T.C.
Kocaeli University
Faculty of Aviation and Space Studies
Department of Aviation Management

SMART AIRPORT: HOW IOT AND NEW TECHNOLOGIES SHAPING THE FUTURE OF AIRPORT INDUSTRY

Final Graduations project

Mohammad Hadi YAQOOBI
151405042

Kocaeli 2019

T.C.

Kocaeli University

Faculty of Aviation and Space Studies

Department of Aviation Management

SMART AIRPORT: HOW IOT AND NEW TECHNOLOGIES SHAPING THE FUTURE OF AIRPORT INDUSTRY

Final Graduations project

Mohammad Hadi YAQOOBI

151405042

Supervisor: Assistant Professor Hakan RODOPLU

Kocaeli 2019

Table of Contents

CHAPTER ONE
Smart Airport

CHAPTER TWO
IoT and other Enabling Technologies for Smart Airport

CHAPTER THREE
Key Players in The Global Smart Airport Market, and Smart Airport Initiatives

CHAPTER FOUR
Cyber-Security

ABSTRACT

According to the International Air Transport Association (IATA), 20 years from now, the number of annual passengers will nearly double to—get this—7.8 billion people. Thanks to exponential growth in passenger footfalls and air traffic, airports are busier than ever before. And this shift requires airports to become smarter more responsive and efficient to create a seamless airport experience.

Airports are increasingly adopting various digital technologies to manage and improve the performance of airport on resource consumption, carbon emissions and quality of end-to-end passenger journey.

This graduation project explores the concepts of smart airports and IoT technology. The primary aims of this project are to study some specific technologies that have a major impact on the evolution of smart airport. The internet of things (IoT) technology forms the basis for this project since we think it's the primary technology behind smart airports. By connecting particularly physical assets, devices, people, and applications, IoT is playing a vital role in driving operational efficiency, improving the passenger experience, and creating new revenue sources for airports. The project further focuses on the role of specific digital technologies, including blockchain, biometrics, indoor positioning systems, cloud computing and big-data, in smart airports.

The research methodology of this project is based on quantitative literature study, and concentrate on large data analysis, including whitepapers, articles, press releases, annual reports, and various studies.

Keywords:

Smart Airport, Digital Transformation, Digitization, Technology, Internet of Things, IoT, Cyber-security.

List of Figures

List of Tables

Acronym Glossary

IATA	International Air Transport Association
IoT	Internet of Things
CUTE	Common Use Terminal Equipment
CUPPS	Common Use Passenger Processing Systems
B2B	Business to Business
SST	Self Service Technology
B2C	Business to Customer
CUSS	Common Use Self Service
CCTV	Closed-Circuit Television
H2H	Human to Human
H2M	Human to Machine
M2M	Machine to Machine
AR	Augmented Reality
ATM	Air Traffic Management
A-CDM	Airport Collaborative Decision Making
ATC	Air Traffic Control
ACI	Airport Council International
API	Application Programming Interface
CATSR	Center for Air Transport Systems Research
ENISA	European Union Agency for Network and Information

COMM's	Communication Management System
ISO	International Organization for Standardization
BLE	Bluetooth Low Energy
RFID	Radio frequency Identification Tag
3G	Third Generation (Mobile Communication System)
4G	Fourth Generation (Mobile Communication System)
LTE	Long-term Evolution (A 4G Mobile Communication Standard)
GPS	Global Positioning System
IPS	Indoor Positioning System
UWB	Ultra-Wideband
R&D	Research and Development
DNA	Deoxyribonucleic Acid
FRT	Facial Recognition System
TEE	Trusted Execution Environment
AI	Artificial Intelligent
ICS	Industrial Control Systems
AOS	Airport Operating System
FIDS	Flight Information Display Systems
EASA	European Union Aviation Safety Agency
CCTC	Community Cyber Threat Center
SOC	Security Operation Center
A-ISAC	Aviation Information Sharing and Analysis Center
ISH	Information Security Hub

Acknowledgment

We would like to use this opportunity to express our sincere gratitude to our family for encouraging us in all of our pursuits and inspiring us to follow our dreams. We are especially grateful to our parents, whose love and guidance are with us in whatever we pursue, they have given us all the riches that life could offer, and without them, we would never be where we stand today. We cannot thank them enough for instilling us with a strong passion for learning and for doing everything possible to put us on the path to greatness. They have given us the greatest gift of all: an education, the best legacy that parents can pass on to their children. We are forever grateful for their undying love, and unconditional support.

And we would like to express our special thanks of gratitude to our supervisor Assistant Professor Hakan Rodoplu for all the support and encouragement he gave us, throughout our time in undergraduate school. We have been blessed by his willingness to be our supervisor, and we appreciate his contributions of time and ideas to make our work productive and inspiring. We are also indebted towards him for his generosity, endless support and especially for his marvelous sense of humor.

The Project's Structure

This graduation project is divided into six main sections: Introduction, smart airport, IoT and other enabling technologies for the smart airport, key players in the global smart airport market and smart airport initiatives, cyber-security, and conclusion. The introductory section briefly introduces the project topic. It shortly discusses key concepts such as the smart airport, and the internet of things (IoT). Chapter one present a full definition of the concept of the smart airport, and further explained the smart airport stakeholder groups and the core assets of the smart airport. Chapter two offers insight into the concept of IoT and some other specific technologies that have a significant impact on the evolution of the smart airport.

Chapter three briefly discuss the key players in the global smart airport market, and also presents some of the most innovative smart airport initiatives which many airports around the world are adopted. And finally, chapter four provide a valuable inside into cyber-security challenges that threatening the smart airports. At the conclusion section, we concluded this graduation project. The thesis structure is shown in Figure 1.

Project Structure	
Introduction	• Introduce the concept of the smart airport • Briefly explain the projects goal
CHAPTER1: Smart Airport	• Presents a full definition of the concept of smart airport and its stakeholder.
CHAPTER2: IoT and other Enabling Technologies for The Smart Airport	• Discuss about IoT and some other specific technology.
CHAPTER3: Smart Airport Initiatives and key players in the Global smart Airport Market	• Discuss about key players in the smart airport market. And smart airport initiatives
CHAPTER4: Cyber-Security	• Provide a valuable inside into cyber-security challenges that threatening the smart airports
Conclusion	• Conclusion of the project

Figure 1. Project's structure

Introduction

When the Wright Brothers took to the sky on December 17, 1903, the world population was almost 1.6 billion. Today the global population are over 7.5 billion and the number of people who flew last year was over 4 billion. Based on current trends, world population numbers will reach 8.7 billion by 2035, and 7.8 billion people are projected to fly by this year.

Thanks to the exponential growth of passengers, the airport's physical and IT infrastructures face a tipping point because they were not designed to handle such a large volume of passenger and diversity of airport customer demands that airports are facing today. These high demands are driving the necessity for more efficient smart airport infrastructure. Smart airports are eco-systems that integrate airlines, logistics, government authorities and other vendors and stakeholders in the airport management system via the digital network. The digital network is the nervous system of the smart airport which touches and controls every interaction point through real-time exchange of data, process integration, high-level security, and collaboration. Smart airports enhance and personalize customer experiences and anticipate services based on their demands.

In order to handle the increasing number of passengers, and cargos in an economical and effective way as well as creating environmentally friendly infrastructure and products, plus meeting the rising security standards required worldwide smart airports are also setting themselves up with a focus to integrate new technologies into their physical infrastructure. In a nutshell, smart airports have placed technology at the heart of its commercial strategy and significantly adopted new technologies such as the internet of things (IoT), advanced biometric systems, big-data, blockchain, cloud computing, BLE-beacons and so on.

The internet of things (IoT) has emerged as a solution which brings together airports, airlines, service providers, vendors, and customers in an ecosystem where systems and processes are interconnected and digitally aware. It has the incomparable ability to combine technology, people, processes and culture to deliver a seamless air travel experience. It has an enormous potential to bring radical changes to airport business models.

This graduation project focuses on explaining the concept of smart airport, some specific technologies which may have an important role in the evolution of smart airport and also the challenge of cyber-security in smart airport. More specifically the aim of this graduation project is to define the concept of the smart airport and the internet of things (IoT).

CHAPTER ONE

Smart Airport

Introduction

Challenges such as inflexible resource allocation, limited ability to expand space, customer dissatisfaction, alongside with some other challenges have pushed airports to leverage emerging technologies, become smarter and be more efficient, and has revealed to the aviation industry a new concept: the "Smart Airport." Does this concept have a specific definition? How can we distinguish a smart airport from the traditional airport? In this chapter, we tried to provide a full explanation of the concept of the smart airport and also the smart airport's stakeholder groups and the core assets of the smart airport. In an attempt to define the smart airport, this chapter also discusses the stages of airport digital transformation from the basic implementation of CUTE rules at Airport 1.0 up to Airport 4.0 where physical systems are designed to assist human’s unkind or hazardous work, to take decisions and to complete tasks autonomously.

1. A Brief History

Airports are going through a profound digital transformation as they emerge from distinct IT systems to connected smart airports, which harness the advantages of digital platforms, big data, cloud, IoT, and collaboration. Over the past few years, a number of new concepts like connected aviation, the airport of the future, intelligent and green airport, the self-service airport and the smart airports come into common usage in the aviation industry. All of these concepts relate to the ongoing digital transformation of airports. Digital transformation for the airport is about developing services and processes to deliver a better customer experience and improve efficiency in daily operation — benefits that are fundamental to the value offered by airports to their customers.

Airports across the world are confronted with the challenge to transform themselves from infrastructure managers to service providers in order to compete successfully in the global market. This transformation is driven by digitalization. While so far, the role of technology was limited in just supporting the business process and thereby enable airports to realize their business models effectually, digital transformation means that new business models are developed around the technology itself (ACI, 2017: 8).

In recent years, we heard a lot of buzzwords in the airport industry, and somehow all these buzzwords are related to the term digitization. The digitization process in the airport industry started back in the 1980s when airlines and ground handlers have shown interests in sharing IT facilities across the airports to reduce the necessary investments when starting new routes, seasonal and charter flights in particular. Meanwhile opening new space and recruiting new check-in agents in the airport was costly and harder to find for airport operators. Hence, through mutual interest for airports and airlines, CUTE (Common Use Terminal Equipment) provides the opportunity to significantly reduce the space needed in order to install check-in desks and to dividing up the necessary investments between the airport and all the airlines using these desks. Back at that time, the main aim of deploying the CUTE system was to support high demand from the 1984 Olympic Games in Los Angeles.

However, the CUTE system proved to be useful and quickly embraced by multiple airports across the globe especially in international terminals used by various airlines.
This huge deployment of CUTE is considered to be the first wave of digitization in the airport industry and carried on until the beginning of the 2000s (Nau and Benoit, 2017: 22-26).

The first wave of airport digitization was then followed by the self-service check-in implementation in airports across the world at the beginning of 2003. Self-service check-in solution offered a great opportunity to replace the check-in agents and accelerated the passenger check-in process. This wave which is also known as the second wave of digitization in the airport industry carried on in different airports across the globe, particularly in the countries where the labor cost is very high such as European countries, US, and some Asia-pacific countries. It is to be noted that by the end of 2018, 98% of the airports in the world were equipped with at least one self- check-in kiosk (SITA, 2018).
The developing of Common Use Passenger Processing System (CUPPS) also started in this wave of digitization. CUPPS was specifically developed to efficiently incorporate new technologies and enacted to allow various airlines, handling agents, service providers and other stakeholders to share physical areas on or off airport simultaneously and consecutively. CUPPS was approved and made available in 2009 to replace the CUTE, however, CUPPS never worked in a way that it was expected, therefore CUTE has never been fully retired, even today it is estimated that more airports are using CUTE than CUPPS (Nau and Benoit, 2017: 22-26).

The Third wave of airport digitization took place at the beginning of 2010. It included massive deployment of self-service machines throughout the passenger journey across the airport: for border control, boarding and luggage deposit. This massive deployment of self-service considered to be an important breakthrough for the customer experience: passengers gain more control over their travel experience. Giving passengers the opportunity to do more of the airport processes themselves by taking advantage of the digital self-service options, helped passengers to better manage their time in the airport (Nau and Benoit, 2017: 22-27).

Following the wave of self-service (Third Wave) the fourth wave of digitization in the airport industry started in mid-2012. This wave of digitization also known as IoT-based transformation is still at its very beginning and is embraced by very few airports around the globe. The fourth wave of digitization is dominated by the replacement of the old mechanism by electric devices. Four powerful technologies are driving this wave: The internet of things (IoT), cloud computing, blockchain, and big-data.

These four waves of digitization are closely related to the adoption of higher levels of automation by airports.
We can distinguish airports according to their digital maturity, based on these four waves of digitization. Meanwhile, these four waves of digitization led to the evolution of four types of airports which explained as which is characterized as follows (Nau and Benoit, 2017: 23);

Airport 1.0: Typically, they offer basic customer services, and almost all processes are done manually. These types of airports operate in a landlord model where the airport provides the land, and normally run a B2B business without any service sold directly to the travelers. IT implementation is limited to specific solutions such as CUTE.

Airport 2.0: Self-service and the massive deployment of CUTE are the main factors that define this type of airports. Self-service implemented partially and is limited just to check-in process, additionally wireless communication technologies such as Wi-Fi being deployed in these types of airports.

Airport 3.0: Self-service technology (SST) is used across the passenger journey at all levels. In most cases, operation management is automated, and mobility solutions are massively deployed both on the terminal side and airside. CUPPS is partially deployed in this type of airports.

Airport 4.0 (Smart Airport): Airport 4.0 features "Smart Airports" that fully exploit the power of transforming technologies such as the internet of things (IoT), big-data, blockchain and cloud computing to enhance the passenger experience and operational efficiency. Airport operators in this type of airports try to create value out of data which is collected by the sensors (IoT) that are deployed across the airport. The systems in this type of airports are built around technology which enables the exchange of real-time information and collaboration between all airport stakeholders. In this particular type of airport, airport operators try to shift their business from B2B to B2C.

BUSSINES TYPE

B2C

SMART AIRPORT

AIRPORT 4.0

- Fully-connected with all stakeholders; higher proactivity and reactivity to adapt to the real-time airport requirements.
- Airport systems are fully integrated within the ecosystem using new technologies
- Using real- time data for a better comprehensive way to analyze passenger profile and generate ancillary revenues

AIRPORT 3.0

- Initiatives to leverage digitalization to optimize flow monitoring and passenger processing.
- The use of digital solutions to improve operations, optimize the usage of resources and enhance the passenger experience
- Self-service fully deployed across the terminal

AIRPORT 2.0

- Implementation of self-service thanks to the automation of some key flow processing tasks (bag-drop, passport check)
- The main objective of this level of digitalization is process automation and cost reduction.
- CUTE is fully deployed and CUSS is set for few airlines

AIRPORT 1.0

- IT is used to run basic services
- Computerized process but manual intervention is required
- Long delay-times between resource requisition and airport demand

B2B

Figure 2. Airport Evolution

1.1. Airport Transitions Between Different Digital Level

Challenges in the aviation industry are the main factors that drove the airport transitions between different digital level. Though, each challenge motivates the choice to move from one level to another differently. For example, the transition operated from 1.0 to 2.0 digital level is motivated completely by the will to achieve operational efficiency, enhance the processes and reduce costs, while starting 2.0 grade, the main goal turns onto the customer: to increase financial success, generate new revenue sources and enhance the customer experience (Nau and Benoit, 2017: 25-28).

