ISBN: 978-628-95207-4-3. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2023.1.1.1673

Review of Internet of Things Applications in Airport Infrastructure and Operations

Jacob Michael Christensen, student*, Owen Guerra-Mondragon Saenz, student†,
Luis Felipe Zapata-Rivera, PhD.†, and Catalina Aranzazu-Suescun, PhD.*
*Embry-Riddle Aeronautical University, USA, Department of Cyber Intelligence and Security,
†Embry-Riddle Aeronautical University, USA, Department of Computer, Electrical and Software Engineering

***Abstract*—The Internet of Things (IoT) is being used in a vast number of fields, from consumer IoT and smart houses to health, smart cities, smart grids, smart agriculture, smart vehicles, and airport services [1]–[3].**

IoT can be defined as a network of interconnected devices that share information about the environment and people to offer intelligent computing services to improve quality of life. In 2022, there was an estimated 13 billion IoT devices connected to the internet, and this number is expected to grow to 30 billion by 2030 [4].

Currently, IoT systems are envisioned in various airport applications, from airport passengers and staff services to luggage management, and security infrastructure. However, these recent technologies have created big challenges, especially in cybersecurity. Most of the commodity IoT devices are inexpensive, resource-constrained, and built by many suppliers, hence not developed using a secure-by-design approach. This makes them vulnerable to the growing spectrum of cyberattacks and warrants that security considerations are made for their applications.

This survey paper presents an overview of the current state of the art of IoT applications in airport services and operations. The analysis includes a comparison of the technological specifications of the implementations and some considerations from the perspective of cybersecurity. It was found that 83% of the implementations analyzed do not have a security mechanism to protect the users and system data.

***Index Terms*—Airport, Applications Internet of Things, Security, Software.**

I. Introduction

In the context of the airport industry, IoT is used to optimize processes, and as a solution for locating staff and equipment, with sensor data to improve safety and productivity. Examples of applications in airports include service equipment, ground-handling equipment indoors or outdoors, monitoring the operational health of automatic doors, escalators, moving walks, operation of heating and cooling units, loading equipment, and power units, among others [5].

Specifically, in the context of Airport IoT Support, Kellton company offers the "Optima" solution, an IoT micro-services-based platform [6]. These types of systems enable airports to offer a connected experience to the customers, optimizing processes such as check-in, parking, security checks, flight boarding, and in-flight services; improving and adding a smart component to the overall experience while users are in the airport facilities.

Airport services supported by IoT include luggage tracking in which airport staff can identify and locate any piece of luggage from their devices. Systems for tracking people are used to identify passengers, and employees through each security point; for this service, the support of biometric and database systems are used. Local weather services are supported by sensors on the runways and by internal and external forecasting systems.

Alert systems are classified as infrastructures that notify to any abnormal events generated inside the airport facility. These alert systems are also implemented to inform passengers about specific conditions throughout the airport, such as expected time for passing security checks or wait times for baggage carrousels. Security services are focused on the detection of unauthorized items and identifying persons of interest within the airport. These services are also needed to improve the surveillance services during off hours. Motion sensors and closed-circuit television (CCTV) cameras are commonly used in these systems.

This paper presents an overview of the current state of the art of IoT applications in airport services and operations and is organized as follows: Section II presents IoT applications for airport parking, baggage, and passenger navigation management. Section III presents a description of IoT applications for airport security and monitoring. Section IV presents an analysis of the IoT systems discussed in the previous sections and an analysis of security issues found in these implementations as well as possible solutions. Finally, Section V states the conclusions of the paper.

II. IoT applications for airports parking, luggage, and navigation management

Several authors have been working on luggage handling and management using IoT systems based on technologies such as Radio Frequency Identification (RFID).

Authors of [7] implemented both handheld and stationary RFID tag-reading devices, in combination with real-time tracking, to prevent accidental loss or mishandling of traveler luggage. Passenger information collected by these devices would be transmitted to a cloud-hosted database (MongoDB)

