

4-2018

Airport Passenger Processing Technology: A Biometric Airport Journey

Vishra Patel

Follow this and additional works at: <https://commons.erau.edu/edt>



Part of the [Aviation Safety and Security Commons](#), and the [Management and Operations Commons](#)

Scholarly Commons Citation

Patel, Vishra, "Airport Passenger Processing Technology: A Biometric Airport Journey" (2018).
Dissertations and Theses. 385.
<https://commons.erau.edu/edt/385>

This Thesis - Open Access is brought to you for free and open access by Scholarly Commons. It has been accepted for inclusion in Dissertations and Theses by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

**AIRPORT PASSENGER PROCESSING TECHNOLOGY:
A BIOMETRIC AIRPORT JOURNEY**

by

Vishra Patel

A thesis submitted in partial fulfillment of the requirements for the degree of
Master of Science in Cybersecurity Engineering
at Embry-Riddle Aeronautical University

Department of Electrical, Computer, Software, and Systems Engineering

Embry-Riddle Aeronautical University

Daytona Beach, Florida

April 2018

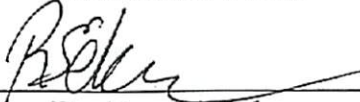
AIRPORT PASSENGER PROCESSING TECHNOLOGY: A BIOMETRIC AIRPORT JOURNEY

by Vishra Patel

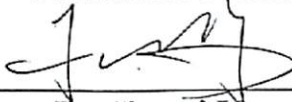
This thesis is prepared under the direction of the candidate's committee chair, Dr. Radu F. Babiceanu, Department of Electrical, Computer, Software, and Systems Engineering, and has been approved by the members of her thesis committee. It is submitted to the Department of Electrical, Computer, Software, and Systems Engineering in partial fulfillment of the requirements for the degree of Master of Science in Cybersecurity Engineering.



Dr. Radu F. Babiceanu
Committee Chair



Dr. Remzi Seker
Committee Member



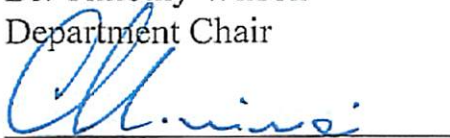
Dr. Jiawei Yuan
Committee Member



Dr. Timothy Wilson
Department Chair

2018-04-03

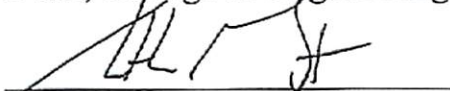
Date



Dr. Maj Mirmirani
Dean, College of Engineering

04/04/18

Date



Dr. Christopher Grant
Vice Chancellor

4/3/18

Date

Acknowledgments

I would like to extend my gratitude to Dr. Radu F. Babiceanu for supporting my research. Dr. Babiceanu worked actively to provide me with his guidance, without which it would have impossible to accomplish the end task. I am immensely grateful to Rebecca Selzar for providing unending inspiration and encouraging me to pursue this thesis. I am also thankful to my thesis committee members Dr. Remzi Seker and Dr. Jiawei Yuan for their support. In addition, I am grateful for Dr. Seker's continuous support and instrumental advising during my time as Master of Science in Cybersecurity Engineering student.

The simulation models included in this thesis were built using the Simio simulation software. Therefore, I would like to thank Simio for making my research a success. Embry-Riddle Aeronautical University uses Simio simulation software under a grant from [Simio LLC \(https://www.simio.com\)](https://www.simio.com).

Lastly, I would like to pay special thankfulness, warmth and appreciation to Ahrash Aleshi for assisting me at every point of my goal and motivating me throughout this endeavor.

Table of Contents

Abstract	1
Chapter 1	2
Introduction.....	2
Chapter 2.....	5
Problem Statement	5
2.1 Background	5
2.2 State of the Art	6
Chapter 3.....	8
Methodology.....	8
3.1 Single Token Passenger Processing Technologies.....	8
3.2 Biometrics	10
3.1.1 Facial Recognition.....	12
3.1.2 Fingerprint Recognition.....	14
3.1.3 Iris Recognition	16
3.1.4 Evolving Biometric Technologies	17
3.2 Importance of Biometrics.....	18
Chapter 4.....	21
Proof of Concepts for Biometric.....	21
4.1 Department of Homeland Security.....	21
4.2 TSA Pre✓	23
4.3 Customs and Border Protection.....	25
4.4 Global Entry	27
4.5 NEXUS.....	28
4.6 Secure Electronic Network for Travelers Rapid Inspection (SENTRI).....	29
4.7 Mobile Passport.....	29
4.8 Clear Me	30
4.9 Automated Passport Control Kiosk.....	31
4.10 SmartGate.....	32
4.11 miSense	33

4.12 IATA One ID Task Force.....	34
4.13 IATA Fast Travel Program	35
4.14 Vision Box Happy Flow Aruba.....	35
Chapter 5.....	37
Barriers to Biometrics	37
5.1 Biometrics Can Be Stolen	38
5.2 Security Issues of Biometrics	40
5.3 Lack of Revocability	41
Chapter 6.....	42
Standards on Using Biometrics at Airports	42
6.1 Mobile Applications	45
Chapter 7.....	47
Concept of Operations	47
7.1 Airport Passenger Flow Simulation Models	47
7.2 Medium-Sized International Airport Model.....	48
7.3 Current Model Approach.....	51
7.4 Proposed Model Approach.....	54
7.5 Distribution of Passengers.....	56
7.5.1 Annual Passenger Traffic	56
7.5.2 Wait Time for International Arrivals	57
7.5.3 Passenger Traffic and TSA Wait Time	58
7.5.4 Passenger Booking and Checking	59
7.5.5 Security Checkpoint	60
Chapter 8.....	62
Analysis, Results and Frequently Asked Questions	62
8.1 Simulation General Description	62
8.2 Simulation Results.....	67
8.3 Frequently Asked Questions	69
References.....	75

List of Tables

Table 3.1: Biometric Characteristics.....	11
Table 4.1: DHS Trusted Traveler Programs with Biometric Identity Services	22
Table 5.1: Potential Attacks on Biometrics	40
Table 7.1: Airport Terminal Details.....	50
Table 7.2: Airport Annual Passenger Traffic.....	57
Table 7.3: Wait Time for International Arrivals.....	58
Table 7.4: Airport Passenger Traffic	59
Table 7.5: TSA Security Wait Time	59
Table 7.6: Passenger Booking and Checking-in Method Calculations	60
Table 8.1: Scaled-down Airport Annual Passenger Traffic.....	67
Table 8.2: Sample Security Processing and Boarding Simulation Results	68

List of Figures

Figure 3.1: Biometric Airport Journey.....	10
Figure 4.1: TSA Risk Category	24
Figure 4.2: TSA Pre✓ vs Standard Screening	24
Figure 4.3: Mobile Passport Process.....	30
Figure 4.4: Automated Passport Control Process	31
Figure 4.5: SmartGate Process	32
Figure 7.1: Airport Statistics.....	49
Figure 7.2: Airport Terminal Layout	50
Figure 7.3: Airport Passenger Flow	53
Figure 7.4: Passenger Survey Results.....	56
Figure 7.5: Passenger Booking and Checking Statistics.....	60
Figure 8.1: Airport Simulation.....	64
Figure 8.2: Airport Simulation with Token ID	65

Abstract

A passengers' traveling journey throughout the airport is anything but simple. A passenger goes through numerous hoops and hurdles before safely boarding the aircraft. Many airports today are implementing isolated solutions for passenger processing. Some of these technologies include automated self-service kiosks and bag tag, self-service bag drop-off, along with automated self-service gates for boarding and border control. These solutions can be integrated with biometric systems to enhance passenger handling. This thesis analyzes the current passenger processing technology implemented at airports around the world and their associated challenges that passengers face. A new passenger processing technology called a biometric single token identification (ID) is presented as a solution to help alleviate current issues. By using a medium-sized international airport as a case study, the results show that a single token ID is beneficial to the time it takes to process a passenger. Furthermore, it demonstrates that implementation of a single token ID with self-service technology can provide enhanced passenger travel experience, improving operational process efficiency, all while ensuring safety and security.

Chapter 1

Introduction

Passenger processing technologies have a great impact on a passengers' experience as they transit through an airport. Passengers go through a cumbersome process of planning and scheduling, check-in steps, baggage management, and security clearance, which, many times, reduces the overall level of satisfaction of the air travelers.

Current technologies such as self-service kiosk check-ins, kiosk bag tagging, airport mobile apps, self-boarding gates, and baggage tracking, all now play an integral part in modern day air travel. While the current technology is well established, it is not necessarily interoperable, reducing the efficiency of moving passengers fast and reliable through their airport journey. Airports across the country are prioritizing the introduction of newer technologies differently, achieving various results with each implementation.

With various checkpoints and security measures to put in place, efficient passenger processing has proven, many times, difficult to achieve. Biometrics can be combined with these current self-service technologies to help meet the challenges of sustaining security while efficiently and quickly processing an increasing number of travelers.

This thesis outlines a new approach for airport passenger processing that integrates biometrics technologies within current airport processes. By using a single token ID linked to biometrics, passenger processing at airports can be expedited. The single token ID works as such. Once a customer books a flight, they are issued a biometric single token ID. Token ID allows passengers to complete the check-in, bag drop, security,

outbound immigration and boarding processes using facial recognition technology, instead of having to present their passport and boarding pass at every checkpoint. The biometric token then serves as their passport.

To evaluate the expected performance of the biometrics single token ID, a model of a medium-sized airport was built and analyzed using the Simio simulation environment. The focus of the simulation study was to model the processes within the medium-sized airport, running the simulation, and get insight out of the reported results. The goal of the entire study was to assess the expected time reduction for passenger processing through the airport, from entering the airport to boarding their flights. Implementation of the single token ID could enhance the travel experience by reducing passenger-processing time, making the journey smoother, less complicated while maintaining security.

Following the tragic events of September 11, 2001, air transportation industry has been widely impacted. After that event, the highest level of security measures was implemented. Airport developments have been centered on increasing security, with less attention made to how the security updates impact customer experience. This thesis entertains the discussion of a seamless airport experience, while maintaining a high level of security guaranteed by the biometrics single token ID.

In response to rapid and radical changes, Chapter 1 explains how passengers undergo an extensive process before arriving at their destinations and suggests that airports must constantly adapt and foresee changes for a positive customer experience. Chapter 2 explains how Passenger Processing Technologies influence a passenger journeys

throughout the airport and emphasize the needed integration of new technologies for a fluid customer experience.

Chapter 3 provides a comprehensive overview of single token ID and biometrics. The chapter suggests that the integration of a biometric single token ID into existing technologies could be the new fast, safe, and secure solution the aviation industry is looking for. Chapter 4 is dedicated to theoretically discussing the way biometric authentication technology has positively influenced various existing Trusted Traveler Programs, common use terminal equipment, and common use self-service. The following fifth chapter in the thesis acknowledges that biometrics have barriers and outlines the defenses for those barriers, while the subsequent Chapter 6 reviews the existing industry standards on biometrics.

Chapter 7 analyzes a medium sized airport's passenger processing flow. A simulation model is built to represent the current passenger flow at the airport. The existing flow is then compared to the proposed model where biometric token ID solution are employed into existing self-service technologies. Chapter 8 presents the results from the simulation study in terms of expected improvement for airport passenger-processing experience. The proposed model shows that integration of a biometric single token ID into existing technologies can seamlessly streamline passenger experience, by improving process speed and convenience, all while improving safety and security.

Chapter 2

Problem Statement

2.1 Background

One hundred and fifteen years ago, in 1903, the Wright brothers designed, built, and flew their first successful airplane. At that time, the global population was 1.6 billion. Today, the world population is seven times that of 1903. With potential 7.6 billion travelers, there has been a tremendous increase in the number of international travelers, as well as the number of airports. Before the tragic events of September 11, 2001, the term “airport/aviation security” was not taken as serious as it is today. After September 11, the national security efforts for air transportation changed forever. Shortly after the tragic events occurred, the aviation industry had to adopt new security measures to keep passengers safe. The United States President at that time, George W. Bush, made available twenty billion dollars for the strengthening of intelligence and implementing tough new security efforts throughout the air transportation industry (Department of State, 2009).

The intelligence and security investment involved the hiring of Transportation Security Administration (TSA) personnel, along with air marshals and K-9 dogs. The new TSA requirements include conducting criminal background checks on travelers, fingerprinting them, and scanning their full body to authenticate the passengers, in hopes of preventing terrorist attacks (McCamey, 2011). Also, the TSA security requirements on baggage

checks were enhanced by X-ray machines and hand inspections, along with stricter carrier rules and list of items allowed on board.

The ability to strike a balance between the growing security needs and the increasing travel demand is bound to create problems moving forward, especially if the current processes are still going to be in practice without additional security measures such as biometric technologies. Security hitches are some of the issues that have been associated with airports and the air transportation industry all over the world. The existing methods of security in airports have a long history of security flaws that range from authenticating, authorizing, personification, illegal ticketing procedure, carrying of illegal goods such as animal parts (e.g. ivory and rhino horns), drugs, firearms, and explosives.

There are also cases where illegal immigrants and/or criminals cross the border with the help of rogue employees who authorize fake stamps and/or visas. In some other instances, it takes the collaboration of the airport staff to facilitate the occurrence of these security mishaps. The existing manual security systems tend to be quite strenuous, challenging, and time-consuming. There are many limitations related to manual security systems, therefore stringent airport security systems need to be adopted. Introducing biometrics technology at airports can enhance passenger and airport security, speed up passenger flow, and promote best practices.

2.2 State of the Art

These days, a passenger's traveling journey is anything but simple, even if using the more self-service-oriented processes. The entire journey is often categorized in four stages:

pre-travel, check-in, baggage management, and security check. Below is the list of actions that a customer must perform to reach their final destination.

- **Pre-travel stage:** search for optimal flight, confirm the ticket, pack luggage, optional online check-in (within 24 hours prior to departure), and travel to the airport.
- **Check-in at the airport:** arrive two hours before the flight for domestic or three hours before the flight for international flight, way finding at the airport, self-service passenger check-in kiosk, and document scanning and verification.
- **Baggage management stage:** self-serve luggage-tagging kiosk and drop off check-in luggage.
- **Security check stage:** immigration exit control, security access, security screening, finding boarding gate, scan the boarding pass, and board the flight.

The process described above can take an average between 1.5 to 3 hours. Ultimately, due to the cumbersome visa processes, long queues as well as overreliance on paper documents makes traveling unfriendly (Sorenson, 2018). Airports around the world need to design an innovative technology to enhance passengers' journeys. Sorenson believes a paradigm shift in how a passenger travels will be made possible by using biometrics at the airports. Also, efficiency in the airports will enable a reimagined air travel-- offering an incredible seamless and hassle-free experience all around the world (Sorenson, 2018). To create a state of the art passenger processing technology, development of a new process occurred in the next section showing the techniques and methodologies used.

Chapter 3

Methodology

3.1 Single Token Passenger Processing Technologies

A key advantage of the new technology is the ability to use and integrate with existing airport infrastructure – including industry standard Common Use Self-Service (CUSS) equipment and Common Use Terminal Equipment (CUTE) (SITA, 2018). By merging key steps of the passenger processing journey, as described in current passenger processing technologies section, with biometric technology, every passenger touchpoint will be expedited and secure (SITA, 2018).