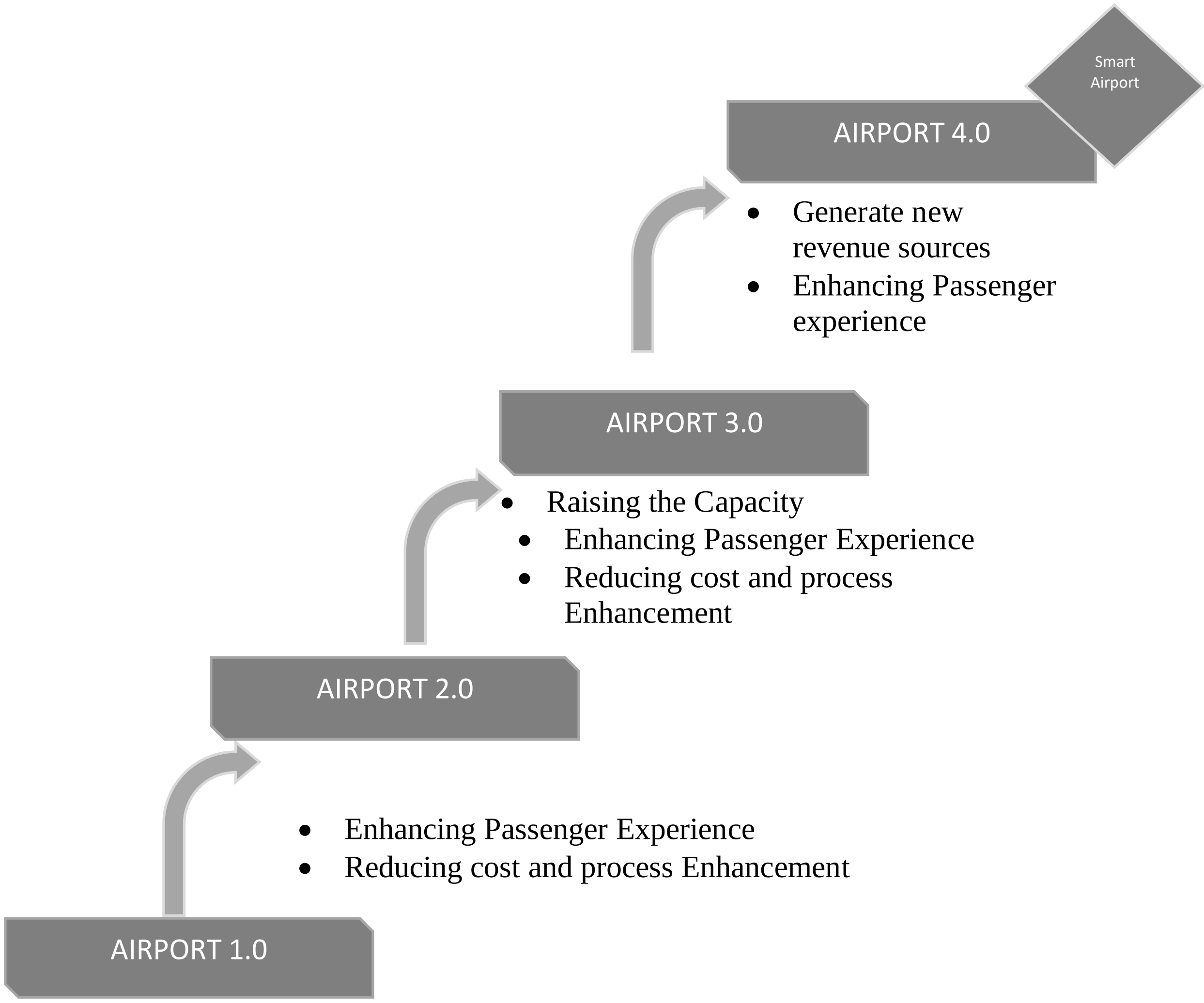


Figure 3. Airport Transitions Between Different Digital Level

2. Defining the Smart Airport

A smart airport is the centerpiece of an interconnected city region with associated smart technologies, intelligent infrastructure and intelligent mobility. Indeed, the smart airport is a determinative subsystem of the smart city, where technology-enabled collaboration is highly evolved throughout the airport. With advanced and pervasively deployed technologies, airport stakeholders share information instantly and seamlessly, enabling smart airports to respond quickly to environmental and operational changes. Literally, a smart airport is a data-rich environment, populated by a range of sensors, actuators and other embedded devices that allow customers to interact with almost every object across the airport. Using intelligent, integrated solutions, ecosystem partners inside and outside the smart airport receive real-time updates on the progress of the passenger's journey and are able to offer services, goods, and transportation based on their travel status. Airport stakeholders such as taxi, hotel, and car rental firms receive the necessary information in case of any delays and make adjustments to their operations in real time. With visibility into the passenger's end-to-end journey, they are able to improve the services they offer and to enhance customer comfort.

In other words, smart airport is the one that knows where its staff is in real-time, including the ability to communicate in real time with all stakeholder to assure that the right services and people are on the right flights at the right time, while assuring traveler security and keeping everyone informed in case of any disruption or changes (SITA, 2011: 7). Furthermore a smart airport knows who its customers are, what is their needs and when they are traveling, so that it can provide personalized service to the customers and also can predict peak demands, plan staff utilization, help customers navigate from long-term parking to the boarding gates in real-time, reduce queues throughout the terminal and also be able to maximize non-aeronautical revenues by marketing the 'right' products to the 'right' passenger at the 'right' time based on their location and preferences and with their approval. To put it simply a smart airport is an airport which fully exploits the power of emerging technologies such as the internet of things (IoT), big-data, mobile apps, to make smarter use of the infrastructure, and enhance the customer experience.

The smart airport aims to modernize, attract traffic, increase operational efficiency and enhance the customer experience. Technology and management vision are the most essential component in delivering each one of these.

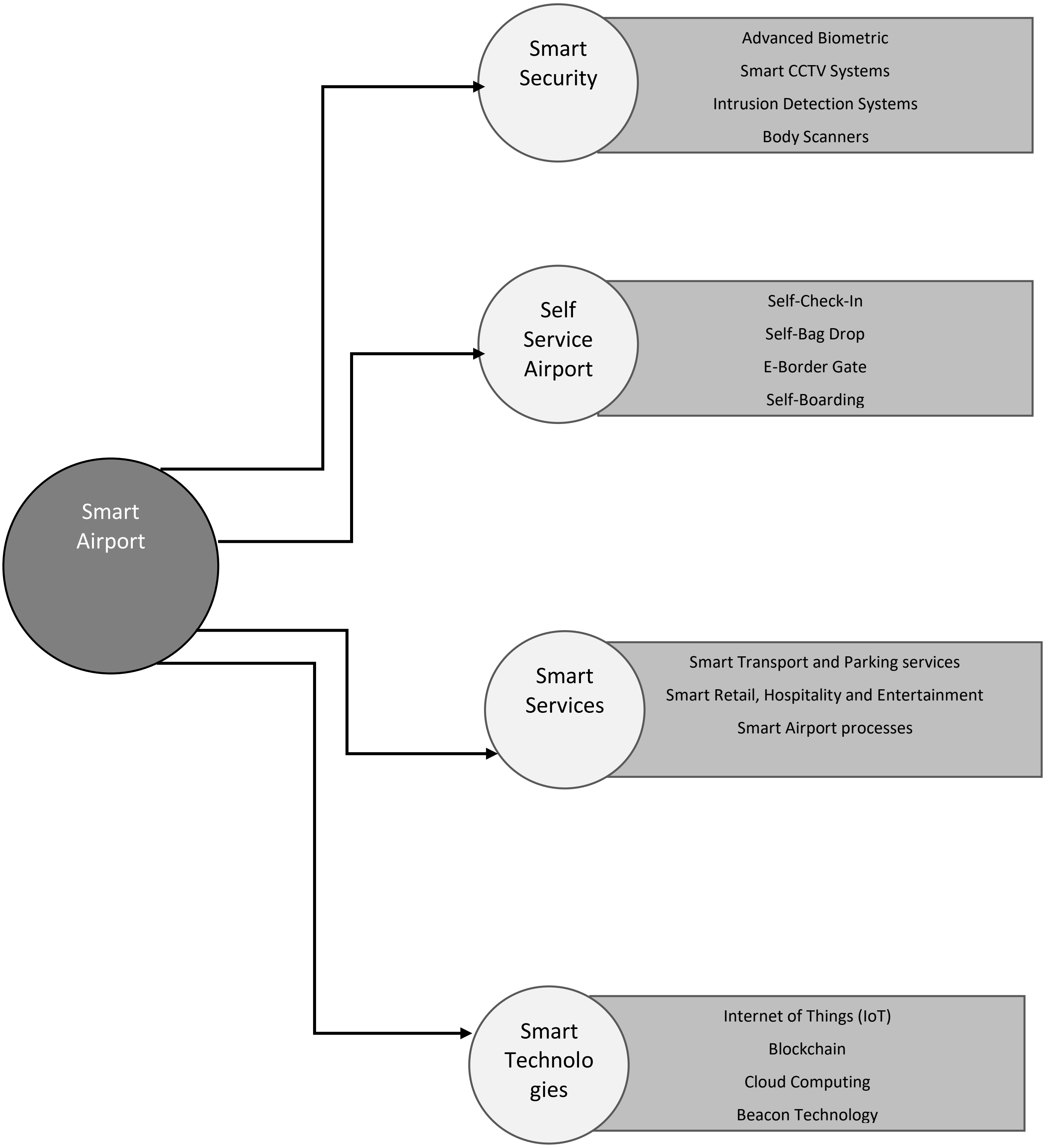


Figure 4. Smart Airport

2.1. Technology is the Backbone of Smart Airport

Technology has had an important role in the development of civilization and society. From burning furnaces of the industrial revolution in Europe to the astronomical prowess of the ancient Sumerian and Hindu civilization, technology has always been the foundation of our evolution. The invention of simple machines like a calculator and the telephone couldn't have been achieved without the advancement of technology. Today, all over the world people are surrounded by technology in one way or the other. In past decades technology has played a leading role in the development of the aviation industry particularly the airport industry, however with growing customer expectation, the role of digital technology has also changed, it's no longer a commercial tool used to attract and retain airlines, in the smart airport, technology is at the heart of every approaches to address passenger demands. Indeed, smart airport is a concept of utilizing technologies and connected objects (sensors) to enhance the passenger experience and making more smarter use of the infrastructure.
According to a survey done by SITA utilizing new technologies not only help airports to optimize resources and reduce costs but make the passengers happier. Not surprisingly this survey also shows that technology helps passengers experience positive emotions while traveling (SITA, 2015).
Through more customer-focused use of technologies, smart airports are evolving into a digitally enhanced entertainment center, where all airport stakeholders are collaborating with each other in real time to offer travelers new levels of convenience and enjoyment.

We can divide digital technologies into three groups based on their level of priority for smart airports (Russel and Blondel (n.d.): 19-22).

First Group: Core Enabling Technologies

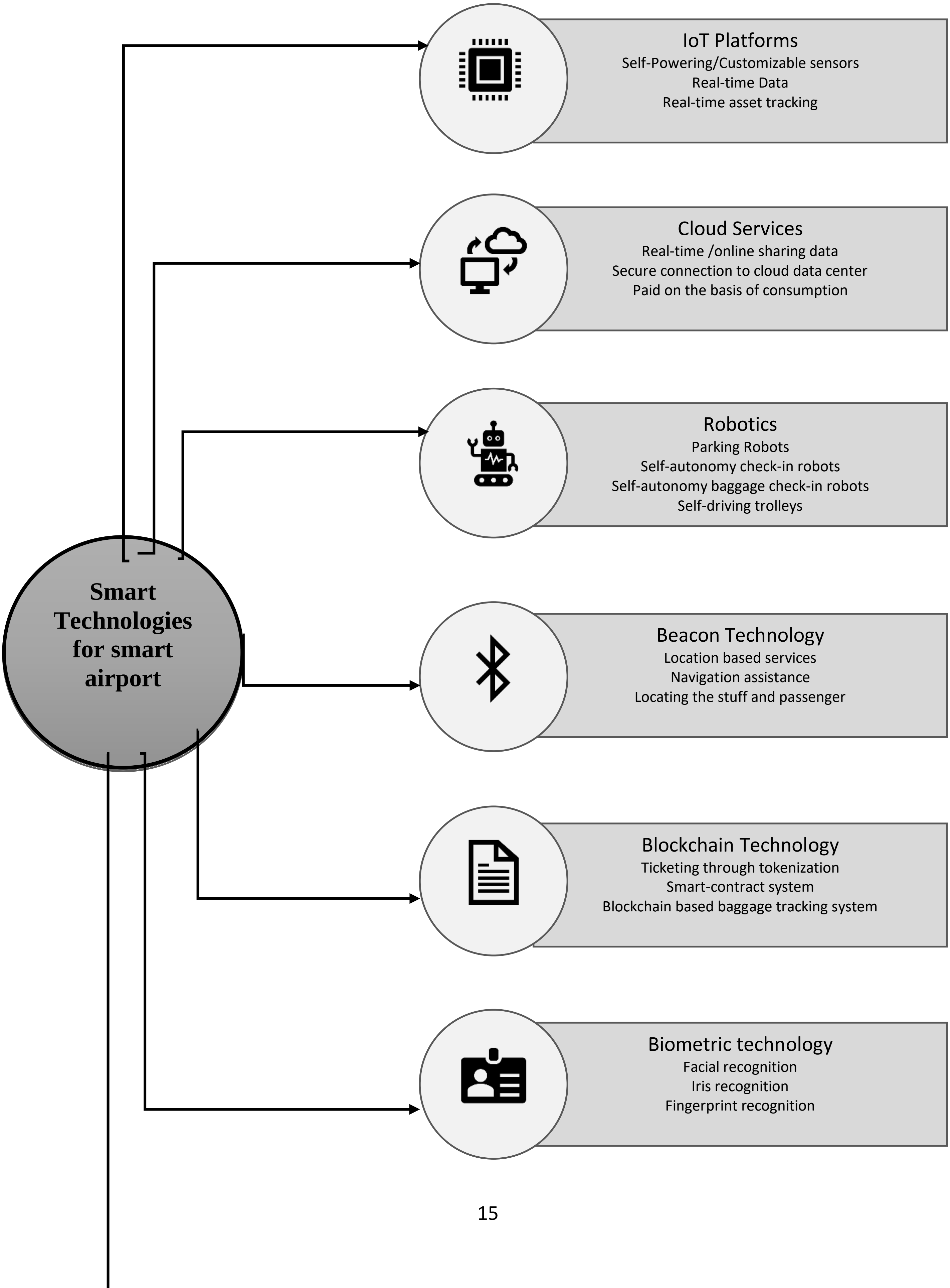
As explained in the above section, advanced analytics, cloud computing, and big-data have played a leading role in the transition from Airport 3.0 to Airport 4.0 and will remain a primary focal point for smart airports digital strategies.

Second Group: Process Automation and Integration

The internet of things (IoT), artificial intelligent (AI), robotics, and mobile technology are the four digital technologies which stood out as being pivotal to the ongoing efforts of smart airports to improve the efficiency and effectiveness of their operations, and will continue to break down organizational boundaries and enhance data sharing, including across human-human (H2H), human-machine (H2M) and machine-machine (M2M) interfaces.

Third Group: Cutting-edge Technologies.

This groups of technologies including augmented reality, autonomous transport systems, are not a high priority for all airports, however, some technologically mature global hubs showed interest to invest in this kind of technologies.


IoT Platforms
Self-Powering/Customizable sensors
Real-time Data
Real-time asset tracking
Cloud Services
Real-time /online sharing data
Secure connection to cloud data center
Paid on the basis of consumption
Robotics
Parking Robots
Self-autonomy check-in robots
Self-autonomy baggage check-in robots
Self-driving trolleys
Smart Technologies for smart airport
Beacon Technology
Location based services
Navigation assistance
Locating the stuff and passenger
Blockchain Technology
Ticketing through tokenization
Smart-contract system
Blockchain based baggage tracking system
Biometric technology
Facial recognition
Iris recognition
Fingerprint recognition

2.2. Smart Airports Enhance t

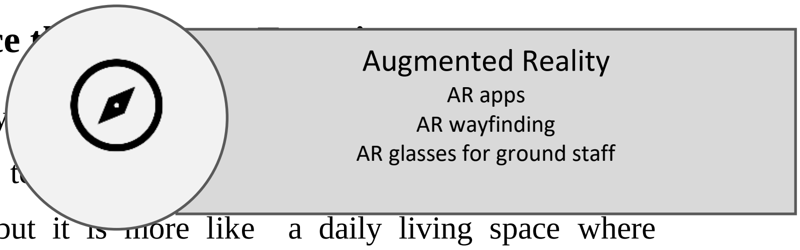


Figure 5. Smart Technologies for smart airport

Airport experience is a relatively airport is no longer a place only t baggage and wait for a flight, but it is more like a daily living space where customers can shop, arrange meetings and be entertained and even in some airports like Changi people are coming to the airport just to take a rest and read a book or using its free Wi-Fi for doing their homework's. Traditionally the physical interaction between airports and its passenger has been defined the passenger experience. However smart airports opened a new era in passenger experience. Physical interaction at the security check, check-in, and boarding are no longer define the passenger experience. Instead, smart airports have maintained a strong and widespread connection with the passenger to interact with them anytime and anywhere. Such capabilities enabled all airport stakeholders to provide relevant information and personalized services to the passenger. Unlike traditional airports, smart airports have reached beyond their physical boundaries to enhance the passenger experience at all stages of their trip this includes online interaction with the passenger. For example, Athens International Airport (ATH) using Facebook Messenger to provide flight updates, retail offers and a variety of ancillary services to the passenger. Passengers can log in to Facebook Messenger on their mobile, to receive real-time flight information simply by providing their flight number (Holland, 2017).

