiers.

E. Computing resource requirements

3. Hardware implementation of the algorithm:

A. Identifier processing speed.

B. Image quality of the identifier (if its graphic image is formed)

C. Service life of the scanner.

D. Sensitivity to external conditions (illumination, etc.), interference, extraneous influences (for example, static electricity), and counterfeits.

4. Software implementation of the algorithm:

A. Advanced business logic.

B. Manageability of the application, its ability to "customize" - fine-tuning to the customer's needs.

C. The possibility of vertical and horizontal scaling.

D. Hot spare and load balancing options.

E. Distributed and service-oriented architecture.

F. Friendly interface.

G. Effective interaction with other components of the IT environment: operating system, DBMS, ERP and CRM systems.

5. The IT environment in which the biometric system operates:

A. Characteristics of the corporate network.

B. The use of modern IT solutions: Microsoft Active Directory, remote access platforms (Citrix, etc.), the ratio of the number of “thin” and ”thick” clients.

C. Quality of communication channels.

6. Organizational and personnel infrastructure of the enterprise:

A. Management hierarchy.

B. The presence of geographically remote branches.

C. The number of personnel and its composition: temporary employees working temporarily, the conditions of part-time, etc.

7. Social and economic environment:

A. Legal regulation of the use of biometric technologies.

B. Public perception of biometric technologies.

C. Customer readiness to invest in high-tech products.

As already noted, the introduction of biometric technologies does not occur in an airless space but in the living “organism” of the customer company. The state of labor discipline, the psychological climate in the team, and changes in public opinion affect the efficiency of biometric systems. Consequently, the transition to biometric technologies should be accompanied by a whole range of informational and organizational-legal measures. Explaining to staff how the biometric system works, and the benefits of automated time tracking will help avoid the suspicion many innovations often encounter when employees of one technical center find out. The need to implement organizational and legal measures is due to the requirements of the Federal Law “On Personal Data” and its by-laws to it. It is required to obtain the written consent of the subjects of personal biometric data to process this information. Furthermore, the operator of the systems where the said processing is carried out (represented by their operator - the administration of the enterprise, etc.) is entrusted with the responsibility to protect personal data. Together with information support, these measures improve the psychological environment and adequate perception of the transition processes to using the biometric system [123].

8 THE RESEARCH PROCEDURE

I carried out two surveys among 70 participants who are airport workers and have more reliable ideas about biometric information. The first targeted travelers and were concerned about their personal experience with biometric verification systems, while the other targeted airport workers and supervisors of these systems to know the efficiency, quality, and cost of biometric systems. The abbreviation list of the terms I used during the research is demonstrated below for a better understanding of the research.

Terms list	
Facial Recognition	A technique for identifying someone or confirming their identity by looking at their face.
Fingerprint	Any surface bears a fingertip's imprint.
Iris Recognition	Identification technique based on distinctive patterns found in the area around the pupil of the eye.
Keystroke Dynamics	The rhythmic and temporal patterns produced by typing.
Retina Scan	A type of biometric scan is carried out by shining a low-energy infrared laser beam directly into a person's eye while they stare through the scanner's eyepiece.
Voice Recognition	The ability of a computer or software to accept and comprehend dictation or to recognize and carry outspoken instructions.
Digital Signatures	A particular kind of signature that serves as identification documentation and is protected by a digital certificate.
Return on Investment	The ratio of investment to net income. A high ROI indicates that

(ROI)	the returns on the investment outweigh the costs.

Before starting the questionnaires, I would like to give more information about the biometric methods and the advantages and drawbacks of them for better understanding. Fingerprint is the most used, inimitable and unique biometric information. Since the 1960s, when the idea of automating fingerprint recognition systems was born, significant progress has been made in both software and hardware used in fingerprint recognition systems [152]. Fingerprint recognition in an automatic fingerprint recognition system (OPTS) is generally based on the comparison of feature points in the fingerprint and their parameters [153]. Face recognition method has increased its attractiveness and usability especially in the last 10 years. Automatic recognition of faces has become a very popular topic due to the increasing fields of military, commercial and legal applications. It is necessary to develop reliable, well-working, fast and efficient algorithms for a fully automatic face recognition system that can process the information in face images and analyze the image. Processes related to face processing can be grouped as face recognition, face tracking, pose estimation, facial expression analysis [153]. Iris recognition systems were developed in the early 1990s and based on the analysis of the iris patterns of individuals, based on the fact that the iris shape of the person does not change throughout the person's life. It is generally used at entry and exit checkpoints that require authentication, such as airports. For precise accuracy, biometric systems using fingerprints have 60 or 70 comparison points, while iris scanning uses about 200 reference points for comparison [154]. The signature, which is defined as a reliable method in authentication and has been used for a long time, can be defined as the way one writes one's own name. People use their signatures in many areas of social life. Two types of information are used in signature recognition. The first of these is the signing time, speed, acceleration, the pressure of the pen, the features related to the signing process such as the pen, and the other is the features of the signature as a pattern. It is difficult for anyone who is not a real user to repeat the signature pattern even if they visually imitate the signature of one of the users in the same way.

Many government organizations, international corporations, institutions, banks, and hospitals, to mention a few sectors, highly approve of biometric solutions. Every industry is seeing growth, but national identity is expanding the fastest, along with finance, banking, workforce, and borders. Principal benefits of biometrics include:

1. Security - Passwords that include letters, numbers, and other symbols are no longer as secure as they once were. There are many hacking incidences every year, and we continually lose money.
2. Accuracy - Conventional security systems often make mistakes that cost us a lot of time, money, and resources. The most popular security measures are passwords, personal identification numbers (PINs), and inaccurate smart cards.
3. Return on Investment - Biometric solutions will provide you with the greatest ROI compared to other security systems. With only one biometric device and software, a major company's thousands of workers may be monitored. On the other hand, managing a large resource to do the same task would take more time than using the right biometric solution.
4. Reputable - According to reports, younger generations value biometric solutions more than others. Banks have already begun using biometric security solutions to increase client security and dependability.
5. Save time - Biometric solutions are very efficient in terms of time. Most of the time, all it takes to pass the system is placing your finger on a gadget or looking at a retina device. On the other hand, the layers of inconveniences and interrogations associated with conventional procedures make them irritating and intolerable.

Another remarkable breakthrough that significantly alters our way of life is biometric technology. The adage "with great power comes even greater responsibility" is particularly applicable to biometric technology. Despite all the excitement over the good news about biometrics, it also has a negative aspect of its own. Compared to its well-known benefits, we know relatively little about biometrics' drawbacks:

1. Physical characteristics cannot be altered - Most biometric modalities rely on physical characteristics like fingerprints, iris, palm veins, etc. We all only have one set of eyes, a certain number of fingerprints, and other fixed physical characteristics. We can change a password, but our fingerprints and retinas cannot be altered since they are fixed. Our biometric information is kept in the databases of the relevant governments or businesses that provide these services.

2. Physical impairment – Some individuals cannot participate in the enrolling procedure. Body parts like fingers or eyes might have been lost or damaged. In this situation, a fingerprint or iris identification device would be humiliating and even disrespectful. These folks will undoubtedly find it difficult to get along with others in the system.
3. Complexity - One of the main drawbacks is the very sophisticated and intricate framework that underpins the whole biometrics procedure. If a non-technical individual tries to comprehend the system, they will flounder like a fish out of water. Companies use highly qualified and experienced programmers to create the system. Therefore, programmers are also needed to maintain the system.

8.1 DEMOGRAPHIC INFORMATION

Figure 19 depicts the demographic information of the participants, which includes gender (A), participants' age (B), education level (C), and nationality (D). The results showed that the majority of the participants were male, constituting 79% of the total number of participants. In comparison, the female participants made up approximately 21% of the total. The age of the participants ranged from under 25 to older than 35, with the largest group being those between 25 and 35 years old, comprising about 60% of the total number of participants. Approximately 27% of the participants were more than 35 years old, and around 14% were under 25 years old. In terms of education level, the majority of the participants held a diploma degree (74.2%), while about 13% held a doctoral degree. The participants in the study came from a variety of countries, with approximately 70% being from Arabian countries.

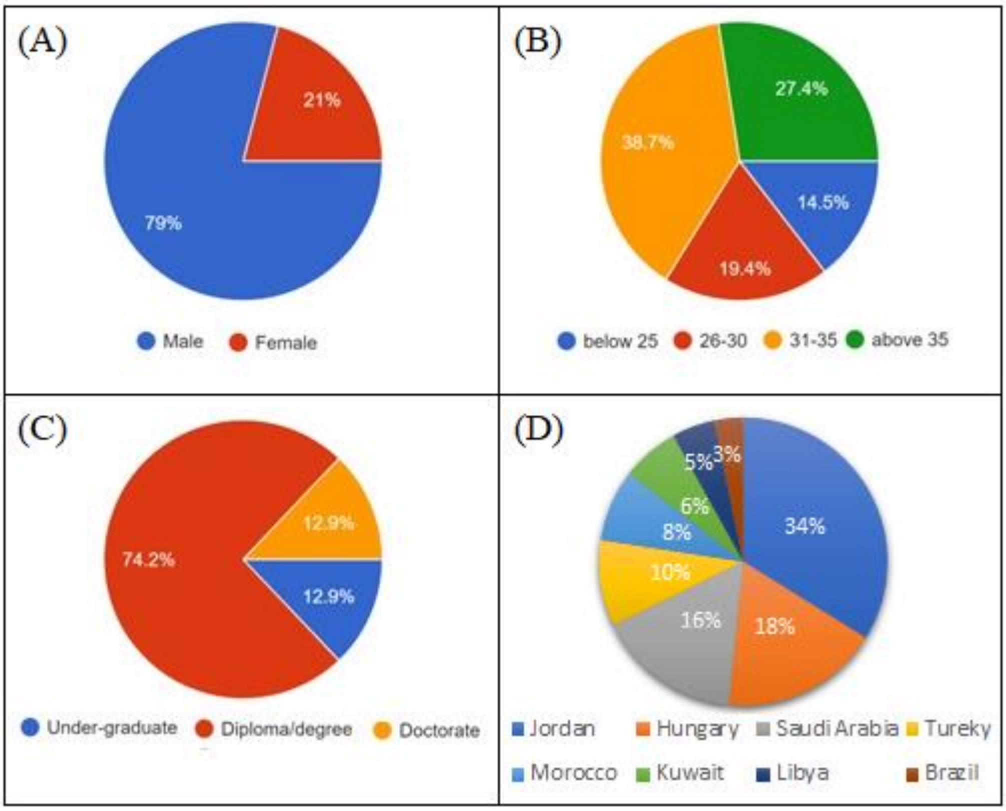

Figure 19 The demographic information of the participants

8.2 FIRST QUESTIONNAIRE

The aim of this questionnaire is to collect information about how people think about the biometric system, what experience they have and how much information they know about this technology, and how they look to the increase of using a biometric system, especially facial recognition, in verification the individual's ID.

This questionnaire is a self-administrated questionnaire with close- end questions. Google form was used to induct this questionnaire. No similar survey was found in the field that can be adapted, so an original survey was constructed to address the research questions depending on the literature review as a basis. After collecting the whole needed responses, a statistician review was done on the survey in order to ensure questions would collect the data necessary to answer the research questions. Sixty-two participants completed the questionnaire. The questions in this questionnaire are divided into two groups. The first group includes four demographic questions to define age, nationality, gender, and education level. The second group includes seven questions related to the research topic.

8.2.1 Results

The result of my first survey is based on nine questions which are aimed to see the important features of biometric methods. The results of my first questionnaire start from Figure 20.

