2020

A holistic review of cybersecurity and reliability perspectives in smart airports

Nickolaos Koroniotis

Nour Moustafa
Edith Cowan University

Francesco Schiliro

Praveen Gauravaram

Helge Janicke
Edith Cowan University

10.1109/ACCESS.2020.3036728
Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., & Janicke, H. (2020). A holistic review of cybersecurity and reliability perspectives in smart airports. *IEEE Access, 8,* 209802-209834. https://doi.org/10.1109/ACCESS.2020.3036728

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON RELIABILITY IN SENSOR-CLOUD SYSTEMS AND APPLICATIONS (SCSA)

Received October 28, 2020, accepted November 1, 2020, date of publication November 9, 2020, date of current version December 3, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3036728

A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports

NICKOLAOS KORONIOTIS[1,2], NOUR MOUSTAFA[1,2], (Senior Member, IEEE), FRANCESCO SCHILIRO[1,3], PRAVEEN GAURAVARAM[1,4], AND HELGE JANICKE[1], (Member, IEEE)

[1]Cyber Security Cooperative Research Centre (CSCRC), Perth, WA 6027, Australia
[2]School of Engineering and Information Technology, University of New South Wales at ADFA, Canberra, ACT 2612, Australia
[3]Australian Federal Police (AFP), Canberra, ACT 2600, Australia
[4]Tata Consultancy Services (TCS) Ltd., Brisbane, QLD 4000, Australia

Corresponding author: Nickolaos Koroniotis (n.koroniotis@unsw.edu.au)

The work was supported in part by the Cyber Security Research Centre Ltd., funded by the Australian Government's Cooperative Research Centres Programme under Grant RG201120.

ABSTRACT Advances in the Internet of Things (IoT) and aviation sector have resulted in the emergence of smart airports. Services and systems powered by the IoT enable smart airports to have enhanced robustness, efficiency and control, governed by real-time monitoring and analytics. Smart sensors control the environmental conditions inside the airport, automate passenger-related actions and support airport security. However, these augmentations and automation introduce security threats to network systems of smart airports. Cyber-attackers demonstrated the susceptibility of IoT systems and networks to Advanced Persistent Threats (APT), due to hardware constraints, software flaws or IoT misconfigurations. With the increasing complexity of attacks, it is imperative to safeguard IoT networks of smart airports and ensure reliability of services, as cyber-attacks can have tremendous consequences such as disrupting networks, cancelling travel, or stealing sensitive information. There is a need to adopt and develop new Artificial Intelligence (AI)-enabled cyber-defence techniques for smart airports, which will address the challenges brought about by the incorporation of IoT systems to the airport business processes, and the constantly evolving nature of contemporary cyber-attacks. In this study, we present a holistic review of existing smart airport applications and services enabled by IoT sensors and systems. Additionally, we investigate several types of cyber defence tools including AI and data mining techniques, and analyse their strengths and weaknesses in the context of smart airports. Furthermore, we provide a classification of smart airport sub-systems based on their purpose and criticality and address cyber threats that can affect the security of smart airport's networks.

INDEX TERMS Cyber security, artificial intelligence, smart airport, Industry 4.0, Internet of Things (IoT).

I. INTRODUCTION

Promising enhanced efficiency due to its modular and interoperable design, the Internet of Things (IoT) has shown tremendous growth, with projections estimating 75 billion devices by 2030 [1], establishing itself as a reliable set of technologies with vast applications. IoT is an umbrella term that covers diverse collections of interconnected devices that have been outfitted with processors and networking hardware, enabling the remote access of their services and data [2]–[4]. The IoT owes its success to the constant miniaturisation of hardware and the rapid development of the Internet, which made possible the design and implementation of small sensors and actuators that can be utilised remotely. Typically, IoT systems consist of three parts: IoT devices, network elements, and sensing data. Network elements connect IoT devices via utilising diverse network protocols with the cloud backend, where sensing data are gathered for analysis and from which users can issue commands to their devices [5], [6]

By recognising the benefits in efficiency and productivity that the IoT offers, several sectors have reinvented themselves. The incorporation of smart things in their business plans has resulted in augmenting and developing services, while the constant flow of information generated by the IoT is harnessed through analytics, and utilised for improvements.

The associate editor coordinating the review of this manuscript and approving it for publication was Md. Arafatur Rahman.

Examples of such sectors include Industry 4.0, smart cities and smart airports. Emerging in 2011 in Germany, Industry 4.0, also referred to as ''the fourth industrial revolution'', was a radical step in the evolution of industry, that sought to enhance its efficiency and productivity by harnessing various new technologies, such as the IoT [7]. The adoption of Industry 4.0 was made possible due to technologies such as Industrial Internet of Things (IIoT) and Cyber-Physical Systems (CPS) that imply one of the main characteristics of Industry 4.0, which is the merging of the cyber and physical worlds, enabling remote management of devices. The benefits of Industry 4.0, have been realised due to the interconnection of users and devices, the real-time processing and centralized aggregation of data which powers the optimisation of the production processes costs and improve services [8]–[10]. Smart airports emerged as a result of the mass adoption of IoT and Industry 4.0, coupled with increases in the frequency of commercial flights around the globe [11]. Contemporary airports have been outfitted with smart ''things'' that improve the reliability of services, minimise human errors in the maintenance of various critical areas like the runways and assert a high quality of experience for customers [12]–[14].