2.3. Collaboration

The airport industry's complicated ecosystem is built on collaboration between different stakeholders: airport operators, airlines, service providers, and so on. To deliver a customer-centric experience, airport and its stakeholders need to collaborate in real-time. Collaboration between airport stakeholders will assure the best overall system outcome while addressing the needs of airport actors, the ATM network, individual aircraft operators and the customers who depend on their services. In a smart airport environment all stakeholders, including the airline and customer, are interconnected through airport collaborative decision making (A-CDM) platform, enabling real-time collaboration between all stakeholders which are responsible for managing a flight, in other words the smart airport is a collaboration between the airport and its stakeholders with the ultimate goal of moving passengers and cargo from departure to arrival in a safe, hassle-free timely manner. In this regard, ACDM (Figure 4) has played an important role in airports to complete its transition from Airport 3.0 to Airport 4.0 (Michael and Papiomytis, 2017: 31).

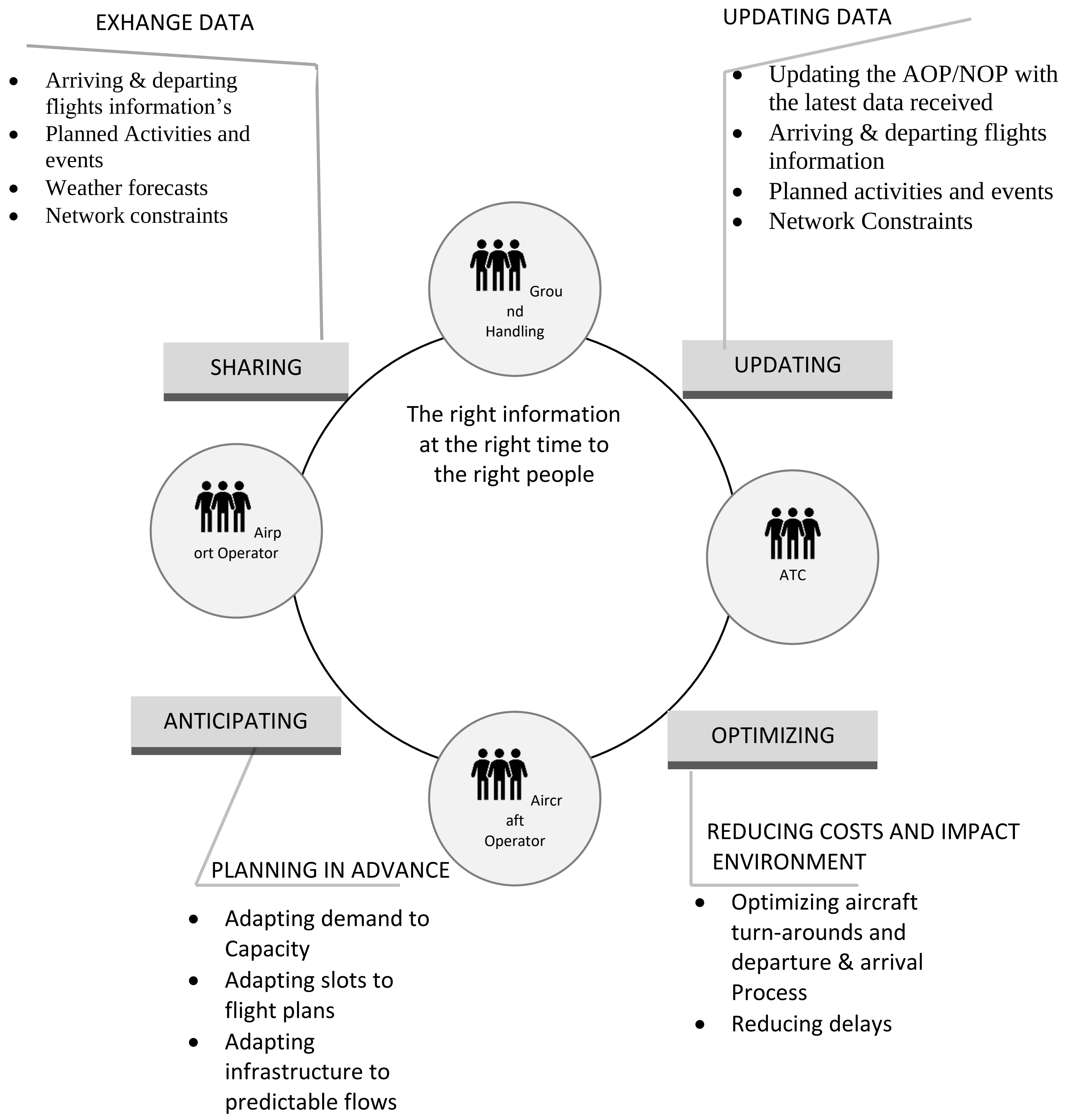


Figure 6. A-CDM Benefits

2.4. Diversifying Airport Revenue

Airport tax and the landing fees were the two sources of revenue for traditional airports (Airport 1.0 and Airport 2.0 in particular). However, knowing the runway capacity and terminal space is limited, airports (Airport 3.0 and Airport 4.0) shifted their business strategy towards non-aeronautical commercial income and ancillary services. According to the Airport Council International (ACI) on average 50% of airports revenue comes from non-aeronautical activities (ACI, 2009: 3).

Thanks to the cutting-edge technologies smart airports have a greater ability to diversify its business. Unlike the traditional airports (Airport 1.0 and Airport 2.0) smart airports shifted from a B2B player (serving ground handlers and airlines) to a B2C player where airports are serving directly to the customer. Since providing services in a B2C mode requires the need to know and understand the customer very well, smart airports have a better understanding of its customer and therefore it can provide more personalized services to its customer.

2.5. End-to-end Passenger Journey

The challenges of balancing the misaligned interests of the different passengers and stakeholders and other factors such as unstable fuel prices and the global financial crisis emphasize the need for reshaping the aviation industry with innovative strategies in order to survive in today's unpredictable economy. Despite incredible growth and the fact that airports are still profitable, they have to face the competition from other airports and the continuously increasing in passenger's expectation, whether they travel for business or for leisure purpose. Accordingly, this will have an impact on the airports revenues too. Today’s passengers expect more from the airports than ever before, meeting that expectations and needs are far from simple, it's very crucial for airports to understand its passengers, in terms of behaviors, demographics, and needs to meet their expectation.

In order to stay ahead of the competition and attract more passengers it is no longer possible for airports to just incentivize on costs. Instead, airports need to collaborate with airlines and other stakeholders to provide better customer experience with taking an integrated approach to every touchpoint along the passenger's end-to-end journey. For instance, airports can offer valet parking to passengers arriving late for a flight, or accommodation services in the case of a delay (Fattah, 2009: 8-11).

The significance of end-to-end passenger experience in aviation has become well understood in the past several years. From an aviation profitability perspective, the provision of end-to-end passenger experience is a necessity rather than an option. The purpose of taking an integrated approach to every touchpoint along the passenger's end-to-end journey is to transform the different steps into one unified customer journey, that makes much easier and quicker to use for passengers. Partly, that means recognizing that the customer experience of a passenger starts at home instead of when they enter the airport.

In building this unified customer journey, the airport's role needs to evolve from a passive landlord to active shareholder, enhancing the customer journey as an important ecosystem partner. For example, Amsterdam Schiphol airport has taken an innovative approach towards providing passengers with a seamless and efficient end-to-end journey that is highly welcomed by passengers. Schiphol International Airport opened a concession which operates a fleet of 167-Tesla model S taxis which are equipped with a tablet and free Wi-Fi and offer door-to-door service to passengers traveling to and from Schiphol airport (Garcia, 2014).

And also, some leading airlines such as United airlines partnered with taxi company UBER to provide an end-to-end travel experience for their customers, for example, passengers can order UBER via the United Airlines smartphone app, at the same time United MileagePlus members can earn United miles for every dollar they spend when purchasing UBER gift cards through the MileagePlus X app (United, 2014).

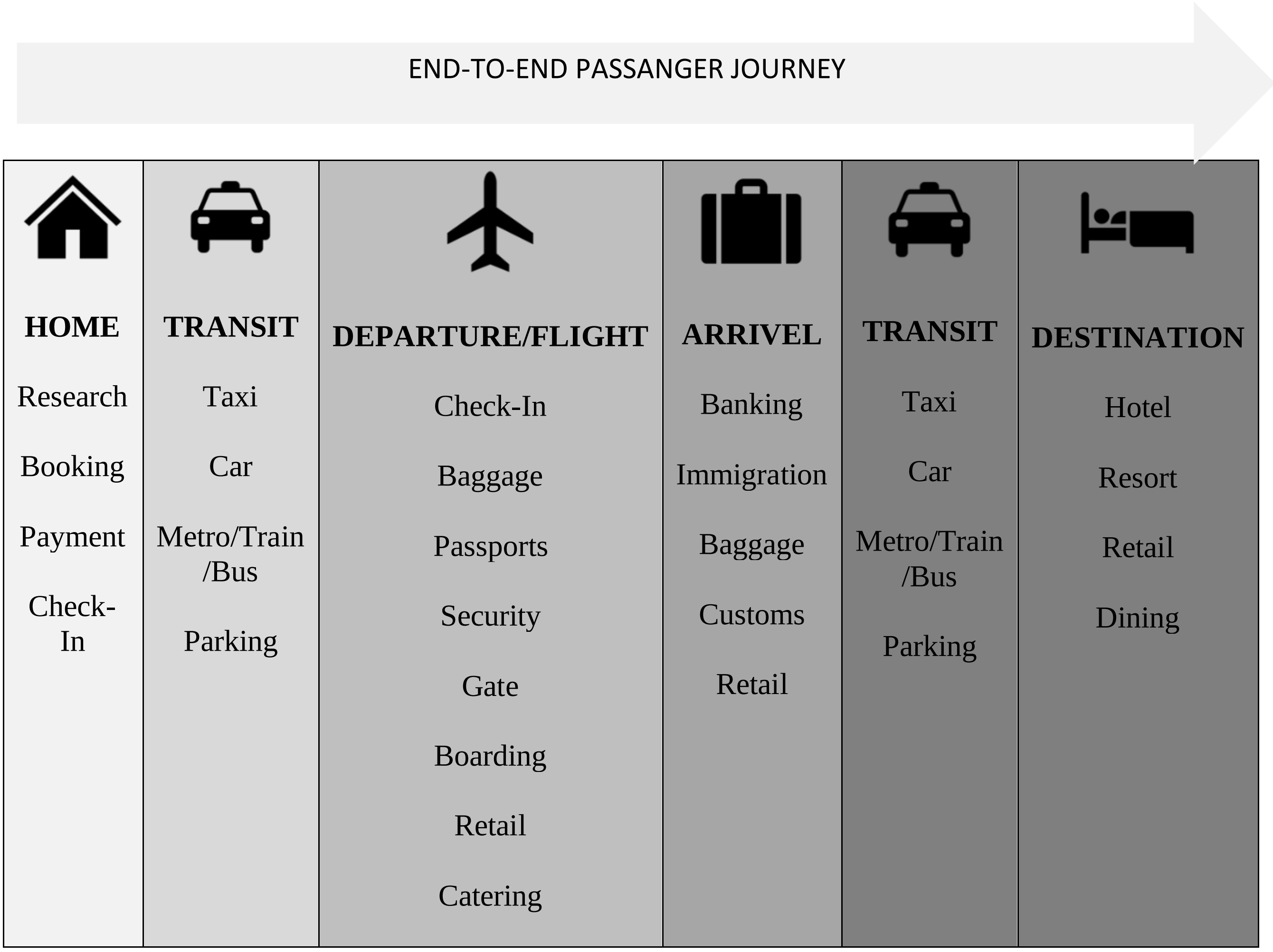


Figure 7. End-to-end passenger Journey

2.6. Multi-Channel Customer Experience

The evolution of new technologies such as the smartphone, wearable devices, and social media has led the airports to readapt their conventional channels of interaction with the customer.

According to the SITA, 97% of air travelers are carrying their own mobile device, for instance, after the website mobile device is the second most used channel for buying extra services or checking flight information (SITA, 2015).

As a result, in order to boost their market share in terms of services sold in terminal or outside (taxi services, parking slots, etc.) smart airport are using different channels that lead to the customer.

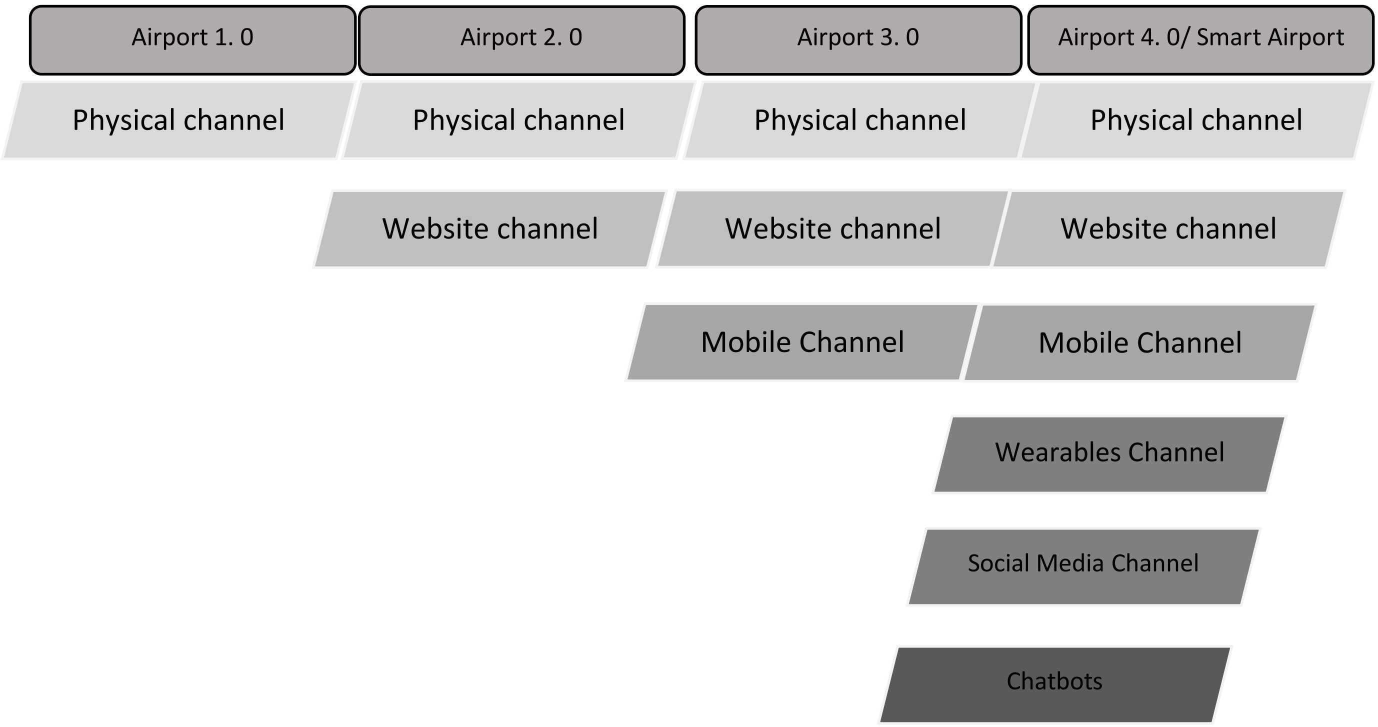


Figure 8. Multi-Channel Customer Experience

2.7. The Smart Airport is Going to Be Driven Through Open API Platforms

To get away from the typical landlord and tenancy relationship with airlines and other stakeholders, and to be a broker of data between airports, airlines, and passengers, smart airports uses open API platforms. Open API platform enables innovation to thrive by opening up airports data to the external world. This open consumption enables many developers to build creative solutions which would not be possible to build by airports alone. To continue this with an example. Schiphol Airport opened up its API platform, allowing the external developers to log into the Schiphol API platform and integrate their services, improving the user experience for both Schiphol customers and their own. TomTom has become the first start-up company which has got real-time insights into departure, delays and waiting times at security, through Schiphol API platform. TomTom uses this information to set up a personalized travel plan for passengers that need to catch a plane. Since TomTom is a navigation company and has an eye on current local traffic conditions too, it can make suggestions to passengers about when to leave their home in order to catch their flight. For additional information about API see appendix 1.