Digital Object Identifier (DOI):
http://dx.doi.org/10.18687/LACCEI2023.1.1.1673
ISBN: 978-958-52071-4-1 ISSN: 2414-6390

where it can be reviewed and managed by airport personnel. In addition, passengers can use a web-based or smartphone application to view the status of their own baggage at the airport. Similarly, authors of [8] proposed a work that allows passengers to track their checked-in luggage in real time using RFID. The baggage would be tracked using access points and an Electric Product Code (EPC), which identifies the baggage's product number and serial number that is uploaded to both the Local and Global Registration Centers. The authors of this paper defined a distributed and centralized solution. The centralized solution dealt with a proprietary closed standard (EPCGlobal), while the distributed solution used an open standard (SIP). The EPCGlobal process has advantages regarding latency but may have potential scalability issues regarding bottlenecks. The SIP process, although similar to the EPCGlobal, requires more steps to save the desired information, which may cause stale data and latencies. Furthermore, the writers of [9] proposed a methodology that integrates RFID with luggage management for the purpose of streamlining the baggage check-in and retrieval process for passengers (See figure 1). Sensors located at various points within the airport will be able to detect and read RFID tag data to ensure that luggage is loaded onto its appropriate aircraft. Upon arriving at the destination, when the luggage is unloaded and transferred from the aircraft, four RFID sensors on the conveyor belt will detect the luggage, so it can be delivered to its respective counter. In addition, passengers will receive a unique identification code sent via Short Message/Messaging Service (SMS), which can be entered at a kiosk found at the destination airport to authenticate themselves for baggage retrieval.

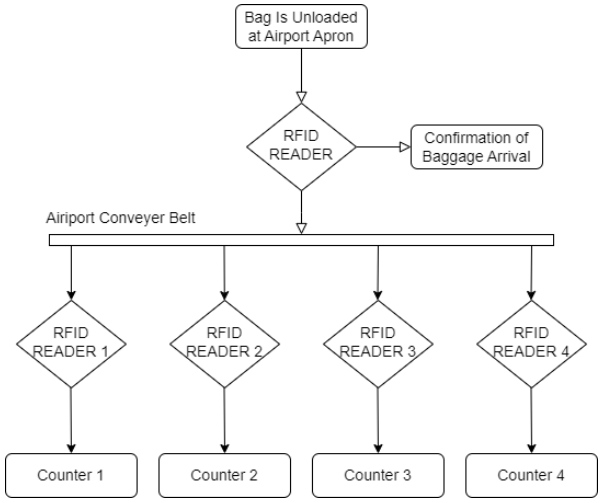

Fig. 1. Depiction of algorithm that appropriately delivers luggage using RFID [9]

Ground handling services are the predominant reason for which passengers' luggage becomes missing as a result of a diversion in the belongings' transfer between airplanes (52%) [10]. RFID sensors accurately route customers' luggage to the airplane in less time and with greater throughput. The authors developed a user-friendly application that uses RFID to minimize the amount of lost luggage. The application software consists of four classes, MasterControlProgram, CheckInTab, Engine, and Manager. The MasterControlProgram class then creates an instance of Engine, which then creates an instance of Manager. The CheckInTab allows the user to input their information and their corresponding flight information. Luggage is then sent through a security screening before arriving at the airplane.

RFID can be also used to optimize the routing of luggage in an airport. Authors of [11] plan and design an architecture called IoT-DRPA (dynamic route planning approach) for an improved baggage transport system. By taking advantage of IoT technologies, real-time tracking information, based on RFID, can be used as an additional input parameter to a routing algorithm for luggage pathing. This algorithm can predict "in-conflict tasks" and can adjust accordingly to avoid congestion, similar to a network load balancer. The concluding results showed a ten percent improvement in efficiency compared with other routing algorithms, with a five percent decrease in throughput time.

Other approaches for baggage handling proposed the use of Wi-Fi communication for tracking luggage pieces with the use of QR codes. Authors of [12] describe, in general terms, how IoT technology can be used at various levels of airport operations. Through a cluster analysis case study, it was concluded that all analyzed airports have some method of automated luggage handling. Authors of [13], claim that one of the biggest reasons for mishandled luggage is poor authentication checks for passenger identification. This research proposes a solution to this problem for when travelers retrieve their own luggage from baggage handling systems using machine learning and quick response (QR) codes. The idea is that the identification process should be automated since manually processing information is inefficient and ineffective.

This system involves two steps: check-in and check-out. During check-in, user information is collected, and a face scan is conducted. This would be stored in a centralized server and a QR code would then be generated and sent to the user. During check-out, a facial recognition scan along with QR authentication needs to be performed before luggage retrieval can occur.

