Future of Airport Security

Prepared by: Talal Abdulla Kamal

شـركة مطـار البحـريـن
bahrain airport company

Future of Airport Security

Table of Contents

Future of Airport Security

INTRODUCTION

In this age of technology, technological advancement is rapidly developing to a stage where airports have no choice but to develop their equipment and infrastructure to cope with the rapid growth in traffic, emerging threats to civil aviation, and to enhance customer satisfaction.

Going back to the days where airport security was very basic to today where various risks and threats emerged which leaves a person wondering whether it is safe to travel via air? Fortunately, with today's advancement in technology we can minimize risks of acts of unlawful interference to an acceptable rate that allows passengers to safely travel.

Airport aviation security (AVSEC) challenges from the writer's point of view will be analyzed and solutions to those issues will be proposed using technologies that are in the market but not fully used to their full capabilities in the aviation/airport security.

Airport security is a very critical element of an airport, which if not properly invested in and appropriately implemented, could lead to ruining the reputation and business of an airport/country. As a result, from that context airports should understand how to properly invest in technology to enhance security while at the same time facilitate passenger experience. This would solve one of the biggest AVSEC concerns: that of evolving irate passengers in view of long queuing times at security and other processing points.

In this paper, several technologies that could be introduced in an airport security environment will be addressed and details of how those technologies could significantly enhance aviation security, as well as facilitate passenger experience/journey through an airport, will be explained. In addition, to complement the use of technologies such as Artificial Intelligence (AI) and Internet of Things (IoT), security concepts will be introduced to further improve aviation security and facilitate the customer's experience.

AIRPORT AVIATION SECURITY CHALLENGES

Airports nowadays are facing several challenges, with some intensifying on yearly basis. In order to reduce the impact on airports and smoothen aviation security processes, research for the adaptation of appropriate existing and emerging technologies should be introduced at the right place and in a timely manner. However, in order to do so, airport challenges should be addressed and analyzed. Below are the main major challenges airports are facing today:

1. Coping with the rapid growth in passenger traffic

The International Air Transport Association (IATA) expects the traffic to reach 8.2 billion passengers in air travel in 2037, (IATA, 2018)

1.1.1 Regional growth

- **Routes to, from and within Asia-Pacific** will see an extra 2.35 billion annual passengers by 2037, for a total market size of 3.9 billion passengers. Its compound annual growth rate (CAGR) of 4.8% is the highest, followed by Africa and the Middle East.
- **The North American region** will grow by a CAGR of 2.4% annually and in 2037 will carry a total of 1.4 billion passengers, an additional 527 million passengers.
- **Europe** will grow at a CAGR of 2.0% and will see an additional 611 million passengers. The total market will be 1.9 billion passengers.
- **Latin American** markets will grow by a CAGR of 3.6%, serving a total of 731 million passengers, an additional 371 million passengers annually compared to today.
- The **Middle East** will grow strongly with a CAGR of 4.4% and will see an extra 290 million passengers on routes to, from and within the region by 2037. The total market size will be 501 million passengers.

- **Africa** will grow by a CAGR of 4.6%. By 2037 it will see an extra 199 million passengers for a total market of 334 million passengers. (IATA, 2018)

1.1.2 Sustainability

In order to sustain and adapt to the annual passenger growth airports must respond to the significant increase by expanding their airport infrastructure which is considered challenging requiring enormous resources and investments. Another option would be to invest in technologies that enhances processes, reduces cost, and requires less manpower to operate. Details of such technologies and how to implement them in airports could be found in the relevant chapters of this paper.

Furthermore, looking at sustainability from security perspective, increase in growth affects the security outcome as well as the customer experience. E.g. (by having longer queues screeners might be under pressure to clear the queue by expediting screening process, and that might compromise security).

2. Terrorism

Having a safe and secure environment is a major concern in aviation security, especially today where threats are emerging, and terrorists are getting more familiar with the current systems and procedures. Commercial aviation will always be an attractive target for extremist, terrorist groups and other perpetrators.