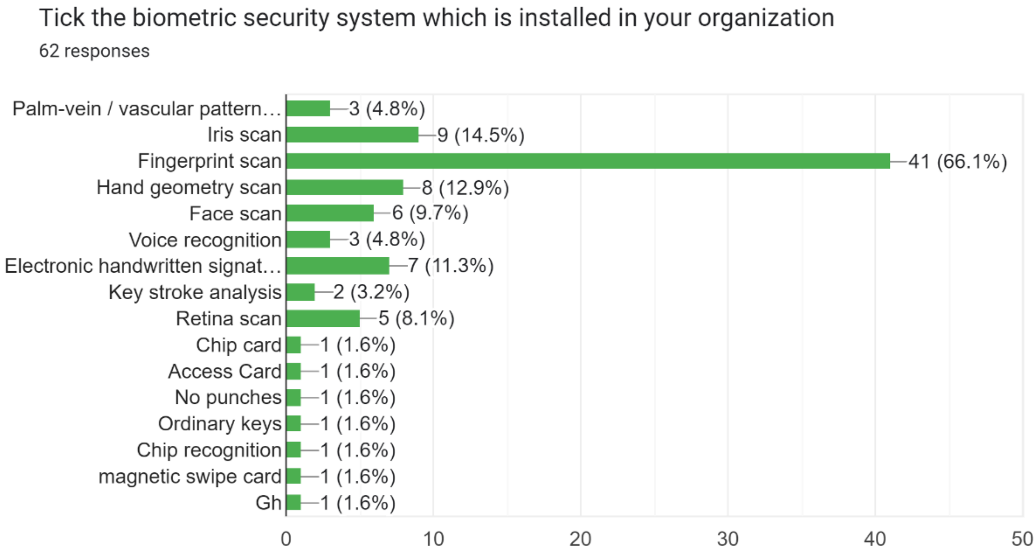

Figure 20 Type of the biometric system installed

Figure 20 illustrates that fingerprint scanning is the most popular biometric system that has been installed, with a total of 66.1% of the systems being fingerprint scanners. This is likely due to the fact that fingerprint scanning is easy to use and relatively affordable compared to other biometric systems. The simplicity of the system likely makes it appealing to businesses and organizations who want to implement biometric security measures but may not want to invest in more expensive or complex systems. Additionally, the economic cost of fingerprint scanning systems may make them a more attractive option for organizations with limited budgets. Overall, the popularity of fingerprint scanning as a biometric system can be attributed to its ease of use and cost-effective nature.

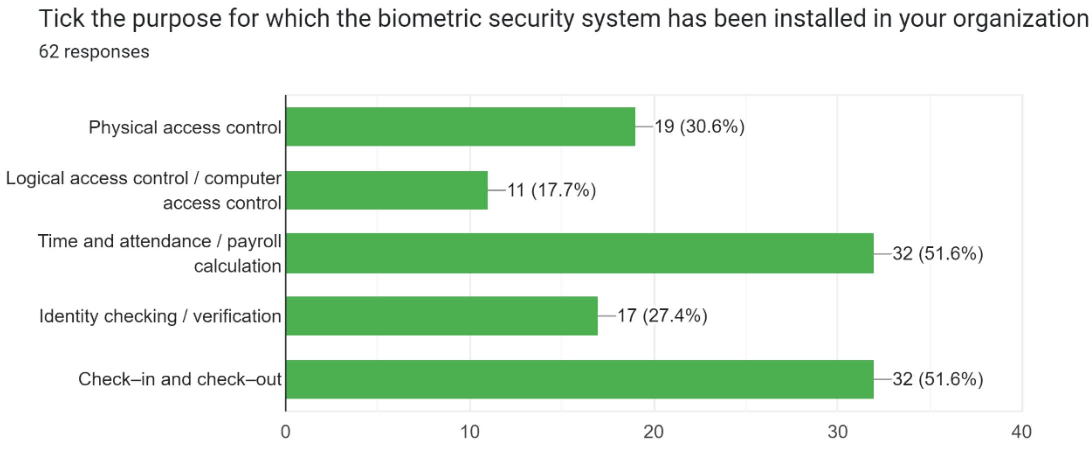

Figure 21 The purpose of the installed biometric system

Biometric systems are now widely used in various companies, workplaces, and institutions for a variety of purposes. According to Figure 21, the primary use of biometrics is to track attendance times of workers and to monitor check-in and check-out processes, with approximately 32% of the systems being used for each of these purposes. This means that a significant portion of the biometric systems are being used to monitor employee attendance and ensure that employees are accurately clocking in and out of work. The use of biometric systems for these purposes can help to improve efficiency and accuracy in tracking employee attendance and can also be used to ensure that employees are following company policies and procedures related to attendance. Overall, the use of biometric systems for attendance tracking and check-in/check-out monitoring is a common practice in modern workplaces.

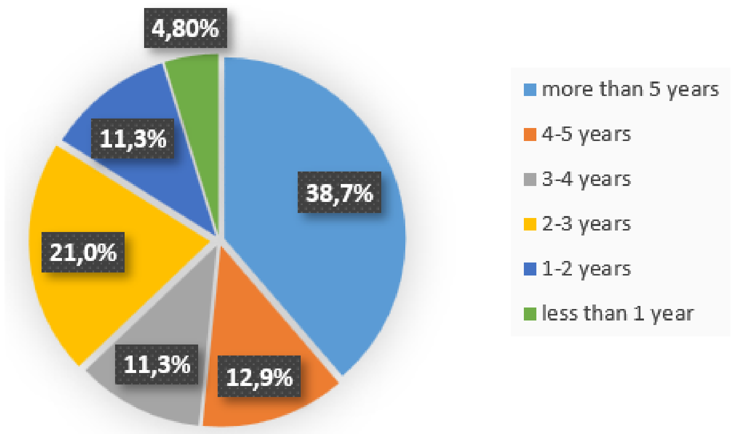

Figure 22 Years of the biometric system has been used at each participant’s organization

Figure 22 demonstrates that the distribution of biometric systems installed is similar to the distribution of nationalities among the participants. This suggests that biometric systems are becoming more widely used in recent years and are being implemented in a variety of countries and regions. Additionally, the data shows that 38.7% of the participants have more than five years of experience with biometric tools, while only 4.8% have less than one year of experience. This indicates that a significant portion of the participants has extensive experience with biometric systems, which can be seen as an advantage for the reliability of the data collected in the survey. Having a large number of experienced participants can help to ensure that the data is accurate and reflective of the overall usage and experiences with biometric systems.

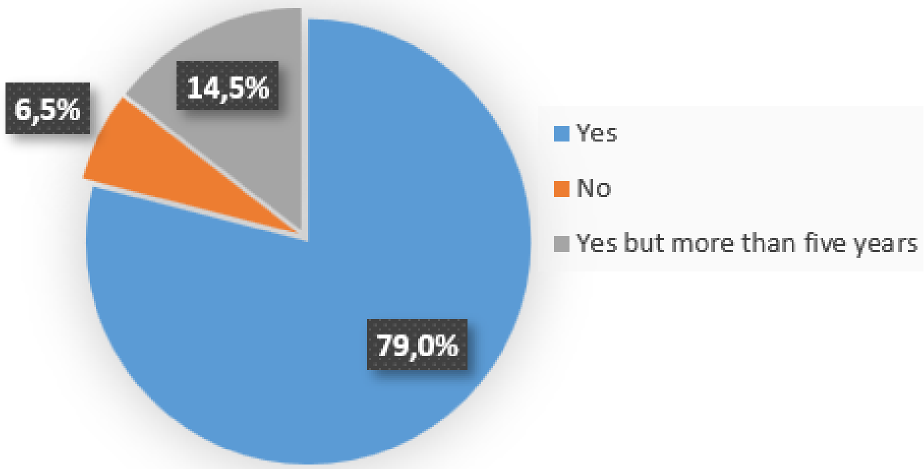

Figure 23 The expectation of participates about the growth of the biometric system at their organization and how long it could take

Figure 23 shows that a significant portion of the participants in the first questionnaire, approximately 79%, believe that biometric technology will continue to grow and develop in the next five years. This suggests that a majority of the participants are optimistic about the future of biometric technology and see it as a rapidly evolving field. This is likely due to the various advancements and innovations in biometric technology in recent years, which have made it increasingly popular and widely used in various industries and sectors. It is possible that the participants believe that biometric technology will continue to evolve and improve in the coming years, leading to even greater adoption and use in various settings.

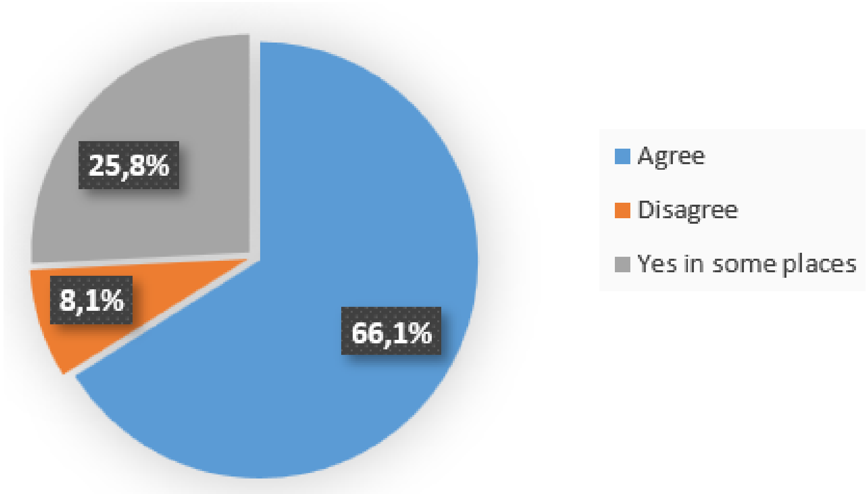

Figure 24 The opinion of participates about using facial recognition in aviation environments and airports for security purposes

Facial recognition is a new and highly secure biometric technology that is primarily used in critical infrastructures and some major airports. According to the results shown in Figure 24, 66.1% of people agree with the use of facial recognition. This suggests that a significant portion of the participants support the use of this technology, potentially due to its effectiveness in providing high levels of security. Facial recognition technology is capable of accurately identifying individuals based on their facial features, making it a useful tool for identifying and tracking people in various settings. It is possible that the participants who agree with the use of facial recognition see it as a valuable tool for improving security and preventing potential threats or asecurity breaches.

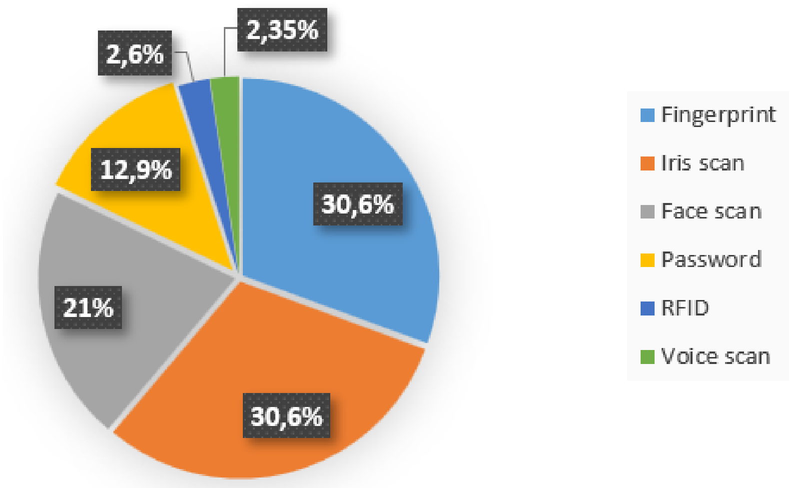

Figure 25 The opinion of participates about the most trust technology to scan their IDs

Figure 25 shows that the most trusted biometric securities are fingerprint scanning and iris scanning, with 30.6% of the participants choosing each of these systems as the most trusted. These biometric systems are based on unique physical characteristics of the body, such as fingerprints and the iris of the eye, which makes them difficult to forge or imitate. As a result, they are considered highly secure and reliable biometric technologies. The third most trusted biometric security is facial scanning, with 21% of the participants choosing it as the most trusted. On the other hand, voice scanning and RFID are the least trusted biometric systems, with only 5% of the participants choosing both of them as the most trusted. This may be due to the perceived vulnerability of these systems to being hacked or bypassed, as well as potential privacy concerns.