In the line of smart parking, the authors of [14] present a system where users can log in, and through a cloud link, they would be able to see their vehicle location. The system administrator can see the IP address link of any given user. Through the Arduino field, they will have access to information about the user's vehicle and parking location. Similarly, authors of [15] proposed another solution to the issues surrounding airport parking that would allow passengers to find, reserve, and pay for vehicle spaces all from the convenience of a mobile application. Sensors would be scattered across the airport's parking lot and could wirelessly communicate with the base station of their availability. There are three actors in this system: the user, the web administrator, and the parking

controller. The user's role is to use the mobile application to find a parking spot. The administrator oversees the processes of the application and updates the application's database. Finally, the parking controller is an error-handling mechanism as it checks for faulty sensors or other anomalies.

For navigation assistance, most buildings have static maps around the area that try to assist users with finding their destinations. However, this may not be ideal when considering more complicated layouts. Authors of [16] proposed a solution to indoor navigation without the use of global positioning system (GPS) technologies. It relies on two technologies: QR codes and Inertial Measurement Units (IMU) to track traveler movements throughout the airport complex. The passenger would scan a QR code for an estimation of their current position. At the same time, the IMU devices would communicate with the user's smartphone to trace their location when moving around. It should be noted that the IMU would be placed on the user's foot which raises questions about the logistic feasibility and general acceptance of this project.

During the COVID-19 pandemic, some authors attempted to ensure the health of airport passengers by refining the maintenance of restrooms. Authors of [17] designed a system that keeps track of bathroom data such as capacity, humidity, temperature, and amount of soap and other supplies. The design included the use of Low-Power wide area networks (LPWANs) and the Long Range (LoRa) protocol. A key feature of the proposed architecture is the ability to adjust based on any error, modification, or irregularities that occur. This feature is achieved by using PANGEA multiagent system. The App Monitoring Database consists of the Control Center, whose inter-workings include the monitor, cleaner, analysis, and alarm. In addition, Organization Smart Monitoring consists of the current temperature, light levels, weight (soap bins), distance (trash cans), human detection, and room humidity. Finally, the Application Interface is responsible for the mobile and web applications to interface with the system.

III. IoT applications for airport security, monitoring, and tracking

IoT systems have been widely used for security in different organizations. In airports, IoT has been used to monitor passengers, anomalous events, and incidents inside the airport facilities and to have access controls of the different facilities. Authors of [18] proposed a facial recognition system for user authentication and secure access control. The paper mentions a wide range of potential use cases, including employee or even criminal identification for security in both the public and private sectors. However, this research paper specifically describes this project for use as a home security system with doorbell integration. In the line of surveillance, authors of [19] combine machine learning and CCTV surveillance cameras for detecting, identifying, and alerting to abnormal human behaviors. The authors propose to break down video frames to train an algorithm with a large dataset of pre-labeled "normal" and "abnormal" activities. In theory, this could be used in conjunction with current security systems to assist staff in locating threats as they occur. To improve facility efficiency and productivity, the authors of [20] propose a digital IoT-based solution for a smart airport monitoring system. With the ability to examine and manage production assets in real-time using GPS and other wireless technologies, passengers can have a better quality of life with travel planning and navigation, while internal staff can quickly respond to emergency situations and prevent incidents before they happen. The main parameters of this system include location, speed, and direction of vehicle movement, operation of the main engine, fuel tank levels, mileage, operating hours, position of the parking brake, and the operation of the aircraft beacon. In addition, smartphones can be used for tracking employees as well as notifying them when they enter dangerous or otherwise prohibited locations (See Figure 2).

RFID can be used to develop tracking systems for luggage and passengers. In the work of [21], the authors presented an implementation of an RFID-driven, IoT-based airport. The proposed operation architecture is centered around the airport, aircraft, apron, and destination being able to communicate via RFID readers connected in a client-server network. Following check-in, passengers are given an RFID tag to pin to their clothing, and a separate RFID tag is attached to their luggage to automate the user's travel experience. The tags are then activated and will be used to keep track of the passenger's trip. This may include passing through security, arriving at the gate, boarding the plane, and finally arriving at their destination. After undergoing a simulation of this methodology applied to the Airport of Birjand, the authors came to the conclusion that this new system significantly decreased passenger wait time and improved security. Similarly, authors of [22] presented a simulation of airport RFID passenger tracking using Terminal 3 of the Chicago O'Hare airport as a model.