The vulnerability of the landside area of an airport is higher since it is public and has less security restrictions than airside and SRA, thus more difficult to control. In fact, in recent days terrorists are targeting such areas of the airport as they prove to be easily accessible. Having said that, there are various ways of enhancing landside security. Methods may include people screening, vehicle searches, other random security controls, CCTV...etc. However, this paper will be focusing on the demonstration of evolving technologies such as Internet of Things (IoT)/ Artificial Intelligence (AI) and their implementation in the field of aviation security aimed at enriching/smoothening aviation security processes.

3. Making profit

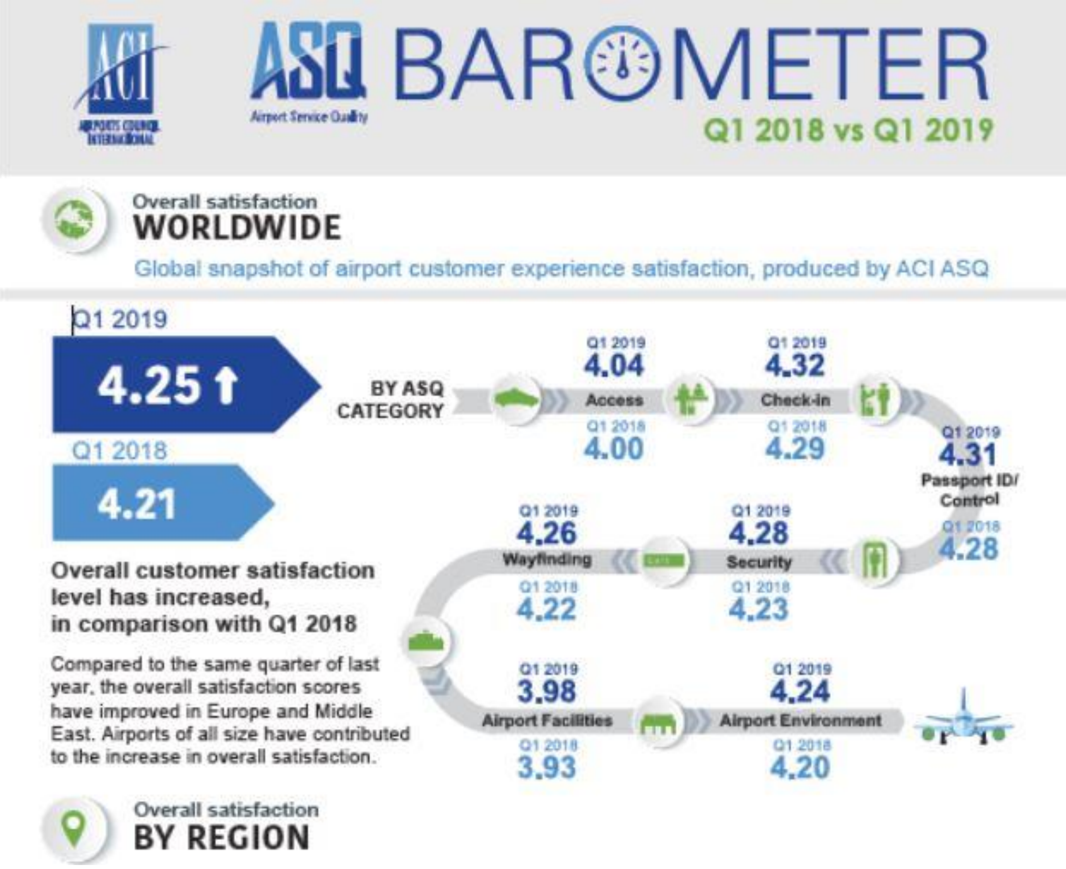
Aviation security is generally looked upon in solitary and as a cost for airports, even though it should be an integral part of airport operations. Airports generally do not make profits from aviation security, as the costs including depreciation and the proper upkeep of security equipment is high, with airport security charges not yielding enough for airports to have an adequate return on investment. One way of recouping the costs or further making profits from aviation security is through an increase of security charges reflected in air-tickets. However, this would have a direct impact on passengers and might influence travel figures.

4. Customer satisfaction

Airport Council International (ACI), Airport Service Quality (ASQ) report states that the overall satisfaction rate increased comparing to the **Q1 2018 4.21** ACI rating to **4.24** in **Q1 2019** (ACI, 2019)

ASQ barometer is a benchmark tool that enables airports to measure their customer experience and satisfaction rates, enabling them to measure their satisfaction rate against their competitors.