3. Smart Airport Stakeholders

According to the analysis done by the Center for Air Transportation Systems Research (CATSR), when it comes to the function and operations of airports, there are two conceptual stakeholder boundaries, particularly these two distinct boundaries are Airport Organizational Boundary and Airport Service Boundary (Figure 8) (ENISA, 2016: 14).

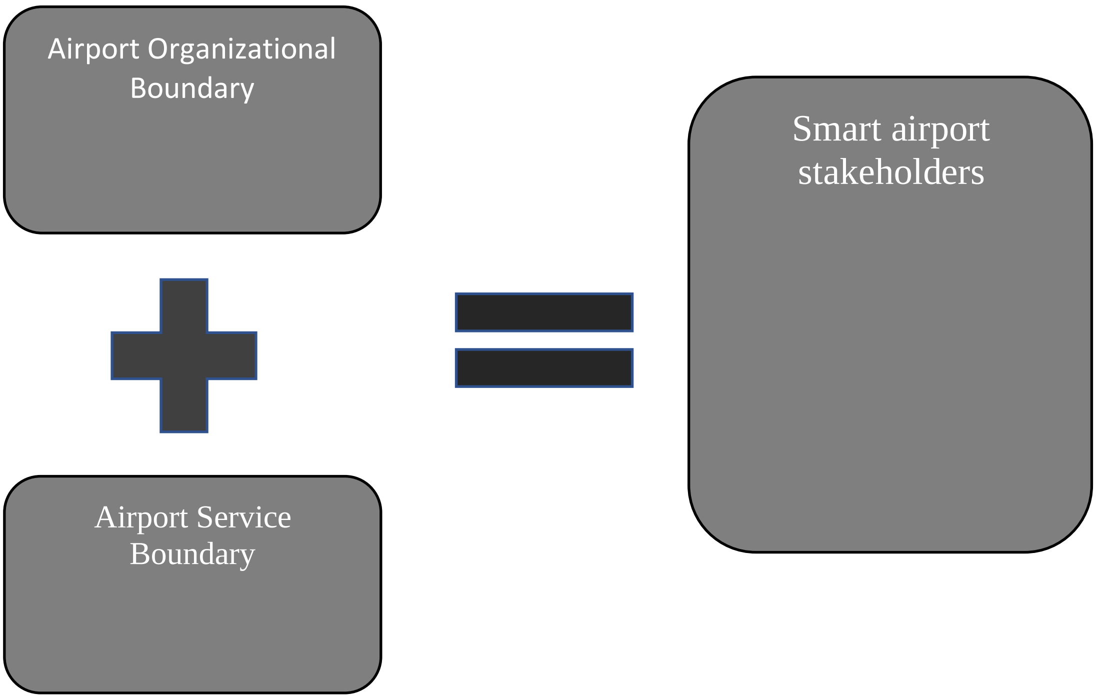


Figure 9. Smart airport stakeholders

3.1. Airport Organizational Boundary

The **airport organizational boundary** shows what is owned or controlled by airport management or authority. These include the design and configuration of airport infrastructures such as IT infrastructure and the operational procedures and processes which underpin the efficiency and effectiveness of its own organization. The groups of this boundary shown in Figure 10 (ENISA, 2016: 14).

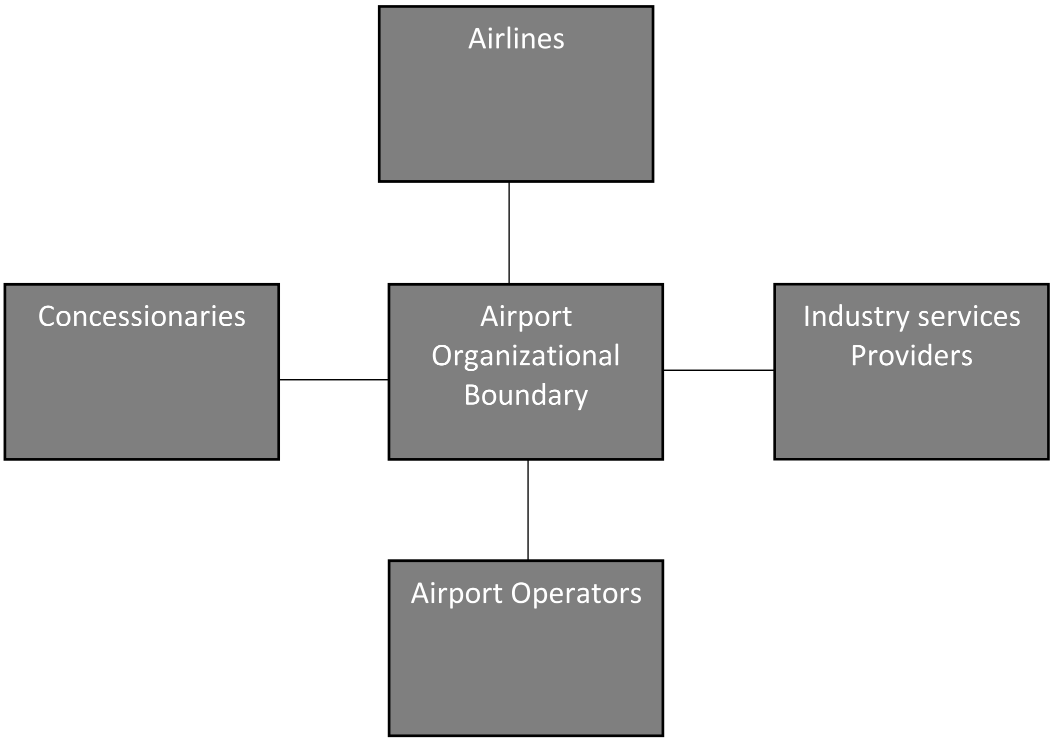


Figure 10. Airport Organization Boundary

3.2. Airport Service Boundary

Airport **Service Boundary** covers the groups which incorporate the airport supply chain and support services that lie outside direct control and management of the airport authority. Among these are IT and support services which are vital to the functioning of the smart airport, it should be noted that IT and support services are mainly operated and maintained by third-party suppliers (Figure 11) (ENISA, 2016: 15).

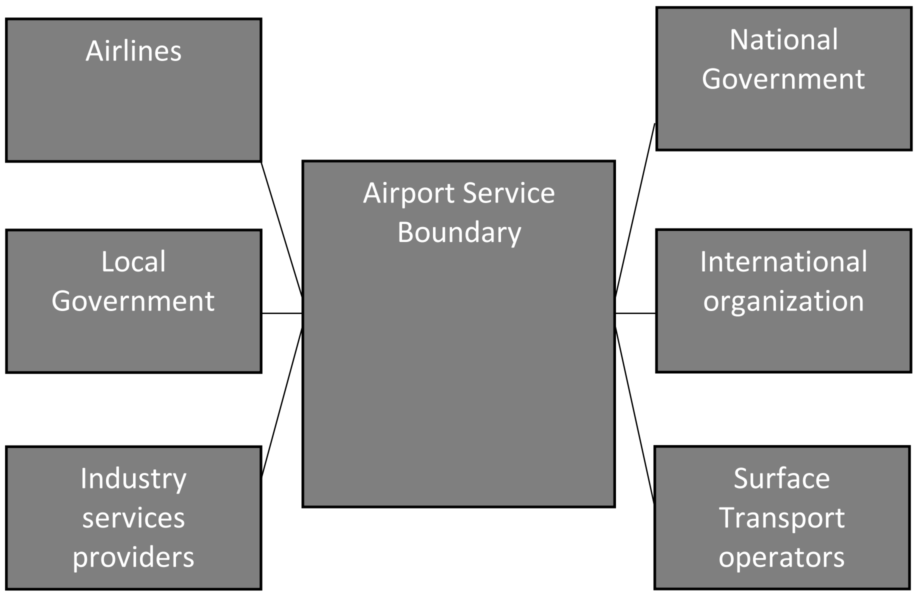


Figure 11. Airport Service Boundary

3.3. Definition of Airport Stakeholder Groups

In order to have a better understanding of the two main boundaries defined in the above section, each identified stakeholder group which contribute to the operation and functioning of the smart airport described as follows:

One of the most important stakeholders is **passengers**; passengers are key customers of the smart airport, who either flying or waiting for a connection between two flights (ENISA, 2016: 16).

Another stakeholder group is **international organizations**, they participate in the airport ecosystem by providing international best practices, regulatory standards for the management of international air-space and operation of the airport (ENISA, 2016: 14).

To continue with, the **national government**, they participate in the airport ecosystem in two different ways: as an operator, concentrating on transportation systems, air traffic control services, security such as baggage handling and screening, and customs and immigration; or as a regulator with regulations applying to airport infrastructure and service providers within airport ecosystems (ENISA, 2016: 14).

On the other hand, depending on the ownership structure **local government** is normally responsible for the strategic direction of the airport in terms of planning decisions and for appointing airport management. And also, it represents the views of local communities and contributes to capital investment projects (ENISA, 2016: 14).

In addition, **industry/ third-party service providers** are a key stakeholder group, which consists of private operators. They offer services both to air carriers and general aviation consumers. These include air traffic management, fuel management, baggage handling and screening, cargo processing services, kiosk devices, way-finding services, transport systems, IT and COMM’s services and security services.

Another stakeholder group is the **surface transport operators**, they provide surface access to the airport these include rail services, taxicabs, buses, private rental cars, and the subway/underground, while parking services may be provided both on and off the airport by the airport's organization or private enterprises (ENISA, 2016: 14).

The **airport operators** are the most important stakeholder groups in the smart airport ecosystem. The airport organizational structure varies and can be comprised of an individual airport or a group of airports managed by the same organization. For example, TAV in Turkey is a single organization that operates Istanbul Ataturk, Izmir Adnan Menderes, Antalya, Alanya Gazipasa and Millas Bodrum airports (ENISA, 2016: 14).

Airlines are one of the other important stakeholder group which provides air transport services for traveling passengers and freight. Airlines use aircraft to provide these services and in some cases form partnerships or alliances with other airlines for codeshare agreements. Usually, airline companies are recognized via an air operating certificate or license issued by a governmental aviation body. The two last groups of stakeholders are the **airport suppliers** and the **concessionaires**. The first group has the airport itself as the end-customer and includes various contractors, equipment and consulting suppliers. As for the second group, it operates passenger services in terminal buildings and may include food and beverage services, retail and accommodation (ENISA, 2016: 14).

4. Core Asset Groups and Assets

In this section, an overview of the core asset groups and assets in smart airports is presented. According to the European Union Agency for Network and Information Security (ENISA), the following are the core asset groups in the smart airport: airport administration, staff management, passenger management, IT and COMM's systems, safety, and security, customer ancillary services and landside operations. Figure 11 shows these core asset groups together with their locations within the airport. Since safety and security, along with IT and COMM's located inside and outside the physical perimeter of the airport, it is identified as a cross-location asset group (ENISA, 2016: 22).

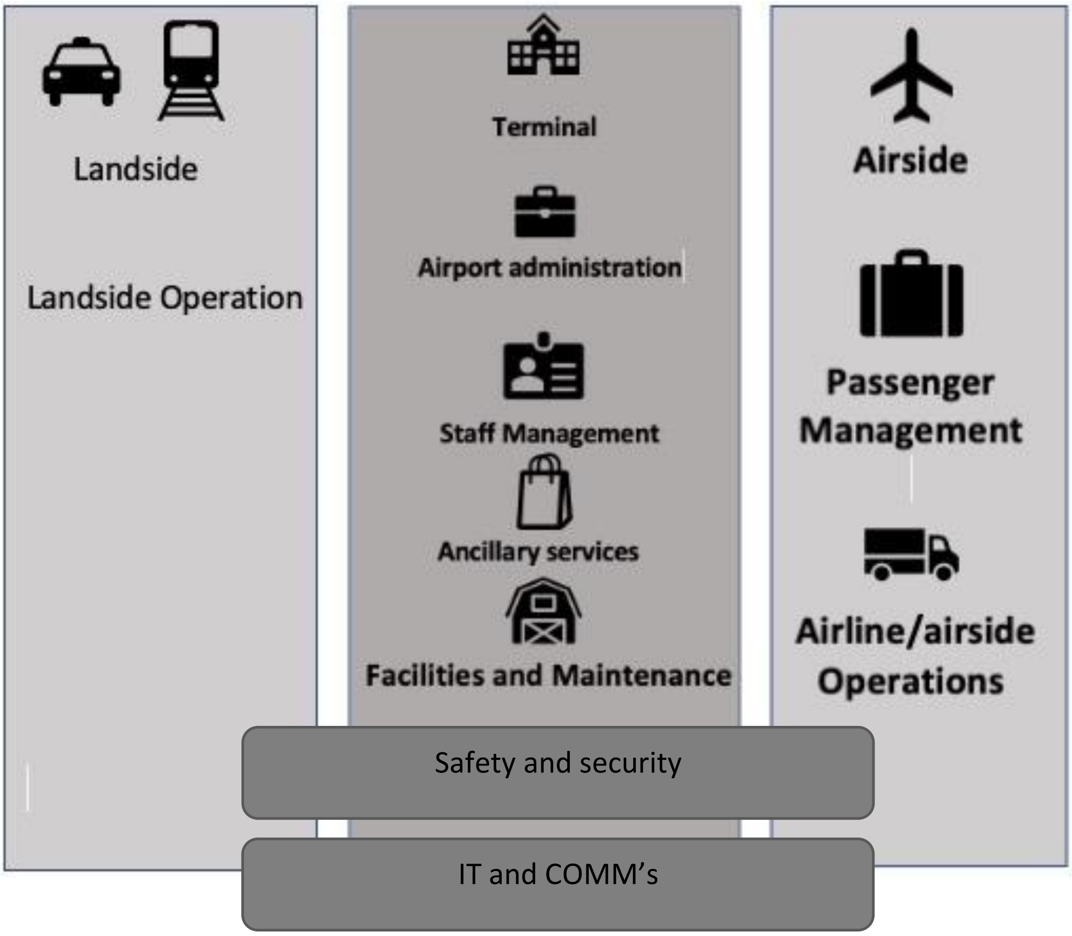


Figure 12. core asset groups and assets

4.1. Core Assets

Based on the asset groups presented in the section above, and ISO 27005, the core assets of the smart airport are categorized into two main categories: **primary assets** and **secondary assets**. These assets are either owned and operated by the third-party service providers or by the airport management.

Generally, primary assets contain of information, business processes, and activities. Primary assets are very crucial to the functioning of an airport regardless of their digital maturity; therefore, mostly primary assets are owned by airport operators. On the other hand, the assets upon which the primary elements rely on are specified as secondary assets. Secondary assets cover all types of deployable systems which enables an airport to execute its primary functions such as hardware, software, network, staff, and site. It's worth to mention that the secondary assets have vulnerabilities which makes it easier for cyber-criminals to impair the primary assets of a smart airport. The assets explained in the table are crucial to the functioning of the Smart airport (ENISA, 2016: 23).