Companies always look towards emerging technologies that have the impact to change the industry. Blockchain technologies are a hot topic now because of their ability to enhance digital security and data privacy (Back, 2017). The blockchain infrastructure is best referenced with Bitcoin, the well-known virtual currency. The blockchain first started with Bitcoin but has since expanded into multiple companies with various use cases. There are multiple types of blockchains, but enterprises are looking towards a ledger-based system. The datatype being stored in these enterprise blockchains can include anything ranging from customer names to full transaction records. Blockchains are based on a Merkle Hash Tree which make the data secure with hashing algorithms such as SHA-256. If data is stored on the record, it can be protected with further encryption and hashing to enhance integrity of the information. The blockchain is a

highly distributed database ledger with thousands of copies of the ledger throughout the world. The hashing algorithm used to connect the blocks of data together, creating the chain, are virtually impossible to break (Bauerle, 2017) (Back, 2017).

A majority of emerging technologies use blockchain to enhance digital identity and data privacy responsibilities (Back, 2018). By applying blockchain technology at an airport, it can authenticate travelers by creating a single token ID based on biometrics. An airport can integrate six various biometric technologies for a fluid customer experience as shown in Figure 1. Once a customer books a flight, they are issued a biometric token ID. Once the passenger arrives at the airport using biometric self-check-in kiosk or online check-in, the passenger authenticates themselves with proper Single Token ID (SITA, 2018).

Doing so on the kiosk will cut down on increasing wait time and give passengers multiple check-in options.

The token ID is issued by capturing the passenger biometric details through a facial scan and finger printing. “Passengers have their photo taken, their face is checked against the image held in the biometric chip of their e-passport, or against an airline’s passenger manifest, and they move on through the airport without the need for a manual identity check” (Silk, 2017). Also, “a biometric token serves as a passport, boarding pass, and ID for the journey” (Thornhill, 2016).

“The key to single token travel is gathering and verifying data as early in the process as possible, in order to establish a robust token. This includes both biometric and biographic information. And then, if necessary, update it with more detailed information at various steps in the journey” (SITA, 2018). Token ID will allow passengers to complete the

check-in, bag drop, security, outbound immigration and boarding processes using facial recognition technology, instead of having to present their passport and boarding pass at every checkpoint (SITA, 2018) (Thornhill, 2016).



Figure 3.1: Biometric Airport Journey (SITA, 2018)

Once a passenger has checked-in with biometric ID, then on the same kiosk the passenger can weigh their bags and tag their own luggage. Once tagging is completed, passengers can easily drop off the bags at an automated bag drop area without having to show passport or boarding pass.

The passenger can then, proceed through security where they can scan their fingerprints for program such as TSA Pre✓®[®], without additional searches (TSA, 2018). The passenger then passes through Automated Border Control (ABC) Gates and at last, the customer gets to board the aircraft with Airport Self-Service Gates using their biometrics. With the single token, passengers will have a smooth time processing throughout the airport.

3.2 Biometrics

Biometrics is a general technical term used for body measurements. Bio refers to life while metric means to measure. Computer science identifies and characterizes biometrics

as a mode of human identification. Biometrics are a digital analysis of biological characteristics captured using a camera or scanner. Biometrics provide a more secure and convenient way for personal authentication. There are two types of biometrics: physical and behavioral. Physical biometrics include iris, fingerprints, hand, retinal, face recognition, and DNA, while behavioral biometrics include gait, voice, keystroke, and signature (BioMetrica, 2018) (Agrawal, 2017). Successful application of biometrics relies on the combination of two or more of these approaches to obtain a considerably strong security system. For passengers, highly applied biometrics processing technology includes facial, iris and finger print recognition. Its characteristics and features are listed in Table 3.1 (Al-Raisi, 2006) (Thakkar, 2016).

Table 3.1: Biometric Characteristics (Al-Raisi, 2006) (Thakkar, 2016)

<i>Characteristics</i>	<i>Facial</i>	<i>Fingerprint</i>	<i>Iris</i>
<i>How it works</i>	Captures and compares facial patterns	Captures and compares fingertip patterns	Captures and compares iris patterns
<i>Cost of device</i>	Moderate	Low	High
<i>Enrollment time</i>	3 min	3 min, 30 secs	2 min, 15 secs
<i>Transaction time</i>	10 secs	9-19 sec	12 secs
<i>False nonmatch rate</i>	3.3-70%	0.2-36%	1.9-6%
<i>False match rate</i>	0.3-5%	0-8%	Less than 1%
<i>User acceptance rate issues</i>	Potential for privacy misuse	Associated with law enforcement, hygiene concerns	User resistance, usage difficulty
<i>Factors affecting performance</i>	Lighting, orientation of face, and sunglasses	Dirty, dry, or worn fingertips	Poor eyesight, glare or reflections
<i>Demonstrated vulnerability</i>	Notebook computer with digital photographs	Artificial fingers, reactivated latent prints	High-resolution picture of iris
<i>Variability with ages</i>	Affected by aging	Stable	Stable
<i>Commercial availability since</i>	1990s	1970s	1997
<i>Universality</i>	High	Medium	High
<i>Uniqueness</i>	Low	High	High
<i>Collectability</i>	High	Medium	Medium
<i>Performance</i>	Low	High	High
<i>Acceptability</i>	High	Medium	Low

3.1.1 Facial Recognition

A facial recognition system refers to a technological application that has the capability to identify and verify a person in relation to a digital image from an already inscribed source. Facial recognition systems are computer-based security systems that are programmed to detect and identify human faces. Facial Recognition Technology (FRT) involves analyzing facial characteristics, storing features in a database, and using them to identify faces. When using the facial recognition system, its primary task is to recognize a human face like patterns and extract it. Once the face is extracted, the system measures special neural mechanisms for face perception such as the distance between the eyes, the shape of the cheekbones and other distinguishable features. These measurements are compared through the entire database of pictures to find the correct match. FRT is categorized in three tasks: face verification, face identification, and watch list (Intona, 2017) (Lu, n.d.).

Face verification is concerned with authentication. Verifying an individual's authenticity can be done by answering the question, whether the user is who they claim to be. To evaluate the facial verification, the verification performance either is a false reject or false accept. The false reject is the rate at which legitimate users are recognized and granted access. The false accept is the system output when the system makes a mistake at which imposters are granted access (Intona, 2017) (Lu, n.d.).

Face identification answers the question to who the user is or what their identity is. Face identification researches and matches it against a database to identify the face. The identification is tested by differentiating between closed-set identification problems and

open-set identification problems. In a closed-set identification problem, the sensor takes facial observation known in the reference database beforehand, whereas open-set identification refers to what the system does not have in the reference database (Intona, 2017) (Lu, n.d.).

Watch list describes the suspect the system is looking for. Watch lists are derived from an open-set identification task. A system compares the entire database to search for a person on the watch list and identifies matches it. Upon a correct match, the system will trigger an alarm (Intona, 2017) (Lu, n.d.). In 2015, U.S. Customs and Border Protection (CBP) tested facial comparison technology at Washington Dulles International Airport. “The results of that testing determined the system successfully performed matches against actual passports and live captured images” (CBP, 2018). Key countries that have already adopted the facial recognition technologies are the Australian border force and the customs services of New Zealand. The automated facial recognition is a boarding system called Smart Gate. Smart Gate compares the travelers face with the data in the passport’s microchip.

To stay ahead of emerging threats at the airport, Customs and Border Protection (CBP) combine their efforts with the Department of Homeland Security (DHS) Science and Technology Directorate “to implement integrated biometric capture capabilities to confirm the departure of non-U.S. citizens at airports and seaports and to more efficiently screen travelers entering the United States” (CBP, 2018). With the help of FRT, the CBP can collect more advanced passenger and biometric information to better identify and validate low-risk passengers earlier in the transit process to ensure their swift movement across our borders (CBP, 2018).

3.1.2 Fingerprint Recognition

Biometric systems integration used in a multifactor authentication system such as combining face recognition software with other biometrics as fingerprint can vastly improve passenger processing. Fingerprint is unique to everyone, which provides security since no one else can guess it (Poza, 2016). Also, due to its biometrics asset, fingerprints are unforgettable (Poza, 2016). All fingerprint data manipulation is performed within a Trusted Execution Environment (TEE) that guarantees confidentiality and integrity of the code and data loaded inside a systems main processor.

As discussed earlier, each fingerprint is unique to its user, and with the help of a fingerprint scanner an image of a digital form of fingerprints is collected. It involves analyzing the bifurcation, short ridge, and ridge ending to differentiate patterns of different people. Each unique fingerprint is converted into a unique code, which enables the device to be secure. At an airport, an automatic fingerprint scanner is often placed at the security checkpoints.

There are three types of scanners: optical, capacitive, and ultrasonic. An optical sensor captures an image of one's finger image. It uses algorithms that helps distinguish unique patterns such as ridges, shapes or marks by analyzing the lightest and darkest areas (Triggs, 2018). An optical scanner is profoundly unsecure, because an adversary can use a 2D picture or a prosthetic to bypass sensitive details (Triggs, 2018).

Compared to optical sensors, capacitive sensors use an array of a tiny capacitor circuits to collect the data of a fingerprint and use small electrical and conductive charges to track the details of a fingerprint. The result of using the conductive plates and ridges is a more

secure fingerprint scanner that allows for a “highly detailed image of the ridges to a fingerprint” (Triggs, 2018). By creating a large enough array of these capacitors, typically hundreds if not thousands in a single scanner, they allow for a highly detailed image of the ridges and valleys of a fingerprint to be created from nothing more than electrical signals (Triggs, 2018).

Meanwhile, the ultrasonic scanners hardware consists of both an ultrasonic transmitter and a receiver. The scanner creates a 3D model of the ridges and distinctive features of a users’ fingerprint by bouncing an ultrasonic pulse. Together, these enable it to see beneath the skin and authenticate that the finger is alive while providing more information as a biometric measure (Triggs, 2018).

Currently, TSA is undergoing a proof of concept to evaluate biometric authentication technology for operational and security impact called TSA Pre✓ (TSA, 2018). By enrolling in this program, the travelers are issued a “Known Traveler Number” which is unique to each passenger. TSA matches passenger fingerprints “against law enforcement, immigration, and intelligence databases along with the government watch list and the Centers for Disease Control and Prevention's list of individuals who are not allowed to travel due to health concerns” (Future Travel Experience, 2015). Using fingerprints to verify passengers’ identities serves as both a boarding pass and identity document. TSA Pre✓ expedites the screening process that can speed travelers through security checkpoint.

3.1.3 Iris Recognition

The iris is the visible colored part of the eye. Similar to fingerprints, no two irises are alike, including that of identical twins. Moreover, even the right and left eye patterns are unique from each other. The iris pattern remains unchanged after the age of two and does not degrade overtime. Iris identification system uses mathematical algorithms that enables the scanner to calculate the position of an individual's eye while extracting the iris. The scanner plots distinct markings and pattern on iris and takes a black and white image from five to 24 inches from the eye. This technology is efficient for use in airports and at border points.

The United Arab Emirates (UAE) developed an iris biometric system for border control points. In 2016, the Dubai airport severed 83.6 million passengers, and it is projected to reach 7.2 billion passengers by 2035. Globally, more than 6,500 passengers travel to UAE daily via seven international airports, three land ports, and seven seaports (Daugman, 2004). Managing a vast number of passenger traffic seemed challenging though, until all border control points adopt a biometric identification system such as iris recognition.

UAE enforced iris recognition at border control points as a mean to ensure that expelled personal will not re-enter the country. To prevent the expelled individual from entering UAE with forged identity and falsified documents the iris codes of all arriving passengers are compared in real-time exhaustively against an enrolled central database. UAE has the largest database of 420,000 irises, with the daily number of iris cross-comparisons of

over 2.7 billion. Out of 2.3 million iris comparison tests, the iris system had only 0.2% false matches (Daugman, 2004).

3.1.4 Evolving Biometric Technologies

Another unique biometrics used for user authentication system includes periocular, retinal, and gait patterns. Similar to the iris, periocular observes the region surrounding the eyes with the densest biomedical features. The features of periocular include the eyelids, the eyebrows and the eyeball, which all vary in shape, size, and color. The periocular region finds a balance between the face and iris recognition. For instance, when a facial image is captured from a distance, the iris patterns can be of low resolution. If just the iris is captured from a close distance, then the facial features are not available. Therefore, the periocular system has an advantage as it captures both facial and eye regions from a wide range of distances. The periocular experiences very little change in shape and location even as an individual progresses in age (Jain, 2009).

While both iris and periocular are characteristics of the eye, another eye biometric modality is retina. The retina is located in the posterior portion of the eye. Biometric systems identify individuals by retinal blood vessels because they are unique and therefore suitable for identification. A retinal biometric is captured in close proximity and by projecting a low-intensity beam directly into pupils to obtain a digital image (Jain, 2009).

Some biometric methods such as application of the gait evaluate the way individuals walk. Gait allows surveillance cameras with low resolutions to pick up human silhouette to identify individuals. Gait can measure how fast, how far and with how much force a

person or an object moves. Gait is noninvasive since an individual does not have to physically touch anything or get near a device. Gait patterns are classified into holistic and feature-based. The holistic ones calculate body movement statistics generated by motion, while feature-based ones calculate stride and kinematics of individuals to better identify them (Jain, 2009).

As biometrics evolve, all these applications can be integrated into more developed security systems such as those in the airports. Successful adoption of the use of biometrics in airports will lead to saving of resources in terms of time and money. Meanwhile, providing seamless yet enhanced security that can bring a whole revolution in air travel.

3.2 Importance of Biometrics

The history of biometrics dates back to the 1800's. Alphonse Bertillon, a French criminologist and founder of anthropometry, a system based on physical measurements (National Law Enforcement Museum, 2011). Bertillon created anthropometry to track and identify criminals, and his method was afterwards referred to as Bertillonage and it was the main criminal identification system during the 19th century (National Law Enforcement Museum, 2011).

Today in the 21st century, biometrics has proven to offer security as it can confirm and establish an individual's identity. There are four main general classifications that enables authentication: it is something an individual knows (password), something that the individual has (token ID), something that the individual is (static biometrics: fingerprint, iris, face) and something an individual does (dynamic biometrics: voice pattern,

handwriting, key strokes) (Stallings, 2015). These four classifications of authentication can be utilized for biometric technologies.

Authentication is the primary line of defense along with authorization. The two processes of authorizing and authenticating are fundamental in securing one's information, which helps to prevent hackers and ease the technological advancements of services to the users. An authentication process consists of two steps: identification and verification. The identification step involves providing proof for the claimed identity. The verification step establishes the validity of the claim (Stallings, 2015).

Authorizing is asserting that a specific user has access to a particular resource, or is granted permission to use various services. Authentication, on the other hand, is verifying that an individual is whoever he or she says they are or claim to be. Authorization and authentication are independent, central to security design, and often confused or used synonymously. Authentication validates a user credentials to gain user access (Todorov, 2007).

As mentioned in an example earlier, UAE handles a large volume of incoming passenger traffic by adopting a biometric identification system such as iris recognition. In UAE, all major entry and exit points are collectively termed as control and management areas. Maximum control is identified and further ensured by authenticity of the people entering and exiting through paramount of security. This enforced iris recognition at border control points helps UAE to authenticate an individual's identity then authorize them to enter the country and assure secure passage into UAE (Daugman, 2004).