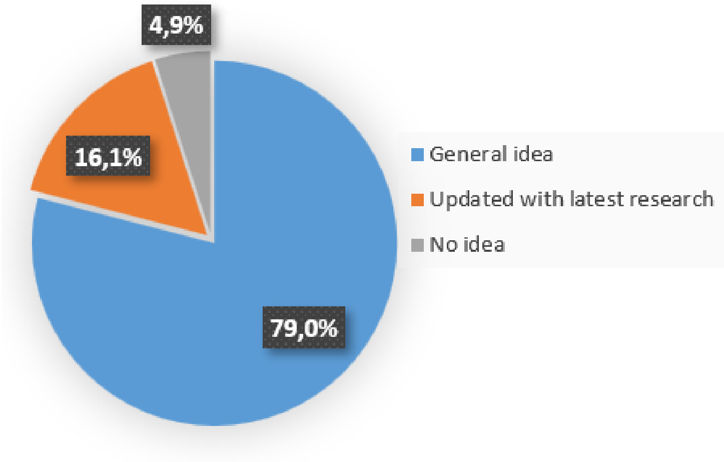

Figure 26 The knowledge of participates about biometric technology

Figure 26 demonstrates that a majority of the participants in the survey sample, approximately 79%, have some knowledge about biometric technology. This suggests that biometric technology is relatively well-known and understood by a large portion of the participants. Additionally, 16% of the participants are aware of the latest improvements in biometric technology, indicating that they are well-informed about the field and are keeping up with current developments. On the other hand, less than 5% of the participants have no idea about biometric technology, indicating that a small percentage of the participants are not familiar with this technology

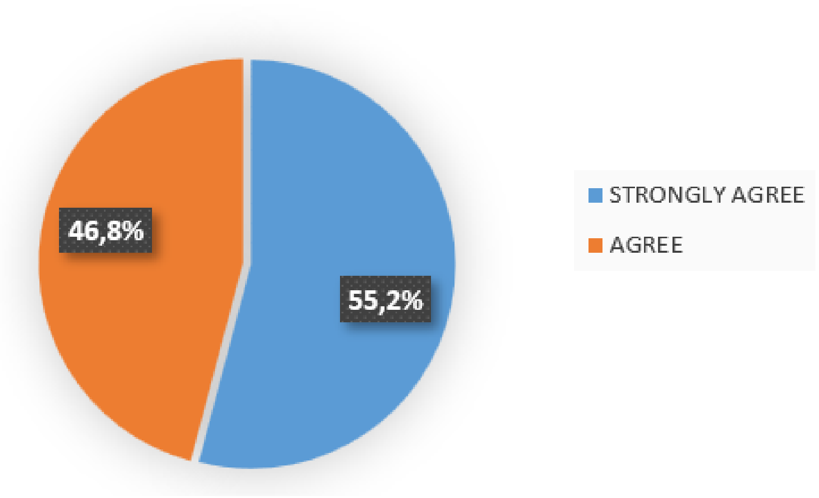

Figure 27 The trust in biometric technology to increase the safety and security in the aviation environment at the airport

Figure 27shows that all of the participants in the questionnaire believe that biometric technology will increase safety in the aviation sector, with more than 50% of them strongly agreeing with this idea. This indicates that a majority of the participants see biometric technology as a valuable tool for improving safety in the aviation industry.

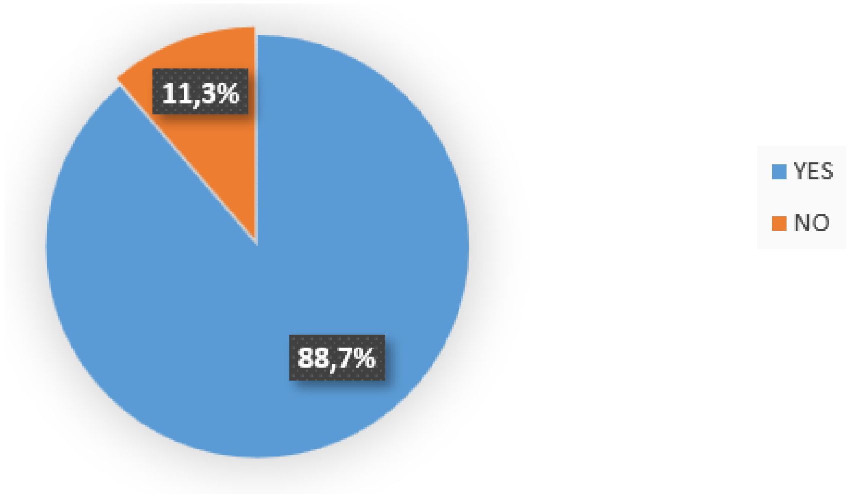

Figure 28 The opinion of the participants on whether they agree or not to install biometric systems in all departments of the airport

The participants, mostly 88,7%, agree with using biometric security tools in all departments of the airport according to the last question, as can be seen in Figure 28.

8.2.2 Discussion

Most of the participants are young, under 35, which gives them a chance to witness more development and growth in using biometric systems, and that is why the participants appeared to be more supportive of increasing using this technology in their organizations and showed their trust in it to increase the safety, especially at important places like airports. However, the knowledge of the participants about biometric systems is not enough. For many participants, using a biometric system, especially for ID checking, is not new; most of them have used it for more than five years. The most common type of biometric system that the participants use is the fingerprint, and that is expected due to the cost of this system, which is considered cheap compared with other biometric system. In addition, fingerprint recognition is easy to use. These reasons helped this technology to be adopted by many organizations. On the other hand, iris recognition is another popular system used to verify an individual’s ID. Iris scanning gives a high level of security, but that is not without a price. The system is considered slow. However, the system is developed in a way that can read a person’s iris from a relatively short distance.

8.3 SECOND QUESTIONNAIRE

The aim of this questionnaire is to collect information about the biometric systems which are used in some airports around the world. The efficiency of these installed systems and the economic cost of them. This questionnaire is a self-administrated questionnaire with close- end questions. Google form was used to induct this questionnaire. No similar survey was found in the field that can be adapted, so an original survey was constructed to address the research questions depending on the literature review as a basis. After collecting the whole needed responses, a statistician reviewed was done on the survey in order to ensure questions would collect the data necessary to answer the research questions. Seventy participants completed the questionnaire. The questions in this questionnaire are in one group. There are no demography questions as they are not related to this kind of survey.

8.3.1 Results

My second questionnaire is mostly based on the economic conclusion of biometric methods, as well as their future expectation, user satisfaction, usability, installation difficulty, security and accuracy, which are included in ten questions. Table 2 presents information about the economic cost of various biometric systems. According to the table, the most expensive biometric method is iris recognition, while fingerprints have an average cost. The costs of other biometric methods can also be seen in the table. It is important to note that the cost of a biometric system can be an important factor in determining which system to use in a particular application. Factors that can affect the cost of a biometric system include the complexity of the system, the materials and resources required for its operation, and the level of accuracy and reliability desired.

Table 2 The economic cost of each biometric system

The name of the used biometric system	The economic cost	response
Gate	Medium	1
Facial Recognition	High	1
	Low	1
	Medium	9
Fingerprint	High	5
	Low	5
	Medium	23
Iris Recognition	High	6
	Medium	7
Keystroke Dynamics	Medium	3
Retina Scan	High	1
	Medium	1
Voice Recognition	Low	1
	Medium	1
Digital Signatures	High	2
	Low	2
	Medium	1

Table 3 shows the performance efficiency of the five most widely used biometric systems in relation to their cost. Based on the table, the economic efficiency of most biometric systems is average. However, iris and voice recognition systems have higher costs compared to their efficiency for a significant number of participants. This means that these systems may not be the most cost-effective options for certain applications. It is important to carefully consider the trade-offs between cost and performance efficiency when selecting a biometric system for a particular purpose. Factors to consider may include the specific needs of the application, the resources available, and the level of accuracy and reliability required.

Table 3 Efficiency of biometric systems are used versus the economic cost

The names of the biometric systems are used	The efficiency versus economic cost	Response
Facial Recognition	High	3
	Low	2
	Medium	7
Fingerprint	High	2
	Medium	10
Iris Recognition	High	5
	Low	4
	Medium	7
Digital Signatures	Medium	6
Voice Recognition	High	5
	Low	2
	Medium	17

Table 4 is focused on the security of various biometric systems. According to the table, participants in the survey were given the opportunity to freely choose their opinions on the security of each system. Based on their responses, it appears that no system was perceived as having poor security by the participants, with the exception of the digital signature system. The rest of the methods were rated as having moderate or high security based on the participants' answers. These results suggest that, in general, biometric systems are perceived as having adequate or strong security by those who took part in the survey. It is important to note that the perceived security of a biometric system can be influenced by a variety of factors, including the effectiveness of the system's security measures, the level of trust that users have in the system, and the perceived potential for abuse or misuse of the system.

Table 4 The security of the used system

The names of the biometric systems are used	Security of system	Responses
Facial Recognition	High	12
	Moderate	12
Fingerprint	High	15
	Moderate	13
Iris Recognition	High	12
	Moderate	12

Keystroke dynamics	High	5
Retina Scan	High	5
	Moderate	2
Voice Recognition	High	8
Digital Signatures	High	4
	Moderate	7
	Poor	2

Table 5 presents the future expectations of survey participants regarding various biometric systems. According to the table, the majority of participants believe that all of the methods need to be developed further, likely due to the continuous advancements in technology. Interestingly, many participants also think that these methods will eventually be replaced by newer technological methods. This suggests that there is a general belief that biometric systems are likely to evolve and change over time and that new methods may emerge that are more advanced and effective than current ones. It is important to note that the development and adoption of new biometric technologies can be influenced by a variety of factors, including the availability of resources, the needs of different applications, and the level of user acceptance and trust in the systems

Table 5 The used biometric system and future expectation

The names of the used biometric system	Future expectation	Responses
Gate	new technologies may replace this system	1
Facial Recognition	depends on the application and the aviation facility	5
	new technologies may replace this system	4

	should be developed and implemented	3
Fingerprint	depends on the application and the aviation facility	14
	new technologies may replace this system	13
	should be developed and implemented	6
Iris Recognition	depends on the application and the aviation facility	5
	new technologies may replace this system	2
	should be developed and implemented	6
Keystroke Dynamics	depends on the application and the aviation facility	1
	new technologies may replace this system	1
	should be developed and implemented	1
Retina Scan	new technologies may re- place this system	1
	should be developed and implemented	1
Voice Recognition	new technologies may replace this system	1
	should be developed and implemented	1
Digital Signatures	depends on the application and the aviation facility	1
	new technologies may replace this system	3

.Figure 29 shows the user satisfaction rate among participants who have used biometric tools. According to the figure, about 68% of the participants indicated that they were satisfied with their experience using these tools. A smaller group (17%) were neutral in their assessment, while less than 15% were dissatisfied. This overall satisfaction rate is relatively high and suggests that users of biometric tools do not have significant issues with these methods. It is important to note that user satisfaction can be influenced by a variety of factors, including the effectiveness and reliability of the biometric system, the ease of use and user experience, and the level of security and privacy provided. It is important for biometric system designers and developers to consider these factors in order to improve the satisfaction of users.

