ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOCTORAL (Ph.D.) THESIS BOOKLET

LAFEE ALSHAMAILEH

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

Professor Dr. Rajnai Zoltán

DOCTORAL SCHOOL ON SAFETY AND SECURITY SCIENCES

30.01.2023

Contents

Summary

The purpose of the research is to see the biometric systems effectiveness on important infrastructures and their role in cybersecurity. Critical infrastructures are playing major role in society`s needs, in the terms of telecommunication, air transportation, electricity distribution, smart city technologies and so on. In the highly technologized and digitalized world, cybersecurity is vital to protect such infrastructures from cyber threats, even when we take into consideration how fast the technology is improving, cybersecurity must be kept up to date at the same speed as technological advancement. I mainly focused on air transportation in my dissertation since there are few works about this topic that are not mainly updated. It would be good to remember that 4.5 billion passengers traveled by air transfer in 2019, even though this number sharply decreased in 2020 and 2021 due to Corona pandemic, it started to grow again in 2022, and, indeed, this number will surpass 2019`s numbers in the future.

About the biometric, the primary goal of biometric technology is to consistently and automatically differentiate persons based on one or more signals collected from physical or behavioral attributes such as the face, fingerprint, iris, voice, hand, signature, and so on. These features are also known as biometric characteristics. Despite the fact that automated person identification has been investigated for more than four decades [2], biometrics was not established as a separate scientific area until the last decade. According to recent references, specific conferences [3], common benchmark tools and evaluations, cooperative global initiatives, multinational consortia committed solely to biometric identity, standardization efforts, and expanding government and industry interest are all examples.

Airports and airlines are incorporating biometrics into boarding permits and frequent-flier cards in order to increase security and speed up the travel experience. Biometric data (often digital pictures and fingerprints) are increasingly included in most nations' passports and identity cards. Biometric technologies are anticipated to be used at every step of travel for all travelers in the near future. If this occurs, such systems must not only serve their stated security goals but also allow travelers to engage with them and find the user experience satisfactory.

Biometric systems' efficiency may be increased by fully integrating them with the enterprise's current management and IT infrastructure. This integration has a synergistic effect and a favorable impact on the company's key performance metrics, which all information technologies, including biometric ones, should serve. Iris scanning and fingerprint recognition are the most prevalent kinds of biometric security among the many biometric systems. Facial recognition and vein pattern (finger and palm) identification, on the other hand, is gaining popularity.

As observed in the first questionnaire, biometric technology has acquired people's confidence since it helps to maintain security and enhances sentiments of safety among individuals. The second questionnaire's results demonstrate the use of several biometric technologies in our regular security applications. It also provides substantial compression between the most commonly used methods and specifies each method on multiple scales. As a result, fingerprint, iris, and face recognition remain the most practical technologies to utilize in low-cost, high-efficiency, and security applications.

In the terms of the results of surveys, technology is always growing and may be found in practically every business today. Biometric solutions have made it possible to do away with traditional security cards and passwords. Because biometric systems are advantageous and secure, the number of applications for them is increasing by the day. That is why it is difficult to draw conclusions regarding biometric technology since it is constantly updated, especially when holes in its use are uncovered. These security systems, which are based on diagnostic-detection controls, are often used at door entrances and exits. As a result, the operational principles of all biometric systems are clearly identical. First, the biometric characteristic of the user is specified, encrypted, and stored in the database.

Summary in Hungarian Language – Magyar nyelvű összefoglaló

A kutatás célja a biometrikus rendszerek hatékonyságának vizsgálata fontos infrastruktúrákon és szerepüknek a kiberbiztonságban. A kritikus infrastruktúrák nagy szerepet játszanak a társadalom szükségleteinek kielégítésében, a távközlés, a légi közlekedés, az áramelosztás, az intelligens városi technológiák és így tovább. A magasan technológiás és digitalizált világban a kiberbiztonság létfontosságú az ilyen infrastruktúrák kiberfenyegetésekkel szembeni

védelméhez, még ha figyelembe vesszük is a technológia gyors fejlődését, a kiberbiztonságot a technológiai fejlődéssel azonos sebességgel kell naprakészen tartani. Dolgozatomban elsősorban a légi közlekedésre helyeztem a hangsúlyt, mivel kevés olyan munka található ebben a témában, amely nem frissült. Jó lenne emlékezni arra, hogy 2019-ben 4,5 milliárd utas utazott légi átszállással [1], bár ez a szám 2020-ban és 2021-ben meredeken csökkent a koronajárvány miatt, 2022-ben ismét növekedésnek indult, sőt, ez a szám a jövőben meg fogja haladni a 2019-es számokat.