Figure 1 ASQ BAROMETER Q1 2018 - Q1 2019



Future of Airport Security

Knowing that airports are continuously working to increase the satisfaction of their passengers/customers, satisfying and possibly going beyond passenger expectations is becoming challenging for airports, as a superior service being delivered by an airport may after time be considered as the norm by passengers, hence at a later stage expecting a further improved or enhanced service and facilities.. Passenger/customers' expectations are always on the demand making it difficult to fully satisfy passengers' expectations.

In addition, an AVSEC technology savvy segment of passengers also tend to become irate if they wait too long in queue, or if the used security procedures are too invasive, knowing that the key to counter such an issue is to invest and bring in technology in order to expedite, enhance and smoothen the screening process.

TECHNOLOGY

There are several upcoming technologies, both current and emerging, that could be incorporated in current AVSEC set ups, and if invested in properly they would significantly enhance the passenger experience, not to mention a better risk-based approach to AVSEC.

Emphasizing the proper use of technology, various emerging technologies will be introduced in this section, and in order to get the best results, a concept combining several technologies shall be introduced.

INTERNET OF THINGS (IoT)

In recent days the IoT has become a growing topic in almost every industry, there are various concept designs on how IoT could significantly positively impact our lives, not only from aviation point of view, but in general the IoT would greatly change the way we do things in life and at the workplace. Analysts predicts that by 2020 the investments spent on IoT services, products and technology will reach $267Billion. (Columbus, 2017)

Future of Airport Security

So, one might ask, “what is the IoT”? Simply the IoT or in some cases referred to as the internet of everything, is an existing concept of connecting devices having an off/on switch to the internet and/or to one another. There are no constraints as to what device can be connected, as any device could be connected to another or to the internet as longs as it has a switch. Taking a passenger’s departure journey as an example, the check in system could be connected to the boarding pass reconciliation system, to emigration, CCTV and finally to x-ray machines. As a result, data could flow from one system to another allowing automatic decisions, based on pre-defined rules fed into the systems. An Example of such a rule could be that if a passenger is acting in a suspicious manner, CCTV picks up his behavior , and sends the data to screening checkpoint alerting through the system that the particular passenger is suspicious, hence the protocol of further questioning and screening him/her thoroughly is to take place before being allowed to proceed further.

Even though the first word of the abbreviation in IoT is ‘’internet’’, it is not necessary to have an internet network connectivity to connect devices to one another and create an IoT network. However, that is not always the case, as in order to fully exploit the capabilities of the IoT it is preferable to connect to the internet especially in an airport environment where one would need to receive live notifications and alerts.

1.1.3 Application at an airport

There are various ways of implementing and exploiting the concept of IoT at an airport environment with very few limitations on what could be connected.

From an airport security perspective, the IoT would enhance aviation security significantly as it will allow for information exchange and facilitate information dissemination to the concerned personnel instantaneously. As a result, it could assist the aviation industry in reducing the probability of planned acts of unlawful interference by providing security stakeholders with timely data vital for risk assessing various situations.

Future of Airport Security

A practical example of how IoT could aid in preventing, detecting or at least reducing the risk of incidents/terrorist attacks, is the case of 9/11 when a series of four coordinated attacks by Al-Qaeda killed at least 2,900 people, injured over 250,000 people causing at least $10 billion in infrastructure and property damage.

Taking 9/11 terrorist attack into consideration, if IoT were used for the collation and timely dissemination as indicated in clause 1.1.4, it should have shed a dubious light on the terrorists thus indicating to security forces that the person(s) needs further investigation before being allowed for onward travel. Providing the necessary and timely data, together with information, which would then be transformed into intelligence would have automatically triggered further questioning and possible additional investigation; thus, precluding the terrorist(s) from travelling. I.e. (by creating an IoT network and connecting systems and machines to one another we would be able to generate and compile the required information at any point in time, and in many cases terrorist profiles are highlighted and detected during the travel process, mainly at the airport.)

As mentioned previously, the IoT connects several devices to one another depending on how vast the connectivity of devices is, aircrafts and navigational aids could also be part of IoT set up. Therefore, all such devices could communicate on another sharing information and sending it to the concerned parties, with the usage depending on the pre-configuration and how the scenarios are predefined during the setting up the IoT network.