The communications model section of the paper described the placement style of the RFID sensors as well as the chosen methodology and protocol. A minimal number of antennas that could cover longer distances was desired. They calculated the minimal effective distance to be 2.5 times larger than the coverage radius of the antennas. Furthermore, the author's system follows the Slotted ALOHA protocol to accurately recognize new tags entering each RFID zone. Finally, the authors categorized the types of passengers to be tracked: departing, arriving, and connecting (with a priority in the first two). Simulating a day with 1,122 flights, the authors concluded that with the Pareto Front, there is an error margin of 14%-20% when tracking departing passengers and 2% for the arriving passengers. Also, authors of [23] use RFID tags for indoor tracking and address the problem of synchronization in ultrasound signals when attempting to track an indoor position. In the first phase, the authors focused on the hardware function in the tag that detects an RF event. The RFID's interrogation pulse is simultaneously read by all tags, allowing the emitters and receivers to begin their functions. The considered machine learning algorithm would be used to eliminate the need for

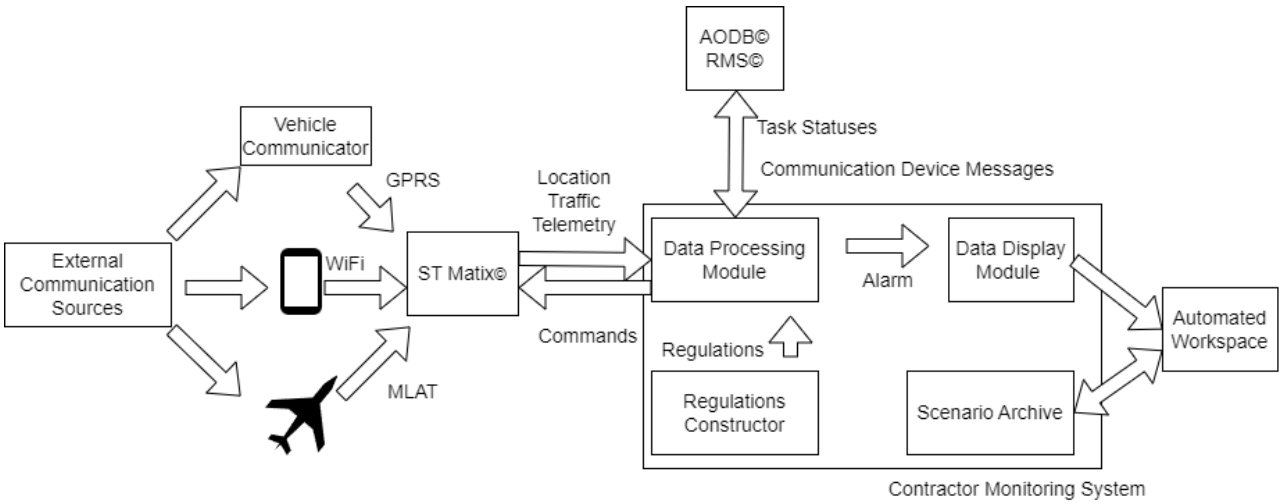

Fig. 2. Architecture of described monitoring system. [20]

calculating cross-correlation. The second approach involves the monitoring/tracking of the RFID tag. The tag obtains coordinates locally; therefore, it would be able to update its position after every frame. When implemented in a normal-sized room, this methodology would have a reported average flaw margin of less than 25cm over 95% of frames.

The authors of the work [24] presented an IoT solution for regulating access control regarding airports. Typically, access doors can be remotely controlled by an operator. However, when problems arise in the system's network, the operator would no longer be able to manually let any authorized personnel into the restricted area. This problem can be solved by introducing a "smart door lock" that automates the control of specific access doors using IoT. The smart door lock is comprised of a NodeMCU microcontroller, a relay, an electric magnetic Lock (Em-Lock), and an adapter with an output of 12VDC. This system would then allow access doors to be controlled by authorized personnel using a smartphone application instead of relying on the operator.

The writers of [25] claim that many current airport IoT network systems struggle to maintain historical and real-time data collection. To help alleviate these issues, this project outlines the implementation of a data storage solution using open-source software and locally hosted devices. By pursuing a centralized approach to data storage, airport staff would have an easier time maintaining their systems and would be able to address security threats efficiently.