Using biometrics has great advantages, as they are durable and long lasting. The key advantage is that biometrics cannot be lost like a key, a smart card, or a token. It cannot be forgotten like a password or pin. Biometrics patterns essentially last a lifetime.

Chapter 4

Proof of Concepts for Biometric

Entities around the globe are undergoing proof of concepts to evaluate a biometric authentication technology for operational and security impact. In this proof-of-concept, the following programs and services are being explored for their use cases of biometrics authentication. Services include standard common-use, self-service equipment already in use across the industry, such as check-in kiosks, bag drop units, gates for secure access, and boarding and automated border control. The existing programs include TSA Pre✓, CBP, Global Entry, Nexus, SENTRI, Mobile Pass, Clear Me, Automated Passport Control, Smart Gate, miSense, IATA one ID task force, IATA Fast Travel Program, and Vision Box Happy Flow Aruba. Each proof of concept was analyzed in depth below.

4.1 Department of Homeland Security

After the brutal terrorist attack on September 11, 2001, the Homeland Security Act of 2002 was signed into law. The Act brought together approximately 22 separate federal agencies to establish the Department of Homeland Security. The DHS aims to protect the nation from foreign threats, and deals with preventing terrorist attacks, lowering our vulnerability to terrorism, and recovering from terrorist attacks. The DHS vision is to enhance security efforts at the airport through biometric capability. This vision involves an integration of other sub-security organizations such as the Customs and Border

Protection, Transportation Security Administration, Citizens and Immigration Services, and Immigration and Customs Enforcement. DHS has launched Trusted Traveler Programs (TTP) with biometric identity services that enable national security and safety decision making as shown in Table 4.1 (Homeland Security, 2018).

Table 4.1: DHS Trusted Traveler Programs with Biometric Identity Services

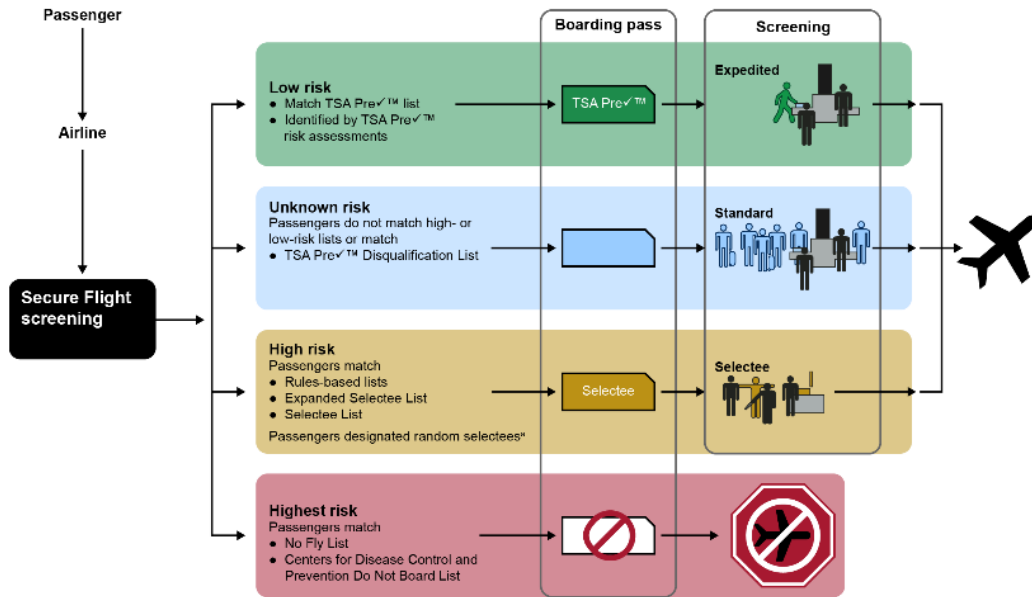
<i>Agency</i>	<i>TSA</i>	<i>Customs and Border Protection</i>		
<i>Program</i>	TSA Pre✓®	Global Entry	NEXUS	SENTRI
<i>Website</i>	www.TSA/tsa-precheck	www.globalentry.gov	https://ttp.cbp.dhs.gov	https://ttp.cbp.dhs.gov
<i>Eligibility Required</i>	U.S. citizens and U.S. lawful permanent residents.	U.S. citizens, U.S. lawful permanent residents and citizens of certain other countries.	U.S. citizens, lawful permanent residents, Canadian citizens and lawful permanent residents of Canada.	Proof of citizenship and admissibility documentation.
<i>Application Fee</i>	\$85.00 (5-year membership)	\$100.00 (5-year membership)	\$50.00 (5-year membership)	\$122.25 (5-year membership)
<i>Passport Required</i>	No	Yes; or lawful permanent resident card	No	No
<i>Application Process</i>	Pre-enroll online, visit an enrollment center; provide fingerprints and verify ID.	Pre-enroll online, visit an enrollment center for an interview; provide fingerprints and verify ID.	Pre-enroll online, visit an enrollment center for an interview; provide fingerprints and verify ID.	Pre-enroll online, visit an enrollment center for an interview; provide fingerprints and verify ID.
<i>Program Experience</i>	TSA Pre✓® expedited screening at participating airports.	Expedited processing through CBP at airports and land borders upon arrival in the U.S. Includes the TSA Pre✓®experience.	Expedited processing at airports and land borders when entering the U.S. and Canada. Includes Global Entry benefits. Includes the TSA Pre✓®benefits for U.S. citizens, U.S. lawful permanent residents and Canadian citizens.	Expedited processing through CBP at land borders. Includes Global Entry and TSA Pre✓® benefits for U.S. citizens and U.S. lawful permanent residents.

DHS provides biometric identification services through its Office of Biometric Identity Management (OBIM), which supplies the technology for matching, storing, and sharing biometric data. OBIM also provides analysis, updates its watchlist, and ensures the integrity of the data. The biometric technology is called Automated Biometric Identification System, or IDENT, and is operated and maintained by OBIM. IDENT currently holds more than 200 million unique identities and processes more than 300,000 biometric transactions per day, which makes it the largest biometric repository in the U.S. government. Since the department caters for overall security, with this information being present in their database, it can deal with crime at the airports in a more convenient way (Homeland Security, 2018).

4.2 TSA Pre✓

TSA was created in the aftermath of 9/11 to oversee security for all transportation systems in America. TSA became part of the Department of Homeland Security to ensure the security and safety of the travelling public. To expedite screening process at the airport, TSA PreCheck (Pre✓) was created. Pre✓ is deployed for automated employment verifications, immunization tracking, exclusion and sanction screening, health and drug testing, license monitoring, and background checks. The program requires passengers to pre-screen themselves at a certified U.S. location and undergo a background check. TSA identifies and assigns passengers a risk category: high risk, low risk, or unknown risk as shown in Figure 4.1 (Hasbrouck, 2014). Passengers that are classified as low risk are the only ones that are able to receive TSA Pre✓ services at nation's airports. Fingerprints are collected from those low risk passengers, who would like to apply for the program. The

collected fingerprints are compared to FBI’s fingerprint repositories and then stored in a database. By going through the TSA Pre✓ lane, passengers bypass the standard slow security lane. Pre✓ passengers do not have to remove shoes, the 3-1-1 liquid compliant bag, laptops, light outerwear, jackets, and belts as shown in Figure 4.2 (TSA, 2018).



Source: GAO analysis of TSA information. | GAO-14-531

Figure 4.1: TSA Risk Category (Hasbrouck, 2014)



Figure 4.2: TSA Pre✓ vs Standard Screening (TSA, 2018)

Currently there are 200 airports and 47 participating airlines nationwide providing Pre✓ services (TSA, 2018). This is whereby the identity and authenticity of precheck approved travelers are verified using contactless fingerprint reader. Eligible passengers flying both domestically and outbound internationally from participating airport showed that 98 percent of passengers waited in line less than twenty minutes and more than 99 percent of TSA Pre✓ passengers waited less than five minutes (TSA, 2018). The TSA Pre✓ expedites the screening process that can speed travelers through security checkpoint.

4.3 Customs and Border Protection

The U.S. Customs and Border Protection (CBP) is America's first line of defense for passengers arriving and exiting the U.S. CBP guards the border entities: land, sea, and airports. The CBP defends, detects, and prevents threats related to customs, immigrations, border security, and agricultural protection. Every day, the CBP "welcomes nearly one million visitors, screens more than 67,000 cargo containers, arrests more than 1,100 individuals, and seizes nearly 6 tons of illicit drugs. Annually, CBP facilitates an average of more than \$3 trillion in legitimate trade while enforcing U.S. trade laws" (CBP, 2018).

CBP is required to verify the identity of all travelers which they do so by biometrics.

Biometric technologies came into effect for non-US citizens after the 9/11 attack. The CBP involves a myriad of biometrics techniques including fingerprint recognition, face, and iris scanning. Machine Readable Travel Documents (MRTDs) are globally interoperable and have been standardized as the best formats for biometric data conveyance. As such, border control systems have the task of ensuring that they check on passengers in the pretext of departure and arrival processing at destination and origin

airports (NIST, 2013). CBP integrated the use of biometric technology in the issuance of visas as well as screening on all non-U.S. citizens entering and exiting the country.

Information is collected on passengers because it is necessary to gather data for immigration and national security. Information is then used to adapt airport infrastructure to accept MRTDs (NIST, 2013).

CBP uses the biometric images to verify each traveler's identity. CBP is authorized to collect this information by the 2002 Enhanced Border Security and Visa Entry Reform Act (Pub. L. 107- 173), the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108- 458), and the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110-53) (CBP, 2018).

In the continuous efforts to improve national security, CBP launched its first facial biometric demonstration at Hartfield-Jackson Atlanta International Airport. After this successful pilot, CBP has expanded the demonstration and developed a robust cloud-based service called the Traveler Verification Service (TVS), and integrated biometric verification into the boarding process at JFK airport in New York City, and Atlanta (CBP, 2018).

CBP provides international trusted traveler programs such as Global Entry, Nexus and SENTRI. These trusted traveler programs require a background check, fee, and interview. Once approved, traveler uses a kiosk each time after arriving in the U.S. These programs collect more advanced passenger and biometric information to pre-identify and validate low-risk populations earlier in the transit process. By enrolling in these programs, the travelers are issued a "Known Traveler Number" which is unique to each passenger. The

trusted traveler programs offer expedited passenger processing and modified screening for pre-approved members. The program improves “security by increasing efficiencies in allocating screening resources and facilitating legitimate trade and travel” (CBP, 2018).

4.4 Global Entry

Global Entry is a program run by the U.S. CBP. This program gives a chance to low-risk travelers who have been pre-approved to get accelerated clearance once they arrive into the United States. It is available at 46 U.S. locations and 13 pre-clearance airports (CBP, 2018). Currently, there are over 2.4 million participants enrolled directly in Global Entry, and over 1.3 million members of NEXUS and SENTRI, who also receive Global Entry benefits. A bonus to Global Entry is that members are eligible for the TSA Pre✓ program. Global Entry users bypass U.S customs and immigration form, hence no paperwork. Members have access to expedited entry benefits in other countries, which provide no processing lines, resulting in reduced wait times (CBP, 2018).

The reason the Global Entry program has had a great success rate is due to it using biometric technologies. Once an applicant applies for Global Entry privileges, the applicants must go through a rigorous interview process. During the interview, fingerprints as well as a digital photo are taken thereby allowing for the finger and face biometrics to be collected in the system. To obtain the service, applicants are required to have a machine-readable passport. While boarding an aircraft in the U.S., a passenger’s image is captured and compared to the passport for verification using the Traveler Verification Service, defined above. TVS uses CBP’s biographic APIS manifest data, “for most non-U.S. citizens, the photograph will be used as a biometric conformation of

departure from the U.S as required by law (8 U.S.C. 1365b).” Then, CBP creates a record of the traveler’s departure from the U.S. in Advanced Passenger Information System (APIS) as well as the Arrival and Departure Information System (ADIS) (CBP, 2018). Overall, Global Entry has reduced wait times by more than 70 percent with more than 75 percent of travelers using Global Entry processed in less than five minutes (CBP, 2018). Global Entry’s eligibility period lasts for five years after which the service can be renewed by paying a renewal fee. Cancellation of Global Entry can occur in the case of criminal conviction.

4.5 NEXUS

The NEXUS program refers to a biometric service that is joint operated between the CBP and the Canada Border Services Agency. Similar to Pre✓ and Global Entry, NEXUS caters to travelers who have been pre-approved and are low-risk passengers. NEXUS members receive a Radio Frequency Identification (RFID) card and biometrics-enabled NEXUS card to use when entering the United States and Canada at designated ports of entry. There are currently over 1.25 million members enrolled in the NEXUS program (CBP, 2018).

When entering U.S. or Canada, the passenger uses a self-service kiosk for an iris recognition scan. Members can expedite customs by simply looking into a camera that uses the eye’s iris as proof of identity. The technology reads each of the 266 unique characteristics in the human iris. NEXUS members benefit by avoiding long ques by using reserved immigration lanes usually present at more than 100 participating U.S. airports and 8 Canadian airports (CBP, 2018).

4.6 Secure Electronic Network for Travelers Rapid Inspection (SENTRI)

Similar to Pre✓ and Global Entry, Secure Electronic Network for Travelers Rapid Inspection (SENTRI) is a CBP program that enables those travelers who have been previously approved and considered to be at low risk to be cleared. For this program, applicants are subjected to a prior rigorous background check and a one-on-one interview before approval.

SENTRI conducts a facial verification at designated port of entries. The facial verification test involves taking video clips that are compared to a SENTRI enrollment database of photographs (General Accounting Office, 2002). Approved members are provided with an RFID card, which enables them to cross the U.S. and Mexico border seamlessly. There are over 425,000 SENTRI members, and they account for 15% of cross-border traffic along the Southwest border (CBP, 2018).

4.7 Mobile Passport

The CBP unveiled Mobile Passport Control Application to expedite entry process into the U.S. Unlike the Trusted Traveler Programs, Mobile Passport is a free app based on an automation program, meaning that it enables one to submit their passport and customs declaration information via mobile device instead of the traditional paper form.

To use this application, users download the associated free mobile passport app. Users use the app to submit their passport information and declaration information to U.S.

Users are required to take a selfie for facial recognition without wearing a hat or sunglasses. All the personal information is then saved into traveler's profile, and it allows one to create profiles for other family members (CBP, 2018).