However, the incorporation of IoT devices in the industrial sector, with examples such as airports and its critical infrastructure, imposes cyber risks. Various research studies [15]–[17] have demonstrated that various IoT devices are not secured properly against cyber-attacks. This insecurity can be attributed to a number of reasons, spanning from users not changing the default credentials necessary to log-in to the device and configure it, to software design flaws and hardware restrictions [18], [19]. As a result, the reliability of services powered by IoT devices in Smart Airports and critical infrastructure is at risk from cyber-attacks that can tamper with data, causing sensors to report erroneous information or make devices and systems entirely unavailable through denial of service attacks [11], [20]. Besides the degradation to services that can result from IoT devices being compromised, another danger is that they can be used as an attack vector to penetrate otherwise secured networks [21], [22]. This can be a considerable cyber threat for smart airports, as cyber-attacks can be launched and target critical systems, resulting in flight disruptions, tampering with automatic checking devices and baggage location systems or otherwise degrade the quality of service and the experience of passengers [23].

The development and configuration of effective security tools to detect attacks and mitigate them is crucial to protect IoT networks of smart airports. Many cybersecurity solutions have been deployed at airport networks that mainly focus on expert systems, which harness rule-based engines [24]. These systems rely on expert knowledge to identify important features and generate rules that are used to filter incoming data. In a dynamic new world where new technologies produce portable devices that are seamlessly connected to well-established, on-line systems, cybersecurity solutions need to be able to be swiftly updated and re-calibrated, so that new cyber threats can be effectively detected and mitigated.

In this paper, we discuss smart airports and their subsystems. We focus on the cybersecurity aspect of smart airports, identify cyber threats and further discuss privacy concerns and the impact of their vulnerabilities. The main contributions of this paper are as follows:

- We analyse the various IoT applications found in contemporary smart airports, the methods utilised for their development and their vulnerabilities.
- We propose a network architecture for contemporary smart airports, focusing on the network architecture of the installed IoT devices.
- We investigate security and privacy issues present in contemporary smart airports, with a focus on their networks.
- We provide a study of security solutions for smart airports, including vulnerability analysis and risk mitigation strategies.

The remainder of this paper is organised as follows. Section II discusses the related studies and surveys related to smart airports and cybersecuirty. Section III discusses the evolution of airports to smart airports and the potential smart IoT systems that enable it. This is followed by explaining cyber Security techniques used in smart airport networks, in Section IV. Section V illustrates risk profiling and its implementation in smart airports. After that, AI-enabled cyber defences in smart airports are described in Section VI. In Section VII, the Cyber Security risks of the smart airport are discussed, along with the challenges in ensuring its security. Finally, concluding remarks are given in Section VIII.

II. RELATED WORK

Due to the financial importance of smart airports to their local and global economies, and with the impact of cyber attacks on the rise, as they not only affect the security of digital systems, but also physical systems by compromising smart things and networks, the subject of smart airport cybersecurity has been the centre of attention for a number of studies [23], [25]–[33]. Table 1 provides existing works on the study of cybersecurity in a smart airport context, providing analysis of their characteristics. The table includes a short description of the focus of each study, along with their associated advantages and limitations.

Chiappetta *et al.* [25] focused on the study of critical infrastructure and provided a review of several critical cybersecurity vulnerabilities found to affect both maritime aswell-as air travel, including smart airports. The majority of the work focused on intelligent ports, where cyber-physical systems are utilised to enhance existing processes such as cargo loading and access control. Smart airports are viewed from the perspective of SCADA systems, where three components cooperate, remote telemetry units (sensors, actuators), communication and relay information channels and a

TABLE 1. Review of existing literature for smart airprot cybersecurity measures.

Research	Premise	Advantages	Limitations
Chiappetta et al. [25] 2017	Research focused on the study of critical infrastructure and provided a review of critical cybersecurity vulnerabilities found in airports. Emphasis was given on SCADA systems.	Indicates a lack of effective security detection and prevention systems for SCADA. Provides a separation of airport areas, based on access restrictions, which is important for designing effective security solutions.	Briefly covers some security issues of airports, mainly focusing on policies. Lacks a technical analysis of the various subsystems commonly found in airports.
Suciu et al. [23] 2018	Research addressed physical and cyber terrorism, focusing on cyberattacks. Existing work was reviewed, and two attack scenarios utilising DDoS and subterfuge were presented.	Realistic view of potential attack scenarios. Can be used as a starting point to design cybersecurity countermeasures.	Lacks a thorough listing of sensitive sub-systems, attack vectors and their impact. Diversity of cyberattacks is limited.
Willemsen et al. [27] 2018	Research provided a study of the security of airports, with emphasis on combining physical security and cybersecurity. The work emphasises the baggage handling system as a potential security weakness.	The work presents existing policies regarding the cybersecurity of smart airports. Terrorism is considered as part of ongoing cyberthreats.	The work does not provide a technical analysis of security weaknesses, attacks and exploits.
Lykou et al. [26] 2018	Research investigates the state of cybersecurity readiness of several contemporary smart airports. The work is based on a brief literature review and the analysis of a survey directed at IT personnel of airports.	Provides a realistic view of the cybersecurity state of several airports considered to be "smart".	Research is based on surveys and thus reports on the perception of IT airport personnel. Does not investigate the existing IoT and IT applications, interactions and weaknesses
Lekota et al. [28] 2019	Research focused on the cyber-readiness of the Sub-Saharan aviation sector. Investigated existing policies, best practices and legacy systems that affect the stability of airports and aircraft in the region.	In-depth review of the cybersecurity state and development of Sub-Saharan and South African smart airports.	The work is focused and thus its value is best realised in the Sub-Saharan and South African regions. Focus on policies and best-practices and not in technical analysis of cyberattacks. Lack of diversity of presented cyber-attacks.
Lykou et al. [29] 2019	Research studied the adoption of cybersecurity countermeasures and security policies in smart airports, along with the magnitude of threats that they face, due to the assimilation of IoT devices in their business processes.	Indicated that the biggest concern in airport IT personnel, related to cybersecurity, is the lack of awareness and proper training.	Provides results of a survey, which are indications of perceived weaknesses of airport security. Lacks technical analysis of security weaknesses of smart airports. Cyberattacks are briefly covered and not discussed in detail.
Aboti et al. [30] 2019	Research reviews the use of IoT devices in smart airports with a particular focus in wearable devices and their impact in airport and aircraft security.	Lists wearable smart devices. Presents several potential attacks. Provides challenges to future research.	Analysis of cybersecurity incidents is brief. The impact of presented cyber-attacks on airport and aircraft security is not discussed.
Suciu et al. [31] 2019	The work reviews cybersecurity threats and attack vectors that contemporary smart airports face. The architecture of a smart airport's cybersecurity system architecture is briefly discussed.	Analyses realistic attack scenarios and provides impact and mitigation tactics. Provides a cybersecurity system architecture for smart airports.	The work is presented from a high-level perspective. Only limited scenarios are discussed. System architecture is briefly discussed, its practical merits not explored.
Rajapaksha et al. [32] 2020	Research focused on the study of smart airports, with particular emphasis given to existing IoT applications and services.	This study thoroughly lists a diverse group of IoT applications commonly found in most contemporary smart airports.	Analysis of cybersecurity mechanisms of smart airports limited. Implications of exploitation of IoT systems in smart airports limited.
Lehto et al. [33] 2020	The research surveys the cybersecurity landscape of the maritime, aviation and automotive sectors. A discussion regarding cybersecurity standards and economic motives for targeting these systems is provided.	The presented work provides an informed perspective on European standards for commercial aviation cybersecurity.	The work is presented from a high-level perspective. The smart airport sub-systems, the associated cyber-threats, and the impact of a potential compromise of these systems is not discussed.