A biometrikus adatokkal kapcsolatban elmondható, hogy a biometrikus technológia elsődleges célja, hogy következetesen és automatikusan megkülönböztesse a személyeket egy vagy több olyan fizikai vagy viselkedési jellemzőkből gyűjtött jel alapján, mint az arc, ujjlenyomat, írisz, hang, kéz, aláírás stb. Ezeket a jellemzőket biometrikus jellemzőknek is nevezik. Annak ellenére, hogy az automatizált személyazonosítást több mint négy évtizede vizsgálják [5], a biometria csak az elmúlt évtizedben alakult ki külön tudományos területként. A legutóbbi hivatkozások szerint konkrét konferenciák [3], közös benchmark eszközök és értékelések, kooperatív globális kezdeményezések, kizárólag a biometrikus identitás iránt elkötelezett multinacionális konzorciumok, szabványosítási erőfeszítések, valamint a kormányzat és az ipar bővülő érdeklődése mind példák.

A repülőterek és a légitársaságok biometrikus adatokat építenek be a beszállási engedélyekbe és törzsutas kártyákba a biztonság növelése és az utazási élmény felgyorsítása érdekében. A biometrikus adatok (gyakran digitális képek és ujjlenyomatok) a legtöbb országban egyre gyakrabban szerepelnek az útlevelekben és a személyi igazolványokban. A biometrikus technológiákat a közeljövőben várhatóan minden utazó utazása során alkalmazni fogják. Ha ez megtörténik, az ilyen rendszereknek nem csak a kitűzött biztonsági céljaikat kell szolgálniuk, hanem lehetővé kell tenniük az utazók számára, hogy kapcsolatba lépjenek velük, és kielégítőnek találják a felhasználói élményt.

A biometrikus rendszerek hatékonysága növelhető, ha teljes mértékben integrálják őket a vállalat jelenlegi irányítási és informatikai infrastruktúrájába. Ez az integráció szinergikus hatást fejt ki, és kedvezően hat a vállalat kulcsfontosságú teljesítménymutatóira, amelyeket minden információs technológiának, beleértve a biometrikusakat is, ki kell szolgálnia. Az írisz szkennelés és az ujjlenyomat-felismerés a biometrikus biztonság legelterjedtebb fajtája a sok biometrikus rendszer közül. Az arcfelismerés és a vénamintázat (ujj és tenyér) azonosítása viszont egyre népszerűbb.

Amint azt az első kérdőívben is megfigyeltük, a biometrikus technológia elnyerte az emberek bizalmát, mivel segít fenntartani a biztonságot, és fokozza az egyének biztonságérzetét. A második kérdőív eredményei számos biometrikus technológia használatát mutatják be szokásos biztonsági alkalmazásainkban. Ezenkívül jelentős tömörítést biztosít a leggyakrabban használt módszerek között, és mindegyik módszert több skálán határozza meg. Ennek eredményeként az ujjlenyomat-, írisz- és arcfelismerés továbbra is a legpraktikusabb technológia az alacsony költségű, nagy hatékonyságú és biztonsági alkalmazásokban.

A felmérések eredményei szerint a technológia folyamatosan növekszik, és ma gyakorlatilag minden vállalkozásban megtalálható. A biometrikus megoldások lehetővé tették a hagyományos biztonsági kártyák és jelszavak felszámolását. Mivel a biometrikus rendszerek előnyösek és biztonságosak, napról napra nő a rájuk vonatkozó alkalmazások száma. Éppen ezért nehéz következtetéseket levonni a biometrikus technológiáról, mivel folyamatosan frissítik, különösen akkor, ha a használatában lyukak derülnek ki. Ezeket a diagnosztikai-észlelő vezérléseken alapuló biztonsági rendszereket gyakran használják az ajtók be- és kijáratainál. Ennek eredményeként az összes biometrikus rendszer működési elve egyértelműen azonos. Először a felhasználó biometrikus jellemzőit adják meg, titkosítják és tárolják az adatbázisban.

1. Introduction

These and other issues frequently emerge in the area of biometric solutions for critical infrastructure. This dissertation examines the security and privacy provided by biometric technology in the context of critical infrastructures. Key infrastructures include airports, nuclear power plants, political institutions, the military-industrial base, main communications and transportation networks, and so forth. Paid shopping, transportation, energy, nuclear power, water, food-agriculture, chemistry, health, emergency services, reproduction-finance, governmental policies, industrial sector, services, and infrastructures all become increasingly important. Not only do we need to be recognized to cross a border, but also to make financial transactions and unlock our devices. To make biometric technologies a permanent component of the security industry, new methods of protecting templates and protecting people's privacy must be developed. This will enhance the technology's security and privacy.

Biometric data must be protected in order to avoid outside assaults that breach subjects' privacy rights and to maximize the benefits that these systems bring to subjects who have donated their information. Hashes [4], cryptographic methods, and fuzzy extractors have been used in biometric templates to achieve this purpose; nevertheless, doing so has resulted in a loss in verification accuracy in the great majority of cases.

Biometrically linked identities, such as using your face as a boarding pass, are one of the critical innovations that will help airlines and ports begin operations more successfully. This will also help to increase passenger confidence and identification verification in order to meet traditional security requirements while minimizing health risks. However, using biometric technology alone will only offer airports and airlines limited benefits. The benefits of integrating biometric technology with other technologies to promote identification integration, traveler automation, and self-service are amplified [5].