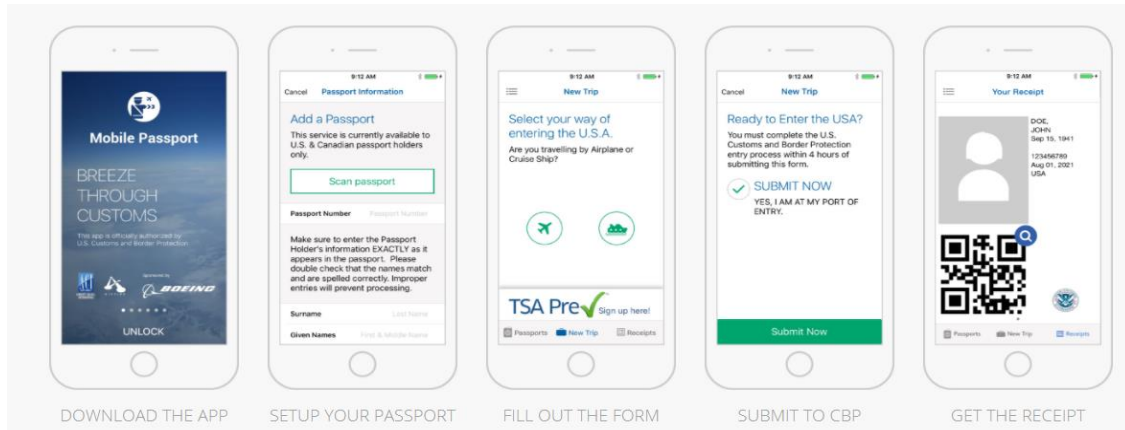


Figure 4.3: Mobile Passport Process (CBP, 2018)

Once the passenger confirms the data on the app appears exactly as it does on their physical passport, the itinerary will be submitted to CBP. Subsequently, CBP will send a digital Encrypted Quick Response (QR) code receipt after they have reviewed a passenger submission as shown in Figure 4.3 (CBP, 2018).

Upon landing in the U.S, the passenger will enter through a designated mobile pass lane, present the QR code to the CBP officer for clearance, identification, and verification. Since the biometrics used is facial recognition, this method is quite convenient and has already been adopted by one cruise port and 24 airports (CBP, 2018).

4.8 Clear Me

Clear Me is another expedited airport security program that allows passengers to travel with ease. Clear Me is a biometric identification program that verifies a person's identity through scanning fingerprints or an iris of the eye. For registration as a member, enrollment can be done online but the last step requires the person to be present at the airports or stadium for confirmation of identity and a linkage of biometrics. Clear Me

digitally authenticates via driver's license or passport, confirms their identity and creates a biometric account. When Clear Me members arrive at the airport, they pass through a lane that is dedicated Clear Me lane. Here, they either look at a camera that can read their iris images, or they can scan their fingerprints on a fingerprint reader. Then a Clear Me employee escorts the passenger directly to the metal detecting machines and bag scanning lines. Currently, there are 24 domestic airports within the United States that offer Clear Me services and more than 1.5 million people are enrolled (Vora, 2017).

4.9 Automated Passport Control Kiosk

Automated Passport Control (APC) is a self-service kiosk that uses finger and facial recognition technology. APC is a CBP program that streamlines the passenger's entry into the United States as shown in Figure 4.4 (CBP, 2018). APC helps respond to CBP inspection related questions and submit biographic information electronically rather than filling out a paper form. APC kiosks authenticate identity by matching passenger faces to the biometric record in their e-passport. APC kiosks collect the passenger's e-passport, flight information, customs declaration data, scan fingerprints, take a photo and issue a receipt to the passenger, who then brings their passport and receipt to a CBP officer for verification. Currently, 42 airports are using APC kiosks in their arrivals area with 40% success rate in wait time improvement (CBP, 2018).



Figure 4.4: Automated Passport Control Process (CBP, 2018)

4.10 SmartGate

SmartGate program enables eligible travelers to self-process through passport control. It uses a system integrated with ePassports and facial recognition technology to perform checks that would otherwise be conducted by a CBP officer. This self-service airport customs includes a two-step system: a kiosk and gate. The first step allows automated border processing systems that compare the travelers face data in the passport's microchip to the data stored in its database. Its facial recognition system refers to a technological application that has the capability to identify and verify a person in relation to a digital image from an already inscribed source. The second step requires a passenger to insert the boarding pass into a slip then look at the camera for facial recognition as shown in Figure 4.5. Once the SmartGate successfully identifies and verifies the passenger, they can proceed to their flight gate (Australian Government, 2017).



Figure 4.5: SmartGate Process (Australian Government, 2017)

Australia has implemented SmartGate at eight major international airports and wishes to get to a 90% automated air travel by 2020 (Nash, 2017). Australia has already rolled-out several biometrics programs with facial recognition information in their database. This

will ensure that passports are completely replaced with facial biometrics in all airports within Australia. The ultimate goal of this program is to enable a seamless travel for the passengers, and to ensure that less time is lost within airports.

Key countries that have already adopted this technology are Dubai and New Zealand.

Dubai deployed smart gates equipped with iris recognition camera to capture both facial and eye biometrics. New Zealand deployed the next-generation biometric-based customs e-gate, named Smart Gate Plus at Auckland International Airport (Iritech, 2017).

SmartGate program enhances the overall traveler experience by providing faster, simplified and user-friendly process times.

4.11 miSense

The miSense biometric airport security trials were performed at Heathrow Airport in the U.K. to seek enrollment of 2000 passengers using Emirates and Cathay Pacific Airlines.

The targeted passengers were traveling to and from Dubai and Hong Kong. The airport authority claimed that the trial period allows passengers to bypass long queues at security and immigration and prevent people from illegally entering the country (McCue, 2008).

During the Heathrow trial, basic and advanced biometric checks were tested. The passengers were asked to scan their passport and the right index at a self-service check-in kiosk before getting a boarding pass. The system involved checking the details of passengers against databases by various intelligence groups before allowing them on board and the information will be stored by the UK immigration service. Once the passport and the fingerprint are successfully cleared and validated, the passenger is then allowed to the boarding gate. With the more comprehensive system design, miSense-plus

can further collect and digitize ten fingerprints, a facial scan and two images of the iris. This information is uploaded onto a smart card allowing the passenger to use it for their future journeys. The system had been formulated in such a way that the card is compatible with fingerprint readers that had been placed at the Dubai, Heathrow and Hong Kong's immigration barriers (McCue, 2008). The miSense trial at Heathrow showed that 87% of the passengers thought that the enrolment process was easy, 66% of the passengers said that it took them less than 15 seconds to bypass the gates, and 72% of the passengers stated that the most important benefit was faster journey times (Find biometrics, 2007).

4.12 IATA One ID Task Force

The essence of this program is to introduce the better management of the identification (ID) of the passenger. In this case, it proposes the introduction of ID management that is supported by a biometric facial recognition that is a single token, which encompasses the passenger's boarding pass and travel document in addition to a digital proof of identity. Notably, a single token is deployed after the passenger is first identified before the identity undergoes authentication and biometric verification. As such, it reduces the need for passengers to present a plethora of documents in the context of numerous touchpoints on the way. In this consideration, the passenger has the propensity to transmit data and own it at will, which implies that passengers have a significant level of control over personal data (IATA, 2015).

4.13 IATA Fast Travel Program

The essence of the Fast Travel Program is to address the future of travel. As such, this comes with reduced industry costs, more choices for clients, and an increase in self-service choices to make. The program lasts for an exceptional six years and it assists the industry to save more than two billion USD (IATA, 2015). Saving such an amount is critical because it makes sure that programs that have been implemented do not end up leading to an embezzlement of funds. On the contrary, they should attempt to assist organizations to streamline processes to the point that these depict their imperativeness to corporate objectives and standards of practice. It also improves the experience of the client by adopting recommended practices and uniform standards it creates within the industry in which it operates (IATA, 2015). One of the services the company provides is passenger facilitation. The service helps in facilitating regulatory requirements, self-boarding, document verification, passenger data, and the use of biometrics in all processes that are deployed for automated border control contexts. Meaningful to note here is that the security is bolstered in this context because all the programs are interoperable with other systems (IATA, 2015). The program allows passengers to self-scan boarding tokens. In this case, they entail biometrics, passports, Near Field Communication (NFC) boarding passes, mobile Barcode Boarding Pass (BCBP) passes, web check-in boarding passes, and paper boarding passes (IATA, 2015).

4.14 Vision Box Happy Flow Aruba

Vision Box Happy Flow Aruba was developed as a collaboration of Vision-Box™, Schiphol Group, KLM, the Netherlands, the Aruba International Airport, and Aruba (Aruba Happy Flow, 2018). The program is a unique initiative that has been in operation

for two years and has two major objectives. Firstly, its essence is to test the pre-clearance border control process from the two American continents to the Schengen area of the European Union. Secondly, the objective is to revolutionize client experience by streamlining passenger-processing incentives. Vision Box Happy Flow Aruba provides one hundred percent self-service where the face is a single biometric token. As such, it is open to passengers age eight and above and it now covers more than thirty-three nations in the world (Aruba Happy Flow, 2018). The expansion of the program is critical to make sure that it encompasses several parts of the world, with the aim of reaching as many nations as possible within the few coming years. Case in point, the success of this venture will be crucial in the context of the world because it will allow other technologies to be devised that may be deployed in a similar format as Vision Box Happy Flow Aruba and be used to streamline biometrics.

Chapter 5

Barriers to Biometrics

Although the use of the most efficient screening and authentication method is the goal of every airline, there are hurdles that could derail the efforts towards achieving them. The topics that are proven to be of a significant challenge are interoperability and technology.

The National Biometrics Challenge, updated report of the National Science and Technology Council (NSTC) discusses the challenges of biometrics and improving system capabilities. Barriers identified by NSTC are as follow (Holdren, 2011):

- Advancing biometrics sensor technology for various modalities.
- Significant improvements in large-scale systems performance.
- Allowing and promoting interoperability between systems.
- Establishing comprehensive and widely accepted open standards for biometric information, and the devices that capture it, to include conformance-testing processes for broadly accepted certification.
- Protecting individual privacy and promoting public confidence in biometric technology and systems.
- Developing a consistent and accurate message across the biometric community.

Other than the above-mentioned barriers, there is also a constraint, which exists due to the lack of complex biometric security systems within all major airports. Outside of U.S.,

the Dubai International Airport faces challenges in implementing a proper biometrics system. As mentioned previously, Dubai is one of the busiest airport in the world handling 83 million passengers in 2016 and projected to welcome 7.2 billion passengers by 2035. The airport is faced with several challenges especially related to use of biometrics for security (Marcellin, 2018).

Some of the challenges prohibiting the development of an effective biometric system at Dubai Airport comes from the large size of the airport. The airport also faces a series of logistical challenges when it comes to biometrics. Due to heavy operational conditions, there are more than 100 boarding gates and often only one gate is used for one airline. Therefore, a huge infrastructure cost is incurred to install and maintain it at each gate and for everyday operation, proving it unreliable (Marcellin, 2018).

The airport serves around 243 thousand travelers per day. During peak hours there are in average 13,000 passengers using the airport. Although 30% of the locals who use the airport are registered biometrically, the other 70% is not. The airport's management argues that registering biometrics of 10,000 people per hour during peak hour would lead to more time wastage. It also notes that for an efficient biometric system to work, there needs to be cooperation from the over 200 airlines serving the airport. However, each airline and airport use a different technology and system, and, as a result, there is an absence of a standardized biometrics system (Marcellin, 2018).

5.1 Biometrics Can Be Stolen

Biometrics are better than passwords, which someone can steal through social engineering, data breaches, and phishing scams. Notably, biometrics entail what

someone is, rather than what he or she knows. In this context, the implication is that biometrics are unique to persons and make it hard for hackers to steal when compared to older technologies. On the contrary, one should note that it is easy to steal biometric data through hacking, in the context of hacking other forms of data stored on devices. Case in point, unless the data is stored in a vault or encrypted, it is susceptible to stealing.

Moskovitch et al. (2009) states that biometrics have been involved in identity theft due to the proliferation of services such as WebMails and eBanks online. They acknowledge that biometrics can be used to bolster security in contexts whereby using the same user-name and password for multiple use cases may be problematic. The major issue with the use of biometrics at all the times is the need for dedicated hardware that may not be available when needed by users, since most of the pieces of hardware are expensive. While recent laptops have devices to verify fingerprints, they lack the popularity required to make them mainstream devices. Similarly, their use in the verification of web applications is extremely limited, which implies redundancy in such contexts. Thus, the implication is that using biometrics requires interacting the user with devices like pointing devices and keyboards.

In the past, biometrics entailed using keystroke dynamics to verify users. More recently, it has been proposed that the mouse be used for this purpose. However, the threat of identity fraud is always present. It may be deployed in terrorism, breaches to national security, stock market manipulation, human trafficking, and money laundering as well as in a broad range of commodity and services, credit card, mortgage, and loan frauds. Once a hacker gains access to the information, he or she may gain the right of entry to services that a network of computers provides (Intranet and Internet). Similarly, biometrics may

be deployed to access information stored locally on mobile devices and personal computers.

5.2 Security Issues of Biometrics

Biometrics are subjected to varieties of attack. Some potential attacks, along with potential defenses, are listed in Table 5.1 (Stallings, 2015).

Table 5.1: Potential Attacks on Biometrics (Stallings, 2015)

<i>Attacks</i>	<i>Definition</i>	<i>Examples</i>	<i>Typical Defenses</i>
<i>Client attack</i>	Adversary attempts to achieve user authentication without access to the remote host or the intervening communications path	False match	Large entropy; limited attempts
<i>Host attack</i>	Directed at the user file at the host where biometrics codes are stored	Template theft	Capture device authentication; challenge response
<i>Eavesdropping, theft, and copying</i>	Adversary attempts to learn the password by some sort of attack that involves the physical proximity of user and adversary	Copying (spoofing) biometric	Copy detection at capture device and capture device authentication
<i>Replay</i>	Adversary repeats a previously captured user response	Replay stolen biometric template response	Copy detection at capture device and capture device authentication via challenge- response protocol
<i>Trojan horse</i>	An application or physical device masquerades as an authentic application or device to capture biometrics	Installation of rogue client or capture device	Authentication of client or capture device within trusted security perimeter
<i>Denial of service</i>	Attempts to disable a user authentication service by flooding the service with numerous authentication attempts	Lockout by multiple failed authentication	Multifactor with token

5.3 Lack of Revocability

Biometrics have permanent association with every individual. If a system is compromised and the biometric credentials are leaked, then revocability of biometric data is impossible. In this case, once a user's biometric has already been entered into a system, then ability to change or recompute an account with new or update biometric is not possible. In cases where a user loses a hand or finger or even suffers from biometric theft, then the biometric can be revoked or cancelled, but cannot be replace or substituted.

Chapter 6

Standards on Using Biometrics at Airports

According to the International Civil Aviation Organization (ICAO), biometric technology has the propensity of providing the unique means of identifying humans based on one or more behavioral or physical characteristics. In this case, it is imperative to point to the fact that current standards of practice are based on iris images, fingerprints, and face photos (IATA, 2017). The Airports Council International (ACI) recommendation for biometrics systems, under FIPS 201-2 compliance, emphasizes the need that airports be implemented systems be conscious of environmental conditions or requirements of each location, certified according to International Organization for Standardization (ISO) and ICAO standards, scalable, reliable, secure, efficient, fast, applicable at airports, performance-based, and interoperable across multiple systems (NIST, 2013).

Gromov (2009) states that the technologies that have been deployed in the development of modern identification systems have been experiencing quick development. As such, despite that many of these systems have not been receiving the required recognition in the world, as opposed to their status in the United States, fingerprinting and facial recognition technology has been deployed in most airports. Nevertheless, biometrics is a technology that the world has come to accept as being relevant to several use cases.