human interface machine that allows a user to monitor and issue commands to the various scattered devices across a deployment (smart airport). The various parts of an airport are separated into three categories, the landside, airside and terminal parts, with each section governed by different access controls and security levels and thus requiring different security mechanisms. A hybrid security system is introduced, called the Hybrid Port system, that seamlessly combines multiple physical and cyber sensors, with their data streams combined in a manner that supports faster decision making,

allowing for the detection of a wider range of security events. This research briefly covers some security issues of airports, mainly focusing on the policies that govern best practices in the European continent, lacking a technical analysis of the various subsystems commonly found in airports.

Suciu *et al.* [23] provided a brief study of the impact of terrorist acts and cyber-attacks to the development of state-of-the-art cybersecurity detection, protection and countermeasures. In their work, the researchers initially presented the terrorist attack of September 2011 in USA, as a primary driving force behind multiple innovations in the airport security and cybersecurity sectors. A review of the existing literature in the developed airport cybersecurity countermeasures revealed that several applications are vulnerable to cyberattacks, and thus sensitive to exploitation which in turn affects their reliability. Although various research groups have been formed to mitigate the security weaknesses of existing solutions, reports indicate that further research is necessary to improve the protection of critical infrastructure assets such as smart airports, a fact that is supported by several researchers that have demonstrated that by harnessing WiFi and malicious applications, critical systems of airports can be compromised. Examples include airport ventilation systems, security sensors and aircraft navigation systems, potentially threatening human life [23], [33], [34]. The researchers next provide realistic attack scenarios against simulated airport infrastructure, their impact and mitigation strategies. Although this work presents a realistic view of potential attack scenarios, which can be used by security experts as a guide to design cybersecurity countermeasures, it neglects a thorough listing of sensitive sub-systems, potential attack vectors and their impact on airport operations. Furthermore, the cyberattack diversity is limited.

Willemsen *et al.* [27] provided a study of the security of airports, with emphasis on combining physical security and cybersecurity. The authors initially illustrate the impact of cyber-related applications in a passenger's journey, by segmenting it into zones, each of which is characterised by different security requirements and applications. They then stress the importance of surveillance systems, in detecting suspicious behaviour and preventing terrorist attacks, emphasising the importance of reliable communication between various entities in high-risk locations, through which the behaviour of passengers can be observed. According to the researchers, an important airport sub-system that is often left in a legacy state (no tech updates), is the baggage handling system, which results in existing unpatched flaws rendering it vulnerable to hackers, malware and other cyber-attacks, further compromising the security of both the airport and the aircraft that transports the screened luggage. Several threats to the security of contemporary airports are identified, with prime examples being the reliance on cloud-based services provided through the Internet, lack of cybersecurity awareness of airport employees and use of insecure third parties. The research concludes by suggesting ways of securing existing, possibly outdated systems in airports, by individually securing sub-systems and relying on advanced monitoring solutions, while stressing the value of collaboration between airports and stakeholders.

Lykou *et al.* [26] researched the state of cybersecurity readiness of airports and their resilience to cyberattacks through best practices. Their work combines a literature review on the cybersecurity of airports, with the results of an online survey which was addressed to IT employees of the most active American and European airports. Out of the 34 complete responses they received, 16% of airports were determined to have minimum incorporation of IoT technology, with 55% moderate and only 27% were classified as ''Smart Airports''. The survey revealed that, according to IT personnel, the highest risk to the cybersecurity of airports was lack of security awareness, with Internet connectivity coming second. The researchers then grouped the existing good practices into three categories according to area of application and purpose, namely: technical, operational and policies & standards. The research concluded that the procedures that airports follow, in order to secure their assets from cyberattacks vary, depending on their adoption of new technologies. Although this work provides a realistic view of the cybersecurity state of several airports considered to be ''smart'', in essence, the research reports and analyses the responses that were provided by IT personnel of these airports. Thus, the work does not investigate the existing IoT and IT applications and their interactions present in smart airports, along with their corresponding cybersecurity-related weaknesses.