The effort necessary to be recognized as a certain individual by a biometric system without access to the proper biometric characteristic is referred to as security. The goal of a security breach is to fabricate identifying papers and maybe defraud security services based on their access control mechanisms. Security has both technical algorithmic and organizational components, which will be discussed below.

Personal information protection: the defined protection target refers to the effort required to obtain biometric data or derives it from the biometric system. An attacker who attempts to breach personal data jeopardizes the affected individual's privacy and hence personal rights and may possibly gain unlawful access. This notion includes simple learnability, efficient and intuitive usage, and the avoidance of errors when using. As a result, user-friendliness is a criterion that is orthogonal to, if not competing with, the two previous acceptance components. When examining a system's user-friendliness, the question of which potential users develop mental models - that is, what conceptions exist about the system's interaction and how these notions differ from real usage - occurs. Because biometric approaches are not yet widely employed, a time of acclimation is possible. Another general usability factor comes into play for IT security systems, which may be expressed as a cognitive burden. Minimizing this cognitive load while maintaining security is thus a crucial problem [6].

Mainly problems and gains through the thesis can be divided into regulatory problems and efficiency gains. The fundamental problem is the lack of global standards and equivalent laws in different regions. As a result, entry and exit will most likely continue to be handled manually for the foreseeable future. This mismatch shows that even passports bearing the ePassport logo are not accepted in all countries. Typically, permissions are only issued in specific countries. A specific resident status or registration with each country's border officials is frequently required. Following the flight, the frequent flyer travels to the lounge, where he or she knows and greets the traveler, while the other biometrically recorded passengers spend the time at the boarding gate. This obviously does not replace group or row-based boarding.

Experts refer to check-in, boarding, and other comparable touchpoints as touchpoints, and biometric approaches are meant to improve efficiency at all of these touchpoints. There is no need to seek identification at the check-in counter, the border may be crossed without stopping at the machines, and the manufacturers claim time savings upon boarding. Airlines and airports have the opportunity to save money. Many tourists only contact security personnel at the checkpoint. If you've ever tried to board a narrow-fuselage aircraft on a short-haul flight, you'll know that even with biometric boarding permits, you can't expect to save time because these planes are routinely overbooked, leading to lengthier boarding times [7].

2. Theoretical Framework and Antecedents of the Research

The use of biometric technologies to identify people crossing international borders has lately risen in airports and other international transit hubs. Using biometrics can substantially assist to eliminate impersonation among tourists and prevent unwanted persons from entering a certain country, hence preventing crimes and terrorist attacks. The major purpose is to reveal the entrance of criminals and terrorists across the border and to speed up the completion of operations inside the airport, resulting in satisfied travelers while saving time and money. The COVID-19 virus has taken a toll on all facets of our life, but the aviation and travel sectors have been particularly severely impacted, necessitating a comprehensive rethink to rebuild and restore passenger trust in safe and healthy air travel. As a result, biometrics in aviation systems have spread comfort and safety because they do not involve touching, merely scanning the face from a distance. Biometric technology transmits data via networks and clouds. It is also directly involved in IoT and clouds. As a result, cyberattacks on biometric databases are extremely risky and can occur at any time. A biometric system should be implemented in a secure environment to protect direct employees from cyber-attacks.

3. Objectives

The primary goals of this research are to investigate how biometrics and occupational safety work in airports, as well as to offer a complete description of what biometric applications exist in the aviation sector. review biometrics evaluation in airports, questionnaires must be applied Extend biometric research into cyber security assaults and their function in biometrics. revamp experimental processes outlining the significance of biometrics and the function of risk management evaluate the biometric efficiency data gathered in the experimental case study to discover a relationship between features determine how biometric applications contribute to workplace safety and security, and integrate airport efficiency, cost, and time variables.

4. The Research Investigation problem, Research Design, Hypotheses and Methodology

The research methods used in this work included the following components: a thorough review of the most recent scientific literature on topics like biometrics, aviation safety, security, biometric applications, and cyber security; preliminary research consisting of a questionnaire about how biometrics affect the aviation industry; the target was random passengers and employees who interact with biometric systems on a daily basis; preliminary research consisting of a questionnaire about the impact of biometrics on the aviation industry; and final research consisting of a questionnaire about the impact of bio The effectiveness of these systems as deployed and their financial costs. The use of biometric systems in the aviation sector is covered in the next chapter, along with detailed explanations of "risk management" and illustrative examples of how to use biometric technology in airports and other aviation-related settings.

In the thesis, I emphasized three hypotheses that the biometric system will gain significant ground with increased usage in the future, that installing a biometric system at airports will improve safety and security, and that when institutions install biometric systems, they do not always consider cost first but rather efficiency in usage.

5. The Biometric System in Aviation Industry

Biometrics is a technique for the automated identification of people that takes into account their behavioral and biological characteristics. The most popular biometric modalities are the face, fingerprints, hand geometry, iris, voice, signature, gait, and keystroke [8].