1.1.4 Passenger journey and data capturing process (Cabin & Hold baggage)

Taking the passengers journey into consideration, there are plenty of data to be captured in a single passenger's journey however this is all dispersed today.

Below is an illustration of a 30-point passenger travel process and what information and data could be compiled and collated in each process via the use of IoT. The suggested technologies to be exploited in the below 30 travel process are:

I. Internet of Things (IoT)
II. Artificial Intelligence (AI)

PROCESS	INFORMATION / DATA GATHERING
1. Purchase of Air Ticket	Passport Details; whether ticket was procured in advance or just before the flight departure; number of tickets purchased; method of payment, bank name (if applicable); PNR; travel duration; any connecting flights; destination; return flight routing etc.
2. Drive Own vehicle or use any other means of conveyance to airport 3. Park vehicle at airport parking areas or dropped at terminal entrance	Vehicle registration number; time; date; vehicle registered owner; facial recognition data; movement/whereabouts using start CCTV systems; taxi/drop off; parking location; any separation from luggage
4.Walk to check-in or Baggage Drop-off / walk to other areas of airport (e.g. cafeteria) 5. Queue for check-in or baggage drop-off	Whereabouts, duration at location(s) meeting who? Is movement normal; is there separation from luggage?; Information from baggage drop-off; number & weight of luggage; automated or FR CCTV footage.

6.Check-in/drop hold luggage/online check-in/Number of hold luggage check-in. 7. Security Questions - Behavior analysis	Did passenger check in solo or in group; behavior of passenger; was passenger accompanied with a non-passenger; does the luggage make sense taking in view the travel plan/phase?
8. Hold Luggage weighed, tagged, accepted & deposited on the departure conveyor 9. Hand luggage also weighed (& at times also tagged). 10. Passenger boarding card issued- aircraft seat allocated,	What type of luggage? Weight; Seat number? Did passenger ask for a specific seat? Facial recognition
11. Hold Luggage is screened by EDS automated process 12. If EDS goes to level 2, hold luggage is further examined 13 Secondary means of screening may be used (e.g. ETD) 14. Examination of hold luggage in the presence of passenger or rep may be performed/other phases as necessary 15. Other AVSEC phases as necessary 16. In certain circumstances EOD/Police/Other entities shall be involved	Luggage Image and content; Does content tally with what passenger says? Other luggage information- does content make sense? Other security procedures- information gained? Any suspicions, gaps, concerns?
17. Passenger goes through access control procedures;	Access control – times/facial recognition Queuing time; Behavior while queuing

Future of Airport Security

18. Queues for departure security procedures	Did a particular check-in hold luggage, while another person presents him/herself for departures security procedures?
19. Divestment of items at security check point 20. Screened via WTMD or Security Scanner or other 21. Cabin baggage is security screened by x-ray/EDSCB or other 22. Any permissible LAGS over 100ml will be screened by LEDS 23 Passenger & hand luggage may be selected for secondary ETD/other security procedures 24 Hand luggage may be hand searched/further examined if screener has concerns or on random basis.	Behavior analysis Automated facial analysis Content of hand luggage Answers to questioning Results from x-ray, ETD, EDSCB; LEDS, EDD, other Apparel, clothing. Does it fit social class and weather conditions at destination?
25 Passenger proceeds to Departures (sterile area) 26. Queues up at departures boarding gate 27 May be subjected to additional security procedures at gate 28. Is transported or walks to departing aircraft 29. Boards departing aircraft 30 Aircraft departs- Passenger onboard.	Behavior Analysis Cred card use at Departures Area Abnormal time in rest areas/other areas Meeting with airport staff or other passengers in sterile areas
LANDS AT NEXT AIRPORT	ADDITIONAL INFORMATION/DATA GATHERING PROCESS

Future of Airport Security

An example of how data is collected is illustrated in table 1 depicting a 30-point passenger travel journey., different airports could come up with other ways of doing it depending on the data they are interested in. Theoretically, there are various ways of capturing date it all depends on airport's perception of risk and areas of interest, whether they are targeting an enhancement in the processes, statistics, improving security…etc. The concept of IoT if planned properly taken into consideration the 30 steps mentioned above could aid airports to enhance their performance, procedures, and customer satisfaction levels, as the key in all of this is ''Data'' being able to manage data, and receive live notifications enhances facilitation and improves security dramatically.