Some authors decided to present a holistic overview of security in airports as they exist currently. For example, in [26], researchers examined the current state of security practices implemented at several airports across the European and American regions through the use of distributed surveys. Of the replies that were received, only half claimed to have security policies that were effective. In terms of what defines best security practices, the researchers broke this down into three subsections: "technical", "organizational", and "policies & standards". As expected, the smart airports – ones with a high integration with IoT systems – typically performed the best in all three categories. However, what is most interesting is that many of the most basic security standards, such as encrypting data and changing default credentials, were reported to have a low rate of implementation.

IV. Analysis of IoT Implementations

This section analyzes multiple IoT implementations in the context of airport infrastructure and operations.

Table I presents the comparison of aspects of hardware, software, communications, and security, including methodologies, integration, and protocols, among others presented in the implementations.

Table II presents an analysis of the security issues identified in the implementations described in the previous sections. Additionally, a proposed solution for each security issue is presented that can mitigate each possible attack discovered in the implementations.

* in the table, means that was defined using the diagrams presented in the papers.

In terms of licensing, many of the analyzed applications did not report enough information to determine the type of licensing (proprietary, open source, or freeware) of the hardware or software elements used for the implementation.

It is important to note that at the software level, the solutions may include combinations of elements with multiple types of licensing, making it difficult to classify them as one single type. The hardware can also be the product of integrating multiple components with multiple licensing properties.

The implementations evaluated are not commercial products; they are research projects that have not been distributed as a commercial solution. Therefore, no licensing for the final product is proposed.

TABLE I: Comparison of implementations characteristics

Category	Ref	Controller	Sensors	Comm Protocol	Network Topology	Target User	User Interface	Encrypt Algorithm	Key Exchange
AI Surveillance	[19]	N/A	Camera	GPS	N/A	Staff	N/A	N/A	N/A
AI Surveillance	[18]	Raspberry Pi	Camera	N/A	N/A	Staff	Website	N/A	N/A
Data Storage	[25]	N/A	N/A	N/A	*p2p, star	Staff	N/A	N/A	N/A
Door Locks	[24]	ESP8266 NodeMCU	N/A	Wi-Fi	*Hybrid: Tree + bus	Staff	Mobile App	N/A	N/A
Indoor Positioning	[23]	STWIN SensorTile wireless node (STEVAL - STWINK1B)	RFID sensor / tag and ultrasonic sensors	RFID	N/A	Passengers and Staff	Mobile App, Website	N/A	N/A
Indoor Positioning	[16]	N/A	Camera / IMU	Bluetooth	N/A	Passengers	Mobile App	SNOW 3G Stream Cipher	ECDH (FourQ Curve)
Indoor Positioning	[22]	N/A	antennas / RFID sensors	RFID	N/A	Staff	N/A	N/A	N/A
Luggage Management	[11]	N/A	RFID readers	RFID	point to point	Staff	Stationary Device	N/A	N/A
Luggage Management	[13]	BCM2835 SOC	8MP camera	RFID	N/A	Passengers	Kiosk, Website	N/A	N/A
Luggage Management	[8]	N/A	RFID Readers	Wi-Fi, Bluetooth, ZigBee, RFID	*hybrid: star + tree, star	Staff	Web App	N/A	N/A
Luggage Management	[9]	Raspberry Pi 3 Model B	RFID Reader / MR6011 Tag	RFID	N/A	Passengers	SMS (Mobile)	N/A	N/A
Luggage Management	[10]	N/A	RFID readers/tag	RFID	P2P	Passengers and Staff	N/A	N/A	N/A

Continued on next page

TABLE I – continued from previous page

Category	Ref	Controller	Sensors	Comm Protocol	Network Topology	Target User	User Interface	Encrypt Algorithm	Key Exchange
Luggage Management	[7]	STM32 F767ZI ESP32	Proximity Sensor	Wi-Fi, RFID	*bus, star	Passengers and Staff	Mobile App, Handheld Device, Stationary Device, Website	N/A	N/A
Monitoring	[20]	N/A	CAN Controller, Relays, Fuel Flow Meter, Inductive, Temperature sensors	GPS	*Hybrid: Star + bus	Staff	*Mobile App	N/A N/A	N/A
Monitoring	[17]	Rocket Scream's Mini Ultra Pro	Passive pyroelectric, pressure, digital time of flight, ultrasonic sensors	LoRaWAN	hybrid: star and ring	Staff	Mobile App, Web App	mentioned but not specified	mentioned but not specified
Passenger Authentication / Tracking	[21]	N/A	OMNI-NGW-2 RFID Reader, IQ-100 tags	RFID	C2S	Passengers	RFID badges / necklaces	N/A	N/A
Smart Parking	[14]	Arduino Uno, ATmega328, ENC28J60	GPS Location Finder	Wireless communication, GPS	*bus	Passengers and Staff	Mobile App, Website	N/A	N/A
Smart Parking	[15]	N/A	N/A	N/A	*hybrid: star+ tree	Passengers and Staff	Mobile App, Web App	N/A	ECC