Working airport professionals and passengers have long wanted to have an “e-passport” that would hold all the information concerning an individual, and which is interoperable with all airport systems in the world. The e-passport has an electronic chip that contains a person’s personal information. The chip also includes a biometric identifier. It should be noted that the essence of this technology has been to strengthen the protection against identity theft, combating of illegal trafficking, people smuggling and illegal immigration, control of legal migration, and security of state actors. The European Union (EU) states that all developed standards should assess the quality of fingerprints and facial image software (Gromov, 2009). The EU recognizes its systems require a high level of robustness to prevent against redundancy of any kind. In terms of actual implementation, the EU uses international standards for MRTDs, specifically the ISO/IEC 19794, and makes sure they accommodate radio frequency (RF) compatibility with several e-travel documents that use electronic chips, and also have the required specifications for security. The compatible chip for this application needs to have a logic structure and be a storage medium with the specifications for biometric identifiers that include fingerprints and facial recognition (Gromov, 2009).

The developed regulations state that travel documents and passports should have additional security requirements and features that entail standards of falsification, counterfeiting, and an enhancement of anti-forgery (Gromov, 2009). ICAO states that the principle of “one person - one passport” should be followed at all times to guarantee the security of airports. ICAO regulations require that the person that holds the passport has the document, as well as biometric features linked to him or her alone. The enhancement

of security in such a context is high, considering that such passports are not transferable to other people, which would lead to a security breach at airports.

As an example, it may be possible to prevent child trafficking from an international viewpoint by having a passport that includes a parent and photographs of children. In such a case, it would be an incremental task to identify the children if ICAO does not demand for the storage of the biometric information of the children (Gromov, 2009). The implemented regulations state that people without the ability to give fingerprints are exempted, as well as children under the age of six, from this requirement. The typical biometric reader should be deployed to acquire raw biometric samples, convert this data into intermediate forms, convert the intermediate data into templates to be stored, and compare the stored information with a reference template.

All of these biometrics systems need to follow several standards of ICAO, such as ISO/IEC 19794 and ISO/IEC 14443 (Gromov, 2009). Firstly, e-passports should be durable, which implies that they should last at least ten years, and be able to receive backward compatible updates in the future that will make them functional for a long time. Secondly, they should be practical in a sense that any standards set should be implemented and operationalized easily. As such, this should be done without introducing several disparate equipment and systems that make sure they meet all possible interpretations of the standards (Gromov, 2009).

Next, they should exhibit a certain level of technical reliability. This requirement asks the developed biometrics systems to provide parameters and guidelines that confirm that member countries implement the technologies with a high level of confidence. As such,

when a country reads the data that another one has encoded, it should be in such a way that provides confidence in the integrity and quality of the information that raises the level of verification of the data. Another requirement, uniformity relates to the capability of the systems to minimize the variants of the responses that member countries provide, which should be uniform for all contexts (Gromov, 2009).

Finally, the passports should be interoperable from a global viewpoint. For these technologies, facial recognition is mandatory from a global context, while iris and fingerprint recognition are optional. In the United States, only iris recognition is optional. The ISO/IEC 19794 states that all passports should conform to these specifications to boost the security across the world (Gromov, 2009).

The vision of ICAO is to have uniformed global standards of biometrics technology. To achieve that, biometrics should not have proprietary elements, to ensure that any nation that invests in the technology is protected from changing suppliers or infrastructure. Secondly, the capability of data retrieval systems should have a validity of not more than ten years. Thirdly, the specification of such technology should be deployed for watch lists, verification, and identification use cases. Finally, the specification of this technology should be interoperable. The requirement in this context calls for the use of the technology interchangeably by document issuers, carriers, and border control use cases (Gromov, 2009).

6.1 Mobile Applications

It is essential that biometric results exchange data with emerging mobile apps. Case in point, it is worth noting that biometrics mobile app development has the ability to make

operations more efficient and effective while improving data sharing associated with the use of biometrics. Under 44 U.S.C. 3542(b)(2) [SP 800-59], Web Service Biometric Devices (WS-Biometric Devices) is a new technology that allows the interfacing of several devices (NIST, 2013). Interfacing of these devices must ensure their interoperability. This technology is used in facial recognition, iris scanning, and fingerprinting technology. “Lossy compression” method for data encoding should be applied for these applications since when compression occurs, information is lost, which may have a negative impact on interoperability and accuracy. Research is still undergoing to improve the best practices of compression, but it is critical to deploy current standards of practice. These authentication systems should stick to Personal Identity Verification (PIV) credentials. PIV credentials are used for authentication to enhance the security of agencies. As such, they are decidedly resilient to identity manipulation, forging, meddling, and deception. They deploy interoperable technology that makes them worthwhile in the context of biometric technology use. These credentials are critical to the identification of individuals from various parts of the world. Therefore, it becomes an incremental task in case passengers do not have information that may be used to identify them, owing to the numerous forms of crime that are prevalent in the current world.

Chapter 7

Concept of Operations

7.1 Airport Passenger Flow Simulation Models

Simulation modeling is widely used to study and improve the existing systems behavior without disrupting the daily operations. The transportation industry is constantly under pressure to increase security and reduce unauthorized person movement, while efficiently and quickly processing an increasing number of travelers. With this objective in mind, airport operators rely on simulation models to assess the impact of newer technology implementation. As such, the impact of moving towards biometric token ID technology can be evaluated using simulation models. The simulation analysis can provide information on how biometric token ID can be combined with self-service solutions to significantly help meeting the challenges of passenger processing at airports across the nation. This thesis focuses on medium-sized airports models, the size of Orlando International Airport.

Modeling airport operations allows simulation analysts to assess the potential passenger processing improvements with biometrics implementation. Biometric modifications to the existing process can accommodate passenger growth, expedite passenger processing, improve public circulation in the ticket lobbies, enhance baggage-handling systems, and improve security.

7.2 Medium-Sized International Airport Model

Since it is the closest medium-sized airport from Embry-Riddle Aeronautical University, we chose the Orlando International Airport as starting point for our model. It is the major international gateway serving the Orlando, Florida metropolitan region. The airport was originally an air force base called McCoy Air Force Base, with an airport code of MCO. In 1976, the Greater Orlando Aviation Authority (GOAA) acquired the airport and renamed McCoy to Orlando International Airport (MCO).

In 2017, MCO welcomed 44.6 million total passengers making it the busiest airport in Florida and thirteenth largest airport in the United States. In September 2017, MCO ranked highest in passenger satisfaction among airports in its passenger count category. MCO operates and provides non-stop service to 84 U.S. and 53 international destinations with the help of 47 airline carriers that fly approximately 910 flights per day. The top airline carrier flying out of MCO is Southwest Airlines, flying over 950 flights every week as shown in Figure 7.1 (GOAA, 2018).

The Airport facilities are distributed in a hub and spoke model. Hub and spoke is a transportation network model that involves a series of nodes (hubs) that are connected by arcs (spokes). It is a process flow with given paths called spokes, which connect to a central location called hubs. MCO is a tri-level complex featuring a main building (hub) connected to terminals A and B that link to four airside concourses (spokes).

To manage the passenger processing, the airport is segregated into three levels as shown in Figure 7.2 (GOAA, 2018). On Level 1, both Terminal A and Terminal B allow access to the ground transportation center from the curb front of the airport where passengers

can enter or exit. It also provides various ground transportation options including public transit, private transportation, and car rental. Arrivals/Baggage Claim Level is on Level 2 where the majority of the passengers are picked up from the airport since baggage claim facilities are located there. Departure area is on Level 3, where the main terminal building is also located. On Level 3, a passenger can utilize check-in and ticketing services. The terminal is well served by concessions: 20 restaurants, six bars, newsstands, shops, business services, currency exchange, and ATMs are also available (GOAA, 2018).

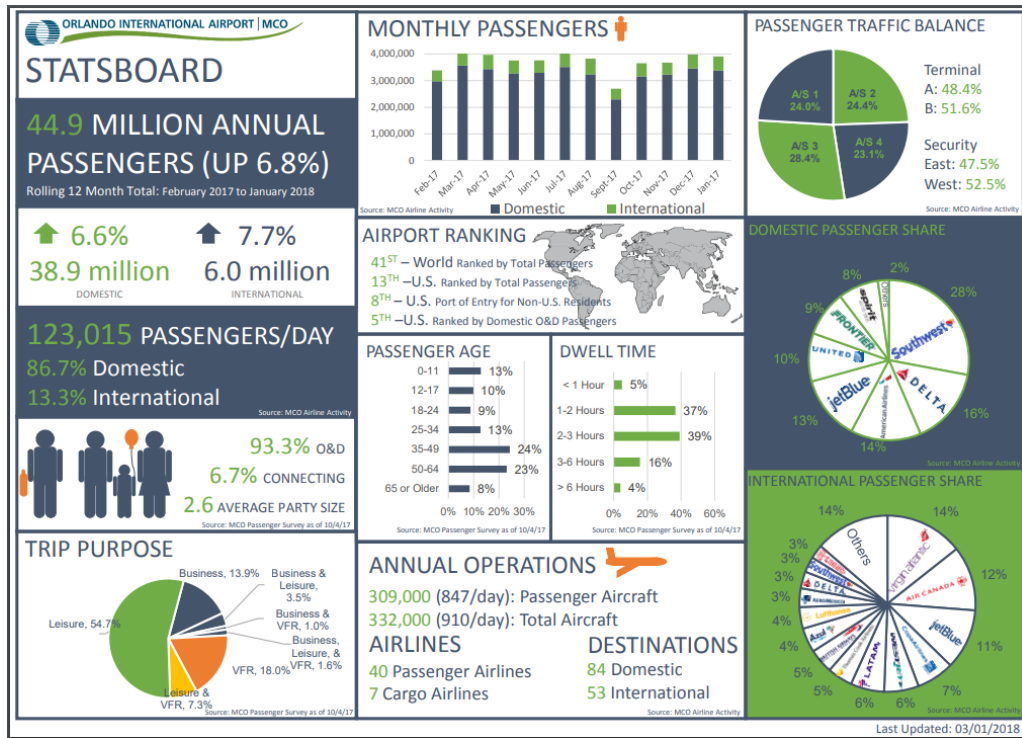


Figure 7.1: Airport Statistics (GOAA, 2018)

The main terminal on Level 3 is divided into two passenger terminals, A and B. Terminal A is on the Northside, and on the opposite side of the same building is Terminal B, which is only 525 feet across. Both terminals A and B are connected to two airside concourses each. Both terminals share two security checkpoints, one in the West Hall leading to

Airsides 1 and 3, and another in the East Atrium, leading to Airsides 2 and 4. After security checkpoint passengers take the airside trams to travel to the appropriate gates. Terminal A is connected to Airside 1 and 2. Airside 1 serves Gates 1-29, which is the secondary international arrivals concourse, while Airside 2 serves Gates 100-129. Terminal B is connected to Airside 3 and 4, Airside 3 serves Gates 30-59, while Airside 4 serves Gates 60-99, which is the primary international arrivals concourse. Each airside terminal serves multiple airlines. The scaled and calibrated, minimum and maximum walking distance on each airside are listed in Table 7.1 (GOAA, 2018).

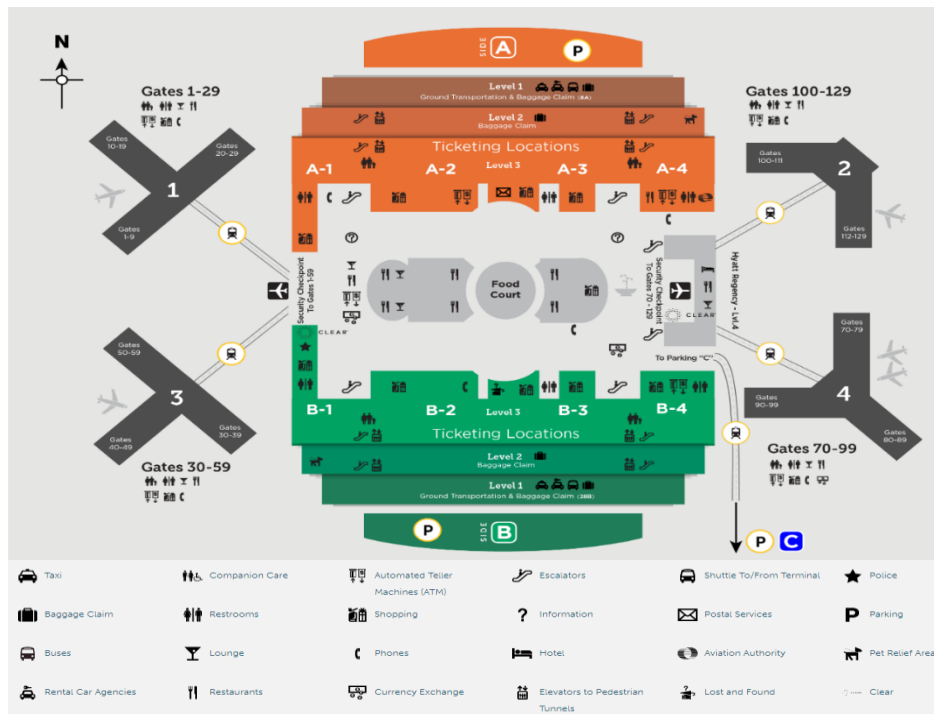


Figure 7.2: Airport Terminal Layout (GOAA, 2018)

Table 7.1: Airport Terminal Details (GOAA, 2018)

<i>Terminal</i>	<i>Concourses</i>	<i>Side</i>	<i>Gates</i>	<i>Minimum</i>	<i>Maximum</i>
A	Airside 1	West	Gates 1-29	515 feet/157 meters	812 feet/247 meters
A	Airside 2	East	Gates 100-129	200 feet/61 meters	600 feet/183 meters
B	Airside 3	West	Gates 30-59	479 feet/146 meters	903 feet/275 meters
B	Airside 4	East	Gates 70-99	467 feet/142 meters	944 feet/288 meters

7.3 Current Model Approach

The current passenger journey for departing at a medium-sized airport is shown in Figure 7.3. A customer starts their journey by planning and scheduling their trip. Currently, the GOAA recommends arriving three hours before a passengers' scheduled departure time due to the extensive process a passenger must go through (GOAA, 2018). Upon arrival to the airport, the passenger begins the check-in process. The check-in process enables passengers to confirm the respective flight, obtain a boarding pass, select their seat, and check-in luggage onto a plane, if desired. A passenger has six options to check-in: online, self-service kiosk, curbside, airline application, automatic or with an agent.

Airlines permit online and application check-in up to 24 hours before departure. The benefits of online or application check-in for travelers to bypass lines allowing to go straight to the counter for bag check-ins. Self-service kiosks allow customers to check-in themselves, eliminating the need for a full-service desk. Curbside check-in is an airline service that allows the passengers to get their boarding passes and hand over their luggage at counters outside of the airport terminal building. The traditional check-in method is with an agent. Automatic check-in applies when the passenger by their ticket in less than 24 hours of the flight, hence the system will automatically check-in the passenger. Upon check-in, if the passenger is not checking in any luggage, then the customer can go straight to the security checkpoint. During check-in, the traveler has the option to check their bags. Checking-in bags can be done in two ways: self-service kiosk or with an agent. At the self-service kiosk, a passenger can easily print the bag tag and check-in their own bags, ultimately reducing the wait time in line. There are also dedicated bag drop facilities for those checking-in prior to arrival or those who check-in

using the kiosks. The bag check-in process with an agent at the counter requires a passenger to present identification, boarding pass and a claim check per bag.