Detectable biological (anatomical and physiological) and behavioral traits are based on automated techniques of identifying an individual in a process known as "biometrics." People employed faces distinguishing between known (familiar) and unknown (unfamiliar) characters before the dawn of civilization. Given that each person's facial features are distinctive, one of the most often used techniques for identification is face recognition based on geometrical traits.

It is a means of giving one's confidence that they are working with people who are well-established and fall into a category with specific rights (or to a group denied certain threats). It relies on the individual's physical and behavioral traits, which vary. The Airport Council International (ACI) published a position paper titled "The Application of Biometrics at Airports" to encourage the development and implementation of biometric border control, passenger simplification, and access control systems because they believe it is crucial forairports to have a strong position on biometrics [9].

Those with a current government security clearance or who have been accepted into the Approved Traveler Program are considered low-risk travelers. High-risk passengers lack a paper trail, and so little is known that it is advisable to assume the worst and conduct a thorough screening of both the individual and the luggage [10]. Ordinary tourists fall somewhat in between the other two risk groups.

This approach would aid in improving security surveillance in terminal lobby areas and outside the airport, as well as in ramp areas and around the airport. Each category will require a unique strategy for both the screening of travelers and the screening of luggage. There are several known biometric modalities, such as (face, hand geometry, iris, voice, etc.), - see below Figure 1 It is important to note that no biometric modality is suitable for all implementations because there are several factors to consider during the modality’s selection and biometric tools, such as security risk, location, number of users, and available data. Furthermore, it is important to remember that biometric modalities vary as the system matures [20].

However, not all biometric modalities are consistent. Physiological measures are often seen to have the advantage of keeping more stable throughout a person’s life. Stress can impair behavior-based identification, but not physical feature assessment.

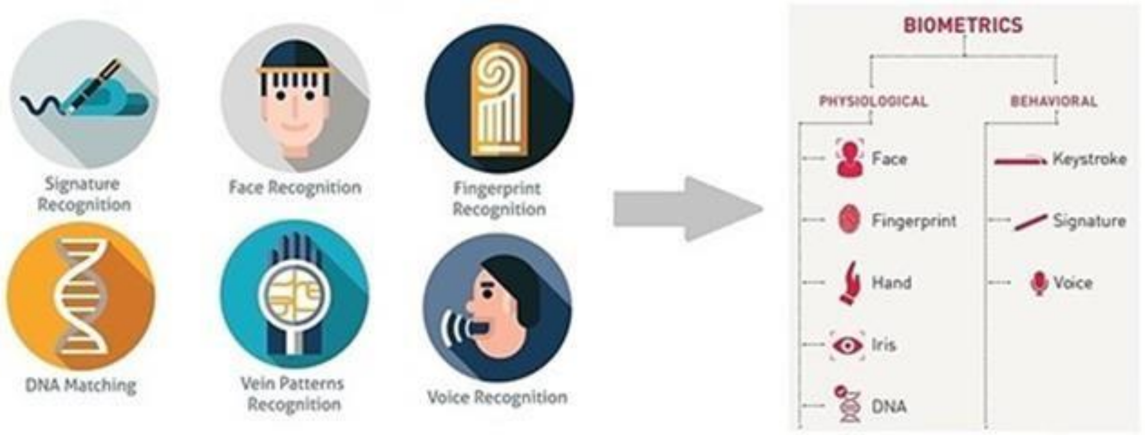

Figure 1. Biometric modalities [24]

The notion of a biometric system is characterized by a series of measures inside a system as a multi-step process; in other words, everyone displays numerous characteristics of oneself or herself; this aspect is then captured by a sensor and translated into an algorithm model. The registered model is then compared to the reference sample or baseline algorithms that have been recorded in the system database. The outcome of comparison dictates the next relevant reaction such as admittance into a secure facility [21].

The notion of a biometric system is described by a sequence of measures within a system as a multi-step process; in other words, everyone displays numerous characteristics of oneself or herself; this aspect is then captured by a sensor and translated into an algorithm model. The registered model is then compared to the reference sample or baseline algorithms contained in the system database [22]. The outcome of comparison dictates the next relevant reaction such as admittance into a secure facility. Figure 2 depicts a schematic diagram for a basic biometric system. A sensor that generates data in the form of signals like an electromagnetic spectrum is the primary part of a biometric system. In the second section, biometric data processing methods use a variety of filtering, transforming, and pattern recognition algorithms. Therefore, many stages of the utilization of biometric data include the usage of decision-making systems. The hardware platform for using these approaches makes up the third element. Typically, the hardware platform for biometric devices and systems consists of a number of CPUs [23].