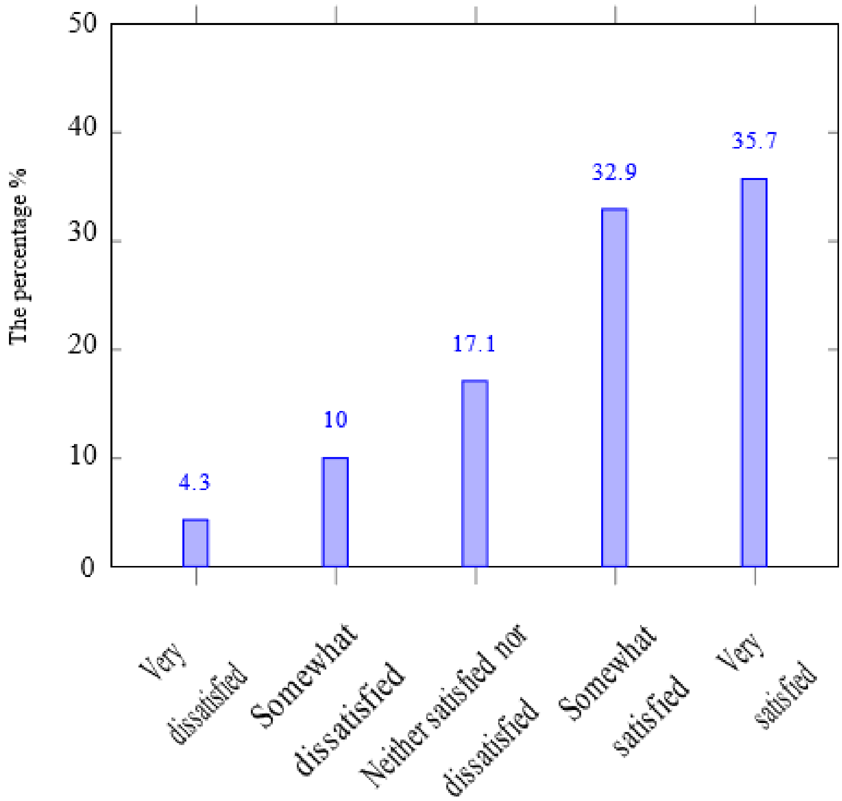

Figure 29 The user satisfaction with using biometric methods

In terms of the difficulty of biometric system installation, approximately 53% of survey actors agree that it is easy to install biometric systems, while around 45% think it is difficult to understand the operations. For details, please refer to Figure 30.

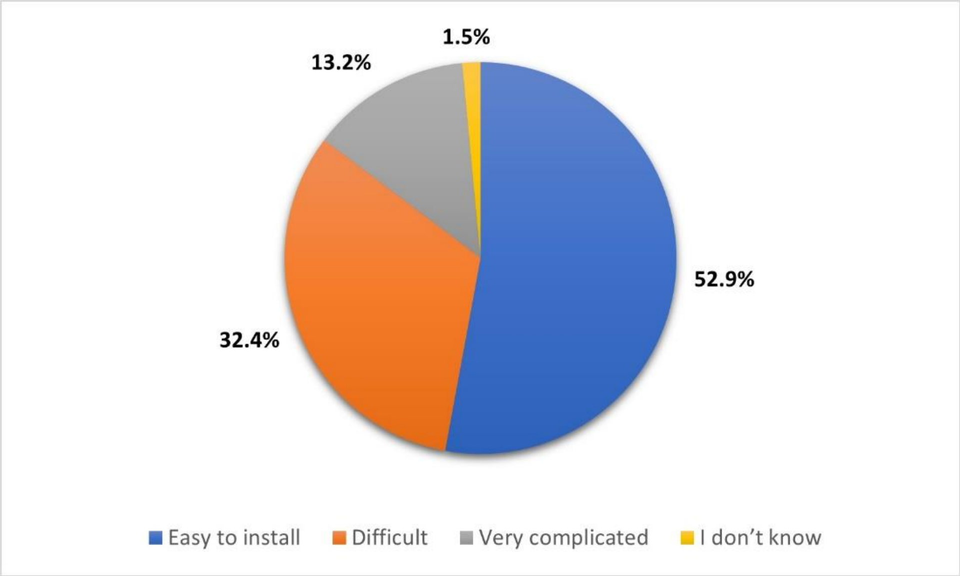

Figure 30 The degree of difficulty in installing this system

A significant number of survey participants, 71%, think that it is easy to use the biometric systems, while only 1.5% agree that it is very simple to understand the biometric methods, as demonstrated in Figure 31.

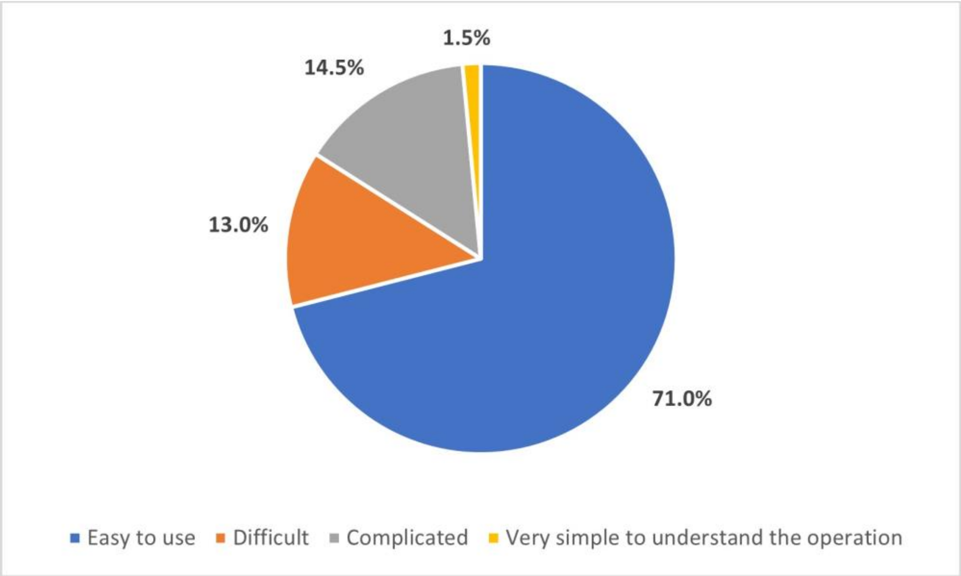

Figure 31 The Usability of the biometric system

As far as the opinion of the survey actors about the reliability and accuracy of the biometric systems is concerned in Figure 32, only 5.9% of them think that the system has low reliability and accuracy means that people mainly trust the biometric systems.

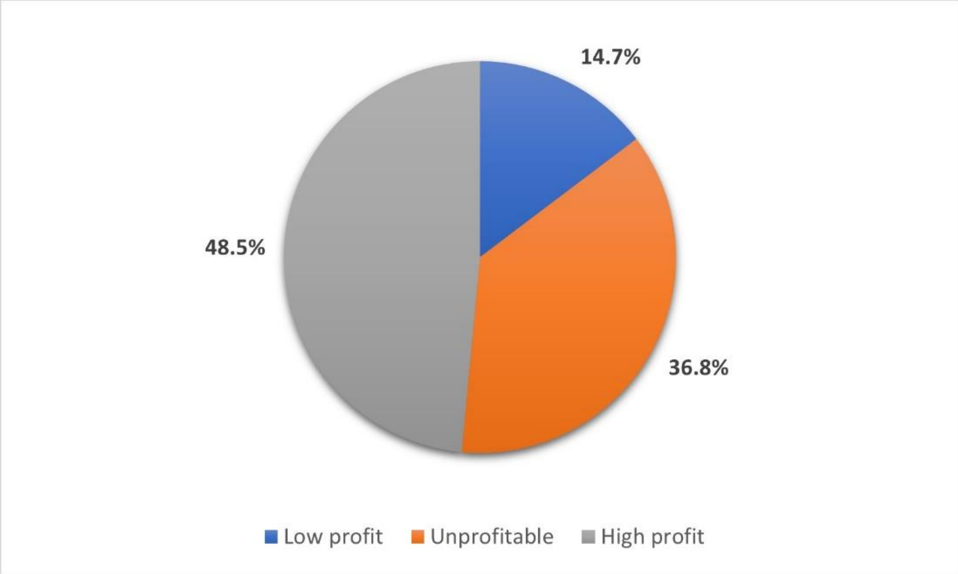

Figure 32 The Reliability and accuracy of the biometric system

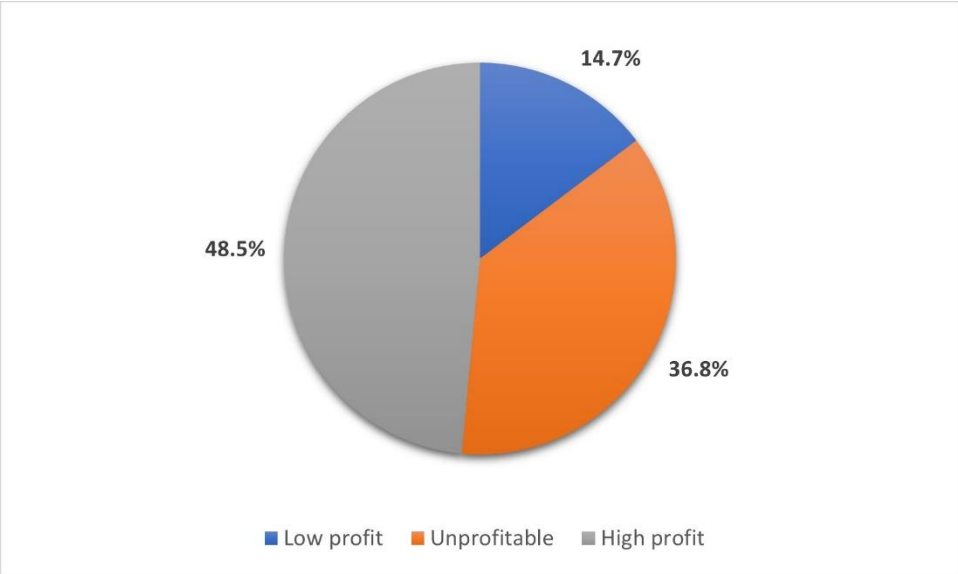

Figure 33 Return on investment (ROI)

Lastly, about profitability, nearly half (48.5%) think that the biometric system has high profitability based on Figure 33. Furthermore, a considerable number of participants (36.8%) think that biometric methods are unprofitable, so the reason why they are used is because of necessary actions.

8.3.2 Discussion

The questionnaire was aimed at employees who work directly with biometric systems in airports. It’s obvious that the fingerprint method is the most used among the other methods. After comes the iris, followed by facial recognition. It's noticed that the main three most used methods are also advanced in many terms that specify the biometric system. Security and method efficiency are the two significant factors, and the record of responses over those factors is quite high. In other words, fingerprint, iris, and facial recognition are still the most trusted methods in the aviation industry. However, I asked what the future expectation about each biometric method and whether it should be installed, developed, or totally replaced. Many participants believe that especially fingerprint and facial recognition methods may either be developed or replaced by new technology, but this also depends on the aviation application and facility. Iris, according to the results, has a more positive impression in terms of implementation. Economic-friendly systems, as obtained, are also a fingerprint and facial recognition. However, the iris is highly efficient and accurate but has a high to medium cost, as recorded. The participant having experience in Keystroke Dynamics agreed that it had not had a high cost, so economically has been reasonable. Also, from the results, I can conclude that the number of systems used is not exactly rational with the economic cost. In other words, we can use more than three methods in one biometric system, and the economic scale will stay at a medium level.