TABLE II: Analysis of security issues identified in the implementations

Ref	Security Issue	Proposed Solution
[7]	Passive sniffing attacks against BHS devices can result in unauthorized access of passenger PII (Personally Identifiable Information) during transmission to the centralized database.	Implement an encryption standard during Tx to the server.
[14]	IP spoofing attacks can be used to compromise user vehicle locations for unauthorized monitoring.	Use encryption algorithms to hide the IP addresses from unauthorized users.

Continued on next page

TABLE II – continued from previous page

Ref	Security Issue	Proposed Solution
[11]	MITM attacks can be used to read/alter RFID data before reaching the stationary devices. This can be used to passively collect information about passengers or actively disrupt the service.	Use RFID tags that use encryption algorithms to send the information.
[21] [8] [22] [10] [9]	RFID cloning can be used to falsely authenticate oneself through airport security.	Use RFID tags that implement security such as encryption, therefore cloning the tag is difficult to do.
[13]	DoS (Denial of Service) attacks against the Web application server and or database can prevent passengers from being able to authenticate themselves and disrupt the baggage collection process.	Using elastic capacity cloud servers, the systems can keep being available while the attack is contained. Implementing blocking of requests coming from IPs out of the expected geographical location can reduce the risk of receiving a DoS attack.
[24]	Social engineering against an employee to compromise their Google account can result in unrestricted access within the airport facility.	Enforce two-factor authentication standards with employee accounts.
[20]	Jamming (or falsely providing) positioning signals from airplanes to the centralized control system can cause disruptions in the service or even physical emergencies.	Have an extra GSM provider that uses different frequencies if jamming occurs. Adding Wi-Fi support to the aircraft to collect and transmit the data from the STAB Liner directly to the server.
[23]	Malicious ultrasonic-emitting devices can jam the communication between the legitimate RFID tags and the RFID reader in the system.	Configure a system that alerts if a jamming attack is occurring and where it is located.
[25]	MAC flooding attacks against switches can force them to default into a hub-like state where data packets are distributed throughout each interface. This can be used by an attacker for network sniffing.	Invest in switches that implement switchport port-security or similar features, e.g., Cisco. Network administrators can implement measures to prevent physical access to the network infrastructure.
[15]	DoS attacks against the web application can render it unavailable for normal users.	Using elastic capacity cloud servers, the systems can keep being available while the attack is contained.
[16]	MITM (Man–In–The–Middle) attack between the IMU (Inertial Measurement Units) and passenger smartphone may lead to the ability to track users.	Use encryption algorithms to send the information from the IMU to the system. Use of dynamic codes for connection.
[19]	Threat actors can wear specific patterns on clothing that confuses image recognition networks from detecting human figures.	Have higher resolution cameras that can distinguish background images and subjects. Implement the most recent machine learning algorithms that can identify and recognize more human shape patterns.
[18]	If data for an authorized facial recognition pattern is obtained, a MITM attack can be performed against the server to authenticate oneself.	Combining biometrics validation such as fingerprint can prevent an attacker from having all the elements needed to impersonate the real user.
[17]	Threat actors could artificially inflate the amount of traffic entering or exiting any connected location by continuously moving across the associated sensors. This would alert sanitation crews earlier than expected and may cause disruptions.	Image recognition systems to determine the direction of the traffic and detect that the same person is entering and exiting. Adding a system that correlates supplies and the traffic of people.

As shown in Table I the identification and location of people and objects is mostly based on the use of RFID communication technology, due to its flexibility, low cost, and possibilities of indoor use. The use of RFID creates the need to evaluate possible security vulnerabilities that this technology may add to these systems. More information about this is presented in Table II.

In terms of controllers and sensor technologies used as IoT node devices, a wide variety of microcontrollers were identified, from basic Arduino to more sophisticated single-board computers such as Raspberry Pi's. The fact that some of these implementations use off-the-shelf devices, generates security risk in terms of the possibility of having back doors due to available not-in-use ports in these devices.