Smart Asset Group	Smart Asset
Airside/Airline Operation	Communication, Navigation and Surveillance (CNS)
	De-icing Systems
	Departure Control Systems (DCS)
	Flight Tracking Systems
	Local DCS and Weight and Balance
	Meteorological Information Systems
	Portable Aircraft Data Loader
	Cargo Processing Systems
	Airport Resource and Infrastructure Management Systems
	Airport Operation Database (AODB)
	Airline Gateway Server Systems
	Systems (including distance measurement equipment)
	Airfield Lighting and Railway Control and Monitoring

	Aircraft Refueling Systems
	Air Traffic Management (ATM), Navigation Aid and Approach
IT and COMMS (Internal)	Local Area Network (LAN) & Virtual Private Network (VPN)
	Passenger Wi-Fi
	Mobile Network and Apps
	Data Centers
	Security Operation Centre (Inc. Computer incident response team)
	IT Equipment (Hardware & Software)
	IT Log Monitoring and Event Notification
	Flight Display System & Management
	Communications Systems e.g. Radio Spectrum Management Systems
IT and COMMS (External)	Wide Area Network (WAN)
	Passenger-Airline Communication Systems
	Network Security Management
	Global Positioning System/ EGNOS/ SBAS/ GBAS
	Geographic Information Systems (GIS)
	Common Communications Network
	Cloud-based Data and Application Services
	Air to Satellite Communication Systems

Airport Administration	Human Resources Management System
	Financial Management System
	Enterprise Management System (including risk systems)
	Asset Inventory Management System
	Policy Management System
	Procurement Management System
Passenger Management	Central Reservation System (CRS)
	Electronic Visual Information Display Systems (EVIDS)
	Kiosk Devices (e.g. e-Ticketing)
	Logistic Systems, within airport
	Passenger Check-in and Boarding
	Passenger Name Records (PNR)
	Stationary Devices (e.g. Desktops, laptops, etc.)
	Stationary Devices (e.g. Desktops, laptops, etc.)
Landside Operations	Lighting Detection Systems
	Parking Management System
	Public & Non-Public Transport Systems (e.g. Railways)
	Way-finding Services (on-airport, off-airport access roads, parking)
	Fuel Management
	Automated Vehicle Identification (AVI)
	Automated Electronic Parking Toll
	Airport Landside Operations Systems Control Center

Customer Ancillary Services	Mobile Payments
	Point-of-Sales Machines
	Private flight, VIP and disability support services
	Commercial cross management services (e.g. Duty free, catering, etc.)
	Automatic Teller Machines
Facilities and Maintenance	Airport Vehicle Maintenance
	Building Control Systems
	Computerized Maintenance Management System (CMMS)
	Elevators, Lifts, Walkways and Air-bridges
	Energy Management (Inc. generators)
	Environmental Management Systems (Inc. wildlife, noise. Environmental conditions, drainage systems
	SCADA (Aprons, Ancillary Areas) SCADA (Roads)
	SCADA (Utilities)
Safety and Security	Customs and Immigration
	Emergency Response Systems (Inc. immigration emergency and plan)
	Fire Fighting Services and System
	Improvised Explosive Detection Systems (IEDs)
	Passenger Screening Systems
	Perimeter Intrusion Detection Systems (PIDS)
	Smart Surveillance Systems E.g. Smart CCTV, Camera,
	Access Control Systems
	Authentication Systems
	Badging Systems
	Baggage Handling System

	Baggage Screening System
	Common-Use Passenger Processing Systems (CUPPS)

Table 1 Core Asset Groups and Assets of smart airport

Chapter Two

IoT and other Enabling Technologies for Smart Airports

Introduction

Technology has played an important role in the airport industry over the last decades. From mobile booking to self-service check-in kiosks, mobile-enabled passenger services, automated boarding gates and automated passport kiosks complete with advanced biometrics, technology has revolutionized the way airports interact with passengers. Airports that are turning “smart” has placed technology at the heart of its commercial strategy and significantly adopted new technologies such as the internet of things (IoT), advanced biometric systems, big-data, blockchain, cloud computing, BLE-beacons and so on. These technologies are playing a central role in the transition from Airport. 3.0 to Airport 4.0 (smart airport). In this section, we explore some of the specific technologies that have a significant impact on the evolution of the smart airport.

1. Internet of Things (IoT)

The internet of things (IoT) is a promising topic of economic, technical and societal importance. It has the potential to considerably drive technology, business, and economic growth over the following decade. The IoT is intended for omnipresent connectivity between various objects, also called things. There is an end-to-end integration between these objects and with the human. These objects become a part of our life that interact smartly with each other to do everyday operations and simplify human life (Evans D. 2011: 1-5). The IoT can be explained from different perspectives. From the **perspective of connectivity**, it is for anyone from anytime, in anywhere, connectivity for anything. And, from the **perspective of communication**, it is a worldwide network of interconnected objects (things) uniquely addressed based on standard communication protocols. From the **perspective of networking**, it is the internet developed from a network of connected computers to a network of interconnected objects. Finally, From the **perspective of services provided by objects**, it is a world where objects automatically communicate with computers and one another (a process called Machin-Machine communication) to provide services for the interest of the human being (ILNAS, 2018: 12-15).

Overall, it refers to the business process and applications of sensed data, information, and content generated from the interconnected world by means of connected devices that exist in the internet infrastructure.

While the internet of things (IoT) will ultimately have a huge impact on customers, companies, and society as a whole, it is still at an early stage in its evolution. Adoption of IoT technology in various domains, such as airports, transport systems, logistics, airlines, and air cargo improve their current operational effectiveness and interaction with the consumers. IoT has the incomparable ability to combine technology, people, processes and culture to deliver a seamless air travel experience. It has an enormous potential to bring radical changes to airport business models. For example, tracking devices, wearables, virtual steamers, beacons are enablers in streamlining the passenger's journey from the point they enter the airport till the time they depart.

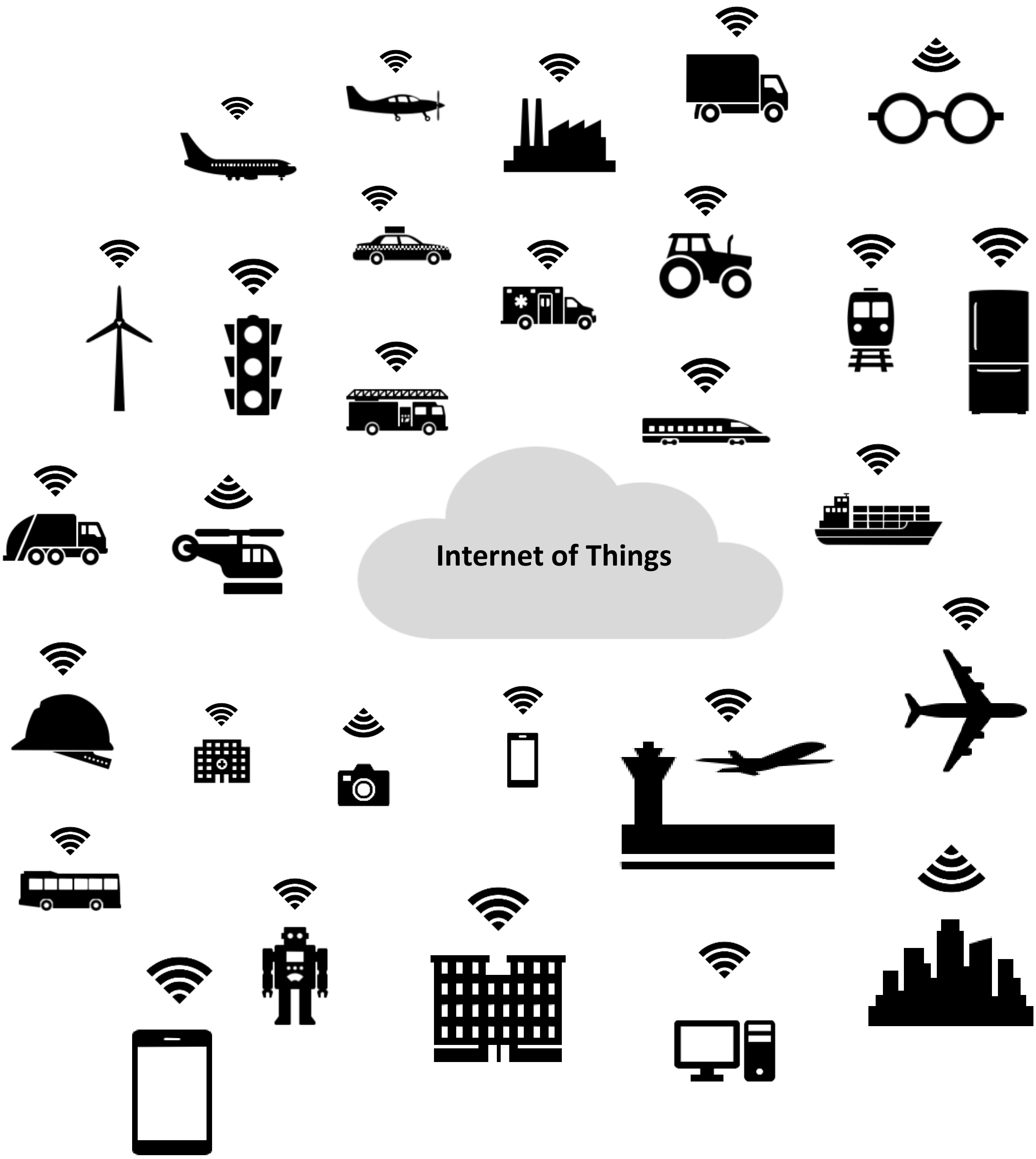


Figure 13. Internet of Things (IoT).

1.2. IoT Conceptual Overview

The internet of things (IoT), refers to the network and communication of uniquely addressable objects through the Internet. When we talk about the internet of things (IoT) we are talking about the interaction between the digital and physical, indeed the vision of the internet of things (IoT) is to connect the physical world to the digital world, and it aims to create a new ecosystem in which smart devices can talk with each other (M2M), direct their transport, adapt to their environments, and become self-monitoring, self-controlling, self-optimizing and ultimately play an active role in their disposal without any human interaction (Vermesan and Friess, 2014: 20-24). The term IoT is relatively new, however the idea of combining computers and networks to monitor and control devices has been around for decades. The term “Internet of Things” (IoT) was first introduced in 1999 by Kevin Ashton the CEO of the MIT Auto-ID Center, a research institution in the field of radio-frequency identification (RFID). Ashton used the term “Internet of Things” to describe a system in which objects in the physical world could be connected to the internet by sensors. He coined the term to illustrate the potential of connecting radio-frequency identification (RFID) tags to the internet in order to count and track goods without the need for human intervention (Rain RFID, 2015). In the general sense, the term IoT encompasses everything connected to the internet, but it is frequently being used to define objects that "talk" to each other. The “Things” in the internet of things are the everyday objects in our house, office, and the car, in aviation case, this "Things" can be any objects in an airport terminal or airside only hooked up to the internet. Web-enabled devices that receive, send and act on data they collect from their surrounding environments using processors, embedded sensors and communication hardware form parts of the internet of things. These smart devices or often called connected devices can talk to each other through a process called machine-to-machine (M2M) communication, and act on the information they get from one another.

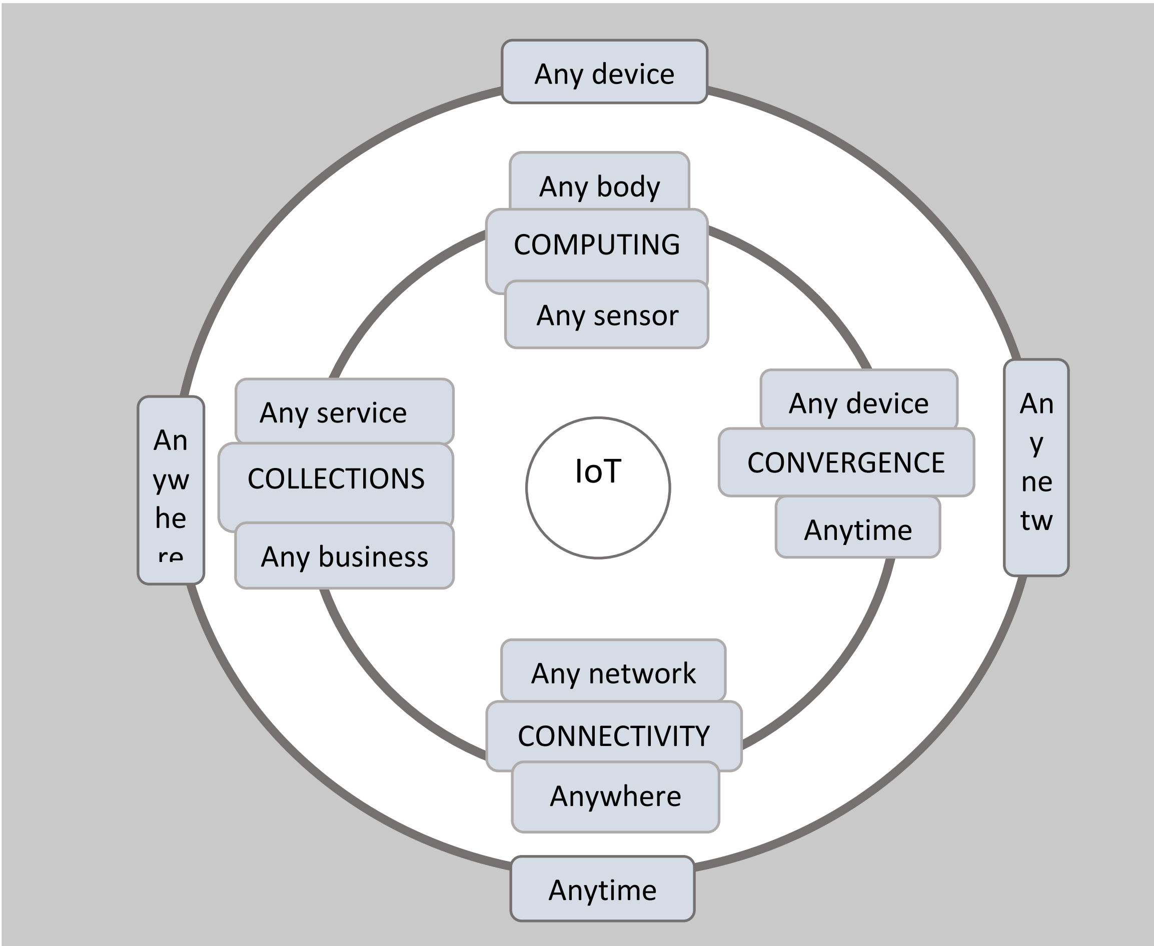


Figure 14. IoT concept.

The A's indicate to the globalization of the technology (anytime, anywhere, any device, any network, etc.) and C's shows the features of IoT, such as collections, convergence, connectivity, computing and so on (ILNAS, 2018: 17).

1.3. IoT Components

The IoT encompasses various components as presented in Table 1.

IoT Components	Description
Sensors	Sensors have the capacity to sense the physical environment
Human	Human can act both as consumers and generators of data.
Actuators	These devices are used to manipulate the physical environment.
Physical objects	Devices(things)
Networking components	The elements of IoT are connected together by networks, using different wireless and wireline technologies, standards, and protocols to provide connectivity.
Virtual objects	Single Token ID, Digital wallet
Data storage and processing	Cloud computing can be an example of data storage and processing technology that is used for: • Processing big data and transforming it into valuable information • Building and running smart applications
Platforms	The middleware used to connect elements such as physical objects, human, and services to the IoT.

Applications	Application domains such as smart airport and smart city.

These components or devices are connected by networks through various communication technologies, such as wireline (Ethernet cable), and wireless technologies (Wi-Fi, 3G, 4G/LTE) (IEC, 2016: 21-30).

Table 2. IoT components

1.4. IoT Application Domains

The internet of things (IoT) is already bringing high-level technological capabilities to various consumer, commercial and industrial market segments. It is practically impossible to give a complete and holistic overview of all possible applications for the IoT because the IoT eventually affect nearly every aspect of human lives; application use cases are found within the areas of commercial aviation, smart airport industry, industrial services, smart cities and so on (Table 2) (Kumar, 2016).

Domain	Sub-domain	Example
Smart Cities	**Smart Airport**	Identity token management
		Automation of check- in desks, baggage collection, and security screening processes
		Asset tracking, asset Performance Management and queue management.
		Enable homeowners to optimize systems such as lighting.

	Smart Buildings/Smart home	Use intelligent sensors to detect temperature changes
		Monitoring and adjusting building systems
	Smart Transport	smarter route mapping to avoid congestion
		Connected and automated driving
		Traffic signal control system
Healthcare	**Medical and Healthcare**	Simultaneous reporting and monitoring of patients
		Provide care for patients in their home

Table 3. IoT application domains

1.5. IoT Smart Airport Domain

It is a well-known fact that airports, as an industry relies massively on the availability of a continuous stream of data that can empower intelligent decision making and efficiency in daily operation. Any technology that makes this possible, like IoT, is almost always embraced immediately by airport management. The internet of things (IoT) is helping the airport management to have real-time knowledge of what is needed to improve the passenger experience and operational

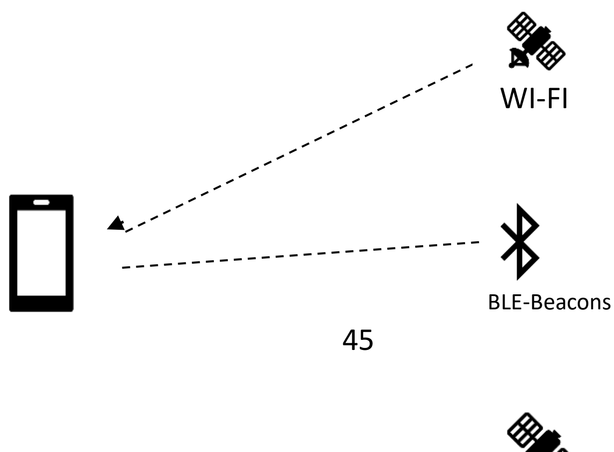
efficiency, such as enabling staff to instantly and effectively deal with airport problems that impact the passengers. This includes customer relations, maintenance, and security staff. The internet of things (IoT) is already having a significant impact on the airport industry, helping airport management move beyond a focus on aeronautical revenue. By connecting particularly physical assets, devices, people, and applications, IoT is playing an important role in driving operational efficiency, enhancing the traveler experience, and generating new revenue sources for airports.
However, the IoT vision goes beyond creating new revenues and better passenger experiences. With the airports becoming increasingly smart, the aim is to bring a significant, paradigm change in the overall experience for both airports and passengers, it has the ability to define a new vision for the airport industry (Allen. 2018; Brizzio 2018). Combining smart airport applications with IoT-based services allow the establishment and enhancement of services such as;

- **Real-time travel services and intelligent transport**: For example, keep travelers informed of flight cancellation, delay or any other travel problems, availability of parking lots in the airport and track passenger throughout every stage of the airport journey, and provide pre-trip travel information, route advice based on traffic conditions, and flight status, via Wi-Fi or a GPS-enabled device.
- **Equipment tracking solutions**: Helping the airport management to keep track of movable equipment to improve equipment availability and utilization. For example, an airport can track wheelchairs with RFID to help decrease the wait for incoming travelers requesting wheelchair support.
- **RFID luggage tagging**: Airports can use RFID tags to detect luggage at a range or out of range, making it easier to find misplaced or missing bags and provide real-time location information to travelers.
- **Fleet management**: Connected vehicles enable batter fleet management, with sensors and devices embedded in the vehicle's, administrators can constantly track the location, status, and movement of each vehicle in real-time, and it gives the ability to identify the potential

problems and fix them before it actually affects the operations. And the data collected from the sensors and devices can be used to develop new business models.