8.4 RESEARCH FINDINGS

One of the digital authentication techniques that became necessary as a result of the digitization of many paper-based transactions was explored in this study: biometric security approaches. Although biometric security systems, which can be described as a person carrying their password on themselves, just recently began to be utilized in actual social life, they are becoming more prevalent every day. Systems that leverage behavioral traits like signature shots and walking styles, as well as fixed physical features like fingerprints, iris, and faces, are quite common nowadays. The report emphasizes biometric systems and the most extensively utilized biometric technologies. The benefits and drawbacks of these technologies are discussed, as well as some ideas for mitigating their drawbacks.

As far as demographic information of surveys participants is concerned, be both genders, different age groups, belonging to different nations, and have at least a diploma degree by participants are upsides of survey actors in general, so such features make the questionnaires strong as these means data variety and quality are suitable for the survey. The first questionnaire shows us the majority of participants are already familiar with the biometric system over the years, and though only 16% of them are updated with the latest news, the majority (79%) have a general idea about the biometric systems illustrated in in Figure 22 and Figure 26. The main purpose of biometric tools in their organizations is to check the time they spend in the facility for security (Figure 21) and for payroll purposes, additionally identify checking, physical access control, and logical access control following them in order. In terms of the biometric method used, the fingerprint is the most famous one by far due to its cost and easy to use, as mentioned in Figure 20 explanation and proved in other questions` results. Additionally, it is worth mentioning that the subject method`s database is much larger than others, as many states and organizations usually keep and store people's fingerprint data. So a small portion of survey participants (6.5%) believe that there will be no development of the biometric system, while 14.5% agree the development will take more than five years. The majority has a common idea that improvements will be faster due to the high-speed advance of technology in Figure 23. Even though people agree to implement the facial recognition system in an aviation environment, the most trusted biometric methods are iris scans and fingerprints, based on Figure 24 and Figure 25**Error! Reference source not found.**. In the end, all participants agree biometric tools serve the purpose of increasing safety. About 11% of survey actors think that biometric tools are needed in all departments. It is good to always mention that whether in the public or private sector, if a critical infrastructure organization is late in making the investments and breakthroughs in response to today's needs, the service it provides to all institutions and organizations connected to its infrastructure may be disrupted, resulting in millions of dollars in loss per second.

In terms of the second questionnaire's results, it starts with Table 2, which describes economic factors, which can be the first thing to discuss when biometric tools are set up for a lot of organizations and even for the government sometimes. While the economic cost of biometric tools is moderate, iris scans and fingerprints can cost more. The more important thing is that are they usually worth their cost? To find out this question, Table 3 helps us so that biometric tools usually satisfy their needs versus their costs. Just for voice and facial recognition, some people agree they do not worth their cost. Furthermore, return on investment seems high profitable based on almost half of the survey participants, while 36% believe that these systems are not profitable, as demonstrated in Figure 33. As far as security of the biometric systems is concerned, fingerprint, facial, and iris recognition have high security, while the digital signature has an average with two poor security answers. It must be mentioned that their security may vary according to what kind of security classification is asked for. People also mainly think that it is easy to install and use these systems, according to Figure 30 and Figure 31. Additionally, people are satisfied with using biometric systems, so only 14.3% do not like the usage of these systems somehow. The general opinion about biometric tools is that they are reliable and accurate (only 6% do not agree with this idea). Lastly, the future expectation about these technologies is mostly about improvement, so if the biometric methods have not been developed frequently, they will be vulnerable to potential threats. As it concerns how these technologies play an important role in the security of critical infrastructures, their advancement has to be at the center of attention

Today, technology is continuously evolving and can be found in almost every industry. Biometric solutions have made it feasible to eliminate the need for traditional security cards and passwords. Because biometric systems are beneficial and safer, the number of applications for them is growing by the day. That is why it is hard to say conclusions about biometric technology as they have been updated frequently, especially whenever gaps are discovered in their usage. From diagnostic-detection controls, these security systems are usually employed at door entries and exits. As a result, it is clear that the operating principles of all biometric systems are broadly similar. First, the user's biometric characteristic is specified, encrypted, and saved in the database. The identification procedure is then completed successfully if the control time matches the new information received from the user in the database.

9 CONCLUSIONS

The need for security is something that nowadays matters to all of us in the different fields and environments in which we are involved daily. This is made possible by the deployment of a biometric identification system for each passenger, whose data is kept in a private and secure database, which enables them to access all airport services and even make automatic payments in the businesses connected. By digitizing this information, user patterns and habits may be studied to enhance their experience in the future. In order to increase security or simplify the flying experience, airport operators and airlines are incorporating biometrics into boarding permits or frequent traveler cards [169]. The majority of nations are beginning to add biometric information to passports and identification cards, often in the form of digital photos and fingerprints. It's conceivable that, soon, biometric technology will be used at every step of the travel process. If this occurs, such systems must not only adhere to their declared security objectives but also be usable by passengers and provide a positive user experience [170].

On the other hand, the biometric technologies and information systems that they implement have already reached a level of efficiency that allows them to be widely used and solve a variety of business problems. It is advisable to use biometric systems both in the back office of the company (administrating the rights of users of information systems, recording working hours, access control) and when serving customers and visitors (escorting passengers, identifying users of payment terminals, etc.).

Given the advantages that distinguish biometrics from other information technologies for identification, the use of biometrics systems has become vital, especially given the growth and diversity of new threats and security challenges.

An assessment of the effectiveness of biometric systems should be carried out at all stages of the system life cycle, and the transition to the use of biometric technologies should be accompanied by a set of regulatory, legal and information support measures.

Increasing the efficiency of biometric systems is facilitated by their maximum integration into the already existing management and IT infrastructure of the enterprise. This integration creates a synergistic effect and positively affects the key performance indicators of the company, which all information technologies, including biometric ones, should serve. Between the different biometric systems, iris scanning and fingerprint recognition are the most common forms of biometric security. However, the detection of facial features and (finger and palm) vein patterns are also becoming more common [171].

The second questionnaire's results demonstrate how different biometric techniques are used in our routine security applications. Additionally, it provides us with substantial compression between the most popular ways and defines each approach in terms of several scales. As a result, still, Fingerprint, iris and facial recognition are the most sensible methods to use in reasonable cost, high efficiency, and security applications.

The concept of the smart city is still developing. The need for a secure way to identify the individual is vital to protecting the user's information and personalizing his experience. Biometrics, in this context, gives the solution. The smart city's inhabitants' biometrics identity guarantees a relabel and secure way to share information and prevent fraud or malicious attacks [148].

As is seen in the first questionnaire, biometric technology has gained the trust of people because it helps in keeping security and increases the feelings of safe between people. However, the knowledge of people about this technology is not enough, so one thing that should be focused on is to enhance the understanding of people about this technology in a way that can make it more popular. While biometric security is a growing industry, it is not at all a new science, and it is familiar to a big percentage of the participants [172].

Electronic commerce, financial transactions, governmental transactions, passports, and so forth. Transactions will also be carried out electronically using biometric identification, with a biometric reader integrated into conventional PCs. However, if we look at the investments and expenditures made in this field, we can see that while the size of expenditures to protect Critical Infrastructure hovered around 133.3 billion USD in 2021, it is expected to reach 157.1 billion USD by 2026, with an average annual growth rate of 3.3% over the next five years [150]. As it is now, the majority of these investments will go toward attempting to avoid data breaches in the future. The harm generated by a cyber assault can be quite large due to malicious uses of data given by data breaches (such as fraud and penetration of corporate network systems). According to the IBM Cost of Data Breach 2022 study, the overall average cost of a data breach globally in 2022 was $4.35 million, up 2.6% year on year. This value averages $4.82 million for breaches of vital infrastructure and $3.83 million for breaches of other businesses. As a result, critical infrastructure intrusions inflict 22.9% more harm than any other type of breach on average [151].

10 IMPORTANCE OF THE STUDY

Assuming biometrics is an effective method for trustworthy automated identity verification. The aviation sector is hesitant to adopt any biometric-based technology without first conducting thorough security and efficiency assessments. The proposed study looked at the usefulness of biometric systems, including user happiness, and recommended novel and general bio-metric elements for use in risk management and cyber-security. The primary impetus for this investigation is the results of related research and the literature cited within. Through my analysis of the surveys conducted for this dissertation, I have come to the conclusion that greater communication between the end-user and the engineers responsible for building biometric systems is required. That's why it's essential to do such a thorough analysis regarding end-users and the system itself. Even the world's most cutting-edge airport has not yet achieved the ultimate aim of implementing a biometric system that excels in all respects, including safety, efficiency, cost-effectiveness, and everything else.

11 `NEW SCIENTIFIC CONTRIBUTIONS

This research is composed of three elements which together contribute to scientific knowledge. They are described as follows:

1. Theoretical Framework: The theoretical framework has narrowed the scope of the research and helped to enhance the existing knowledge about biometrics, and the use of biometrics in aviation, in addition to defining the concept of the smart city and the role of biometrics in the smart city. It also gave insight into the importance of cyber-security. This theoretical framework consists of a comprehensive literature review of relevant scientific documents for understanding biometric technology and its use in aviation. It served as the basis for formulating hypotheses regarding the use of biometrics in aviation in general and at airports.
2. Experimental Procedure: The experimental procedure was performed to modify or test hypotheses. It consisted of two surveys:

A. The first questionnaire was collected from the user about their individual experience when they used the biometric systems at the airport and how it could be described. The aim of this questionnaire was to study the opinions and perceptions of passengers towards the use and implementation of biometric systems at the airport. This survey helped study the customer’s background and knowledge about the biometric system and determine the preferred system based on the customer’s opinion.

B. The second questionnaire collected information about the biometric systems used at the airports, and this information was provided by employees working at airports in many different countries. This survey gives insight into the efficiency and economic cost of these proven systems.

3. Discuss the results: In this part of the research, the statistical analyzes performed on the acquired data set described in the Experimental Procedures section are explained in order to validate or reject the hypotheses proposed in the first section. Accordingly, based on the theoretical framework and the results of statistical analysis, the formulated hypotheses were accepted. Hypotheses have proven that the use of biometric systems in aviation not only enhances security at airports but is also a customer-friendly system. Moreover, the study shows that the economic cost of this technology for installation and maintenance is usually not high. Therefore, biometric systems are increasingly used all over the world and in many sectors.

12 FURTHER RESEARCH, RECOMMENDATIONS, LIMITATIONS

In order to gain a full understanding of the role of biometric systems in the aviation industry, it is necessary to research aspects such as the algorithms that this technology uses to identify an individual by their anatomical or behavioral traits. What are the limitations, and how can they be improved? Furthermore, research that analyzes how airlines can work alongside airport management to implement and use biometric systems in a way that increases the efficiency of these systems and provides a better customer experience is vital to be carried out.

The two questionnaires conducted in this research focus on the use of biometric systems in airports. Data were collected from passengers and employees. However, as can be seen in this data, most airports use multi-biometric systems, so it is also necessary to research how these multi-biometric systems work and compare them to traditional biometric systems.

More research, including the importance of biometric systems at airports, especially during epidemics such as COVID-19, is needed to get a general idea of how biometric systems can help during these situations and examine ways in which biometric systems can be used to reduce the impact of such situations on the aviation industry

REFERENCES

[1] A. K. Jain, A. Ross, and S. Pankanti, “Biometrics: a tool for information security,” IEEE transactions on information forensics and security, vol. 1, no. 2, pp. 125–143, 2006.