Lekota *et al.* [28] conducted research that focused on the cyber-readiness of the Sub-Saharan aviation sector, seeking to determine existing policies, best practiced and legacy systems that might threaten the stability of airports and aircraft in the region. Initially, the researchers directly compare the state of cybersecurity readiness in international airports and Sub-Saharan Africa. The importance of Policies for the creation of shared incident management is emphasised, with international efforts being isolated and driven by private organisations, while progress is slow due to the severity of cyberthreats being underestimated. In south Africa and the Sub-Saharan region, cybersecurity for the aviation sector is not prioritised, with response measures lacking. There is no central authority for defining policies and cyber-readiness plans, instead management is handled locally, with the primary focus still being on physical rather than cyber security. The researchers then state the importance of developing frameworks for improving the cybersecurity of airports and other critical infrastructure, reviewing several cybersecurity incident response and best practices standards, grouping their processes into three classes, Planning, Communication and Analysis. The study concludes by asserting the importance of Computer System Incident Response Teams (CSIRT) in a secure collaborative aviation infrastructure for the orchestration of wide-range incident response actions. Furthermore, they assert the lack of CSIRT in South and Sub-Saharan

Africa, the establishment of which would help to better shield airport infrastructure in the region.

Lykou *et al.* [29] researched the adoption of cybersecurity countermeasures and security policies in smart airports, along with the magnitude of threats that they face, due to the assimilation of IoT devices in their business processes. The research was based on both existing literature, as-well-as a survey which was addressed towards IT personnel of airports, with the goal being to determine the readiness of airports in the event of a cybersecurity incident, and the level of adherence to best practices. It is determined, that although measures are taken by airports to defend against or otherwise mitigate isolated hacking incidents, a more collaborative approach, with the various sub-systems and stakeholders that coexist in an airport is lacking. By reviewing the literature, the researchers determined that there is a lack of work, regarding the cybersecurity of ground control and other smart airport sub-systems, which needs to be addressed, as the incorporation of smart things into sometimes outdated systems introduces new attack surfaces that can be exploited, and lead to equipment damages, degradation of services and even loss of life. The authors identified best practices for smart airports and illustrate the importance of a well organised response system with seven attack scenarios. They concluded that the perceived security concern by the majority of the survey responders was building cybersecurity awareness, while a framework of trust needs to be defined, that would allow various stakeholders to collaborate and shield the aviation industry from next-generation cyberattacks.

Aboti *et al.* [30] compiled a review of IoT applications in the commercial aviation sector. The research initially addresses the rapid development exhibited by the IoT, and the observed trend of incorporating smart applications in diverse settings, including the aviation sector. A core issue that is identified by this work is the lack of security measures in the IoT, with the most prominent security concerns including data privacy, service availability, default device administration credentials and the role of AI in analysing IoT-generated data. The benefits of incorporating smart devices in airports is stressed by the presentation of a model describing the interaction of passengers with the augmented smart facilities of an airport, often through the use of smartphones, software applications or wearables. Emphasis is given on smart wearable devices and the benefit they provide to both the passengers as-well-as the airlines and their personnel. The benefits such devices, however, are counterbalanced by the potential security risks that they introduce. The researchers stress the need for investigating new attack surfaces introduced by the IoT, listing some attacks that can exploit the weaknesses of such devices and cause harm to smart airports or aircraft. However, the impact of these attacks on airport and aircraft security is not discussed.

Suciu *et al.* [31] investigated the cybersecurity weaknesses of smart airports, and reviewed new attack vectors that are made possible as a result of introducing smart things to airports and aircraft. One trend that has gained popularity in contemporary airports, and that the researchers indicate requires further attention, is the Bring Your Own Device (BYOD) practice, where passengers travel with their personal smart devices, that they use to connect the Internet either on the ground, or during flight. This can pose a threat to mission-critical airport and aircraft systems, as attackers can exploit the passengers' devices, utilising them as a springboard to bypass security measures and compromise otherwise unreachable internal networks and devices. The research then demonstrates several use-cases, where an Airport Operations Centre (AOC) is analysed in order to determine potential weaknesses. The scenarios include a spear phishing campaign that aims to stealthily compromise an airport's IT infrastructure and exfiltrate data, and a data spoofing attack aiming to spread misinformation about the details of flights, causing disruptions to flights. An architecture for a security system designed for smart airports is then proposed, consisting of a classification-like decision engine, that determines if the incoming data is normal or indicative of an attack. In the event of an attack, a mitigation module is launched, taking appropriate action depending on the attack and its severity. Although the work presents realistic attack scenarios that can be applied to a smart airport, describing the attack methodology, impact and potential mitigation tactics, the work is presented from a high level of abstraction.