After successfully completing check-in, passengers proceed to TSA security checkpoint. Passengers again have two options: standard or expedite screening. Standard screening requires passengers to remove certain items (shoes, laptops, liquids, belts, and jackets) and place them on the X-ray belt for screening. Passenger enrolled in TSA Pre✓, Global Entry, or Clear Me qualify for expedited screening. With expedite screening, pre-screened passengers speed through security without the need to remove any items. At the security checkpoint each passenger is subjected to undergo screening. TSA uses millimeter wave advanced imaging technology and walk-through metal detectors to auto-detects potential threats to screen passengers (TSA, 2018). Once completing the security checkpoint, passengers can proceed to the general lounge and to the gate holding area to embark on their journey. A visual representation of the arrival process is also shown in Figure 7.3. During the arrival flight journey to the airport, passengers fill-out U.S. CBP I-94 and customs declaration forms. After disembarking the aircraft, passengers present their passport at the immigration counter to undergo an immigration inspection. To expedite the arrivals process, instead of the traditional paper form passengers have the option to complete the form on a self-serve kiosk or via a mobile application. Automated Passport Control (APC) is a facial recognition technology self-service kiosk used to respond to CBP inspection related questions and submit biographic information rather than filling out a paper form. Another self-service kiosk option for pre-approved members is Global Entry. Travelers using Global Entry kiosk present their passport and undergo fingerprint verification.

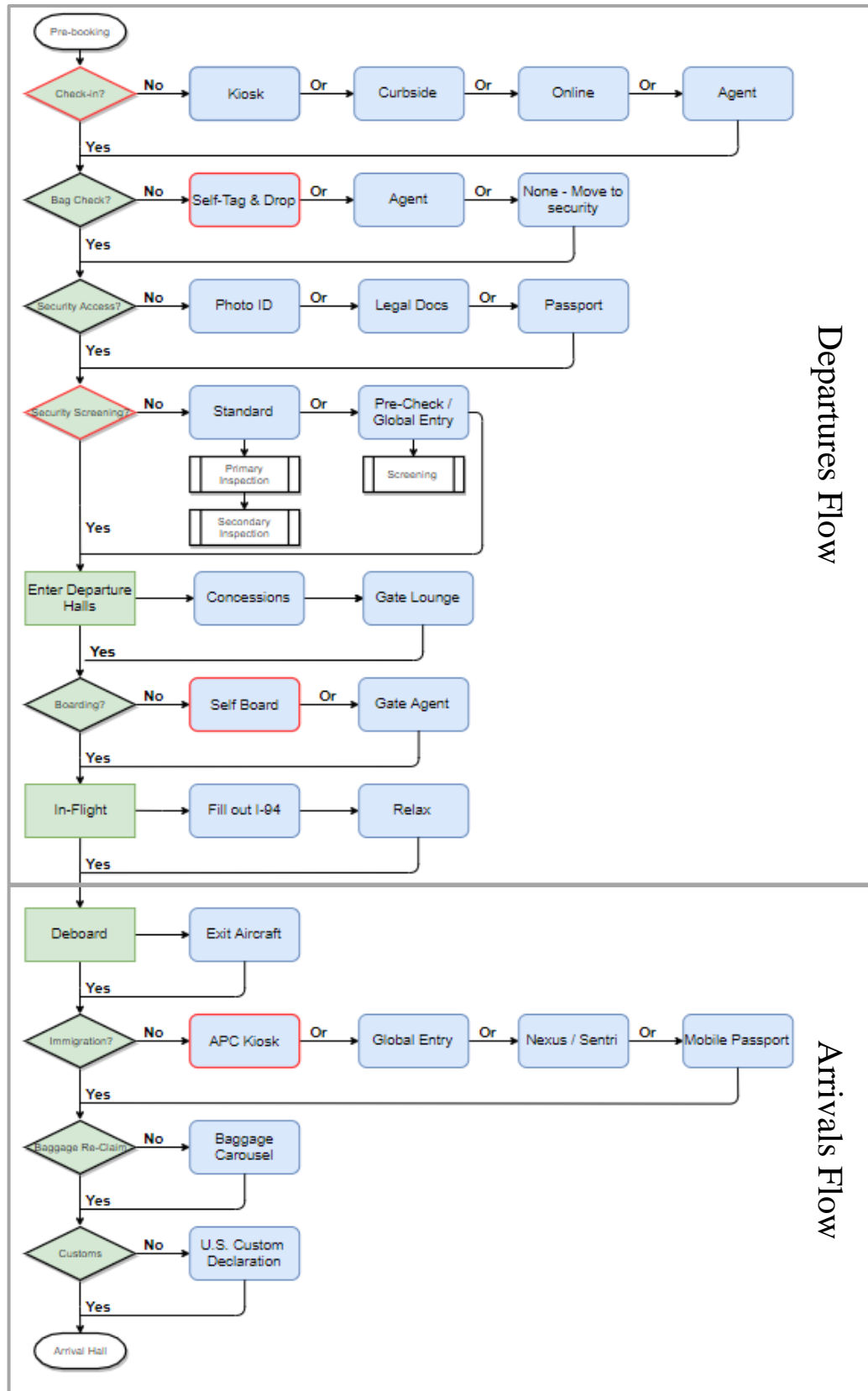


Figure 7.3: Airport Passenger Flow

Meanwhile, the CBP Mobile Passport Control allows passengers to submit their passport and customs declaration information via mobile device by taking a selfie for facial recognition. When the immigration inspection is complete, passengers refer to the respective information boards, check the airline name and flight number, and proceed to the baggage claim area. Using the baggage claim check-in receipt, passengers ensure that the bag in possession is theirs and take custody of it. Once their baggage is in possession, passengers must present Declaration of Personal Effects and Unaccompanied Articles at the customs checkpoint. After passing through customs, arriving passengers proceed to the arrivals lobby.

If a passenger has a connecting flight, then passengers still undergoes immigration and proceeds to baggage claim. At the baggage, the passenger will need to place their bags on the belt for transfer to the next departure terminal, depending on the transfer flight. After exiting the customs checkpoint, transfer passengers then take escalator or stairs up to the air tram to the connecting terminal, picking up bags, re-checking them in and proceeding through security check and on to their airside gate.

7.4 Proposed Model Approach

After analyzing the current operations within airports such as the MCO airport, it became apparent that there is room for improvement. These airports have only implemented isolated technology solutions for passenger processing. Therefore, they could seize the opportunity to implement biometric single token ID and processes on existing automated self-service kiosks and bag tag, self-service bag drop-off along with automated self-service gates for boarding and border control. These solutions are highlighted in red in

the airport flow of Figure 7.3 and can be integrated with biometric systems to enhance passenger handling.

A Passenger IT Trends Survey conducted by SITA, the world's leading specialist in air transport communications and IT solutions, shows customers reiterated interest in self-service technologies with biometric implementation. The survey indicates that 57% of passengers would use biometrics for every stage of their travel journey. “The single biometric travel token is expected to become a viable alternative to current passenger identity processes” (SITA, 2018). In the next ten years, 54% of airlines plan to evaluate the single biometric token technology. The survey reports that 92% of passengers are satisfied with the self-service technology and would use it on future trips. Self-service technologies have revolutionized the ability to streamline and improve the passenger-processing journey and it should be the focus for the future. The key findings are based on an online survey of 7,031 respondents from 17 countries across the Americas, Asia, Europe, Middle East and Africa. The infographic of the survey results is depicted in Figure 7.4 (SITA, 2018).

Once passengers arrive at the airport using biometric self-check-in kiosk or online check-in, they authenticate themselves with a valid Single Token ID. The single token ID contains their biometric identifier through facial recognition and finger printing. The traveler’s credentials are checked against the biometric chip of their e-passport. The token ID will, “serve as a passport, boarding pass, and ID for the journey” (Thornhill, 2016). Biometrics can provide assurance of identity and ensure each traveler presenting documents is the same individual to whom it is legally issued.



Figure 7.4: Passenger Survey Results (SITA, 2018)

Once the passenger has undergone the biometric match with the token ID at a checkpoint reader, the passenger can proceed to the rest of the journey. The token ID will allow passengers to complete the five critical tasks: check-in, bag drop, security, outbound immigration, and boarding processes using facial recognition technology as highlighted in red in Figure 7.3. Facial recognition eliminates the need to present the passport and boarding pass at every checkpoint (SITA, 2018) (Thornhill, 2016).

7.5 Distribution of Passengers

7.5.1 Annual Passenger Traffic

Since passenger security and satisfaction are of essence for passenger processing technologies, realistic, if not actual numbers need to be fed in the model. Using an extensive database of passenger enplaned and deplaned profiles from GOAA, Table 7.2 shows the 2017 Traffic Summary Report calculations. In 2017, MCO enplaned

22,115,929 total passengers and deplaned 22,395,336 total passengers. MCO served 123,015 passengers per day and 44 million passengers annually, out of which 86.7% were domestics and 13.3% international (GOAA, 2018). MCO offers more flights than any other airport in Florida and provides non-stop service to more major U.S. destinations than most other cities in the U.S. Due to MCO's high volume of travelers, it is ranked fifth busiest for domestic origin and destination passenger airports in the nation (GOAA, 2018).

Table 7.2: Airport Annual Passenger Traffic (GOAA, 2018).

<i>Passenger Traffic</i>	<i>Domestic Enplaned</i>	<i>International Enplaned</i>	<i>Domestic Deplaned</i>	<i>International Deplaned</i>	<i>TOTAL</i>
<i>January</i>	1,611,877	225,048	1,552,520	226,858	3,616,303
<i>February</i>	1,465,431	197,034	1,510,371	211,675	3,384,511
<i>March</i>	1,717,169	242,572	1,853,310	260,191	4,073,242
<i>April</i>	1,738,873	263,688	1,693,861	271,552	3,967,974
<i>May</i>	1,660,641	246,200	1,615,401	233,687	3,755,929
<i>June</i>	1,632,419	235,699	1,661,493	233,971	3,763,582
<i>July</i>	1,745,628	277,464	1,768,459	312,095	4,103,646
<i>August</i>	1,638,768	292,472	1,598,221	302,226	3,831,687
<i>September</i>	1,137,477	204,969	1,155,619	199,824	2,697,889
<i>October</i>	1,553,886	242,811	1,604,626	253,848	3,655,171
<i>November</i>	1,601,738	232,623	1,623,242	221,557	3,679,160
<i>December</i>	1,692,725	258,717	1,765,215	265,514	3,982,171
TOTAL	19,196,632	2,919,297	19,402,338	2,992,998	44,511,265

7.5.2 Wait Time for International Arrivals

The same considerations for realistic passenger processing should stand for international travel. MCO, the prototype medium-sized airport model chosen, has two international arrivals concourse. In Terminal B, Airside 4 is the primary international arrivals concourse, while Terminal A, Airside 1 is the secondary international arrivals concourse. MCO raised its international arrivals from 1.49 million in 2009 to 2.83 million in 2016,

which is an 89 percent increase in seven years (IFly, 2018). The rolling 12 months total for international arrivals (April 2017-March 2018) is shown in Table 7.3 (CBP, 2018). CBP officers who screen the passengers upon arrival also closely monitor the flight processing times, and thus can provide historical data for the wait times. The average wait time is 23 minutes, however, it is reported that at peak times passengers can be stuck on their planes for up to one hour due to CBP congestion. To alleviate the peak time waiting, CBP added 39 self-service kiosks for international passengers to speed up passenger flow through customs (IFly, 2018).

Table 7.3: Wait Time for International Arrivals (CBP, 2018)

<i>Month</i>	<i>Airside 1- West side</i>		<i>Airside 4- East Side</i>		<i>Airside 1 and 4</i>	
	Total passengers	Average Wait Time	Total passengers	Average Wait Time	Total	Average Wait time
<i>Jan 2018</i>	72286	23.54071661	105361	26.58064516	177647	25.06807131
<i>Feb 2018</i>	58428	21.1037037	98952	23.14802632	157380	22.18641115
<i>Mar 2018</i>	42286	21.93888889	63812	19.57788945	106098	20.69920844
<i>Apr 2017</i>	86119	20.99186992	109390	28.4488189	195509	24.03210273
<i>May 2017</i>	76321	18.01666667	108742	23.77011494	185063	20.43478261
<i>Jun 2017</i>	80456	18.56571429	104269	25.69958848	184725	21.48903879
<i>Jul 2017</i>	98592	25.96542553	144992	33.34228188	243584	29.22700297
<i>Aug 2017</i>	83609	24.75692308	151178	31.4375	234787	28.07131783
<i>Sep 2017</i>	76182	20.80066445	89601	25.40707965	165783	22.77609108
<i>Oct 2017</i>	84155	21.75073314	112891	25.78486056	197046	23.46114865
<i>Nov 2017</i>	85540	25.42982456	76524	23.59111111	162064	24.70017637
<i>Dec 2017</i>	102489	31.05524862	89096	28.71875	191585	30.08737864
<i>Grand Total</i>	946463	22.92814834	1254808	26.60247855	2201271	24.57297297

7.5.3 Passenger Traffic and TSA Wait Time

With 44.6 million passengers, MCO is a busy airport for security checkpoint. The total passenger traffic is distributed as follows: 48% of the passengers use Terminal A and

52% use Terminal B. Passenger traffic for each terminal's two airside concourses is further broken down in Table 7.4 (GOAA, 2018).

Table 7.4: Airport Passenger Traffic (GOAA, 2018)

<i>Airside</i>				<i>Terminal</i>		<i>Security</i>	
Airside 1	Airside 2	Airside 3	Airside 4	Terminal A	Terminal B	Security East Side	Security West Side
24.0%	24.4%	28.4%	23.1%	48.4%	51.6%	47.5%	52.5%

Both terminals share two security checkpoints, one in the West Atrium leading to airside 1 and 3, with passenger traffic of 52.5%, and the other one located in the East Atrium leading to airside 2 and 4 with 47.5% of passengers. Considering that the West Atrium has a higher foot traffic, the wait time on average is 14.7 minutes, while that in the East Atrium is at 13.7 minutes as shown in Table 7.5 (Orlando Sentinel, 2018).

Table 7.5: TSA Security Wait Time (Orlando Sentinel, 2018)

<i>Row Labels</i>	<i>EAST Checkpoint Average Wait Time</i>	<i>WEST Checkpoint Average Wait Time</i>
<i>Sunday</i>	16	14.75
<i>Monday</i>	15.4	17.6
<i>Tuesday</i>	13.4	13.6
<i>Wednesday</i>	16.4	12.4
<i>Thursday</i>	13.2	14.2
<i>Friday</i>	9	14.8
<i>Saturday</i>	12.4	15.2
<i>Grand Total</i>	13.7	14.7

7.5.4 Passenger Booking and Checking

According to SITA (2018), 80% of the passengers book their flights on the web. Refining this percentage, which is also shown in Figure 7.5, an estimate for MCO's passenger booking and check-in were calculated as shown in Table 7.6. For example, to find the

percent of passengers that book their flight on the web, a simple calculation of 80% of 44,511,265 (total passengers from Table 7.2) is used.