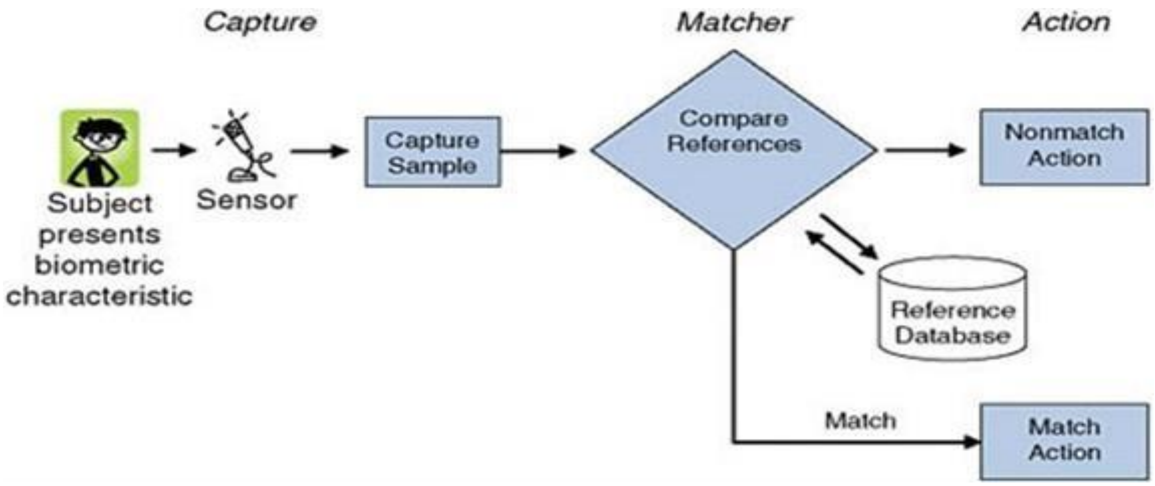

Figure 2. Schematic diagram for basic biometric system [26]

A biometric system, however, does not save biometric information since incomplete or unprocessed biometric information cannot be utilized to conduct biometric competitions. Enrollment is the process through which the user's biometric information is initially collected, examined, dealt with, and recorded in the form of a prototype [11]. The three-step strategies for identification are data collecting, methodologies, and computing platform. Implementing application-specific methodologies (methods, algorithms, and programs) on a computing platform results in the creation of a biometric system [24].

In conclusion, the method of identifying oneself using one's behavior, anatomy, physiology (such as fingerprint or iris), or even speech patterns, is known as biometric authentication [12], One's biometric picture must be taken, encrypted, and saved in order to be used in the future [13]. Research indicates that 52% of biometric systems worldwide use fingerprints [14]. The precision of fingerprint photographs is what has made fingerprint biometrics so popular [15]. The biometric authentication technique has an advantage over other approaches in that it necessitates the presence of real use in order for the verification process to occur [16].

6. Cybersecurity

A new level of danger is introduced by new technology. Smart grid security is a challenge. The AMI network provides access to functions that regulate the whole grid, which might compromise the setup's security or data availability if an unauthorized individual were to get access. Human safety and the confidentiality of customer data may be seriously jeopardized by this. Therefore, it is crucial for this technology to safeguard the system and reduce the danger of cyberattacks [17]. Biometric systems are vulnerable to attacks if suitable inspection methods are not employed to confirm them during the development phase. regulated entry and exit, authorization, and controlled access to these systems are some examples. Given that the systems are used in crucial industries, it is generally recognized that attackers have a very strong motivation to compromise them [25]. Biometric data, which is used in these systems and is specific to each user, presents issues since, unlike knowledge-based encryption techniques, it cannot be easily changed. In order to evaluate the reliability of the biometric system, it is crucial to safeguard its accessibility, integrity, and privacy [26].

A typical security study should be performed on the component design and system integration of a biometric system, taking into consideration threat models and scenarios where potential security problems might arise. A threat model that is suitable for the system's components should be built by looking at the intended application, environment, and users of the biometric system. Before designing such a system, it is essential to evaluate the tools attackers can use, past attack trends, and probable scenarios. 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 disturbs the peace. Although the definition varies from nation to nation, it is generally agreed that critical infrastructure is the infrastructure that, when compromised in terms of accessibility, confidentiality, or structure, poses a risk to human life, and significant economic harm [27]. We may point to the transportation and energy industries as examples of essential infrastructures. Infrastructures for the food industry, space exploration, and nuclear and chemical research are all seen to be crucial components of a nation's infrastructure.

In terms of the power grid, the conventional grid power is transformed into a smart power grid based on two-way digital communication, which supports a lot of other technology like intelligent monitoring and measurement, which offer more effective power management and increase the reliance on renewable energy. It is difficult to protect all components and communication lines from cyberattacks or unforeseen breakdowns since the complex system has several flaws in communication technologies, software, and equipment that operate in a smart power grid [18]. As a result, the smart power grid generates a new class of challenges, some of which we are unable to fully understand, and which require further study, analysis of the circumstances, and identification of possible weak points before being resolved. Figure 3 shows the typical smart grid communication network design. It is clear how each portion of the power grid is physically isolated from the others, allowing for a more secure connection [19].