Rajapaksha *et al.* [32] provided a review of smart applications in relation to the passenger terminal processes among other airport subsystems. Initially, the researchers provide a basis for the concept of smart airports, and their principles. A thorough analysis of existing IoT applications is provided, with information about their purpose and their relative location within the airport infrastructure. With efficiency as the main target, smart applications prioritise the augmentation of experience for both passengers and airport employees. Further benefits of smart airports are identified, such as faster response time to crises, more thorough screening processes, data collection for analysis and service/operational augmentations and resource utilisation optimisation. In a section listing challenges associated with the development and sustainability of smart airports, the authors provide a brief overview of the impact that cybersecurity has on smart airports. They specify that, due to the inability of a considerable percentage of IoT applications found in a smart airport to cooperate seamlessly, and due to various security flaws that such devices have been shown to have, new attack surfaces are introduced that threaten the stability of the smart airport, aircraft and thus the security of passengers. A need for cybersecurity incident detection and mitigation methods is argued, while the importance of formally educating airport personnel is stressed. The study lists a diverse set of IoT applications commonly found in most contemporary smart airports. However, the analysis of the cybersecurity mechanisms of smart airports is limited.

Lehto *et al.* [33] provided a study of three fields, maritime, aviation and automotive, from the perspective of cybersecurity. Initially, the severity of contemporary cyber-threats

were discussed, with a focus on Advanced Persistent Threats (APTs), that are often utilised by well organised hacker groups or foreign governments, in order to target, manipulate or outright disable critical infrastructure entities such as electric power stations, traffic control systems and airports. It is evident that the sophistication of these types of attacks has risen, in accordance with the increase of value that is placed on electronic assets such as personal documents and control systems in IoT-enabled sites. With regards to the aviation sector, the authors first stress its importance to the global economy, as its role is to enable commerce and travel. As such, any disruptions that the aviation sector may face, could cause tremendous financial impact, while unchecked security compromises can also lead to loss of life. As the sophistication of both smart airports as-well-as aircraft is elevated, critical security-related processes are increasingly managed by smart devices (IoT devices), and increasingly more entities are connected, exchanging sensitive information and thus providing new attack vectors that can be exploited by remote attackers. Contemporary airports tend to shift towards the smart airport paradigm, with IoT devices deployed in various subsystems, providing augmentation, real-time data collection and efficient management. Evolving standards in aviation cybersecurity tend to promote a management system that incorporates threat and risk management mechanisms that can function on any level (airprot, aircraft, hanger, etc.).

The researchers reported that further work is necessary, in order to develop solutions and well-thought standards that promote cyber-resilience for commercial aviation on a global scale. Although the presented work provides an informed perspective on European standards for commercial aviation cybersecurity, the work is presented from a high-level perspective, with only two real-world examples included to support the necessity of this work. Sub-systems, the associated cyber-threats, and the impact of a potential compromise of these systems is not discussed. Although there is significant work on studying the levels of cyberattack readiness in smart airports, there is a lack in assessing their technical capabilities and security protocols for defending against both well-established and novel security threats. The introduction of IoT devices in airports and aircraft, although beneficial towards enhancing the experience for passengers and augmenting efficiency for airport management, introduces new attack surfaces that can be exploited by hackers, malware and other threats that operate on the Internet, with consequences varying depending on the severity of the intrusion, the affected smart airport or aircraft sub-systems and the resources of the attackers. In this work, we will analyse these new attack surfaces and exploitation tactics, which have not been analysed in the existing literature that primarily focused on addressing commercial and governmental standards or best practices.

III. EVOLUTION OF AIRPORTS TO SMART AIRPORTS

Airports play an important role in the global economy, by bringing together people from around the globe, expanding business prospects, enabling international tourism and generating revenue from commerce and taxes [35]. The importance of airports has also been asserted by studies that have indicated a link between airports and the growth of regional economies [35], [36], which is understandable, as ease of access is an important factor for both promoting tourism and establishing collaboration between businesses situated in geographically remote locations while also facilitating the swift transport of goods, thus accelerating trade. On a more local perspective, airports also provide employment opportunities, first during construction, and then for various tasks, including management, maintenance for both the airport itself as-well-as aircraft and for day-to-day operations. As such, it is understandable that airports would be gradually modernized, in order to keep up with the constantly increasing flows of travelers and improve the quality of service through the application of emerging technologies.

A. EVOLUTION OF THE AIRPORT

Throughout history, airports have experienced a significant change to their operations and the services they provide, moving from simply providing transportation, towards enhancing the quality of service and ensuring a comfortable and entertaining experience for passengers. The evolution of airports brought about by the advancements and assimilation of technology, such as the IoT, can be viewed in three consecutive stages, Airport 1.0, Airport 2.0 and Airport 3.0 [11], [37]. In the first stage, Airport 1.0, much attention is given towards ensuring the safe operation of aircraft such as takeoff, refuelling and landing, with standard services provided to passengers, related to boarding and disembarking the aircraft, and minimum amenities. The collaboration of various services and stakeholders is not prominent in such airports.

The second stage, the ''agile airport'' or Airport 2.0, includes airports that are flexible and can adjust their workload according to demand. In these airports, collaboration through seamless data sharing is prominent, with a single network often employed to connect the various parts of the airport under a single administration system, and network-enabled systems such as IP-telephony and video surveillance are present. Compared to Airport 1.0, Airport 2.0 allows for improved efficiency and greater customer experience. Finally, Airport 3.0 corresponds to what is known as the ''smart airport'' and is the natural successor of Airport 2.0. Somewhat owing their existence to Industry 4.0, and powered by the IoT, airports in this category employ a unified network of entities, including the airport, aircraft and airlines, with multiple sensors and actuators deployed throughout the airport to power services that augment the experience of passengers, while further enhancing the airport's operations through a seamless collaboration of multiple sub-systems and real-time data sharing and analysis. Powerful technologies including big data, biometric technology and artificial intelligence are harnessed to power the contemporary smart airport.