2. Indoor Positioning Systems (Beacons Technology)

The indoor positioning system estimates the indoor location of a user to provide the service he/she needs. Since GPS is unreliable in interior spaces because there is no visual contact with the GPS satellites, an IPS (indoor positioning system) must use other positioning methods. These include, for example, the typical consumer standards Wi-Fi or Bluetooth Low Energy (BLE) Beacons, but also solutions based on Ultra-wideband (UWB) or passive RFID (Figure12). With so many passengers today carrying smart devices, beacons are a perfect way for airports to connect with them — providing information that helps them have a less stressful and more relaxing journey and gathering data, about habits and behavior that help airports to present a more interactive and personalized travel experience.
Beacons also help airports and airline service providers to have the visibility and compliance it needs to deliver better and faster service to passengers and reduce service costs. From wheelchair assistance to terminal cleaning and cabin appearance, all types of support services can be improved with beacon technology.



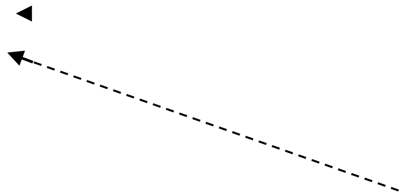


Figure 15. Passenger positioning methods

2.1. What is BLE-Beacon Technology?

Bluetooth beacons transmit a low-power signal which can be picked up by close Bluetooth-enabled devices such as smartphones and tablets. Beacons themselves are not collecting data. They broadcast short-distance signals that can be read by Bluetooth-enabled devices in near proximity to a beacon (Starling. Stephany. 2014: 2-5).

In many cases, beacons can provide a mobile device with location information with higher accuracy than that given by alternative technologies, such as Wi-Fi, GPS, and cell tower triangulation. Importantly, beacons also work fine in remote areas, enabling them to be used in a wide variety of applications in the smart airport, such as triggering mobile boarding passes onto the display of a passenger's smartphone just as they arrive. In some cases, the mobile device may require to use a cellular or Wi-Fi connection to display related content, while in most cases the app can simply pull up the content from a local cache (Starling and Stephany, 2014: 2-5).

2.2. Deployment of Beacons in Airports

Implementing of beacons in airports well open up a range of low-cost opportunities for communicating with passengers, such as: Passenger location: especially airlines, with their apps stored on a passenger's phone, will be able to combine the app's data of the travelers, such as who they are, their destination, and in which class they travel, with accurate knowledge of their location in the airport, derived from detecting the nearest beacon. This can be helpful not just for sending relevant information to the passenger, but also for locating them at the airport if they are late to the gate. There are many benefits to utilize beacon technology. Ultimately, it helps vendors to communicate with passengers more actively in this segment, we'll break down a few benefits to using beacons in smart airport (SITA,2014; ACI and IATA (n.d.): 9-11).

- **Triggering mobile boarding passes**: Beacons installed at traveler's touch points such us check-in, passport control, bag drop, and departure gates can be used to 'pull' mobile boarding passes onto the display of a passenger's mobile devices just as they arrive.
- **Navigating passenger at the airport**: Beacons can provide a more reliable and lower cost way for airport operators to guide travelers throughout the terminal and find the right gate. There are some alternatives for indoor mapping using triangulation technologies, such as cellular signals, and Wi-Fi but if deployed correctly, BLE-based beacons provide much more accurate information and require less complex infrastructure. For example, a passenger carrying a BLE-enabled mobile device can receive a GPS location from any beacon nearby and use the data in a mapping app to navigate through an airport.
- **Proximity and nearby marketing**: The beacon technology can help retailers to inform passengers near to their stores about their discounts, products, or can send welcome messages and coupons to passengers' mobile device when they enter their stores.
- **Baggage reclaims**: Deploying beacon technology in luggage reclaim area can provide a less stressful experience for passengers which are waiting for their luggage to come, for example it could send a message to arriving passengers telling them which conveyor their baggage will come on and how long they will need to wait.

3. Biometric Technology

Multiple checkpoints managed by various stakeholders, and tight security measures in place, make the ambition of creating a seamless passenger journey difficult to achieve.

Biometric technology is the emergence of integrated end-to-end biometric authentication solutions that comprises security, boarding, immigration, and automated check-in and bag-drop, it has the potential to holistically change the way airports identify passengers. By Implementing a biometric system, smart airport operators accelerated passenger processing while maintaining the highest level of security. According to SITA, 77% of airports and 71% of airlines are planning major programs or R&D in biometric ID management over the next five years (Garcia, 2018).

3.1. What are Biometrics?

Biometrics is a common technical term used for personal authentication. Bio refers to life while metric means to measure. Biometrics idea is specifically to find or authenticate the identity of individuals from intrinsic features. Computer science classifies and characterizes biometrics as a method of human identification. Biometrics is a digital analysis of biological characteristics obtained using a camera or scanner. Biometrics provide a more reliable and convenient way for individual authentication (Jaiswal, 2011) Biometrics, either alone or in concert with other technologies, presents huge opportunities for smart airports, to make identity verification cheaper, more convenient and less vulnerable to fraud. There are two types of biometrics: physical and behavioral. Physical biometrics include DNA, fingerprints, retinal, hand, face, recognition, and iris, while behavioral biometrics encompass voice, gait, signature and keystroke (BioMetrica, 2018). Successful application of biometrics depends on the integration of three or more of these methods to achieve considerably strong security.

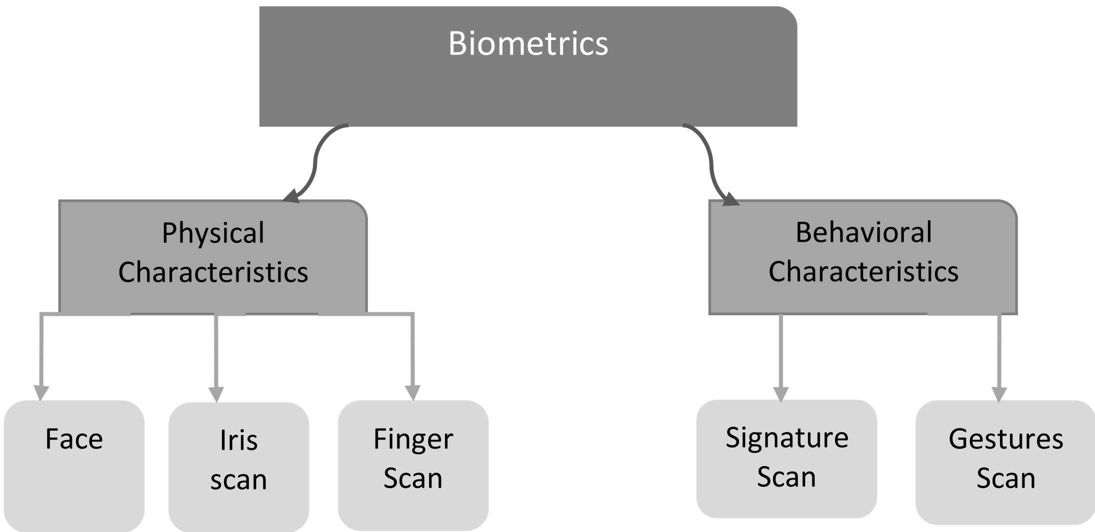


Figure 16. Biometric

3.2. Most Commonly Used Biometric Types in Smart Airports

3.2.1. Iris Recognition

Iris biometric systems are highly reliable biometric systems among other physical biometrics. It works at a very low false acceptance rate. In Iris Recognition method a person is identified by the iris which it is a thin, circular structure in the eye, using pattern matching or image processing concepts of neural networks. The purpose is to identify individuals in real time, with high efficiency and accuracy through analyzing the random patters visible within the iris of individuals eye, by implementing a canny edge detector algorithm (Kak, 2010). The major applications of iris biometrics so far have been substituting for passports (automated international border crossing); aviation security and controlling access to restricted areas at airports; database access and computer login. Like fingerprints, the two irises are not the same. Besides, the right and left eye patterns are different from each other.

3.2.2. Facial Recognition

A facial recognition method is a computer application for automatically recognizing or verifying an individual, using a set of recognizable and verifiable data such as a digital image or a video frame unique and specific to that individual. Facial Recognition Technology (FRT) involves analyzing individual facial features, and storing these features in a database or cloud, and using them to identify that individual faces. While using the facial recognition system, its main task is to identify an individual face like patterns and extract it. When the face is extracted, the system measures specific neural mechanisms for face perception like the shape of the cheekbones, the distance between the eyes, and other identifiable features. These measurements are compared against the entire database of images to find the right match. Facial Recognition technology is categorized into three tasks: face verification, face identification, and watch list (Introna and Nissenbaum, 2017).

3.2.3. Fingerprint Recognition

Fingerprint recognition provides a reliable way to process passenger in a fast and hassle-free manner. Since every individual has a unique fingerprint, using fingerprint recognition system can improve the security since no one else can guess it. All fingerprint data manipulation is performed within a Trusted Execution Environment (TEE) that ensures confidentiality and integrity of the code and data stored inside a systems central processor (Rani and Jose, 2016). At an airport, an automatic fingerprint scanner is often installed at the security checkpoints.

4. Blockchain Technology

The blockchain perhaps is the most significant invention since the internet itself. Its 10 years since the Blockchain made its public debut but still, there's a misconception among people that Bitcoin and Blockchain are one and the same, however, blockchain technology is about far more than just Bitcoin. Today blockchain technology is used for a wide variety of applications, such as data management, digital identity, identification& authentication, ticketing, asset tracking, frequent flyers programs and so on.

4.1. Where the Term Blockchain Come? And How it Works?

Started as the underlying architecture for the Bitcoin cryptocurrency back in 2008, blockchain is the brainchild of a person known as Satoshi Nakamoto.
Satoshi Nakamoto is believed to be the most mysterious character in the world of technology. To date, no one knows about this individual.
Blockchain technology made its public debut when Satoshi Nakamoto released the whitepaper "Bitcoin: A Peer to Peer Electronic Cash System " back in 2008, since then it becomes a hot topic and the subject of various studies in sectors outside the cryptocurrency to which it has often confined in the past. The Blockchain is a technology that allows digital information to be stored and exchanged on a peer-to-

peer network, in a nutshell, the blockchain technology is a new type of internet that allows digital information to be to be distributed but not copied, data are decentrally distributed over various individual computers instead of being stored on a single server thereby it is innately hard to attack by cybercriminals because all the distributed copies of data need to be attacked simultaneously for a cyber-attack to be successful. Further, the digital information stored in distributed ledgers is immune to malicious changes by a single party (Rutland, 2018).

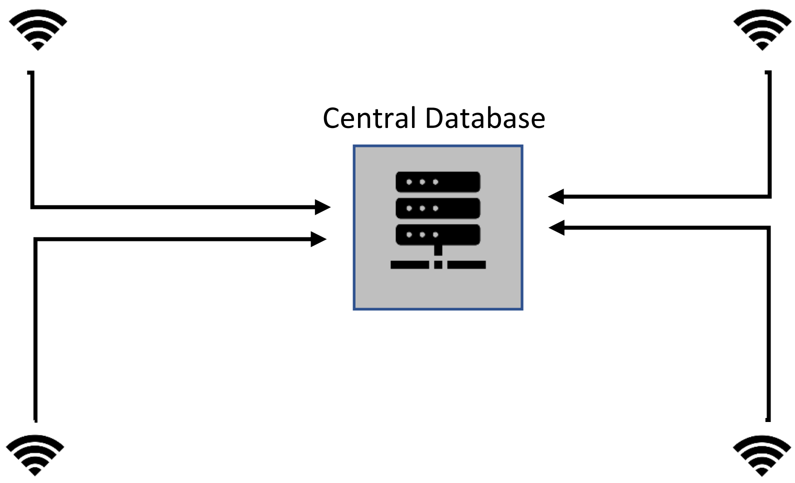


Figure 17. Centralized Database

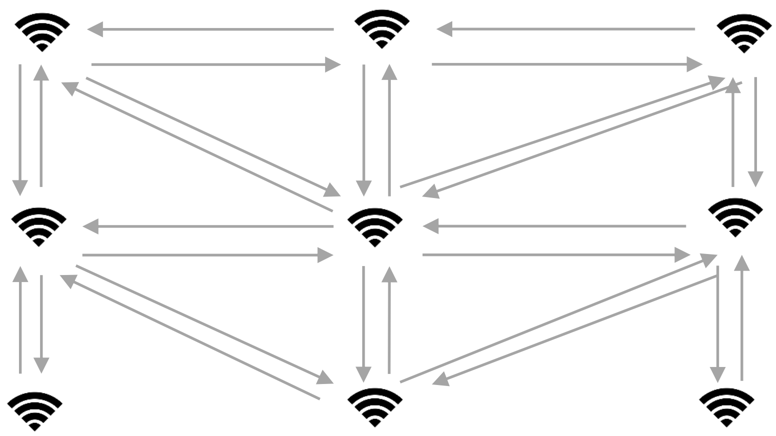


Figure 18. Decentralized Database

4.2. Blockchain Smart Airport Domain

Merging blockchain technology and the internet of things (IoT) will remove non-necessary intermediaries involved in daily processes, and build trust between main stakeholders, by providing full transparency of various transactions, also it helps airports to provide a unified, seamless airport experience for each passenger by storing and sharing information in real-time (IATA, 2018). According to **2018 SITA Air Transport IT Insights**, 59% of airlines and 34% of airports are planning blockchain R&D programs by 2021 (SITA, 2018). Blockchain technology has a wide variety of use cases in the smart airport industry such as;

- **Improving security and identity management in the airport:** Due to its decentralized nature blockchain is highly reliable and secure, and this makes Blockchain technology ideal for improving the way passengers are identified during their journey. An integration of biometric and blockchain can open a new era in identity management. It could facilitate biometrics to be used beyond borders, without the need to store the passenger's information by the various authorities (IATA, 2018)**.**
- **Improving baggage tracking**: Blockchain distributed ledger used by all stakeholders within an airport and among different airports would allow for a bag and the details about its owner to be automatically logged on a blockchain. This would deliver baggage

information records shared among different stakeholders and make it much easier to track the status and location of bags as they change custody (IATA, 2018).

Chapter Three

Smart airport initiatives, and key players in the Global smart airport market

Introduction

The global smart airport market has shown upward trends in the past few years. The significant growth of the smart airport market was recorded in 2015, owing mainly to a large number of greenfield airport developments, and the generalization of new technologies such as cloud computing, IoT, big-data and self-service technology. And thanks to the evolution of new technologies and the exponential growth in the airport's IT expenditure the smart airport market is expected to experience the fastest market growth over the next years.

Emerging technologies and innovations in the area of IT, electronics & control systems, mechanical systems, robotics, and analytics are the major driving factors of smart airports. Aside from Emerging technologies, the exponential growth in air passenger traffic is forcing airport operators to opt for smart airport technologies. In this Chapter, we profiled the key smart airport market players and also at the end of this chapter we explore some of the smart airport initiatives which adopted by various airports across the globe.

1. Key Players in The Global Smart Airport Market

The global smart airport market is extremely fragmented, with only a few players dominating the market. And unlike the traditional airport, the smart airport market is highly competitive because of the presence of small start-up companies that compete with each other and large players such as SITA and Amadeus.