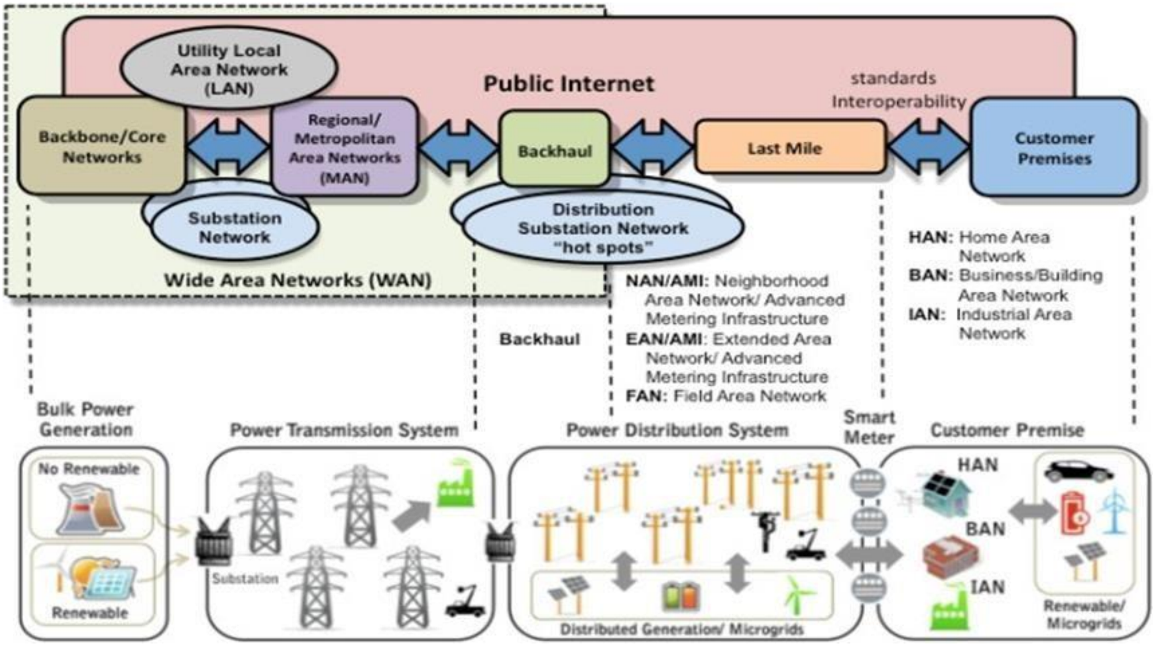
Utility Local Area Network (LAN)
Public Internet
standards
Interoperability
Backbone/Core Networks
Regional/ Metropolitan Area Networks (MAN)
Backhaul
Last Mile
Customer Premises
Substation Network
Distribution Substation Network "hot spots"
Wide Area Networks (WAN)
NAN/AMI: Neighborhood Area Network/ Advanced Metering Infrastructure
EAN/AMI: Extended Area Network/ Advanced Metering Infrastructure
FAN: Field Area Network
HAN: Home Area Network
BAN: Business/Building Area Network
IAN: Industrial Area Network
Backhaul
Bulk Power Generation
No Renewable
Renewable
Power Transmission System
Substation
Power Distribution System
Distributed Generation/ Microgrids
Smart Meter
Customer Premise
HAN
BAN
IAN
Renewable/ Microgrids

Figure 3. The communication network on the smart grid [134]

7. Research Procedure

I made two questionnaires for my research. Male participants made up 79% of the total number of participants in this survey, despite being the bigger number of participants overall. In contrast, female individuals make up only 5% of the total participant population. The participants' ages span from under 25 to over 35; the most significant age category, which makes up around 60% of the total participants, is between 25 and 35 years old. 74.2 percent of the participants have a diploma, and they are from eight various countries.

Based on the result of the first questionnaire, the majority of participants are young, under 35, giving them the opportunity to see more advancement and growth in the use of biometric systems. As a result, the participants appeared to be more supportive of increasing the use of this technology in their organizations and demonstrated their confidence in its ability to increase safety, particularly at important locations like airports. The participants' understanding of biometric systems is insufficient, though. Many participants are accustomed to utilizing biometric systems, especially for ID verification; the majority have done so for more than five years. The fingerprint biometric system is the one that participants use the most frequently, which is to be anticipated given that it is less expensive than other biometric systems. Additionally, using fingerprint recognition is simple. These factors encouraged several enterprises to embrace this technology. Iris recognition, on the other hand, is a common technology used to confirm a person's ID. The below Figure 4 shows us that fingerprint scan so far is the most popular biometric system installed. This is because of the easy-to-use and economic cost of the system.