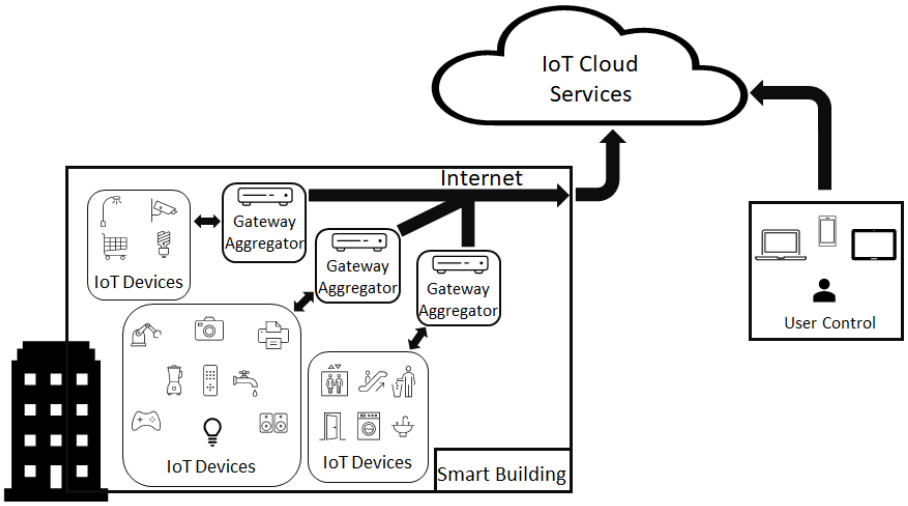


FIGURE 1. Abstract view of a typical IoT network.

However, as is the case with the IoT, smart airports do not have a solid and commonly accepted definition, as there is a general lack of common standards for their implementation and development.

B. SMART AIRPORT DEFINITIONS

As is the case with the IoT, smart airports are an emerging trend and as such, there exists no commonly accepted definition for them that encapsulates all their benefits, and characteristics. In Table 2, we list existing definitions, including their source, advantages and limitations, that can be found in literature, most produced from a different perspective of the smart airport such as the business side, the operational side and the technical side.

Existing definitions have focused on describing a domain-specific aspect of the smart airport, for example the business [38], [39], operations [41] or passenger experience side [39]–[41] of smart airports. We propose a comprehensive definition to a smart airport, which is *a smart airport is any airport, which has been augmented by the incorporation of cybersecurity-aware IoT devices, with an aim to improve efficiency, productivity, security and service*. There are no commonly accepted standards for developing IoT devices [2], [42], causing them to be heterogeneous both in the technologies/protocols they utilise, as-well-as in the implementation methods that different vendors apply.

An abstract view of a typical IoT deployment that shows its basic components grouped based on their function is shown in Figure 1. In an IoT system, various sensors connect to a local bridge/data-aggregation device, which connects the various sensors/actuators that may utilise diverse wireless network technologies, to the cloud back-end server. From there, authorised users can manage their devices and issue commands, through the use of specialised software such as smartphone applications or a web interface. Managing the smart devices that can be found in a smart airport or aircraft in a unified manner, and ensuring their cybersecurity, is a challenge. In the next sub-section we will analyse the architecture of a smart airport, the devices, technologies and protocols that often constitute the deployed smart things.

C. PROPOSED SMART AIRPORT ARCHITECTURE

The incorporation of IoT devices has greatly altered the dynamic of traditional airports, and has introduced new subsystems made up of sensors and actuators, that are often interconnected, allowing the system and airport personnel to swiftly respond to events, often in an automated manner. A proposed architecture of a smart airport's interior and exterior are presented in Figures 2 and 3, highlighting smart automations that are often combined, in order to provide complex services. Figure 2 illustrates the area where IoT-powered applications have been deployed, and their corresponding purpose. Depending on the area of the airport where IoT applications are deployed, and their core functionality, different network protocols and technologies are utilised. For instance, the RFID technology is used in the luggage handling process, where airport personnel either directly (manually), or indirectly (robotic arms) sort, load or unload the correct cargo to an aircraft.

Often sensors would use Bluetooth, ZigBee or other such small to middle range wireless technology to communicate with aggregator devices that gather incoming data from the sensors/actuators and connect them to the backend, thus assuming the role of a network bridge. In contemporary airports and aircraft, passengers have the option to connect to the Internet through complementary open WiFi. It is important that any devices/services that the airport may host for internal use, should not be connected to this open WiFi, and instead use either Ethernet solutions or secondary, secured WiFi networks. This method helps reduce the attack surface, as passenger devices can be used as "trojan horses" and malware can spread to the airport's network. Some of the

TABLE 2. Existing definitions of the smart airport.