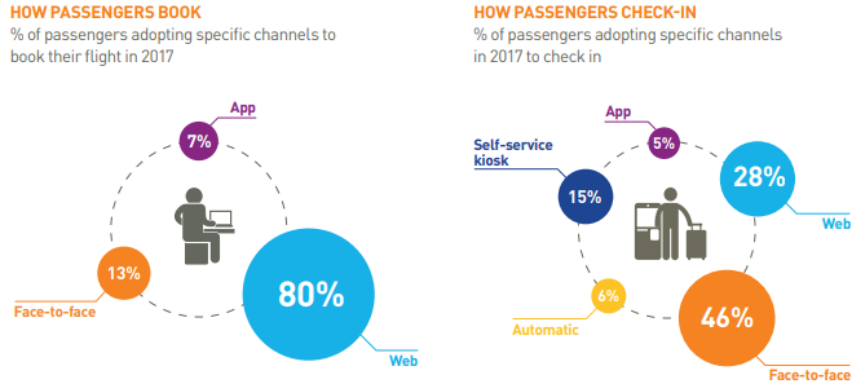


Figure 7.5: Passenger Booking and Checking Statistics (SITA, 2018)

Table 7.6: Passenger Booking and Checking-in Method Calculations

<i>Passenger Booking</i>		<i>Passenger Checking-in</i>	
Method	Number of Passengers	Method	Number of Passengers
Face-to-face	3115788.55	Self-Service kiosk	6676689.75
App	5786464.45	App	2225563.25
Web	35609012	Web	12463154.2
		Automatic	2670675.9
		Face-to-face	20475181.9

7.5.5 Security Checkpoint

To predict the number of passengers using photo ID, legal documentation, or passport an educated assumption was made. MCO serves 123,015 passengers per day and 44 million passengers annually, out of which 86.7% were domestics and 13.3% international (GOAA, 2018). Based on this fact, it is safe to state that at least 14% of passenger use passports while 86% uses legal documents.

According to TSA (2018), there are passengers signed up for Pre✓. To calculate how many percentage of passengers should be distributed for check vs standard lane a simple

calculation of 44,511,265 divided by 5 million was performed. Resulting in 8.9% passenger that use Precheck.

The Government Accountability Office reported TSA denied 1,384 individuals of the right to travel by air due to unsatisfactory evidence of identity (Hasbrouck, 2014). Doing the calculations, it would result in 0.00022036 % out of 44,511,265 passengers.

Chapter 8

Analysis, Results and Frequently Asked Questions

8.1 Simulation General Description

This thesis used the Simio simulation environment to create the simulation of a hypothetical mid-size international airport, approximately the size of MCO airport. The simulation model was designed to be fed with the publicly available passenger distribution of the MCO airport, presented in Chapter 7. All the other publicly available MCO operations data that were reported in Chapter 7 were also included in the model: distance traveled within the airport, several wait time statistics, international travel data, and booking and checking-in statistics. Still, not all data needed for building simulation model details are publicly available, in which case the best estimate was used based on similar processes.

The first eight steps of the simulation model, shown in Figure 8.1, represent the passengers' departures. The general process flow is as follows:

1. Departing passengers arrive at the airport.
2. Within the model's properties, there are 5 options that can be set for check-in. Passengers selects one of the 5 check-in options: kiosk, curbside, automatic, online/web or airline employee. These 5 properties can be varied within the experiment to evaluate various scenarios.

3. Passengers proceed to check-in their bags. They have two ways to check-in their bags: self-tag and drop, or with an airline employee. Passengers without a check-in bag proceed directly to security.
4. After check-in, all passengers move to the security area. Passengers will undergo security access, where they can either present their legal ID or Passport to prove their identity, so the passenger is authorized to enter sterile area of the airport.
5. Passengers go through x-ray screening procedures and they have two lane options: standard security or Precheck/Global Entry. Passengers that are pre-screened are eligible for Precheck and/or Global Entry. Others proceed to standard security lane. To prevent prohibited items entering the sterile area of the airport, passengers' carry-on bags also go through x-ray screening. At the security checkpoint bags are separated from the passengers, and both the passenger and the bag continue through their own x-ray process. If the bag or the passenger is suspected for any given reason, then both the passenger and the bag undergo secondary security. In case of a threat, a passenger will be denied further access.
6. Once the passenger is cleared by security, the passenger enters the sterile area to take a tram to the gates.
7. There are four airside concourses, with each airside having multiple gates. To board their flights, passengers have two options: self-boarding or being serviced by a gate agent.
8. Passenger is in flight, and out of the model.

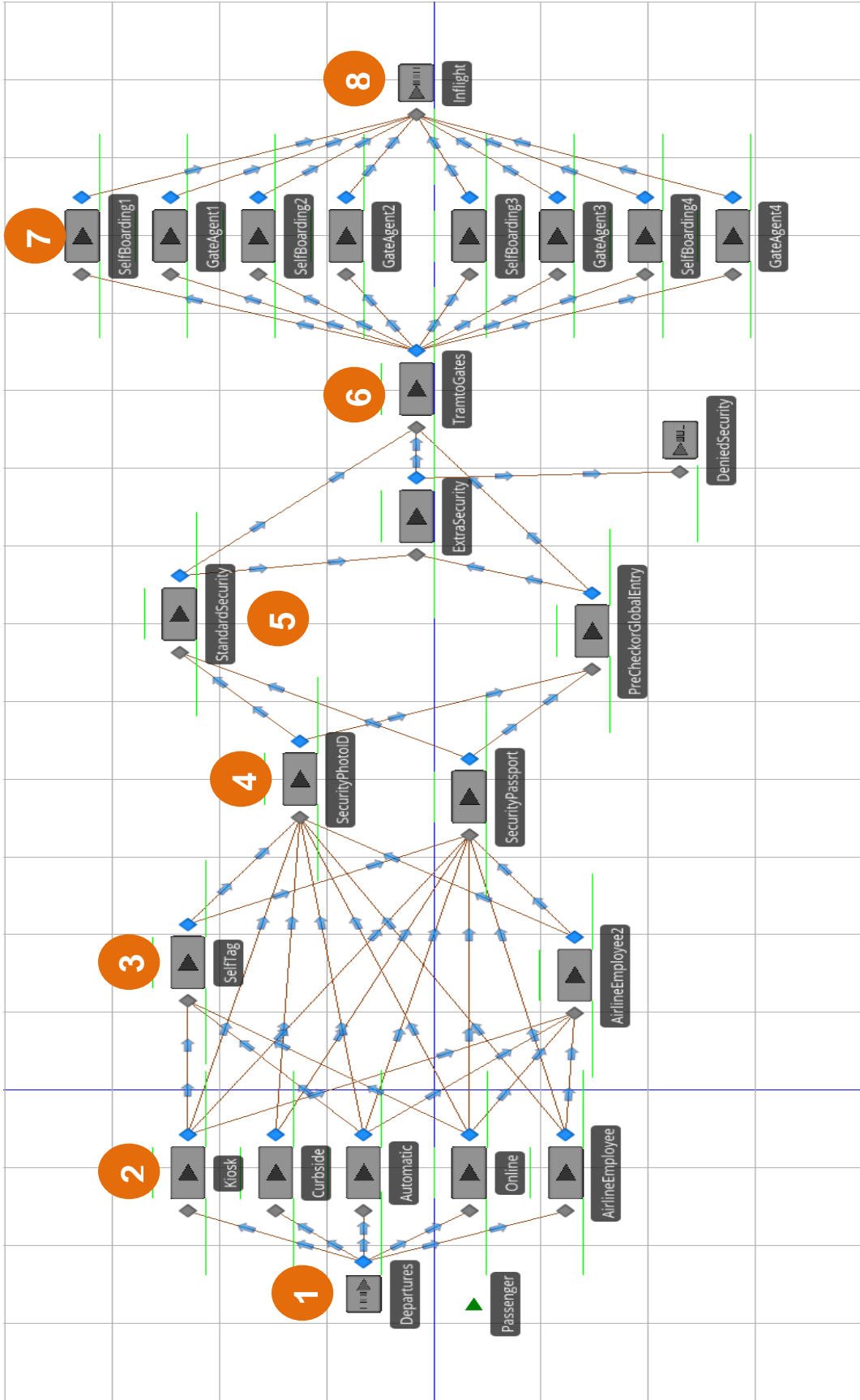


Figure 8.1: Airport Simulation

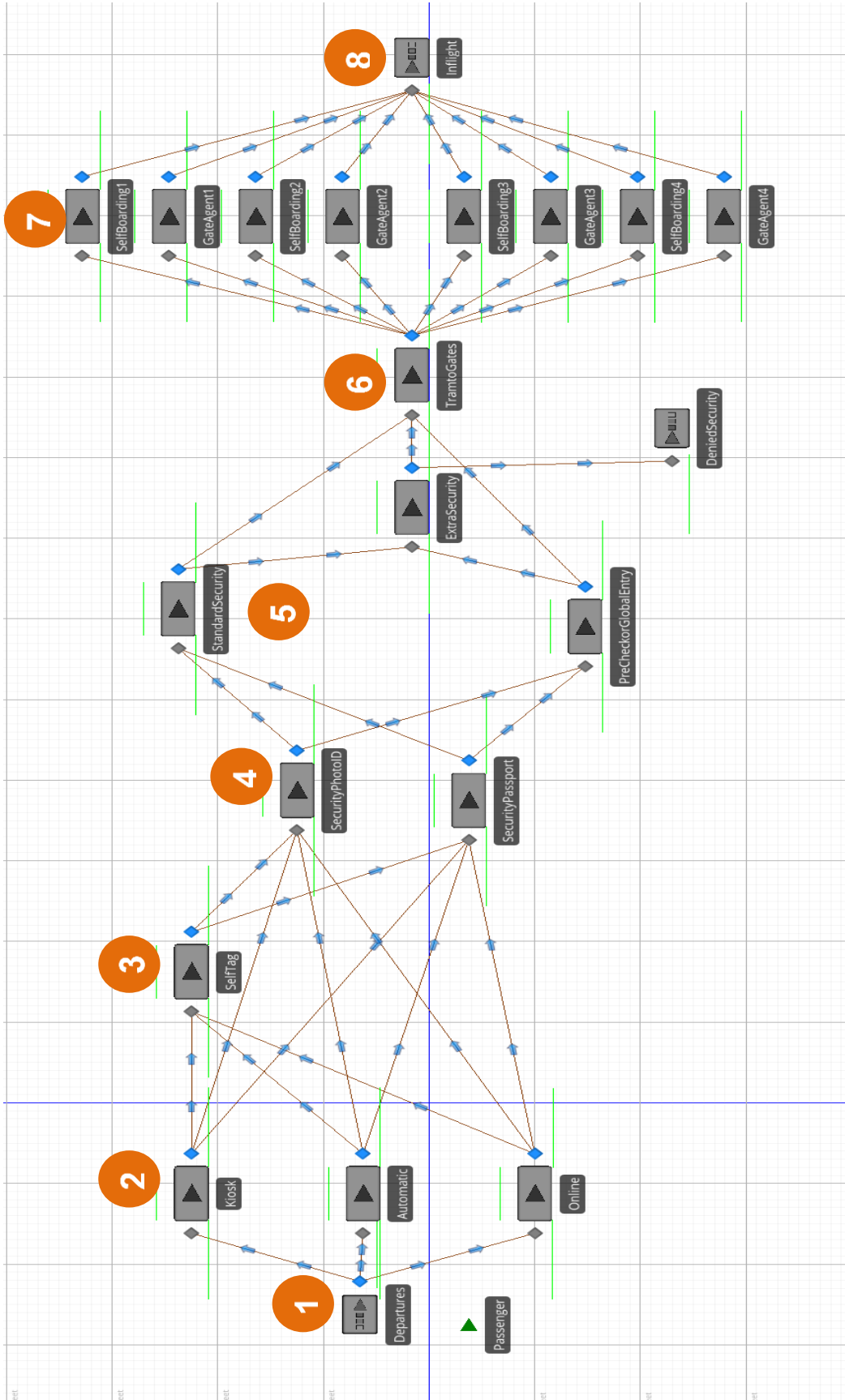


Figure 8.1: Airport Simulation with Token ID

Using the same passenger distribution as airport passenger input, as for the previous model, described in Chapter 7, the proposed Simio model for single token ID was formulated. The first eight steps shown in Figure 8.2 above, show the general process flow as follows:

1. Departing passengers arrive at the airport.
2. Within the model's properties, there are three self-service options that can be set for check-in. Passengers select one of the three check-in options: kiosk, automatic, online/web. Boarding pass data, identity document data and biometric details are captured wherever a passenger first touches the airport.
3. Passengers proceed to checking-in their bags with the single token ID. They check in their bag at a self-tag and drop kiosk. Passengers without a check-in bag proceed directly to security.
4. After the check-in, all passengers move to the security area. Passengers will undergo security access, where they positively identify themselves with the biometric token ID to enter sterile area of the airport.
5. Passengers go through self-service x-ray screening procedures and they have two lane options: standard security or Precheck/Global Entry. Passengers that are pre-screened are eligible for Precheck and/or Global Entry other proceed to standard security lane. To prevent prohibited items entering the sterile area of the airport passengers' carry-on bags also go through x-ray screening. At the security checkpoint, bags are separated from the passengers, and both the passenger and the bag continue through their own x-ray process. If the bag or the passenger is

suspected for any given reason, then both the passenger and the bag undergo secondary security. In case of a threat, a passenger will be denied further access.

6. Once the passenger is cleared by security, the passenger enters the sterile area to take a tram to the gates.
7. There are four airside concourses, with each airside having multiple gates. To board, passenger can have two options: self-boarding or being serviced by a gate agent.
8. Passenger is in flight, and out of the model.

8.2 Simulation Results

Due to the limited computational power on the laboratory workstations for modeling the more than 44 million passengers, per one year of simulated time, a reduced scale Simio model approach was run, without compromising the distribution of passenger traffic data, as shown in Table 8.1.

Table 8.1: Scaled-down Airport Annual Passenger Traffic (GOAA, 2018).

<i>Passenger Traffic</i>	<i>Per Month</i>	<i>Per Day</i>	<i>Per Day Reduced</i>	<i>Per Hour</i>
<i>January</i>	3,616,303	116,655	3,763	157
<i>February</i>	3,384,511	120,875	4,317	180
<i>March</i>	4,073,242	131,395	4,239	177
<i>April</i>	3,967,974	132,266	4,409	184
<i>May</i>	3,755,929	121,159	3,908	163
<i>June</i>	3,763,582	125,453	4,182	174
<i>July</i>	4,103,646	132,376	4,270	178
<i>August</i>	3,831,687	123,603	3,987	166
<i>September</i>	2,697,889	89,930	2,998	125
<i>October</i>	3,655,171	117,909	3,804	158
<i>November</i>	3,679,160	122,639	4,088	170
<i>December</i>	3,982,171	128,457	4,144	173
<i>Total</i>	44,511,265	1,462,715	48,108	2,004

By analyzing the results of simulation of passengers’ processing with biometric token ID against the standard process, it results that current practice passengers spend a significant amount of time waiting in line for a full manual service such as check-in, bag check, security check, and boarding. This is in contrast with the simulated token ID processing that moves the passengers through the airport processes much faster. The most significant improvement was noticed at the security process, which is also the place where, currently, passengers tend to wait in line the most at airports nationwide. Table 8.2 reports a sample of the statistics for the domestic flights passengers that were processed through security in both models.