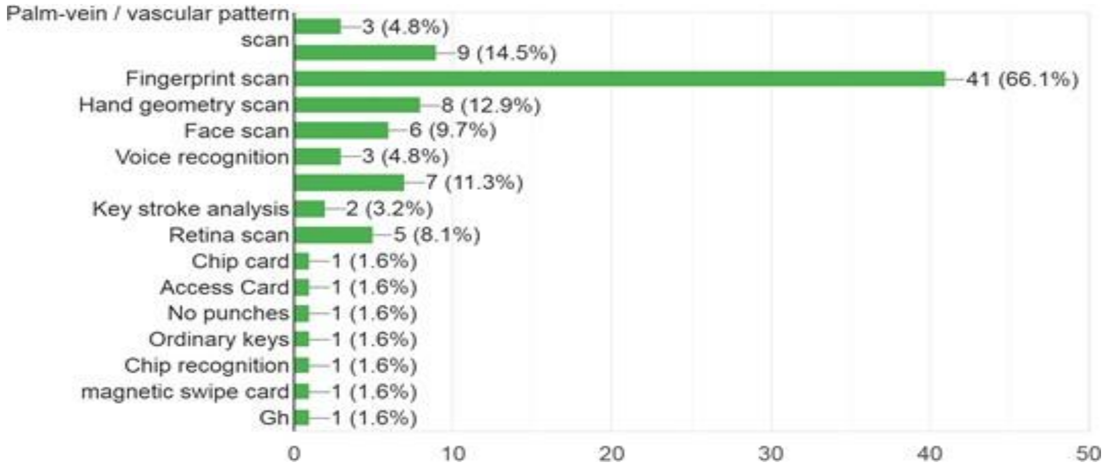

Figure 4. Type of the biometric system installed

High levels of security are provided through iris scanning, albeit at a cost. The system is regarded as being sluggish. The technology, however, was created in a way that allows it to read an individual's iris from a close distance. In many businesses, workplaces, and other institutions today, biometric technologies are employed for a variety of functions. Figure 5 shows that the biometric is mostly used to determine a worker's attendance time and/or to track check-in and check-out.

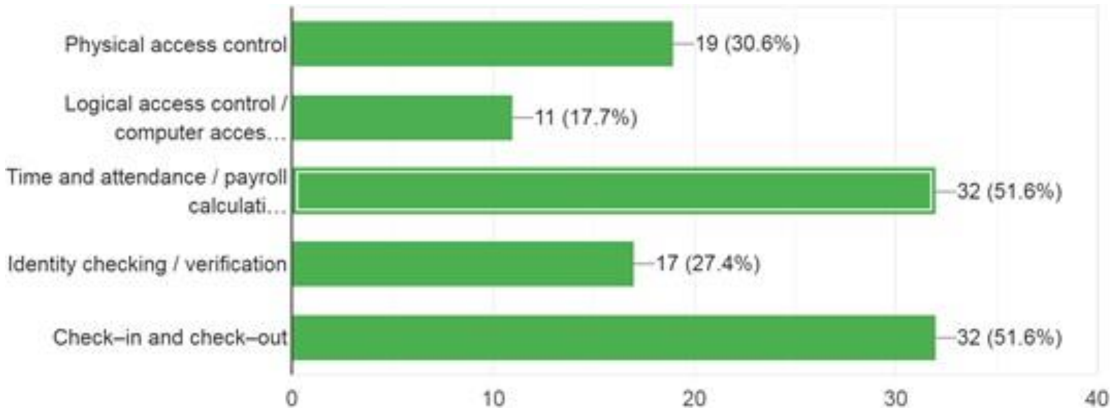

Figure 5. The purpose of the installed biometric system

The second questionnaire's objective is to gather data regarding the biometric technology used in several airports across the world. The effectiveness of these systems as deployed and their financial costs. Close-ended questions are included in this self-administrated survey. This survey was created with Google Forms. Since there were no adaptable, comparable surveys in the area, a unique survey was created using the literature study as a guide to be answering the research questions. A statistician assessed the survey after receiving all the required responses to make sure the poll's questions would gather the data required to address the research topics. The survey was completed by seventy participants. The below mentioned Table 1 describes the security of the most famous biometric technologies based on the second questionnaire.

It is clear that among the other ways, the fingerprint method is the most popular. The iris method is next, followed by face recognition. It has been observed that the top three techniques are also the most sophisticated in terms of the biometric system. Security and technique effectiveness are the two important elements, and solutions to both aspects have a very good track record. In other words, the most reliable methods in the aviation sector continue to be fingerprint, iris and face recognition. However, I enquired as to what was anticipated for each biometric technique in the future and if it needed to be implemented, expanded upon, or entirely replaced. Many participants believe that new technology, particularly in the area of aviation, may develop or replace existing facial and fingerprint identification systems. The results show that Iris has a higher favorable impression in terms of execution. Also available are systems that use fingerprint

Table 1: The security of the used system

The name of the used biometric system	Security	Responses	Totals
Gate	High	5	1
Facial Recognition	High	3	1
		4	2
		5	3
	Moderate	3	2
		4	2
		5	1
Fingerprint	High	2	2
		3	2
		4	4
		5	13
	Moderate	2	2
		3	1
		4	3
		5	5
	Poor	1	1
Iris Recognition	High	3	2
		4	1
		5	6
	Moderate	3	1
		4	2
		5	1
Keystroke dynamics	High	1	1
		4	2
Retina Scan	High	5	1
	Moderate	2	1
Voice Recognition	High	3	1
		5	1
digital signatures	High	4	2
	Moderate	3	1
		4	1
	Poor	1	1