Source	Definition	Advantages	Limitations
Fattah et al. [37]	Airport 3.0 comprises "smart airports" that fully exploit the power of emerging and maturing technologies, with advanced and pervasively deployed sense-analyze-respond capabilities. Systems are built around a "digital grid": a single, converged, often carrier-class IP network that enables high-speed broadband traffic throughout the entire ecosystem, including the airport, airport city, airlines, seaport, logistics, authorities, and other parties.	• Unifies various stakeholders • Allows for interconnection and collaboration.	• Implies that all IoT devices are interconnected under a singular network outright, which is not always the case. • Somewhat generic in its view of IoT devices and their role in a smart airport. • It neglects to address the cybersecurity state of the smart airport.
Nau et al. [38]	A smart airport is not about complete digitization of the airport, it is more how it can provide a competitive edge to the company. A roadmap will help to prioritize and coordinate the implementation of solutions which are more and more interconnected.	• This definition is agile. • Promotes a technology-independent definition for smart airports. • Focuses more on desired characteristics.	• Primarily focuses on a business perspective. • Neglects the automation and security aspects of deploying IoT devices in a smart airport.
Nagy et al. [39]	The "smart" airport is a determinative subsystem of the "smart city". It is the place where urban life and aircraft movements are connected, while several other activities are realized. This interface role is also significant regarding the information management. Accordingly, information is exchanged among urban transportation management, systems of air traffic control and airlines.	• Acknowledges the potential collaborative value of smart airports and their subsystems. • Provides an inherent connection between smart airports and smart cities.	• Primary focus on optimisaiton of airport operations and quality of service for passengers. • Overlooks the significance of security the deployed IoT systems.
Qi et al. [40]	Smart airport will be an "man-machine cooperation" system combining software and hardware. Passengers, airports, airlines, service providers and other related participants will involve in it to achieve service providing, information dissemination and interaction. It will make a more refined, personalized and efficient service process.	• Indicates the merits of incorporating automated systems in airprots. • Focuses on efficiency and augmentation of pre-existing airport services.	• Neglects to discuss the cybersecurity aspects of smart airports.
ENISA 2016 [41]	Smart airports are those airports making use of networked, data driven response capabilities that, on the one hand, provide travellers with a better and seamless travel experience and, on the other hand, aim to guarantee higher levels of security for the safety of the passengers and operators.	• Simple and concise definition. • Covers the main ideas associated with smart airports. • Addresses the security enhancements possible through the IoT.	• Does not link to the essential units that allow an airport to be called "smart", the IoT. • Focuses on physical security and neglects cybersecurity.

existing smart airport systems that have been augmented by the IoT are:

- **Automated check-in** [41], [43], [44]: Passengers can avoid long queues and procure their boarding passes by checking-in prior to their flights through their smartphones and completing the process through the Internet or by accessing smart kiosks found throughout the airport. Associated with these methods of checking-in is also another trend, automated bag drops where, by using one of the kiosks, passengers print the necessary barcode stickers, affix them to their own luggage and drop them off at appointed areas to be further processed by the airport's system. Utilising either kiosks or web-interfaces implies an Internet connection, and thus several attacks can be launched against these systems. Thus, malicious actors can launch attacks, such as MiTM or otherwise intercept network traffic between kiosks, mobile phones and backend servers, targeting and stealing sensitive information such as credit card or passport details, effectively breaching a passengers' privacy. Furthermore, a legitimate passenger's reservation can be invalidated, and boarding passes falsified, thus enabling unauthorized individuals to board a flight instead of the passenger. Other attacks can falsify or spoof information that is attached to luggage tags, that are printed in self-service kiosks, altering the identity of a legitimate owner and their destination, and causing the luggage to be lost.

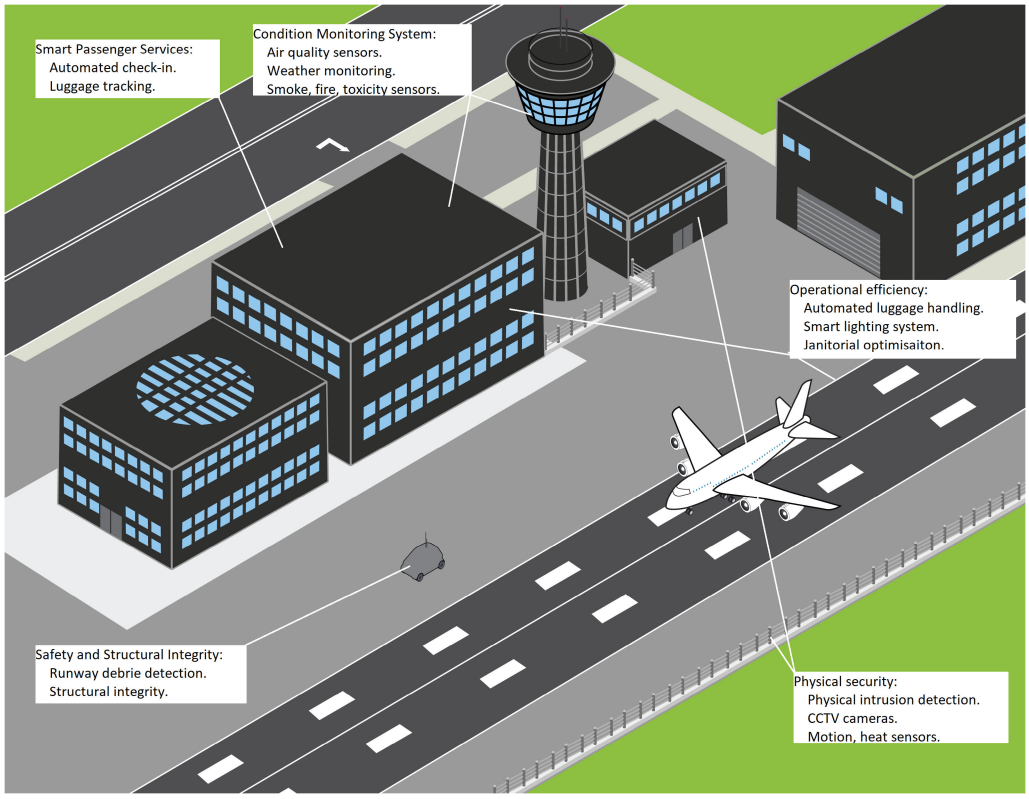


FIGURE 2. Proposed smart airport architecture.