Table 8.2: Sample Security Processing and Boarding Simulation Results.

<i>Statistic</i>	<i>Standard Processing</i>	<i>Token ID Processing</i>
<i>Domestic Security Number Processed</i>	40,897	41,320
<i>Domestic Security Average Number Waiting</i>	553.87	11.82
<i>Domestic Security Average Waiting Time</i>	47.98	3.68
<i>Number in Flight – out of the model passengers (includes both domestic and international flights)</i>	47,703	48,088
<i>Number of passengers entering the airport (model assumes that all passengers are expected to board their flights)</i>	48,108	48,108

In average, the waiting time in line for security has the potential to be reduced significantly. The simulation models reported a 92.33% decrease, from 47.98 minutes to 3.68 minutes needed for Token ID passengers. The number of passengers waiting in the security line given by the Token ID processing is decreased by 97.86% from an average of 12 passengers compared to 54 passengers. Also, due to the faster processing through security, and other steps from airport arrival to boarding, the number of passenger missed flights decreased by 1%, from 405 to 20.

Although manual services are still being practiced in airports, they exhibit a number of difficulties among others wastage of time, which are detrimental to the overall customer experience at airports. From the simulation analysis, it is apparent that the process of using biometrics is quite seamless. Airports, therefore, need to consider going away with the traditional and manual security processes and in their place, adopt the application of biometrics token ID. The token ID helps advance security by reducing the margin of human error all while protecting passenger's privacy.

The simulation results show that allowing passengers to take control of their own process with a self-service solution has its clear advantages such as improved passenger satisfaction, shorter passenger queues, and expedited processing. Token ID is a significant step toward fundamentally changing and improving the travel experience throughout the world.

8.3 Frequently Asked Questions

1. When implementing biometrics at an airport, who should collect the biometrics?

Border control and airports collect biometrics. In a sense, it should be noted that Airports Council International has recognized the benefit of the deployment of biometrics in the context of airport access control systems, airport passenger processing, and border control. As such, these use cases are critical in a sense that they improve facilitation, efficiency, and security of information (NIST, 2013). The objective of this implementation is to reduce unnecessary delays at airports, while increasing the speed of clearance, as well as boosting the security.

2. *When a passenger arrives at an airport and the check-in and bag drop-off is processed with biometrics, who should collect biometrics, airport or airline?*

Airports gain returns on investment with the implementation of MRTDs. As such, they need to have the opportunity in financing the implementation of these systems as a way of boosting immigration security and national security issues (NIST, 2013). Of vital importance is the security of passengers travelling with a certain airline. As such, biometric recognition technologies have the ability to assist in the achievement of interoperable, automated, and integrated security systems. This solution ensures that airports have smooth passenger flow and facilitation within the terminal, which notably improves their security, as well as that of the airline that transports them. Checking the information of passengers against national watch-lists and Interpol for terrorists and criminals is critical to avoid jeopardizing the lives of innocent travelers. This implies that airports should also collect passenger information before allowing them to board their airplanes.

3. *Who owns biometrics for all access such as check-in, drop off, or boarding pass or passenger screening? Is it an enrollment process for airlines, airport, provider of technology, DHS?*

The Department of Homeland Security, the provider of technology, the airport, and the airlines should have full access to passenger information such as passenger screening, boarding pass, drop off, and check-in. As such, the security at the airport is a matter of interest to all entities involved, which they should address with serious consideration (NIST, 2013). All entities need to ensure that

they identify the best ways to share this information to bolster immigration and national security.

4. *Do passengers have to opt-in for biometrics?*

Passengers do not have to opt-in for biometrics. On the contrary, they should be informed that the collection of such information is a matter of national security. Notably, passengers who understand that doing this is for their benefit may have no way to argue against the implementation of biometrics to keep them, and their country, safe from terrorists and criminals who may take advantage of the aircraft and cause unknown mass killings and human suffering (NIST, 2013).

5. *Who is responsible for liability of biometrics when stolen or falsified?*

The falsification or stealing of biometrics is a liability of all concerned officials: the DHS, provider of technology, airport, and airlines. These stakeholders have full access to passenger information such as passenger screening, boarding pass, drop off, and check-in. Thus, the officials they appoint to office should make sure they deploy current standards of practice that keep information safe from stealing or falsification of any kind.

6. *“What are the legal authorities that allow CBP to collect biometrics on travelers exiting the U.S.” (CBP, 2018)?*

“The authorities include:

- *1996 Illegal Immigration Reform and Immigrant Responsibility Act*: Creation of an automated system to record arrivals and departures of non-U.S. citizens at all air, sea, and land ports of entry.
- *2002 Enhanced Border Security and Visa Entry Reform Act, the Intelligence Reform and Terrorism Prevention Act of 2004, and the Implementing Recommendations of the 9/11 Commission Act of 2007*: Establishment of a nationwide biometric entry-exit system.
- *Consolidated Appropriations Act of 2016*: CBP Authorization to spend up to \$1 billion in certain visa fee surcharges collected over 10 years for biometric entry and exit implementation.
- *Executive Order 13780*, “Protecting the Nation from Foreign Terrorist Entry into the United States” March 9, 2017: DHS requirement to “expedite the completion and implementation of a biometric entry-exit tracking system for in-scope travelers to the United States.”
- *8 U.S.C. §§ 1185(b)*: Discusses the requirement for U.S. Citizens to have a valid passport for both entry and exit.”

7. “How does CBP secure traveler photos” (CBP, 2018)?

“CBP is committed to protecting the privacy of all travelers. Toward this end, CBP has embedded four primary safeguards to secure the data and reduce the potential that the photos may be lost or stolen:

- *Secure Encryption:* CBP uses HTTPS/SSL encryption for data transfer between the camera, the Virtual Private Cloud (VPC) and CBP systems as well as for PII at rest.
- *Biometric Templates:* CBP creates biometric templates of each of the historical photos, and newly captured exit photos for matching and storage. Biometric templates properties include: (a) Strings of multiple numbers representing images; (b) Can be matched against other templates that represent facial images; (c) Irreversible, cannot be reverse-engineered for viewing by anyone outside of CBP.
- *Brief Retention Periods:* All photos and templates are deleted from CBP systems within 14 days of capture and are purged from the TVS cloud matching services before the conclusion of the flight. However, CBP biometrically confirms the exit of in-scope U.S. citizens, creates an exit record and maintains these records in accordance with the published PIAs and System of Records Notices (SORN).
- *Secure Storage:* Facial images are stored in secure CBP systems and secure cloud environment (for a very brief period of time), thus mitigating potential privacy risks.
- *The Cloud Service Provider (CSP)* will adhere to the security and privacy controls required by National Institute of Standards and Technology (NIST) Special Publication 800-144, “Guidelines on Security and Privacy in Public Cloud Computing,” and the DHS Chief Information Officer.”

8. *“Do airline partners use CBP authority to collect photos” (CBP, 2018)?*

“CBP partners do not collect photographs under CBP authorities. The air carriers, who work in partnership with CBP, are collecting images pursuant to their relationship with the travelers. They may use the photographs consistent with that authority, choose to share those images with CBP for the purposes of efficiencies and the enhanced accuracy of traveler identity verification, which meet the statutory biometric exit mandate.”

References

- Agrawal, A. (2017). "User Authentication Mechanisms". IT. Print.
- Al-Raisi, A., & Al-Khoury A. (2006). Iris Recognition and The Challenge of Homeland and Border Control Security In UAE. Retrieved from https://www.id.gov.ae/userfiles/iris_paper.pdf
- Aruba Happy Flow (2018). Aruba Happy Flow. Retrieved from <http://www.arubahappyflow.com/>
- Australian Government (2017). Arrivals SmartGate. Retrieved from <https://www.homeaffairs.gov.au/Trav/Ente/GoIn/Arrival/Smartgateor-ePassport>
- Back, A. (2017). Using Blockchain for Digital Identity & Crypto Assets. Retrieved from medium.com/blockchain-review/self-sovereign-identity-and-the-digitization-of-real-world-assets-738e87dc530c
- Bauerle, N. (2017). What is Blockchain Technology? Retrieved from <https://www.coindesk.com/information/what-is-blockchain-technology/>
- BioMetrica (2018). Biometric – Theory. Retrieved from <http://biometrica.com/biometric-theory>.
- CBP (2018). Customs and Border Protection. Retrieved from <https://www.cbp.gov>
- Daugman, J., & Malhas, I. (2004). Iris Recognition Border-Crossing System in the UAE. Retrieved from <https://www.cl.cam.ac.uk/~jgd1000/UAEdeployment.pdf>

Department of State (2009). The Global War on Terrorism: The First 100 Days.

Retrieved from <https://2001-2009.state.gov/s/ct/rls/wh/6947.htm>

Find Biometrics (2007). Biometric Technology Gets Thumbs Up from Airport

Passengers. Retrieved from <https://findbiometrics.com/ncipher-completes-successful-airport-biometric-security-trials-biometric-technology-gets-thumbs-up-from-airport-passengers/>

Future Travel Experience (2015). Biometric Technology Enabling Seamless Airport

Vision. Retrieved from <http://www.futuretravelexperience.com/2015/07/biometric-technology-driving-seamless-airport-vision/>

General Accounting Office (2002). Technology Assessment: Using Biometrics for

Border Security. Retrieved from <https://www.gao.gov/new.items/d03174.pdf>

GOAA (2018). Orlando International Airport. Retrieved from <https://orlandoairports.net/>

Gromov, G. (2009). International Standards for the Use of Biometrics. Retrieved from

http://www.tsi.lv/sites/default/files/editor/science/Research_journals/Computer/2009/V3/6_international_standards_for_the_use_of_biometrics.pdf.

Hasbrouck, E. (2014). GAO Audit Confirms TSA Shift to Pre-Crime Profiling of All Air

Travelers. Retrieved from papersplease.org/wp/2014/09/22/gao-audit-confirms-tsa-shift-to-pre-crime-profiling-of-all-air-travelers/.

Holdren, J. (2011). The National Biometrics Challenge. Retrieved from

<https://webcache.googleusercontent.com/search?q=cache%3ApVJHGfa2TPwJ%3Ahttps%3A%2F%2Fwww.fbi.gov%2Ffile-repository%2Fabout-us-cjis->

- fingerprints_biometrics-biometric-center-of-excellences-biometricschallenge2011.pdf%2B&cd=1&hl=en&ct=clnk&gl=us
- Homeland Security (2018). Retrieved from <https://www.dhs.gov/>
- IATA. (2015). International Air Transport Association. Retrieved from <https://www.iata.org>
- IFly (2018). Orlando MCO Airport. Retrieved from <https://www.ifly.com/orlando-international-airport>
- Intona, L., & Nissenbaum, H. (2017). Facial Recognition Technology. Retrieved from https://www.nyu.edu/projects/nissenbaum/papers/facial_recognition_report.pdf
- Iritech (2017). Will Biometric Smart Gates Become the Future of Airport Security? Retrieved from <http://www.iritech.com/blog/biometric-smart-gates-1116/>
- Jain, A. K., Ross, A., & Park, U. (2009). Periocular Biometrics in the Visible. Retrieved from http://www.cse.msu.edu/~rossarun/pubs/ParkRossJain_Periodular_BTAS09.pdf
- Lu, X. (n.d.). Image Analysis for Face Recognition. Retrieved from http://www.face-rec.org/interesting-papers/general/imana4facrcg_lu.pdf
- Marcellin, F. (2018). Dubai Airport's Biometric Challenge. Retrieved from <https://www.airport-technology.com/features/dubai-airports-biometric-challenge/>
- McCamey, W. (2001). Editorial. *Journal of Security Administration*, 24 (2), 111.
- McCue, A. (2008) Heathrow Testing Biometric Security Checks. Retrieved from <https://www.cnet.com/news/heathrow-testing-biometric-security-checks/>

- Moskovitch, R., Feher, C., Messerman, A., Kirschnick, N., Mustafic, T., Camtepe, A., ... & Elovici, Y. (2009, June). Identity theft, computers and behavioral biometrics. In Intelligence and Security Informatics, 2009. IEEE International Conference.
- Nash, E. (2017). Facial Recognition to Replace Passports in Radical Security Overhaul at Australian Airports. Retrieved from <https://tottnews.com/2017/01/22/facial-recognition-australian-airports/>
- National Law Enforcement Museum (2011). Retrieved from <http://www.nleomf.org/museum/news/newsletters/online-insider/november-2011/bertillon-system-criminal-identification.html>
- NIST (2013). Standards for Biometric Technologies. Retrieved from <https://www.nist.gov/speech-testimony/standards-biometric-technologies>.
- Orlando Sentinel (2018). Airport Security Wait Times. Retrieved from <http://www.orlandosentinel2.com/data/travel/news/airport/>
- Poza, D. (2016). Fingerprint Authentication Gives You High Security and Low Friction Auth0. Retrieved from <https://auth0.com/blog/how-fingerprint-auth-gives-you-security/>
- Silk, R. (2017). Biometrics: Facial Recognition Tech Coming to An Airport Near You: Travel Weekly. Retrieved from <http://www.travelweekly.com/Travel-News/Airline-News/Biometrics-Facial-recognition-tech-coming-airport-near-you>
- SITA (2018). SITA. Retrieved from <https://www.sita.aero>

- Sorenson, A. (2018). A Paradigm Shift in How We Travel. Retrieved from https://www.linkedin.com/pulse/paradigm-shift-how-we-travel-arne-sorenson-1/?trackingId=a4BJrFrz9F1wMNEGQ6Yyxg%3D%3D&lipi=urn%3Ali%3Apage%3Ad_flagship3_search_srp_content%3BnWePi4GxTuq7E3Fm%2FwAfdQ%3D%3D&licu=urn%3Ali%3Acontrol%3Ad_flagship3_search_srp_co
- Stallings W., & Brown L. (2015). Computer Security: Principles and Practice, 3/E, Prentice Hall, ISBN-10: 0133773922
- Thakkar, D. (2016). An Overview of Biometric Iris Recognition Technology and Its Application Areas. Retrieved from <https://www.bayometric.com/biometric-iris-recognition-application/>
- Thornhill. T. (2016). Inside the Airport Of 2040 Where There Are NO Security Queues Thanks to Super-Fast 'Molecular Scanners'. Retrieved from <http://www.dailymail.co.uk/travel/article-3957806/Inside-airport-2040-NO-security-queues-thanks-super-fast-molecular-scanners.html>
- Todorov, D. (2007). Mechanics of User Identification and Authentication: Fundamentals of Identity Management. Retrieved from http://www.infosectoday.com/Articles/AU5219_C01.pdf
- Triggs, R. (2018). How Fingerprint Scanners Work: Optical, Capacitive, And Ultrasonic Variants Explained. Retrieved from Web. <https://www.androidauthority.com/how-fingerprint-scanners-work-670934/>
- TSA (2018). Transportation Security Administration. Retrieved from <https://www.tsa.gov>

Vora, S. (2017). How Clear Can Speed Up the Airport Screening Process. Retrieved from <https://www.nytimes.com/2017/11/17/travel/clear-airport-screening.html>