The above is only brief of the information that could be gathered using IoT, some of those data are already available in today's operations. However, such data is dispersed. At the same time, currently it is difficult to get hold of certain data at a specific point in time. As a result, IoT provides a solution by integrating the systems that are used to complete a passenger's journey, connecting them to one another, with predefined rules for the system to automatically takes decisions If not, one can also opt for a system which alerts security personnel where a suspicious case has been identified..

1.1.5 Challenges in IoT implementation at an airport

Like any other technology there are pros and cons to the use of IoT. It is the writer's belief that the pros overcome the cons. The unique thing about IoT is that the user can be as creative as his mind can think, as the system allows limitless integrating of various systems, therefore, the benefits are endless.

There are several IoT vulnerabilities depending on the set up, with the main challenges as follow:

Future of Airport Security

1.1.5.1 Security

The main challenge in IoT is the network security. Since IoT connects several devices and components to one another, in theory if one device/component is targeted and hacked, the entire network may be at risk in view of the overall connectivity.

This vulnerability can be mitigated by installing a holistic cyber security framework. For this to be achieved, cyber security experts need to have a thorough understanding of how the devices send and collect information, the way they are connected to systems, in what way they can be managed, how to stop intruders, and how to preserve access logs in cases of cyber incidents. Finally, cyber security experts would need a full understanding of the information flow from one device to another a how such devices can be secured. As a result, having a full understanding of the system, could enable airports to securely implement and benefit of the vast advantages of IoT. (Pratt, 2019)

1.1.5.2 Connectivity concerns

Like data security, data privacy is again one of the biggest concerns in todays interconnected world.

In IoT where data is constantly being captured, compiled, stored and transferred, from one device to the other, one may find several challenges., Challenges vary with a primary one being the resistance between entities to create an IoT network. Some entities resist the idea of connecting their system to others, an example of such a need which may be resisted is the need of interconnectivity at an airport., Various aviation stakeholders interact in a passenger's journey, having access to a large amount of timely and important data. Hence, connecting their systems together would provide a great deal of information which can be eventually be used for aviation security, operations, facilitation and other functions. However, some entities especially governmental entities may opt to resist for their systems to be linked to a different network. Reasons vary from protecting their data, to protecting their networks.

The second connectivity concern is that since the IoT connects several systems and devices together, this may prove to induce a vulnerability in the system as several entities could potentially access to the data in the interconnected network, with a risk to illicit data access or leakage.

ARTIFICIAL INTELLIGENCE (AI)

AI is one of the emerging technologies that greatly helps in every aspects of the aviation industry and is currently being adopted by some airports worldwide. Recent x-ray machines have AI embedded in the software automating partially or fully the screening processes. Since this introduction, AI has facilitated and reasonably secured passengers' travel through several innovative security equipment incorporated with AI. One direct example is the incorporation of Explosion Detection Systems (EDS), and Liquid Explosive Detection System (LEDS) embedded in x-ray machines. Even though the development of the AI is not 100%, it's still a major game changer, by significantly enhancing the screening process and allowing the screener to automatically detect explosives, both liquid and solid. A game changer where before the development of such technology, the aviation security industry had to solely rely on the capability of the screener to detect such prohibited articles.

A key component when using AI in AVSEC operations is the capability of the system to adapt and learn generally referred to as ''machine learning''. In general, AI improves on the information fed into the system. Moreover, another benefit of the incorporation of AI is that it learns from its errors, enhancing its capability, it enables the machine to take a Signiant amount of data into consideration leading or assisting in decision making.

From a passenger standpoint, AI helps to facilitate and enhance the customer experience in a way that it allows passengers to proceed through security checkpoints with all their items including laptops inside their carryon bags. (An example of such a security equipment which allows such facilitation is the CT C3).

1.1.6 Application at an airport

There are several ways of introducing AI in an airport security environment, with one of the most efficient ways of using it is in the incorporation of x-ray machines, CT scanners and security scanners (previously known as body scanners) which allows AI to automatically identify threats.