[2] E. Kelkboom, X. Zhou, J. Breebaart, R. N. Veldhuis, and C. Busch, “Multi-algorithm fusion with template protection,” in 2009 IEEE 3rd international conference on biometrics: Theory, applications, and systems, pp. 1–8, IEEE, 2009

[3] M. Fang, N. Damer, F. Kirchbuchner, and A. Kuijper, “Micro stripes analyses for iris presentation attack detection,” in 2020 IEEE International Joint Conference on Biometrics (IJCB), pp. 1–10, IEEE, 2020

[4] A. K. Jain, A. A. Ross, and K. Nandakumar, Introduction to bio- metrics. Springer Science & Business Media, 2011

[5] G. of India, “Unique identification authority of India kernel de- scription.” https://uidai.gov.in/, 2012.

[6] E. Comission, “Smart borders kernel description.” http:// ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/index_en.htm., 2013

[7] B. Schneier, “The uses and abuses of biometrics,” Communications of the ACM, vol. 42, no. 8, pp. 136–136, 1999

[8] A. Konga, K. Cheung, D. Zhang, M. Kamel, and J. You, “An analysis of bio hashing and its variants. pattern recognition,” 2006

[9] S. Rane, “Standardization of biometric template protection,” IEEE Multimedia, vol. 21, no. 4, pp. 94–99, 2014

[10] M. Gómez Barrero, “Improving security and privacy in biometric systems,” 2016.

[11] P. Komarinski, Automated fingerprint identification systems (AFIS). Elsevier, 2005

[12] “How biometrics can help airlines take off again,” Biometric Technology Today, vol. 2021, no. 1, pp. 8–11, 2021

[13] E. Indrayani, “The effectiveness and the efficiency of the use of biometric systems in supporting national database based on single id card number (the implementation of electronik id card in Bandung),” Journal of Information Technology & Software Engeneering, vol. 4, p. 129, 2014

[14] M. Fernandez-Carmona, B. Fernandez-Espejo, J. Peula, C. Urdiales, and F. Sandoval, “Efficiency based collaborative control modulated by biometrics for wheelchair assisted navigation,” in 2009 IEEE International Conference on Rehabilitation Robotics, pp. 737–742, IEEE, 2009

[15] S. G. Weber, “Biometrische it-sicherheit—eine frage des finger-spitzengefühls?,” Datenschutz und Datensicherheit-DuD, vol. 37, no. 6, pp. 371–375, 2013.

[16] N. R. Council, W. B. Committee, et al., Biometric recognition: Challenges and opportunities. National Academies Press, 2010.

[17] Biometrics in Government Post 9/11. Report. National Science and Technology Council, 2008.

[18] The Application of Biometrics at Airports. ACI World headquarters- Geneva-Switzerland, 2005.

[19] Accenture, Insights into Automated Border Clearance. Accenture: High performance. Delivered. Chicago, IL: Accenture, 2010.

[20] Frontex, “Biopass ii. automated biometric border crossing systems based on electronic passports and facial recognition: Rapid and smartgate,” 2010.

[21] A. K. Jain and A. Kumar, “Biometrics of next generation: An overview,” Second generation biometrics, vol. 12, no. 1, pp. 2–3, 2010.

[22] R. W. Poole Jr, “Airport security: time for a new model,” The Economic Costs and Consequences of Terrorism, 2006.

[23] A. Oszi and T. Kovács, “Theory of the biometric-based technology in the field of e-commerce,” in 2011 IEEE 12th International Symposium on Computational Intelligence and Informatics (CINTI), pp. 567–571, IEEE, 2011.

[24] "Biometrics: definition, use cases, latest news," Thales group. Retrieved from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics, 2021.

[25] U. Army, "Commander's guide to biometrics in Afghanistan: Observations, insights, and lessons," Center for Army Lessons Learned (CALL). Retrieved from https://info. public intelligence. net/CALL-Afghan Biometrics. pdf, 2011.

[26] N. R. Council, Biometric Recognition: Challenges and Opportunities. Washington, DC: The National Academies Press, 2010.

[27] S. N. Yanushkevich and A. V. Shmerko, "Fundamentals of bio- metric system design: new course for electrical, computer, and software engineering students," in 2009 Symposium on Bio- inspired Learning and Intelligent Systems for Security, pp. 3–8, IEEE, 2009.

[28] N. Bartlow, D. Waymire, and G. Zektser, "Holistic evaluation of multi-biometric systems," BRTRC, October, 2009.

[29] B. Schneier, "Attack trees," Dr. Dobb's journal, vol. 24, no. 12, pp. 21–29, 1999.

[30] E. P. Haas, "Back to the future-the use of biometrics, its impact of airport security, and how this technology should be governed," J. Air L. & Com., vol. 69, p. 459, 2004.

[31] L. Hong and A. K. Jain, "Multimodal biometrics," in Biometrics, pp. 327–344, Springer, 1996.

[32] N. G. Levenson, System safety and computers. Addison Wesley Boston, 1995.

[33] I. Grundschutzhandbuch, "Bundesamt für sicherheit in der informationstechnik," Bonn, DIN-Berlin, vol. 2003, 2000.

[34] US-VISIT Program, Increment Privacy Impact Assessment. Accenture: High performance. Delivered. Chicago, IL: Accenture, 2003.

[35] Press Release, ACLU, supra note 180.

[36] L. Alshamaileh and A. Őszi, "Biometric system in aviation industry (second part)," Biztonságtudományi Szemle, vol. 3, no. 1, pp. 25–33, 2021.

[37] S. N. Yanushkevich and A. V. Shmerko, “Fundamentals of bio- metric system design: new course for electrical, computer, and software engineering students,” in 2009 Symposium on Bio- inspired Learning and Intelligent Systems for Security, pp. 3–8, IEEE, 2009.

[38] “New biometric technology improves security and facilitates us entry process for international travelers,” US-VISIT Editorial Content. Retrieved from https://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_10-fingerprint_consumer_friendly_content_1400_words.pdf, 2009.

[39] U. Riehm, “Bundesamt für sicherheit in der informationstechnik (hrsg.): Virtuelles geld-eine globale falle?,” TATuP-Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis, vol. 8, no. 1, pp. 91–97, 1999.

[40] L. Hong and A. K. Jain, “Multimodal biometrics,” in Biometrics, pp. 327–344, Springer, 1996.

[41] C. McGinnis, “Biometrics boom at the airport,” SF- GATE. Retrieved from https://www.sfgate.com/chris-mcginnis/article/Delta-other-airlines-bring-biometrics-to-more-12782175.php, 2018.

[42] M. P. Down and R. J. Sands, “Biometrics: An overview of the technology, challenges and control considerations,” Information Systems Control Journal, vol. 4, pp. 53–56, 2004.

[43] R. T. Hans, “Using a biometric system to check-in and check-out luggage at airports,” in 2014 International Symposium on Biometrics and Security Technologies (ISBAST), pp. 63–66, 2014.

[44] M. A. Sasse, “Red-eye blink, bendy shuffle, and the yuck factor: A user experience of biometric airport systems,” IEEE Security & Privacy, vol. 5, no. 3, pp. 78–81, 2007.

[45] A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” IEEE Transactions on circuits and systems for video technology, vol. 14, no. 1, pp. 4–20, 2004.

[46] A. K. Jain and A. Kumar, “Biometric recognition: an overview,” in Second generation biometrics: The ethical, legal and social context, pp. 49–79, Springer, 2012.

[47] S. Farrell, “How airports can fly to self-service biometrics,” Bio- metric Technology Today, vol. 2016, no. 1, pp. 5–7, 2016.

[48] M. Maguire, “The birth of biometric security,” Anthropology To- day, vol. 25, no. 2, pp. 9–14, 2009.

[49] P. Pickett, “Air watchdog mulls biometrics: Four Canadian airports to become testing ground for wide-ranging initiative,” Net- work World Canada, vol. 14, no. 6, 2004.

[50] R. Silk, “Delta set to launch first’ biometric terminal’ in US at Atlanta airport,” Travel Weekly, 2018.

[51] A. Alterman, “a piece of yourself”: Ethical issues in biometric identification,” Ethics and information technology, vol. 5, no. 3, pp. 139–150, 2003.

[52] A. Jain, L. Hong, and S. Pankanti, “Biometric identification,” Communications of the ACM, vol. 43, no. 2, pp. 90–98, 2000.

[53] A. Marchenko, “Fingerprint identification,” Elektronika: nauka, tehnologiya, biznes, vol. 6, no. 56, pp. 20–21, 2004.

[54] K. Bowyer and C. Middendorff, “Multi-biometric approaches to ear biometrics and soft biometrics,” 2010.

[55] R. Hans, “Using a biometric system to control access and exit of vehicles at Tshwane university of technology,” pp. 230–233, 09 2014.

[56] V. Arutyunov and N. Natkin, “Comparative analysis of biometric systems for information protection,” Scientific and Technical Information Processing, vol. 37, pp. 87–93, 04 2010.

[57] M. Normalini, T. Ramayah, et al., “Trust in internet banking in Malaysia and the moderating influence of perceived effective- ness of biometrics technology on perceived privacy and security,” Journal of Management Sciences, vol. 4, no. 1, pp. 3–26, 2017.

[58] C. Riley, K. Buckner, G. Johnson, and D. Benyon, “Culture & biometrics: regional differences in the perception of biometric authentication technologies,” AI & society, vol. 24, no. 3, pp. 295–306, 2009.

[59] G. Nowacki and B. Paszukow, “Security requirements for new threats at international airports,” TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, vol. 12, 2018.

[60] G. A. Prasanna, K. Anandakumar, and A. Bharathi, “Multi modal biometric systems: a state-of-the-art survey,” Int Res J Eng Technol, vol. 3, no. 04, 2016.

[61] G. Nowacki and B. Paszukow, “Security requirements for new threats at international airports,” TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, vol. 12, 2018.

[62] M. Saini and A. K. Kapoor, “Biometrics in forensic identification: applications and challenges,” J Forensic Med, vol. 1, no. 108, p. 2, 2016.

[63] P. Sillers, “AIRPORT BIOMETRICS: HOW NEW CUS- TOMS TECHNOLOGY IS GOING TO MAKE SECURITY QUEUES A THING OF THE PAST KERNEL DESCRIPTION.” http://web.archive.org/web/20080207010024/http://www.808multimedia.com/winnt/kernel.htm, 2017. Accessed: 2017-07-30.

[64] A. S. Osman Ali, V. S. Asirvadam, A. S. Malik, and W. Rasheed, “A combined face, fingerprint authentication system,” 2014.

[65] A. Jain and S. Aggarwal, “Multimodal biometric system: A sur- vey,” International Journal of Applied Science and Advance Technology, vol. 1, no. 1, pp. 58–63, 2012.

[66] R. Arora, A. Garg, and M. Sareen, “Framework for augmenting security systems at airports,” in 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence), pp. 231–235, IEEE, 2016.

[67] G. Blalock, V. Kadiyali, and D. H. Simon, “The impact of post- 9/11 airport security measures on the demand for air travel,” The Journal of Law and Economics, vol. 50, no. 4, pp. 731–755, 2007.

[68] N. A. R. Negri, G. M. R. Borille, and V. A. Falcão, “Acceptance of biometric technology in airport check-in,” Journal of Air Trans- port Management, vol. 81, p. 101720, 2019.

[69] A. Oliveira, M. Maia, M. Fonseca, and M. Moraes, “Customer preferences and self-service technologies: hospitality in the pan- demic context,” Anatolia, pp. 1–3, 2020.

[70] J. J. Robertson, R. M. Guest, S. J. Elliott, and K. O’Connor, “A framework for biometric and interaction performance assessment of automated border control processes,” IEEE Transactions on Human-Machine Systems, vol. 47, no. 6, pp. 983–993, 2016.