Due to the presence of various players range from small startup company like ParkConnect to highly mature and big companies like SITA it will be more accurate to categorize the market players into five groups; IT Integrators, Airline IT editors, Start-ups and small companies, Software editors and tech giants.

1.1. IT Integrators

These players have been dominated the airport IT industry in past decades. Their market share in traditional airport IT is exceeding 80%. However, with the evolution of smart airport, this airport IT specialists are facing the arrival of new actors on this increasingly attractive market. To compete with new actors in the Smart Airport market these players are strengthening their positions by having an innovative brand powered by a large international presence. Switzerland's SITA the Spanish Amadeus, the American UNISYS and the German T-SYSTEMS are the good examples of these players. These players are still having a large market share in the airport IT deliveries. For example, the Geneva-based IT company SITA, which is mostly known for its aviation IT solutions, is still the leader of the market, dominating almost 25% of global IT&T deliveries.

1.2. Start-ups and Small Companies

The traditional industry players must now deal with the more than 100 startups ready to shake up the airport industry in the context of the current technology boom. Innovation and agility are the two main characteristics which define these new players. Their very small structure and organization enable them to provide innovative solutions for airports especially the airport 3.0 and airport 4.0 (smart airport). Their agility and quick deliveries are something especially requested by airports when it comes to new technologies, inducing a high level of uncertainty (uncertain business model, uncertain need, uncertain technical feasibility, and so on). These tech-focused innovators pose an existential threat to traditional airport companies by carving fresh paths into airport digitization.

These new players are primarily focused on specific cutting-edge technologies, for example, Vision-Box for security solutions in border control, Fox stream for smart video monitoring, BLIP Systems for BLE based indoor geo-localization and PACIFA Decision for 3D modeling and flow management. To accelerate innovation, smart airports are increasingly turning to these players, in order to get higher adaptability and agility, particularly during the experimental phase.

1.3. Airline IT Editors

These competitors are posing a huge risk to Airport IT pure players. For example, Amadeus IT Group, or Sabre Corporation are increasingly evolved in a similar airport environment, so they know the ecosystem very well in terms of their need. They build a strong relationship with the industry stakeholders (ground handlers, airlines and airports), Their strong relationship with industry stakeholders enables them to easily enter the smart airport market. They are also very strong in terms of financial performance and can have very important investment capabilities.

1.4. Software Editors

Unlike the integrators, these players are capable of providing all levels of support on-site or off-site whereas integrators provide support just at level three or the second level at their best. These players also have much greater expertise in the solution which they designed and implemented. Aside from this the operation IT including RMS (Resources Management System), AODB (Airport Operational Database) and FIDS (Flight Information Display System), are well consolidated directly by software editors like RESA (France) and SITA (Switzerland).

1.5. Tech Giants

Aside from being among the world's most innovative companies, these players are also extremely strong in terms of financial performance, advance technology, and reputation. In fact, these companies are well known and have a high reputation in the technology industry. Their reputation, high financial performance, and most importantly advance technology makes them so attractive to the airport authority. However, these players are new in the airport IT industry, and have no previous experience in this field. And also, they do not pose an immediate threat to traditional players, because they are mainly focused on new technologies which traditional players are not able to develop. For example, Huawei Technologies Co. is primarily focused on providing 5G Network to smart airports, and Samsung Electronics focused on providing Indoor LED and Indoor Wi-Fi network to smart airports. The other players in this group are; Nokia, Motorola, Siemens. Apple, and Clear.

While these tech giants may not pose an immediate threat to the traditional players, but they have the potential to become a serious rival for traditional players in the future. These tech giants benefit from a diverse revenue base from multiple resources, whereas traditional players mostly have fixed revenue sources.

On the other hand, these tech giants have state-of-the-art machinery outfitted with the most advanced digital technology from inception. Their late entrance in the airport IT industry enables a competitive advantage — with traditional players burdened by older machinery that is ill-equipped (and economically inviable) for a technological overhaul.

2. Smart Airport Initiatives

2.1. BRUcloud

BRUcloud is an open data sharing platform which enables the air cargo stakeholders to work more integrated and act as a unified network. It's a secure platform which allows all supply chain stakeholders to share their data in the cloud, this enables everyone to have access to the information at the same time. This creates a new opportunity for them to efficiently process their shipments and quickly move their business forward independent from the location or transport mode used.

The Brussels Airport initiated the BRUcloud initiative in 2016, with a vision to enable end-to-end collaboration between all cargo companies across the Brussels airport (Schoeters, 2016).

After a few years of pilot study using BRUcloud, the airport launched its first application using Blockchain technology, strengthening its position in digital innovation in the air cargo industry. Brussels airport aims to improve the efficiency in tracking cargo movement from freight forwarders to ground handlers by connecting this new Blockchain based application to the existing application such as the Slot Booking App (Schoeters, 2016).

Companies like DHL, Global Forwarding, and WFS are shown interest in using the BRUcloud and its Blockchain application, in fact, these companies were involved in development of the BRUcloud from the beginning.

2.2. Aruba Happy Flow

The technology company vision-box developed the Aruba Happy Flow passenger process in collaboration with Aruba airport authority, the Government of Netherlands and Aruba, Schiphol Group, and KLM (Aruba Happy Flow, 2018).

In this innovative passenger process system, passengers need to show his/her face just once throughout the whole journey across the airport. Passengers use their face in order to proceed to check-in, drop off baggage, pass the border and board the airplane, all without being asked to show their passport or boarding pass. Aruba Happy Flow identifies the passenger from their face, a process called facial recognition technology. A photo of the passenger is taken when he/she checks in at a self-service kiosk, which is then authenticated against, and linked with, their e-passport, while at the same time all of the regular border control background checks are performed. Later, at each of the following checkpoints such as bag drop, immigration, and boarding – instead of being asked to show their documents, the passenger just has to stand in front of a camera, which automatically identifies their face, which is matched against their boarding pass and passport, and give approval to proceed their journey. Each process is completed in a matter of seconds (Aruba Happy Flow, 2018).

2.3. Leo and Kate

LEO and her sister Kate were built by SITA Lab to make the check-in process faster for passengers. Leo is an entirely self-ruling, self-propelling baggage robot which has the ability to check in, print bag tags and move up to a weight of 32kg. The passenger can easily place their baggage inside the robot’s storage compartment.

After the passenger scan, their boarding passes Leo prints out a sticker to place on the bag. Finally, Leo closes its baggage compartment, prints out a receipt for the bag tag and goes off to the luggage handling area, where someone directs the luggage toward the right flight. It’s to be noted that Leo is named after the Italian Renaissance inventor and engineer Leonardo da Vinci (Trew, 2017).

In the other hand, Leo's sister Kate is an intelligent check-in kiosk. Benefiting from the power of artificial intelligence (AI) and geo-navigation KATE identifies where additional check-in stations would be needed, then it can move autonomously to that place. Once the robot is stationary, travelers can start scanning their passports or boarding passes to check in and later move straight to security. One of the key benefits of this robot is that it can be dispatched anywhere inside the airport as well as outside locations such as train stations (Trew, 2017).

2.4. Gatwick car parking Robots

Later this year the UK's second busiest airport Gatwick will start a pilot project for robotic valet parking with the aim to optimize its existing car park areas. Under the plans, passenger drive into the airport and leave their car in a “cabin.” A touch screen kiosk on the cabin would enable them to confirm their parking booking. After the booking has been confirmed, the valet robot arrives to collect the car, sliding its carrier underneath the vehicle and transporting it to a nearby parking area. The car parking service will be connected to the passenger's flight information so when the passenger returns his/her car will be retrieved by the robot and returned to a preferred vehicle cabin ready for the passenger's arrival (Clerk, 2019).

2.5. AI Powered Chatbot (Bebot)

In the past century, science-fiction authors imagined a future where Artificial Intelligent (AI) chat and interact with humans, and they were right. But they did not imagine one thing: that the first places where AI will interact and chat with humans would be an airport (D’Mello, 2018).

Yes, that's true Narita International airport launched the world's first AI Powered chatbot (Bebot), to assist the traveler in obtaining information about airport services, facilities, and transport links (D'Mello, 2018).

Customers only need to scan a QR code to get access to Bebot and get the most out of their trip to Narita and Japan via chat. The QR codes are installed on posters and stickers in different locations across Narita Airport. Customers only need to verify themselves by either giving their location or entering their flight number to start chatting (D'Mello, 2018).

Services on offer include assistance in locating airport buildings and services, as well as relevant information about transportation alternatives to and from the airport (D'Mello, 2018).

Chapter Four

The Challenges of Cyber Security in Smart Airports

Introduction

Cybercrime is a global problem which has been dominating the news cycle as no crime did before; it poses a threat to individuals security and privacy, and an even greater threat to large enterprises such as airports. In the past, cybercrime was primarily committed by individuals or small groups, at the present big organized crime groups function like startups and often employ highly-trained developers to exploit the speed, simplicity, and obscurity of the internet to commit a wide range of criminal activities. This individuals or groups know no borders, either virtual or physical and cause severe harm and pose genuine threats to the smart airports. Most smart airports have preventative security software to prevent certain types of attacks but no matter how secure their systems are cybercrime is going to happen. We're rapidly entering a new phase of airport evolution, in which pretty much everything in the airport (landside and airside) is connected to the internet. While these provide plenty of new and exciting possibilities, it also brings challenges and the biggest challenges of all involving security. Every internet-enabled device is potentially vulnerable to cyber-attack so imagine the risks when virtually every object and appliance in the airport is connected. The internet and its underlying infrastructure have been vulnerable to a wide variety of risks, since day one, this include stemming from physical and cyber threats. The hackers or other cyber criminals exploit vulnerabilities in the internet infrastructure to steal data or in some cases money, and they can disrupt, destroy, or threaten the delivery of critical services. Individuals with limited or no specific cyber knowledge can use widely available attack tools to cause significant disruption in an airport by disabling or interfering with automated processes and services such as wireless networks, baggage handling systems, electronic signage, air-conditioning, automated parking services, automated boarding gates, and so on.

In addition to generalized cyber threats, the aviation sector especially airports (usually the bigger and digitally mature ones) remains a specific target for cybercriminals. According to the European Aviation Safety Agency (EASA), an average of 1,000 attacks occur per month on aviation systems.

The cybersecurity threats to Smart airports are detailed in this chapter.

1. Cyber Security in the Airport Context

Cyber is a prefix used in an increasing number of concepts to explain new terms that are being made possible by the outspread of computers. And in the airport, cyber comprises the common IT infrastructure. This encompasses sensors, servers, computers, and network components; the software utilized, and the data transmitted across this infrastructure; and industrial control systems (ICS) such as Airport Operation System (AOS), airfield lighting, baggage handling systems, air conditioning, energy management, and Flight Information Display Systems (FIDS) collectively, these empower the advancement and maintenance of airport facilities, check-in, and screening of customers, and a wide range of additional activities. It is important to be noted that any infrastructure where bits or bytes pass through is vulnerable, regardless of whether or not it's connected to the internet. The cyber-threats come in various forms and diversify in the level of motivation and complexity. They vary from low-skilled 'script kiddies' to extremely skilled and motivated groups which in some cases backed by countries. Within these two extremes there are additional threat actors that can cause impairment to an airport system, including hackers, criminal organizations, and disappointed employees (PA, 2018).

1.2. Cyber Security in Smart Airport

By becoming truly ‘smart’ and ‘connected' and adopting new technologies, smart airports will usher in a new era for both airport operations and customer experience. However, to tap the full value of smart airport, airport administrators will need to grapple with a number of unique challenges. Perhaps the most significant challenges are related to Cyber-security, integrating the airports’ systems within the global ecosystem, providing third parties access to the airport’s critical systems, associated by the fact that smart airports are willing to transfer to the cloud in the coming years, will dramatically raise the risk of cyber-attacks.

Before the evolution of big data, cloud, and IoT airport systems were not usually targeted by cyber-criminals because the systems were independent, isolated and not accessible by third parties. At present, providing access to the airport systems through APIs, in order to accelerate innovation and development, doubles the risk of cyber-attacks. On the other hand, the deployment of IoT technology in airports comes with its own set of cybersecurity challenges. Due to the ability of IoT devices to connect to the internet and their extensive usage, IoT sensors become the main target for cybercriminals. The smart airports (Airport 4.0) have some of the most stringent security processes of any public facility. However, while tight physical measures have been set in place to assure the safety of personnel, infrastructure and customer the demand for network connectivity could leave devices and systems such as ICT and electronic systems easy prey to cyber-attacks.

2. Two Key Trends That Make Smart Airport More Vulnerable to Cyberattacks

1 Application Programming Interface (API)

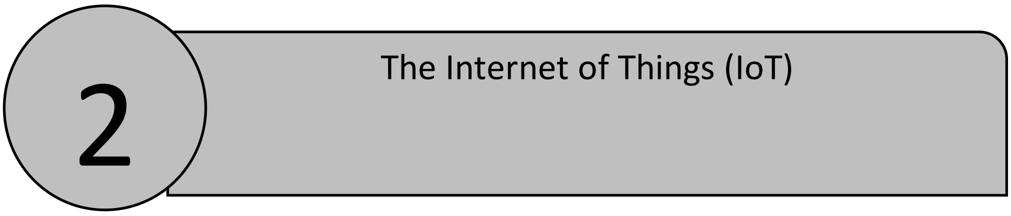


Figure 19. Two Key Trends That Make Smart Airport More Vulnerable to Cyberattacks

2.1. Application Programming Interface (APIs)

With cyber-attacks on airport networks becoming more sophisticated airport operators have stepped up perimeter security by adopting the latest firewall, data and endpoint protection, as well as intrusion prevention technologies. In response, cybercriminals are moving to the path of least resistance and looking for new avenues to exploit. It's expected that the next wave of airport hacking will be carried out by exploiting Application Programming Interfaces (APIs).

The authors of this project think APIs are the key foundation of airport digital transformation in that enables airports to open their business functionality to the outside world (developers) in order to unlock the real value of their digital assets, create business agility and empower innovation and collaboration. However, the authors of this project also believe that steering airport’s systems towards open APIs and their integration with outside systems broaden their vulnerability to an increased risk of cyber-attacks. In fact, cyber criminals are already targeting APIs when organizing their attacks. The data breach at Google+ is a good example. Earlier this year Google announced that Google+ had suffered a massive data breach; this incident forced Google to shut down the entire social media network.
According to Google one of Google+’s APIs allowed the hackers to steal private information of more than 52.5 million users including their name, email address, occupation, and age.

This raises the question of how smart airports can reduce the increasing cybersecurity risk associated with APIs without hindering the benefits they present in terms of agile development and expanded functionality.

2.2. The Internet of Things (IoT)

The Internet of Things (IoT) has emerged as a solution which brings together airports, airlines, service providers, vendors, and customers in an ecosystem where systems and processes are interconnected and digitally aware. As explained in the section above the internet of things (IoT) is already having a significant impact on the airport industry, helping airport management move beyond a focus on aeronautical revenue. By connecting particularly physical assets, devices, people, and applications, IoT is playing an important role in driving operational efficiency, enhancing the traveler experience, and generating new revenue sources for airports. The emergence of the IoT definitely presents a vast opportunity for the airport industry; however, it can also expose airports to new risks and undiscovered threats. Regardless of their form, all of the IoT devices and technologies are kind of computer that connects to a network. And the moment computers begin to communicate with each other through network; they have become vulnerable, it is perhaps, the nature of computers. However, due to the lack of security standards and poor quality, IoT devices are even more susceptible to cyber-attacks than a regular computer.

Beside this, cybercriminal may also use the IoT device to attack airport infrastructure.

The extensive Distributed Denial of Service (DDoS) attack (see appendix 2), that brought down the Dyn servers is a perfect example. In 2016 a massive cyber-attack brought down the servers of Dyn, a company that dominates much of the internet's domain name system (DNS), the attack was the largest of its kind in internet history and brought down popular websites such as Twitter, the Guardian, CNN, Netflix and so on. Hackers have organized these attacks using a weapon called the Mirai Botnet. What makes special about this attack is that unlike traditional botnets (see appendix 3), which are typically made up of the computer, the Mirai Botnets was mainly made up of IoT devices.

According to Dyn, the attack had involved some 100,000 malicious devices.

Based on the number which Dyn claim (100,000 devices), Mirai botnet attack which happened on 21 October is almost twice as powerful as any similar attack in history. Clearly, cyber-attacks of such scale can cause significant damage to any enterprises specially airports.