The key of having an efficient AI system relies on the data fed into the system. The more information is fed into a system, the more the AI systems improves. This is generally referred to as machine learning.

A major advantage with the incorporation of AI is that machine learning can be used to thoroughly identify data. With the result of enabling systems to identify threats much faster than humans would. Instead of relying of the human element to perform such screening, why not 'train' a computer, feed it with accessible and vital data, thus allowing it to perform the necessary security functions for us?

Moreover, another advantage of AI is that it does have an artificial brain, allowing it to learn from its own mistakes in a way that they are not repeated.

A straightforward example occurs during the testing and development phase of security equipment (before the equipment is rolled out commercially). During this phase, the equipment is 'fed' with an amount of data in order to test the detection capability, and the False Alarm Rate (FAR). While testing the equipment, it continuously and on the go 'fed' with additional prohibited articles and/or various forms of explosives and Improvised Explosive Devices (IEDs). Whenever a prohibited article is undetected, the equipment technical staff notify and re-configure such items into the system by highlighting the threats individually. As a result, the security equipment learns and adapts, allowing its detection capability to continuously be updated, refined and grow.

Future of Airport Security

In general AI is embedded into a system or machine e.g. (X-rays, body scanners, CT etc.) hypothetically, in the writers view, it is key in having an automatic screening process which will enhance security, save cost, increased throughput, customer experience due to fast clearing process.

AI will present a significant impact on airport security, and as stated above below are the benefits of implementing it for aviation security:

1.1.6.1 Enhanced Security

The more systems are fed with data the more the increase and the development of the detection capabilities. Machine learning is one of the major benefits of AI, allowing the machine to intelligently learn and update the threat library to later be detected. In addition, since there is no human interaction or distraction, human error is eliminated, thus leading to enhanced airport security detection standards.

1.1.6.2 Cost saving

Introducing AI to a system is one key of automation, in current aviation security set up. AI is used in CTs enabling explosives detection for both solid through EDS and liquid via LEDS. However, the way it is used today is semi-automated as the detection capability of the AI is not yet fully mature, thus allowing percentage of false alarm rates. To date, systems are not yet ready to go for a fully automated solution. In order to proceed for a full automated screening solution, the industry has to await that AI is developed enough to enable items to be screened thoroughly with a very high detection capability and a low false alarm rate.

Having said that, a mature and developed AI, should in turn drive Aviation Security Regulators at National levels to allow airports to consider fully automated screening processes (which would initially be under trial phases)thus saving the industry a percentage of the cost of security personnel deployment , at security points. Such savings may however be condensed if one considers the high costs associated with AI related costs such as data maintenance, recovery, system codes and upgrades.

1.1.6.3 Increased throughput and customer experience

Enhanced detection capability brings forth other benefits for the aviation industry. The advanced detection capabilities of AI allow bags and people to be cleared at a faster rate than when operating the customary x-ray equipment and a walk-through metal detector. In addition to throughput, the quality of screening proves to be much better, allowing automatic detection of various prohibited items. As a result of this, passenger satisfaction rate would be expected to increase due the fast and less invasive screening process.

1.1.7 Challenges for AI implementation

Similar to any other innovation AI also has its own implementation and operational challenges. For example, if one compares the human brain with an AI machine, it would be realized that even though AI reduces drastically human error, it would be extremely difficult to perfectly mimic the God endowed human intelligence carried in the human brain.

The major difference between AI and humans is that AI does not carry emotions and moral values. AI driven equipment only perform what they are programmed and developed. AI also does not have the emotions to judge right from wrong from a humane perspective, and if encountered with an unfamiliar situation, the machine would be expected to either perform deficiently or breakdown.

RISK BASED SCREENING

In order to complement the use of IoT and AI, Risk Based Screening (RBS) is recommended. RBS is a security concept that uses the information of the passenger to categorize the risk he/she imposes, based on the risk score the type of screening is determined. One way of implementing

Future of Airport Security

RBS is identifying travelers considered low risk (majority of travelers). Once identified, such passengers may have an expedited different level of security screening.

Such a RBS approach would benefit both the passenger and the airport from security perspective and a facilitation point of view., RBS allow that if their risk score is low, hence considered low risk then the security provisions applied will be in line with the low risk, hence faster and not as thorough as unknown and high risk passenger.