Within many cybersecurity circles, it is generally well known that product functionality often has priority over security, especially when it comes to designing home and general-use IoT devices. However, not much attention is given to industrial IoT design in the public sector.

As is illustrated in Table II, many of the implementations meant to enhance airport infrastructure have severe vulnerabilities in their security that could result in disruption of the service or even loss of personal information. Many of these issues could be resolved with some simple alterations; however, it was found that only 17% of the implementations analyzed had an encryption and/or key exchange schema to protect the information transmitted in the network.

Also was found that none of the implementations use any type of digital signature algorithm for authentication and authorization control. Even then, the authors of [16] decided to use a steam cipher (SNOW 3G), which is not known to be as secure as other alternatives such as AES-GCM.

Finally, the research found in [26] is thus additional evidence to support how cybersecurity is often an afterthought in public IoT architecture design. This finding poses a security concern in the line of confidentiality, integrity, and availability of the information shared in airport networks and other related systems.

V. Conclusions

The most common implementations using IoT systems in airports are in the line of luggage management, and smart parking. Also, IoT-based systems have been used for surveillance of incidents and passengers. However, 83% of the implementations analyzed in this paper do not have any security components mentioned in their design. This poses a security concern about the confidentiality, integrity, and availability of the information transmitted in the systems.

Some of the implementations use off-the-shelf devices, which generates security risks such as back doors, due to extra hardware and software elements that are not used for the operation of the system. As a recommendation, it is possible to create customized controllers that include only the strictly required elements.

References

[1] J. M. Talavera, L. E. Tobón, J. A. Gómez, M. A. Culman, J. M. Aranda, D. T. Parra, L. A. Quiroz, A. Hoyos, and L. E. Garreta, Review of IoT applications in agro-industrial and environmental fields. Computers and Electronics in Agriculture. Volume 142. November 2017. DOI: 10.1016/j.compag.2017.09.015

[2] B. Pradhan, S. Bhattacharyya, and K. Pal, IoT-Based Applications in Healthcare Devices. Journal of Healthcare Engineering. March 2021. DOI: 10.1155/2021/6632599

[3] A. Alghadeir, and H. Al-Sakran, Smart Airport Architecture Using Internet of Things. International Journal of Innovative Research in Computer Science & Technology (IJIRCST). Volume-4, Issue-5, September 2016. (Online): https://ssrn.com/abstract=3534138 [Last accessed: January 31, 2023

[4] Statista - Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030 (Online): https://www.statista.com/statistics/1183457/iotconnected-devices-worldwide/ [Last accessed: January 15, 2023]

[5] IoT FOR AIRPORTS, (Online): https://www.wittra.io/iot-for-airports/ [Last accessed: January 22, 2023]

[6] Kellton, Airport IoT Solutions: Redefine Personalization and Customer Experience, (Online): https://www.kellton.com/kellton-tech-blog/iot-ushering-new-era-smart-airports [Last accessed: January 29, 2023]

[7] A. Hamidah Salman, T. Adiono, I. Abdurrahman, Y. Aditya, and Z. Chandra, Aircraft Passenger Baggage Handling System with RFID Technology. International Symposium on Electronics and Smart Devices (ISESD). Bandung, Indonesia, June 2021 DOI: 10.1109/ISESD53023.2021.9501689

[8] A. Al-Khateeb, Where in the World is My Suitcase? Air Passenger Luggage Tracking Using RFID Tags. IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). Vancouver, BC, Canada, October 2021. DOI: 10.1109/IEMCON53756.2021.9623128

[9] A. Singh, S. Meshram, T. Gujar, and P. R. Wankhede, Baggage tracing and handling system using RFID and IoT for airports. 2016 International Conference on Computing, Analytics and Security Trends (CAST). Pune, India, December 2016. DOI: 10.1109/CAST.2016.7915014

[10] D. P. F. Möller, H. Vakilzadian, and A. Deutschmann, Intelligent System Demonstrator for Secure Luggage Handling. 2018 IEEE International Conference on Electro/Information Technology (EIT). Rochester, MI, USA, May 2018. DOI: 10.1109/EIT.2018.8500248

[11] X. Yang, R. Feng, P. Xu, X. Wang, and M. Qi, Internet-of-Things-augmented dynamic route planning approach to the airport baggage handling system. Computers & Industrial Engineering journal. Vol 175. August 2021. DOI: 10.1016/j.cie.2022.108802