With the continued adoption the IoT devices, it is more vital than ever to build security into these devices from the beginning to disrupt the cyber actors and avoid exposing airports to severe threats.

3. Incidents and Complexity of Cyber-Attacks Are on The Rise

With the tremendous increase in the use of digital technology in the airports, there has been an increase in the number of potential ways for cybercriminals to gain access to airports network. Over the past years, the number of airport-related cyber-attacks has increased significantly. As noted, before according to European Union Aviation Safety Agency (EASA) aviation systems face an average of 1,000 cyber-attacks per month. However, this number is likely to increase with the advancing digitalization in the airport industry. The following section provides a timeline of the 2013-2019 cybersecurity-related incidents in airports.

June 27, 2017

Hackers launched a massive cyber-attack on Ukraine's Boryspil International Airport, as a result, the Boryspil airports lost access to its systems; The official site of the airport and the scoreboard with the schedule of flights were also down. Though this attack was not just targeting aviation systems yet resulted in an interruption to Boryspil airport services. Cybersecurity experts believe that the virus, named Petrwrap or Petya, seemed to work likewise to the WannaCry ransomware that affected more than 230,000 computers in 150 countries back in 2017 (PA, 2018).

July 29, 2016

The so-called pro-Beijing hackers disrupted the website of Vietnam Airlines and flight information screens in Hanoi and Ho Chi city airports. They temporarily seized flight information screens and sound systems inside the two major airports. Instead of departure and arrival information, the airports' flight screens and speakers broadcasted anti-Vietnamese and Philippines slogans. As a result of this attack, the entire systems connected to the internet were halted, and all the operations were carried out manually in these two major airports. This incident clearly shows that alongside cybercriminals the so-called pro-government hackers also chose airports as their main target (PA, 2018).

2013

A complex virtual spying operation directly impacted 75 US airports. The interruption occurred by a high-level persistent threat attack, which means an incursion was carried out by highly trained hackers who are usually sponsored by a state. According to the US government, the hackers could have been driven by a desire to know who would be on certain flights, as well as the cargo they would be carrying (PA,2018).

4. Industry Initiatives to Prevent Cyber Attacks

Despite some small airports (less than 1 million travelers/year) which have a serious lack of cybersecurity expertise and solutions, larger airports, which are technologically advanced especially smart airports, have a good awareness and expertise in this area, and even some airports like Munich airport in Germany went further and established a center to fight cyber-crimes in the airport industry.

According to the SITA's 2018 Air Transport Cybersecurity Insights, last year airlines and airports have spent $3.9 billion on cybersecurity. And according to the same survey, Airlines spend an average of 7% of their entire IT budget on Cybersecurity, compared to a higher airport investment at 10%.

4.1. Community Cyber Threat Center (CCTC)

In 2017 the IT company SITA has launched the Community Cyber Threat Center (CCTC). According to the SITA, the aims of the CCTC initiative is to support the industry to decrease the cyber threat through data sharing and better collaboration. The initiative embraces cyber-attacks classification, enterprise assets protection, cyber-attack detection, and incident response (SITA, 2018).

The CCTC supports a community- broad response by encouraging a proactive exchange of contextualized, actionable cyber threat data among SITA's members. A customized alarm system presents a prompt notification of vital information (such as hijacked credentials) exposed to the cybercriminals (SITA, 2018).

4.2. Security Operation Center (SOC)

Airbus has partnered with SITA to address the aviation industry's distinct cybersecurity concerns and has launched a unique initiative called Security Operation Center (SOC).

The SOC acts like a cyber operation tower with an integrated combination of processes, people and digital technology to identify, analyze, and react in case of any cybersecurity incidents. SOC provides airlines, airports and other stakeholders with the monitoring of malicious cyber activity which may affect business continuity. With global capabilities, the SOC offers appropriate containment and response ensuring that airports digital assets are safe from attack.

Airbus has been a pioneer in the cybersecurity area for a long time. Its subsidiary company Airbus Cybersecurity is a specialist in this filed, with the aim and experience of shielding governments, armies, enterprise organizations and vital public infrastructure from cyber threats. And since SITA has a huge experience in airport technology together this two company can provide an advanced security solution for the airport industry (Futuretravleexperience, 2018).
Indeed, the result of their partnership turns out to be very effective to protect airport industry from the cyber threat.

4.3. Aviation Information Sharing and Analysis Center (A-ISAC)

The Aviation Information Sharing and Analysis Center (A-ISAC) formed in 2014 by major Airlines and Airports, it is a non-profit organization for sharing security information in the aviation industry. The A-ISAC gathers information about threat and vulnerabilities, that may threaten the aviation industry across the Globe. According to the A-ISAC, they gather their information from sources such as government agencies, academic institutions, open source, and other trusted sources. Its goal is to share the information in a timely manner between its members (A-ISAC).

4.4. Munich Airport Information Security Hub (ISH)

At a special ceremony on January 2018, Munich Airport introduced its Information Security Hub (ISH)- a cybersecurity operation center in which IT and cybersecurity experts with the Munich airport operating company (FMG) work together with specialists from the European aviation sectors to develop strategies for protecting airport and airlines against cyber-attacks and new approaches to the fight against cybercrime. In building the ISH Munich airport operator FMG has collaborated with different IT companies such as ERNW INSIGHT, HvS-Consulting, and IT-CUBE SYSTEMS.

According to the officials, the ISH facilities and services are also available to other companies and enterprise organizations from any sector; enterprise organizations, public authorities, and other businesses can train security specialists for their organizations and conduct comprehensive testing of digital technologies and processes (ISH, 2018).

Conclusion

Based on an in-depth examination of existing knowledge as well as studying various airports, which are highly mature in terms of technology, it's clear that new technologies especially the internet of things (IoT) have a significant role to play in the evolution smart airport, however, addressing the challenges of an airport to exploit the power of a smart airport is not only about utilizing new technology; it is about business transformation in a digital environment. It is both the deployment of new technologies as well as the integration of existing technologies, processes, and services to provide a greater experience to passenger and other stakeholders.

This graduation project mainly concentrated on explaining the role of new technologies in the evolution of the smart airport, and in defining the smart airport, the project primarily considered the digital maturity of airports which describes the level of technology adoption in an airport.

Having a look and a review on the digital performance of more than 10 airports which considered to be profoundly advance and mature in terms of technology, we spot that the smartest ones are in many cases small to medium airports, such as Copenhagen International Airport and Munich International Airport.

And also, this project has exposed the cyber-security as the most critical challenges that smart airports will face in the near future, however, the authors of this project suggest that while taking the issue of cyber-security serious smart airports must not underestimate the cultural change, as they face up to the need to embrace new technologies.

In conclusion, any activity that automates management of airport business in association to the processing of customers can be determined as a characteristic of the smart airport, that either supports the decision-making process through the provision and acquisition of up-to-date data or infrastructure automated processes that reduce manual actions and limit human error.

Bibliography

ACI (2017). Airport Digital Transformation: Best practice.

ACI and IATA (n.d.). Airport Terminal Beacons Recommended Practice.

Allen kelly. (2018). Smart Airports: IoT is Taking of. https://www.smart-industry.net/smart-airports-iot-is-taking-off/ Accessed 10 December 2018.

Amadeus (n.d.) Reinventing the Airport Ecosystem.

Aruba Happy Flow (2018). Aruba Happy Flow. http://www.arubahappyflow.com/ Accessed 2 January 2019.

Aviation ISAC (n.d.). https://www.a-isac.com / Accessed 2 January 2019.

BioMetrica (2018). Biometric-Theory. http://bio-metrica.com/biometric-theory / Accessed 3 January 2019.

Brizzio Pablo. (2018). IoT for Smart Airports: Building Digital Business Excellence. https://cxm.world/iot-for-smart-airports-building-digital-business-excellence/ Accessed 10 December 2018.

Clerk Eve. (2019). Robots May Soon Be Parking Cars at Gatwick Airport. https://www.internationalairportreview.com/news/80468/robots-parking-gatwick/ Accessed 29 January 2019.

D'Mello, Yollanda (2018). Aithority Interview Series With Akemi Tsunagawa, Founder and CEO, Bespoke Inc. https://aithority.com/interviews/ait-megamind/interview-with-akemi-tsunagawa-founder-and-ceo-bespoke-inc/#/Accessed 29 January 2019.

ENISA (2016). Securing Smart Airports.

Evans Dave (2011). The Internet of Things: How the Next Evolution of the Internet is Changing Everything. CISCO IBSG.

Fattah Amir, Howard Lock, William Buller, Shaun Kirby. (2009). Smart Airport: Transforming Passenger Experience to Thrive in the New Economy. Cisco Systems.

Futuretravleexperience. (2018). Cybersecurity – Industry Collaboration Key to Meeting "very real threat of cyberattacks". https://www.futuretravelexperience.com/2018/02/cybersecurity-industry-collaboration-key-to-meeting-very-real-threat-of-cyberattacks/ Accessed 3 January 2019.

Garcia, Marisa (2017). When an Airport Opens Its API to Encourage Innovation. https://www.phocuswire.com/When-an-airport-opens-its-API-to-encourage-innovation /Accessed 20 November 2018.

Garcia, Marisa (2014). Amsterdam's Schiphol Airport Is Psyched About its New Tesla Taxis. https://skift.com/2014/10/07/amsterdams-schiphol-airport-is-psyched-about-its-new-tesla-taxis/ Accessed 28 November 2018.

Garcia Marisa. (2018). Biometric Technology is Taking off as 77% of Airports and 71% of Airlines Review Digital ID Options. https://www.forbes.com/sites/marisagarcia/2018/09/29/biometric-technology-is-taking-off-as-77-of-airports-and-71-of-airlines-review-digital-id-options/#6bc95406704d/ Accessed 20 December 2018.

IATA (2018). Blockchain In Aviation.

IEC (2016). IOT 2020: Smart and Secure IoT platform. Geneva

ILNAS (2018). Internet of Things (IoT). Luxembourg: ANEC.

Introna, Lucas and Helen Nissenbaum. (2017). Facial Recognition Technology.

ISH (2018). Hands on Cyber Security Building Bridges with the Information Security Hub.

Jaiswal Sushma, Sarita Sing Bhadauria, Rakesh Sing Jadon (2011). Biometric: Case Study. Journal of Global Research in Computer Science, Vol.2 No.10 October 2011.

Kak Neha, Rishi Gupta, Sanchit Mahajan (2010). Iris Recognition System. International Journal of Advanced Computer Science and Applications (IJACSA). Vol.1 No.1, 2010.

Kumar Ram, Hima Sampathrao, Vijay kumar Burgari (2016). Application Domain of Internet of Things: A survey. International Journal of Engineering Technology science and Research (IJETSR). Vol.3 No 10 October 2016.

Michael Alexander, Papiomyties Diogenis (2017). Strengthening the Airport Value Proposition. Frost & Sullivan and Amadeus.

Nau, Jean-Batiste and Frank Benoit (n.d.). Smart Airport. Wavestone

PA (2018). Overcome the Silent Threat.

Pell, Russel and Mathieu Blondel (n.d.). Airport digital transformation: From Operational Performance to Strategic Opportunity. Amadeus and Arthur D Little.

Rain RFID (2015). RFID and The Internet of Things.

Rani, E. and John J. (2016). Fingerprint Based Biometric Authentication. International Journal of Computing and Science and Mobile Computing (IJSCMC). Vol.5 No. 9 September 2016: 6-15.

Rose, Karen, Scott Eldridge and Lyman Chapin (2015). The Internet of Things: An overview. The Internet society (ISOC).

Rutland, Emily (2018). Blockchain Byte. R3 Research.

Schoeters, Marcel (2016). BRU Airport's Cloud Platform is Taking Shape – Part1. https://www.cargoforwarder.eu/2016/07/18/bru-airport-s-cloud-platform-is-taking-shape-part-1/ Accessed 1 January 2019.

Schoeters, Marcel (2016). BRU Airport's Cloud Platform is Taking Shape – Part 2. https://www.cargoforwarder.eu/2016/07/24/part-2-bru-airport-s-cloud-platform/ Accessed 2 January 2019.

SITA (2011). The Intelligent Airport- Unleashing the Potential.

SITA (2018). 2018 Air Transport IT Insights.

SITA (2015). The future is Personal in Air Travel. https://www.sita.aero/pressroom/news-releases/the-future-is-personal-in-air-travel / Accessed 24 November 2018.

SITA (2015). Airline Passengers Happiest When Using Technology. https://www.sita.aero/pressroom/news-releases/airline-passengers-happiest-when-using-technology / Accessed 2 December 2018.

SITA (2014). Connecting to Passengers-Are Beacons the Breakthrough.

SITA(2018). SITA improves its Arsenal in Battle Against Cyber Threats. https://www.sita.aero/air-transport-it-review/articles/sita-improves-its-arsenal-in-battle-against-cyber-threats /Accessed 3 January 2019.

Sterling, Greg, Jules Polonetsky and Stephany Fan (2014). Understanding Beacons: A Guide to Beacon Technology. Local Search Association & Future of Privacy Forum.

Trew, Marissa (2017). Introducing SITA'S KATE, LEO the Baggage Robot's Self-Check in Sister. https://www.webintravel.com/sita-kate-leo-baggage-robots-self-check-in/ Accessed 2 January 2019.

United Airlines (2014). United Airlines the First Airline to Offer Uber Services Via Mobile App. https://united.mediaroom.com/2014-08-20-United-Airlines-the-First-Airline-to-offer-Uber-Service-via-Mobile-App / Accessed 26 November 2018.

Vermesan, Ovidiu and Peter Friess (2014). Internet of Things- From Research and Innovation to Market Deployment. Denmark: River Publishers.

Appendix

1. Application Programming Interface (API)

API stands for Application Programming Interface, and it is a software intermediary that allows two applications to talk to each other. For example, we want to search for a flight online we have a wide range of options to choose from, including direct, or transit flights, different cities, departure, and return dates and so on. Let's imagine that we are booking our flight on an airline website. We pick a departure city and date, a return city and date, cabin class, as well as other variables. In order to book our flight, we interact with the airline's website to obtain information from their database and see if a seat is available on those dates and what the prices might be. However, what if we are not using the airline's website—a channel which has direct access to the information? What if we are using an online travel service, such as Skyscanner, which aggregates information from a number of airline databases?

In this case, the travel service interacts with the airline's API. The API is the interface that can be asked by that online travel service to get information from the airline's database to book seats, baggage options, etc. The API then takes the airline's response to our request and delivers it right back to the online travel service, which then shows us the most updated, relevant information.

2. Distributed Denial of Service (DDoS)

A distributed denial-of-service (DDoS) attack is a malicious effort to interrupt regular traffic of a targeted server, service or network by confusing the target or its encompassing infrastructure with a wave of Internet traffic. DDoS attacks achieve effectiveness by using various compromised computer systems as sources of attack traffic. Used devices can include computers and other networked devices such as IoT devices. From a high level, a DDoS attack is like a traffic jam clogging up with highway, preventing regular traffic from arriving at its desired destination.

2.1. How does a DDoS attack work?

A DDoS attack needs an intruder to obtain command of a network of online devices in order to carry out an attack. Machines, computers and other devices (such as IoT devices) are infected with malware, turning each one into a bot (or zombie). The intruder then holds remote control over the group of bots, which is named a botnet.

When a botnet has been installed, the intruder is capable to control the devices by installing updated instructions to every bot by a method of remote control. When the IP address of a victim is targeted by the botnet, each bot will respond by sending requests to the target, potentially causing the targeted server or network to overflow capacity, resulting in a denial-of-service to normal traffic. Because each bot is a genuine Internet device, separating the attack traffic from normal traffic can be challenging.

3. What is a Botnet?

A botnet is a group of computers or devices (such as IoT devices) which have been infected by malware and have come under the direction of a malicious actor. The word botnet is a portmanteau from the terms robot and network and each infected machine is called a bot. Botnets can be created to perform unlawful or malicious tasks including sending spam, stealing data, ransomware, fraudulently clicking on ads or distributed denial-of-service (DDoS) attacks.

While some malware, such as ransomware, will have an immediate result on the targeted device, DDoS botnet malware can have various levels of visibility; some malware is designed to take the entire direction of a machine, while other malware operates quietly as a background process while remaining quietly for directions from the attacker or “bot herder.”

Self-propagating botnets obtain extra bots through a variety of different channels. Pathways for infection include the exploitation of website vulnerabilities, Trojan horse malware, and breaking weak authentication to obtain remote access. Once access has been achieved, every one of these methods for infection occurs in the installation of malware on the target machine or devices, providing remote control by the operator of the botnet. Once a device is affected, it may attempt to self-propagate the botnet malware by recruiting other hardware devices in the surrounding network.