The reason why RBS would greatly complement IoT is that IoT already provides a live and continuously updated information set up., Such a continuous live updating system would prove similar to having continuous risk assessment on an airport. When the risk goes up the system will automatically alert security personnel. Alerts would be based on predefined rules input in

It is acknowledged that IoT integrates several systems to one another. Hence, thanks to the use of IoT passenger profiling would be easier to implement. This would be made easier, since as mentioned in Table 1, at each of the 30 processing points, data is captured and analyzed, providing a gradual clearer picture until the boarding process takes place. Such analysis places the system to categories the passenger as a low or high-risk passenger, highlighting alerts for the mitigating security procedures necessary in line with the risk.

FIFTH GENERATION TECHNOLOGY

Since the writer’s proposal incorporates the capturing and managing of live information and actions, the fifth-generation technology (5G) would have a big role in enabling live responsive IoT network, due to the increased bandwidth, and lower latency,

As a result, from a technical perspective, it is being proposed that IoT should be complemented with 5G network to enable most of the IoT capabilities.

CONCLUSION

In the writer’s view, the best set up for capturing the indicated passenger data is by utilizing a combination of both IoT and AI in aviation security.

IoT would gather any required data delivering it at the right time to the required channels, providing security personnel an opportunity to perform the necessary security procedures which would be all based on a number of corroborated data. Besides moving away from the ‘one size fits all’ technique, this RBS approach would also reduce the inconvenience for the genuine passenger.

REFERENCES

ACI. (2019). *The ASQ Barometer Q2 2019*. Retrieved 09 24, 2019, from ACI. AERO: https://aci.aero/customer-experience-asq/services/asq-barometer/

Bates, J. (2019). *Customer Satisfaction Level Rise at World's Airports*. Retrieved 09 24, 2019, from airport-world: http://www.airport-world.com/news/general-news/6870-customer-satisfaction-levels-rise-at-the-world-s-airports.html

Columbus, L. (2017, Jan 29). *Internet Of Things Market To Reach $267B By 2020*. Retrieved from Forbes: https://www.forbes.com/sites/louiscolumbus/2017/01/29/internet-of-things-market-to-reach-267b-by-2020/#12d9fa11609b

Grover, A. (2019, March 26). *Airport IoT Solutions: Redefine Personalization and Customer Experience* . Retrieved from kelltontech: https://www.kelltontech.com/kellton-tech-blog/iot-ushering-new-era-smart-airports

Hoggan, K. (2019, September 11). *Will Artificial Intelligence Improve Airport Security?* Retrieved from h4-solutions: https://www.h4-solutions.com/blog/will-artificial-intelligence-improve-airport-security

IATA. (2018, Oct 24). *IATA Forecast Predicts 8.2 billion Air Travelers in 2037*. Retrieved Sep 17, 2019, from Iata.org: https://www.iata.org/pressroom/pr/Pages/2018-10-24-02.aspx

International Civil Aviation Organization. (2011). *Aviation Security Manual.* International Civil Aviation Organization.

Mann, C. (2017, March 27). *Ensuring quality screening and passenger experience alongside astronomical growth*. Retrieved from internationalairportreview: https://www.internationalairportreview.com/article/33547/security-screening-smiths-detection/

Morgan, J. (2014). *A Simple Explanation Of 'The Internet Of Things'*. Retrieved 09 30, 2019, from Forbes: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#310ec1191d09

Pratt, M. K. (2019, Feb 18). *Top challenges of IoT adoption in the enterprise*. Retrieved from internetofthingsagenda.techtarget: https://internetofthingsagenda.techtarget.com/feature/Top-challenges-of-IoT-adoption-in-the-enterprise

Future of Airport Security

Reddy, K. (2019). *Artificial Intelligence Advantages and Disadvantages*. Retrieved from content.wisestep: https://content.wisestep.com/advantages-disadvantages-artificial-intelligence/

Rouse, M. (2016). *Internet of Things (IoT)*. Retrieved from internetofthingsagenda: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

Violino, B. (2019, April 15). *Will 5G play a role in IoT security?* Retrieved from zdnet: https://www.zdnet.com/article/will-5g-play-a-role-in-iot-security/