Totals responses	70

and face recognition that are cost-effective. Despite the iris' excellent efficiency and accuracy, it is reported to have a moderate to medium cost. A participant with experience in keystroke dynamics concurred that the cost has not been prohibitive and that it has been appropriate economically. Additionally, one of the key factors of biometric tools is their future development just like in all technological gadgets as the technology is improving so fast. The development way of hacking these technologies has the same path as technological advancement so biometric tools have to be improved more since they are used for security in critical infrastructure. The below Table 2 describes what is the most widely used biometric technologies' future anticipation.

Table 2: The used biometric system and future expectation

The name 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 replace 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
Totals responses		70

This research looked into one of the digital authentication procedures that became essential as a result of the digitization of many paper-based transactions: biometric security measures. Although biometric security systems, which can be defined as a person carrying their password on them, have just lately begun to be used in real-life situations, they are growing more common by the day. Systems that use behavioral attributes such as signature shots and walking movements, as well as fixed physical features such as fingerprints, iris, and faces, are becoming increasingly widespread. The paper focuses on biometric systems and the most widely used biometric technologies. The advantages and disadvantages of these technologies are examined, as well as some suggestions for alleviating their disadvantages.

Technology is always growing and may be found in practically every business today. Biometric solutions have made it possible to do away with traditional security cards and passwords. Because biometric systems are advantageous and secure, the number of applications for them is increasing by the day. That is why it is difficult to draw conclusions regarding biometric technology since it is constantly updated, especially when holes in its use are uncovered. These security systems, which are based on diagnostic-detection controls, are often used at door entrances and exits. As a result, the operational principles of all biometric systems are clearly identical. First, the biometric characteristic of the user is specified, encrypted, and stored in the database.

8. Contribution and Achievements of the Study

Assuming that biometrics can reliably be used for automated identity verification. Without doing extensive security and effectiveness studies beforehand, the aviation industry is reticent to implement any biometric-based technology. The suggested research examined the value of biometric systems, including user satisfaction, and advised the adoption of brand-new and generic biometric components for risk management and cyber-security. The findings of similar studies and the literature they referenced served as the main inspiration for this work. I've concluded from my examination of the surveys used to gather data for this dissertation that better communication between end users and the engineers designing biometric systems is necessary.

Three components make up this study, and they all advance our understanding of science. The theoretical framework, which has helped to focus the research and advance knowledge about biometrics and their application in aviation, as well as define the idea of the smart city and biometrics' place in it, is the first thing I can highlight. It also revealed the significance of cyber security. This theoretical framework includes a thorough assessment of pertinent scientific literature to comprehend biometric technology and its use in aviation.

The second is an experimental technique that was used to alter or test hypotheses. In the initial questionnaire, users were asked about their individual experiences using the airport's biometric technology and how those experiences may be characterized. This survey assisted in examining the client's background and level of familiarity with the biometric system in order to select the system that the customer liked. Employees working at airports in many different nations answered the second questionnaire, which collected data on the biometric systems used at airports. This survey sheds light on the effectiveness and financial burden of these tried-and-true approaches.

Finally, the statistical analyses done on the obtained data set mentioned in the Experimental Procedures section are detailed in order to confirm or reject the hypotheses given in the first part in order to evaluate the results. As a consequence, the proposed hypotheses were accepted based on the theoretical framework and statistical analysis results. Hypotheses have demonstrated that the adoption of biometric technologies in aviation not only improves airport security but is also a customer-friendly solution. Furthermore, the study demonstrates that the economic cost of this technology for installation and maintenance is often not expensive. As a result, biometric technologies are rapidly being employed throughout the world and in a variety of industries.

9. Conclusion

In the many industries and settings in which we work and live today, the need for security is something that concerns us all. 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 and 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 [28]. In order to increase security or simplify the flying experience, airport operators and airlines are incorporating biometrics into boarding permits or frequent traveler cards. 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.

Contrarily, the biometric technologies and information systems that they utilize have already attained a degree of effectiveness that enables widespread usage and the resolution of a wide range of commercial issues. It is advisable to employ biometric systems while interacting with clients and guests as well as in the back office of the business (managing information system user rights, keeping track of working hours, and access control) [29].

To improve people's comprehension of this technology in a way that can increase its popularity, as people's knowledge of it is insufficient, is one item that should be prioritized. Although the field of biometric security is expanding, it is by no means a new one, and most players are already familiar with it.

References

[1] https://www.icao.int/Pages/default.aspx (International Civil Aviation Organization`s official website).

[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. Konga, K. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of bio hashing and its variants. pattern recognition," 2006

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

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

[7] 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

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

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

[10] 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.

[11] 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.

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

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

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

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

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

[17] 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.

[18] 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.

[19] “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.

Author`s Publications

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

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

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

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

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

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

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

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

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

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