[71] S. K. Lippert and C. Govindarajulu, “Technological, organizational, and environmental antecedents to web services adoption,” Communications of the IIMA, vol. 6, no. 1, p. 14, 2006.

[72] K. M. Sumner, Airport security: Examining the current state of acceptance of biometrics and the propensity of adopting biometric technology for airport access control. University of Central Florida, 2007.

[73] R. Mayer, “Airport classification based on cargo characteristics,” Journal of Transport Geography, vol. 54, pp. 53–65, 2016.

[74] M. A. Sasse, “Red-eye blink, bendy shuffle, and the yuck factor: A user experience of biometric airport systems,” IEEE Security & Privacy, vol. 5, no. 3, pp. 78–81, 2007.

[75] D. THAKKAR, “Biometric Access Control is Poised to Supersede the Humble Password in Ubiquity.” https://www.bayometric. com/biometric-access-control-supersede-password/.

[76] R. Beale, P. Benoit, and J. Shea, “Biometric based airport access control,” Sept. 2 2004. US Patent App. 10/290,810.

[77] F. Bifulco, M. Tregua, C. C. Amitrano, and A. D’Auria, “ICT and sustainability in smart cities management,” International Journal of Public Sector Management, 2016.

[78] H. Yeh, “The effects of successful ict-based smart city services: From citizens’ perspectives,” Government Information Quarterly, vol. 34, no. 3, pp. 556–565, 2017.

[79] K. Su, J. Li, and H. Fu, “Smart city and the applications,” in 2011 international conference on electronics, communications and control (ICECC), pp. 1028–1031, IEEE, 2011.

[80] A. Ross, S. Banerjee, and A. Chowdhury, “Security in smart cities: A brief review of digital forensic schemes for biometric data,” Pattern Recognition Letters, vol. 138, pp. 346–354, 2020.

[81] H. Han and S. Hawken, “Introduction: Innovation and identity in next-generation smart cities,” City, culture and society, vol. 12, pp. 1–4, 2018.

[82] S. Ijaz, M. A. Shah, A. Khan, and M. Ahmed, “Smart cities: A survey on security concerns,” International Journal of Advanced Computer Science and Applications, vol. 7, no. 2, pp. 612–625, 2016.

[83] A. A. Azeta, D.-O. A. Iboroma, V. I. Azeta, E. O. Igbekele, D. O. Fatinikun, and E. Ekpunobi, “Implementing a medical record system with biometrics authentication in e-health,” in 2017 IEEE AFRICON, pp. 979–983, IEEE, 2017.

[84] J. J. Hathaliya, S. Tanwar, S. Tyagi, and N. Kumar, “Securing electronics healthcare records in healthcare 4.0: a biometric- based approach,” Computers & Electrical Engineering, vol. 76, pp. 398–410, 2019.

[85] D. Shawl, “Biometrics–implementing into the healthcare industry increases the security for the doctors, nurses, and patients,” Journal of Computer Sciences & Applications, vol. 12, no. 1, pp. 22–32, 2013.

[86] Y. Mittal, A. Varshney, P. Aggarwal, K. Matani, and V. K. Mittal, “Fingerprint biometric based access control and classroom attendance management system,” in 2015 Annual IEEE India Conference (INDICON), pp. 1–6, IEEE, 2015.

[87] N. I. Zainal, K. A. Sidek, T. S. Gunawan, H. Manser, and M. Kartiwi, “Design and development of portable classroom attendance system based on arduino and fingerprint biometric,” in The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M), pp. 1–4, IEEE, 2014.

[88] J.-W. Kim, “Implementation of smart classroom information dis- play system using rfid,” in Computer Applications for Security, Control and System Engineering, pp. 314–321, Springer, 2012.

[89] R. J. R. Yusof, A. Qazi, and I. Inayat, “Student real-time visualization system in classroom using rfid based on utaut model,” The International Journal of Information and Learning Technology, 2017.

[90] I. Milenković, U. Šošević, D. Simić, M. Minović, and M. Milovanović, "Improving student engagement in a biometric class- room: the contribution of gamification," Universal Access in the Information Society, vol. 18, no. 3, pp. 523–532, 2019.

[91] B. K. Mohamed and C. Raghu, "Fingerprint attendance system for classroom needs," in 2012 Annual IEEE India Conference (INDI- CON), pp. 433–438, IEEE, 2012.

[92] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon, "Biometric- rich gestures: a novel approach to authentication on multi-touch devices," in proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 977–986, 2012.

[93] M. Chong, A. Habib, N. Evangelopoulos, and H. W. Park, "Dynamic capabilities of a smart city: An innovative approach to dis- covering urban problems and solutions," Government Information Quarterly, vol. 35, no. 4, pp. 682–692, 2018.

[94] D. Kyriazis, T. Varvarigou, D. White, A. Rossi, and J. Cooper, "Sustainable smart city iot applications: Heat and electricity management & eco-conscious cruise control for public transportation," in 2013 IEEE 14th International Symposium on" A World of Wire- less, Mobile and Multimedia Networks"(WoWMoM), pp. 1–5, IEEE, 2013.

[95] S. B. Kelley, B. W. Lane, B. W. Stanley, K. Kane, E. Nielsen, and S. Strachan, "Smart transportation for all? a typology of re- cent us smart transportation projects in midsized cities," Annals of the American Association of Geographers, vol. 110, no. 2, pp. 547–558, 2020.

[96] R. Kannavara and K. L. Shippy, "Topics in biometric human- machine interaction security," IEEE Potentials, vol. 32, no. 6, pp. 18–25, 2013.

[97] Z. Guo, N. Karimian, M. M. Tehranipoor, and D. Forte, "Hard- ware security meets biometrics for the age of iot," in 2016 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1318–1321, IEEE, 2016.

[98] S. Ergin, A. K. Uysal, E. S. Gunal, S. Gunal, and M. B. Gulme- zoglu, "Ecg based biometric authentication using ensemble of features," in 2014 9th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1–6, IEEE, 2014

[99] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (iot): A vision, architectural elements, and future directions,” Future generation computer systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[100] M. Rostami, A. Juels, and F. Koushanfar, “Heart-to-heart (h2h) authentication for implanted medical devices,” in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, pp. 1099–1112, 2013.

[101] M. T. Brown and J. K. Bussell, “Medication adherence: Who cares?” in Mayo clinic proceedings, vol. 86, pp. 304–314, Elsevier, 2011.

[102] R. A. Brown, P. K. Davis, W. L. Perry, P. Roshan, P. Voorhies, and D. Yeung, Using behavioral indicators to help detect potential violent acts: a review of the science base. RAND, 2013.

[103] G. M. Ezovski and S. E. Watkins, “The electronic passport and the future of government-issued rfid-based identification,” in 2007 IEEE International Conference on RFID, pp. 15–22, IEEE, 2007.

[104] J. Stanton, “Icao and the biometric rfid passport: History and anal- ysis,” Playing the identity card: Surveillance, security and identification in global perspective, pp. 253–67, 2008.

[105] G. Gromov, “International standards for the use of biometrics,” Computer Modelling and New Technologies, vol. 13, no. 3, pp. 49–57, 2009.

[106] D. Maltoni, A. Franco, M. Ferrara, D. Maio, and A. Nardelli, “Biolabicao: A new benchmark to evaluate applications assessing face image compliance to iso/iec 19794-5 standard,” in 2009 16th IEEE International Conference on Image Processing (ICIP), pp. 41–44, IEEE, 2009.

[107] Z. H. Choudhury, “Biometrics passport authentication using facial marks,” 2019.

[108] C. Busch, “Standards for biometric presentation attack detection,” in Handbook of Biometric Anti-Spoofing, pp. 503–514, Springer, 2019.

[109] B. Schouten and B. Jacobs, “Biometrics and their use in e-passports,” Image and Vision Computing, vol. 27, no. 3, pp. 305–312, 2009.

[110] S.-H. Cho and H.-Y. Yoon, “A research on the analyzing bio- metric aviation security system and proposing global standardization to improve aviation safety,” Journal of the Korea Academia- Industrial cooperation Society, vol. 21, no. 5, pp. 637–647, 2020.

[111] A. Nourbakhsh, M.-S. Moin, and A. Sharifi, “Facial images quality assessment based on iso/icao standard compliance estimation by hmax model,” Journal of Information Systems and Telecommunication (JIST), vol. 3, no. 27, p. 225, 2020.

[112] R. Abeyratne, “E-passport and the public key directory consequences for icao, the,” Air & Space L., vol. 30, p. 255, 2005.

[113] S. Kundra, A. Dureja, and R. Bhatnagar, “The study of recent technologies used in e-passport system,” in 2014 IEEE global humanitarian technology conference-South Asia Satellite (GHTC-SAS), pp. 141–146, IEEE, 2014.

[114] D. Malčík and M. Drahanskỳ, “Anatomy of biometric passports,” Journal of Biomedicine and biotechnology, vol. 2012, 2012.

[115] M. Ferrara, A. Franco, D. Maio, and D. Maltoni, “Face image conformance to iso/icao standards in machine readable travel documents,” IEEE Transactions on Information Forensics and Secu- rity, vol. 7, no. 4, pp. 1204–1213, 2012.

[116] M. Abid, S. Kanade, D. Petrovska-Delacrétaz, B. Dorizzi, and H. Afifi, “Iris based authentication mechanism for e-passports,” in 2010 2nd International Workshop on Security and Communication Networks (IWSCN), pp. 1–5, IEEE, 2010.

[117] P. Drozdowski, C. Rathgeb, A. Dantcheva, N. Damer, and C. Busch, “Demographic bias in biometrics: A survey on an emerging challenge,” IEEE Transactions on Technology and Society, vol. 1, no. 2, pp. 89–103, 2020.

[118] A. K. Jain and A. Kumar, “Biometric recognition: an overview,” Second generation biometrics: The ethical, legal and social con- text, pp. 49–79, 2012.

[119] T. Duarte, J. P. Pimentão, P. Sousa, and S. Onofre, “Biometric access control systems: A review on technologies to improve their efficiency,” in 2016 IEEE International Power Electronics and Motion Control Conference (PEMC), pp. 795–800, IEEE, 2016.

[120] D. Zanotelli, L. Montagnani, G. Manca, and M. Tagliavini, “Net primary productivity, allocation pattern and carbon use efficiency in an apple orchard assessed by integrating eddy covariance, biometric and continuous soil chamber measurements,” Biogeosciences, vol. 10, no. 5, pp. 3089–3108, 2013.

[121] D. Zanotelli, L. Montagnani, G. Manca, and M. Tagliavini, “Net primary productivity, allocation pattern and carbon use efficiency in an apple orchard assessed by integrating eddy-covariance, bio- metric and continuous soil chamber measurements.,” Biogeo- sciences Discussions, vol. 9, no. 10, 2012.

[121] F.-M. E. Uzoka and T. Ndzinge, “An investigation of factors affecting biometric technology adoption in a developing country context,” International Journal of Biometrics, vol. 1, no. 3, pp. 307–328, 2009.

[123] P. J. Phillips, A. Martin, C. L. Wilson, and M. Przybocki, “An introduction evaluating biometric systems,” Computer, vol. 33, no. 2, pp. 56–63, 2000.

[124] Y. Lee, J. J. Filliben, R. J. Micheals, and P. J. Phillips, “Sensitivity analysis for biometric systems: A methodology based on orthogonal experiment designs,” Computer Vision and Image Understanding, vol. 117, no. 5, pp. 532–550, 2013.