[12] D. Smotlâk, A. Novâk, and T. Lusiak, Use of IoT in Air Transport. 2022 New Trends in Aviation Development (NTAD). Novy Smokovec, Slovakia, November 2022. DOI: 10.1109/NTAD57912.2022.10013617

[13] S. Noel, M. Navya, D. Likitha, K. Manjula, and S. V. Keerthi Priya, A Smart IoT Based Real-Time System to Minimize Mishandled Luggage at Airports. 2021 5th International Conference on Computing Methodologies and Communication (ICCMC). Erode, India, April 2021. DOI: 10.1109/ICCMC51019.2021.9418041

[14] M. Suresh, P. Saravana Kumar, and T. V. P. Sundararajan, IoT Based Airport Parking System. IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems. Coimbatore, India, March 2015. DOI: 10.1109/ICIIECS.2015.7193216

[15] M. Coulibaly, S. Belkhala, A. Errami, H. Medromi, A. Saad, M. Rouissiya, and A. Jaafari, Development of a demonstrator smart-parking. 2018 19th IEEE Mediterranean Electrotechnical Conference (MELECON). Marrakech, Morocco, May 2018. DOI: 10.1109/MELCON.2018.8379088

[16] I. Santos-Gonzalez, A. Rivero-Garcıa and P. Caballero-Gil, Secure Indoor Location For Airport Environments. 2018 4th International Conference on Big Data Innovations and Applications. Barcelona, Spain, August 2018. DOI: 10.1109/Innovate-Data.2018.00016

[17] A. Sales Mendes, D. M. Jiménez-Bravo, M. Navarro-Cáceres, V. Reis Quietinho Leithardt, and G. Villarrubia González, Multi-Agent Approach Using LoRaWAN Devices: An Airport Case Study. Electronics Journal. Vol 2020, Issue 9. DOI: 10.3390/electronics9091430

[18] P. Balraj Balla, and K. T. Jadhao, IoT Based Facial Recognition Security System.

2018 International Conference on Smart City and Emerging Technology (ICSCET)Mumbai, India, January 2018. DOI: 10.1109/ICSCET.2018.8537344

[19] E. Elbas, Reliable abnormal event detection from IoT surveillance systems. 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS). Paris, France, December 2020. DOI: 10.1109/IOTSMS52051.2020.9340162

[20] S. V. Khadonova, A. V. Ufimtsev, and S. S. Dymkova, "Digital Smart Airport" System Based on Innovative Navigation and Information Technologies. 2020 International Conference on Engineering Management of Communication and Technology (EMCTECH) Vienna, Austria, October 2020. DOI: 10.1109/EMCTECH49634.2020.9261529

[21] R. Jalali, and S. Zeinali, Smart Flight Security in Airport Using IOT (Case Study: Airport of Birjand). International Journal of Computer Science and Software Engineering (IJCSSE), Volume 7, Issue 6, June 2018. [Online]: https://api.semanticscholar.org/CorpusID:212474238

[22] J. J. Garau Luis, B. Cameron, E. Crawley, and M. Sanchez Net, System Architecture for Tracking Passengers inside an Airport Terminal Using RFID. 2018 IEEE Aerospace Conference. March 2018. DOI: 10.1109/AERO.2018.8396429

[23] M. Merenda, L. Catarinucci, R. Colella, D. Iero, F. G. Della Corte, and R. Carotenuto, RFID-Based Indoor Positioning Using Edge Machine Learning. IEEE JOURNAL OF RADIO FREQUENCY IDENTIFICATION, Vol. 6, 2022. DOI: r 10.1109/JRFID.2022.3182819

[24] S. Budiyanto, L. Medriavin Silalahi, I. Uli Vistalina Simanjuntak, F. Artadima Silaban, G. Osman and A. Dendi Rochendi, Smart Door Lock Prototype Design at Internet of Things-Based Airport. 2022 5th International Conference of Computer and Informatics Engineering (IC2IE) . Jakarta, Indonesia , September 2022. DOI: 10.1109/IC2IE56416.2022.9970074

[25] Ch. Qian, W. Tang, W. Xiong and H. Chen, Design and Implementation of Airport Security System Based on IoT Data Cloud Platform. 2022 International Conference on Algorithms, Data Mining, and Information Technology (ADMIT) Xi'an, China, September 2022. DOI: 10.1109/ADMIT57209.2022.00019

[26] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. Sensors 2019, Vol 19, issue 1. DOI: 10.3390/s19010019