[125] L. Gkatzikis, I. Koutsopoulos, and T. Salonidis, “The role of aggregators in smart grid demand response markets,” IEEE Journal on Selected Areas in Communications, vol. 31, no. 7, pp. 1247–1257, 2013.

[126] A. Ghosal and M. Conti, “Key management systems for smart grid advanced metering infrastructure: A survey,” IEEE Communications Surveys Tutorials, vol. 21, no. 3, pp. 2831–2848, 2019.

[127] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, “A survey on cyber security for smart grid communications,” IEEE Communications Surveys Tutorials, vol. 14, no. 4, pp. 998–1010, 2012.

[128] D. U. Case, “Analysis of the cyber-attack on the Ukrainian power grid. (2016),” Electricity Information Sharing and Analysis Center, vol. 388, 2016.

[129] J. Zhou, L. He, C. Li, Y. Cao, X. Liu, and Y. Geng, “What’s the difference between traditional power grid and smart grid? — from dispatching perspective,” in

2013 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), pp. 1–6, 2013.

[130] Y. Cunjiang, Z. Huaxun, and Z. Lei, “Architecture design for smart grid,” Energy Procedia, vol. 17, p. 1524–1528, 12 2012.

[131] K. Anjana and R. Shaji, “A review on the features and technologies for energy efficiency of smart grid,” International Journal of Energy Research, vol. 42, no. 3, pp. 936–952, 2018.

[132] C. Greer, D. A. Wollman, D. E. Prochaska, P. A. Boynton, J. A. Mazer, C. T. Nguyen, G. J. FitzPatrick, T. L. Nelson, G. H. Koepke, A. R. Hefner Jr, et al., “Nist framework and roadmap for smart grid interoperability standards, release 3.0,” 2014.

[133] “Ex-post evaluation of pasr activities in the field of security.” https://ec.europa.eu/home-affairs/sites/default/ files/e-library/documents/policies/security/pdf/ aviation_case_study cses_en.pdf.

[134] R. Mattioli and K. Moulinos, Communication network interdependencies in smart grids. European Union Agency For Network And Information Security (ENISA), 2015.

[135] A. Hahn and M. Govindarasu, “Cyber attack exposure evaluation framework for the smart grid,” IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 835–843, 2011.

[136] A. Bendovschi, “Cyber-attacks–trends, patterns and security countermeasures,” Procedia Economics and Finance, vol. 28, pp. 24–31, 2015.

[137] K. I. Sgouras, A. D. Birda, and D. P. Labridis, “Cyber-attack im- pact on critical smart grid infrastructures,” in ISGT 2014, pp. 1–5, IEEE, 2014.

[138] J. Yan, H. He, X. Zhong, and Y. Tang, “Q-learning-based vulnerability analysis of smart grid against sequential topology at- tacks,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 1, pp. 200–210, 2016.

[139] S. N. Islam, Z. Baig, and S. Zeadally, “Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures,” IEEE Transactions on Industrial Informatics, vol. 15, no. 12, pp.6522–6530, 2019.

[140] F. Aloul, A. Al-Ali, R. Al-Dalky, M. Al-Mardini, and W. El-Hajj, “Smart grid security: Threats, vulnerabilities and solutions,” International Journal of Smart Grid and Clean Energy, vol. 1, no. 1, pp. 1–6, 2012.

[141] S. Paul and Z. Ni, “Vulnerability analysis for simultaneous attack in smart grid security,” in 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1–5, IEEE, 2017.

[142] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, “The 2015 Ukraine blackout: Implications for false data injection at- tacks,” IEEE Transactions on Power Systems, vol. 32, no. 4, pp. 3317–3318, 2016.

[143] R. Khan, P. Maynard, K. McLaughlin, D. Laverty, and S. Sezer, “Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid,” in 4th International Symposium for ICS & SCADA Cyber Security Research 2016 4, pp. 53–63, 2016.

[144] C. Konstantinou, M. Sazos, and M. Maniatakos, “Attacking the smart grid using public information,” in 2016 17th Latin-American Test Symposium (LATS), pp. 105–110, IEEE, 2016.

[145] E. Egozcue, D. H. Rodríguez, J. A. Ortiz, V. F. Villar, and L. Tarrafeta, Smart Grid Security: Recommendations for Europe and Member States. European Union Agency For Network And Information Security (ENISA), 2012

[146] Bulent Caliskan, and Baris Celiktas, Siber Guvenlik ve Savunma Standartlar ve Uygulamalar Siber Guvenlik Cilt 3, 2012

[147] Şeref Sağıroğlu and Sedat Akleylekand, Volume 6 Siber Güvenlik ve Savunma: Siber Güvenlik Ontolojisi, Tehditler ve Çözümler, 2022

[148] Şeref Sağıroğlu -Mustafa Şenol, Volume 2 Siber Güvenlik ve Savunma: Problemler ve Çözümler, 2019

[149] ENISA, Analysis of the European R&D Priorities in Cybersecurity, https://www.enisa.europa.eu/publications/analysis-of-theeuropean-r-d-priorities-in-cybersecurity, p:8, 01.12.2018

[150] Markets & Markets, Market Research Report – Critical Infrastructure, (https://www.marketsandmarkets.com/Market-Reports/criticalinfrastructure-protection-cip-market), 01.06.2021

[151] IBM Data Breach Report 2022, The average cost of a data breach in critical infrastructure organizations (https://www.ibm.com/downloads/cas/3R8N1DZJ), p:37, 27.07.2022

[152] Halici U.; Jain L. C.; Hayashi, I.; Lee, S.B.; Tsutsui T., Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC press, USA, 1999.

[153] A Biometric Identification System Based on Palmprints and Fingerprints, Elena Battini Sönmez, Nilay Özge Özbek, Önder Özbek

[154] New Approaches for Preprocessing Used in Automatic Fingerprint Recognition Systems, Şeref Sağıroğlu ve Necla Özkaya, Gazi Üniv. Müh. Mim. Fak. Der. Cilt 21, No 1, 11-19, 2006.

AUTHOR`S PUBLICATIONS

[155] Biometric System in Aviation Industry (first part), Lafee Alshamaileh and Arnold Őszi, pp 2-3, 2020

[156] Biometric System in Aviation Industry (first part), Lafee Alshamaileh and Arnold Őszi, pp 4-6, 2020

[157] Biometric System in Aviation Industry (first part), Lafee Alshamaileh and Arnold Őszi, p 8, 2020

[158] Biometric System in Aviation Industry (second part), Lafee Alshamaileh and Arnold Őszi, pp 1-3, 2021

[159] Biometric System in Aviation Industry (second part), Lafee Alshamaileh and Arnold Őszi, p 4, 2021

[160] Risk management of biometric systems at international airports, Lafee Alshamaileh and Kovacs Tibor, p 2, 2020

[161] Risk management of biometric systems at international airports, Lafee Alshamaileh and Kovacs Tibor, p 3, 2020

[162] Risk management of biometric systems at international airports, Lafee Alshamaileh and Kovacs Tibor, pp 4-5, 2020

[163] Risk management of biometric systems at international airports, Lafee Alshamaileh and Kovacs Tibor, p 7, 2020

[164] Cyberattack on the Smart Power Grid, Lafee Alshamaileh and Kovacs Tibor, pp 1-2, 2021

[165] Cyberattack on the Smart Power Grid, Lafee Alshamaileh and Kovacs Tibor, p 3, 2021

[166] Cyberattack on the Smart Power Grid, Lafee Alshamaileh and Kovacs Tibor, p 4, 2021

[167] Cyberattack on the Smart Power Grid, Lafee Alshamaileh and Kovacs Tibor, pp 5-6, 2021

[168] Cyberattack on the Smart Power Grid, Lafee Alshamaileh and Kovacs Tibor, p 8, 2021

[169] Biometric Effect on the Aviation Environment, Lafee Alshamaileh and Arnold Őszi, pp 2-3, 2023

[170] Biometric Effect on the Aviation Environment, Lafee Alshamaileh and Arnold Őszi, p 5, 2023

[171] Biometric Effect on the Aviation Environment, Lafee Alshamaileh and Arnold Őszi, p 7, 2023

[172] Biometric Effect on the Aviation Environment, Lafee Alshamaileh and Arnold Őszi, p 8, 2023

LIST OF TABLES

LIST OF FIGURES

APPENDICES

Appendix I: First questionnaire

A.1 Demographic question

1. The gender

(a) Male

(b) Female

2. The age

(a) Under 25

(b) 25-30

(c) 31-35

(d) above 35

3. The education level

(a) Undergraduate

(b) Diploma degree

(c) Doctorate

4. Nationality

(a) Brazil

(b) Libya

(c) Kuwait

(d) Morocco

(e) Turkey

(f) Saudi

(g) Hungary

(h) Jordan

A.2 The research questions

1. Type of the biometric system installed

(a) Palm-vein/ vascular pattern

(b) Fingerprint

(c) Hand geometry scan

(d) Face scan

(e) Voice recognition

(f) Key stroke analysis

(g) Retina scan

(h) Chip card

(i) Access card

(j) No punches

(k) Ordinary keys

(l) Chip recognition

(m) magnetic swipe card

2. The purpose of the installed biometric system

(a) Physical access control

(b) Logical access control/ Computer access

(c) Time and attendance/ payroll calculation

(d) Identity checking/ verification

(e) Check-in and check-out

3. Years of the system has been used at each the organization

(a) Less than one year

(b) 1-2

(c) 2-3

(d) 3-4

(e) 4-5

(f) More than 5 years

4. The expectation about the growth of the biometric system at the organization and how long it could take

(a) No

(b) Yes

(c) Yes, but it needs more than 5 years

5. The opinion about using facial recognition in aviation environment and airport for security purpose

(a) Agree

(b) Yes, in some places

(c) Disagree

6. The most trust technology to scan the IDs

(a) Voice scan

(b) RFID

(c) Password

(d) Face scan

(e) Iris scan

(f) Fingerprint

7. The knowledge about biometric technology

(a) No idea

(b) Updated with the last research

(c) General idea

8. The trust in biometric technology to increase the safety and security in aviation environment at airport

(a) Agree

(b) Strongly agree

(c) Disagree

9. Install biometric systems in at all departments of airports

(a) No

(b) Yes

Appendix II: Second questionnaire

1. Number of biometric systems are used

(a) 1

(b) 2

(c) 3

(d) more than 3

2. The name of the used biometric system

(a) Fingerprint

(b) Facial Recognition

(c) Voice Recognition

(d) Iris Recognition

(e) digital signatures

(f) Keystroke Dynamics

(g) Retina Scan

3. The degree of difficulty to install this system.

(a) Easy to install

(b) Difficult

(c) Very complicated

4. Usability

(a) Easy to use

(b) Difficult

(c) Complicated

5. Security

(a) Poor

(b) Moderate

(c) High

6. Reliability and accuracy

(a) Low

(b) Moderate

(c) High

7. The economic cost

(a) Low

(b) medium

(c) High

8. Return on investment

(a) unprofitable

(b) low profit

(c) high profit

9. The user satisfaction

(a) Very dissatisfied

(b) Somewhat dissatisfied

(c) Neither satisfied nor dissatisfied

(d) Somewhat satisfied

(e) Very satisfied

10. Future expectation

(a) should be developed and implemented

(b) depends on the application and the aviation facility

(c) new technologies may replace this system

ACKNOWLEDGMENTS

My heartfelt thank goes to Prof. Dr. Tibor Kovács for his advice and continuous guidance and also to Prof. Dr. Zoltán Rajnai for his generous help. I would like to thank the administration of the Doctoral School of Safety and Security Sciences Erika Hronyecz and Katalin Lévay for their support throughout my studies in Hungary.

My doctoral thesis would not have been possible without the encouragement of my family in Jordan.