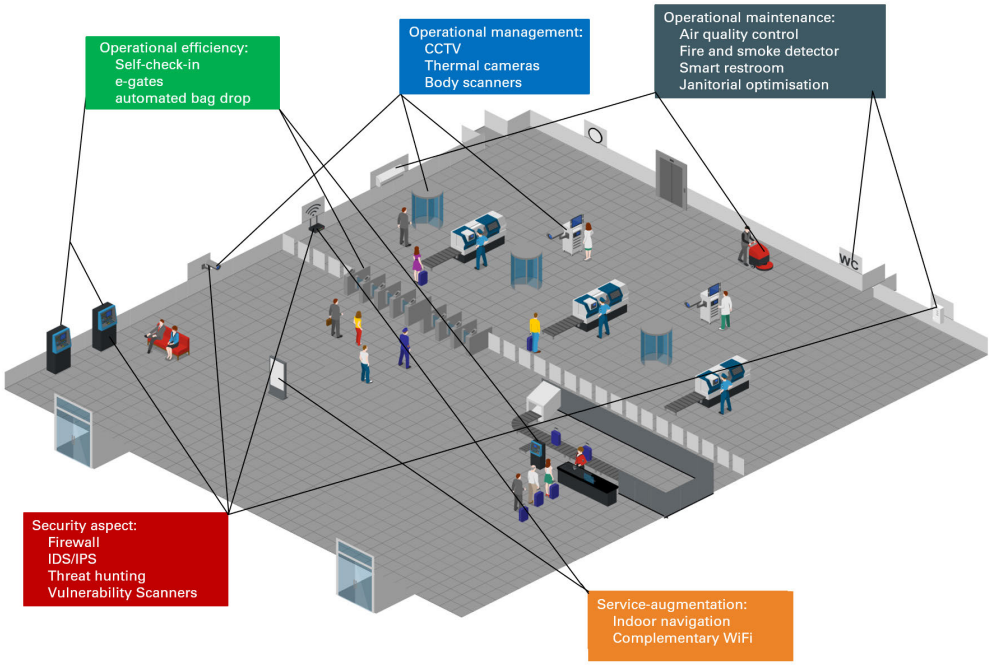


FIGURE 3. Proposed smart airport architecture interior.

- **eGates** [45]–[48]: Prior to boarding an aircraft, passengers have to undergo a border control process. Traditionally, this process involved an office manually inspecting a passenger's passport and verifying their identity. In contemporary smart airports, instead of relying on such manual processes, an automated gate, called electronic Gate (eGate), is utilised. In Australia, eGates are called SmartGates. eGates function by scanning the

microprocessor found in the ePassports, through the use of RF-enabled contactless smart card technology [49]. An eGate's check relies primarily on acquiring biometric data from a passenger, for example facial recognition or a fingerprint check, and matching the obtained information to the data stored in the ePassport. Additionally, eGates maintain connections to biometric databases, for further ID verification of passengers, and to border and immigration servers, where the identity of passengers is cross-referenced against blacklists, to flag dangerous individuals. Although these systems were developed to speed-up the border control process, potential attacks can undermine their efficiency and credibility. Attackers can attempt to compromise eGates, by either gaining access to an airport's intranet, or by physically tampering with the gates' hardware. Potential attacks may result in stealing sensitive passenger information (held in the ePassport) thus resulting in privacy violations. Attackers can also launch a DoS by disabling the system or a MiTM attack which can allow dangerous travelers from entering a country or flagging innocent passengers and preventing them from crossing the border.

- **Luggage tracking and handling** [41], [44], [48], [50], [51]: One issue that contemporary airports have faced as a result of increased passenger flows and human error is luggage misplacement and mishandling. One solution to this problem that has gained some traction in recent years is the application of RFID technology for tagging and tracking luggage. The RFID tag stores information about the passenger and their luggage, along with a unique ID created during check-in. During a flight, at the source, middle and destination airports, the RFID tags of luggage are scanned, with that information shared between airports, allowing passengers to view their luggage location through smartphone applications and online platforms. This application of RFID tagging was implemented, to reduce the number of lost luggage due to mishandling, and to promote efficiency. Another IoT application that is utilised in luggage handling is the incorporation of robotic arms for loading and unloading luggage. These automated systems are tasked with sorting, conveying and loading the checked-in luggage, prioritizing the efficient utilisation of space and handling heavy loads which would otherwise need to be handled manually, while security scanning is applied to the luggage, to scan for harmful and prohibited materials. The system is controlled by a centralized software-based system, where collected information about the system performance and the luggage can be accessed through a web-based interface or a hand-heled device. However, security incidents can affect or disrupt the workflow of luggage handling systems. Attackers can target the network and control system, resulting in a DoS attack by shutting down the conveyor belts, or re-direct luggage to incorrect destinations. Additionally, the screening system can be targeted, either to cause an excessive false alarm rate, which would result in delays, or forcing a false negative rate, which would result in potentially dangerous and prohibited items to be loaded onto an aircraft.
- **Physical airport security** [52]–[54]: As part of the physical security measures that are maintained in an airport, certain areas are to be accessed by authorized personnel only. To enforce these necessary restrictions, airports, similarly to other organisations, utilise what are known as electronic gates in conjunction with CCTV and motion sensors. Installing CCTV, IP cameras, thermal cameras and motion sensors allows for the monitoring of the airport's interior, with particular focus placed on high-risk areas. Restriction of physical access is enabled through the use of key-cards enabled by RFID, Near Field Communication (NFC) technology, smartphone apps, smart cards or the use of alphanumeric codes and electronic locks. These measures can also be applied at the airport's perimeter, to prevent unauthorised access of the runway and aircraft hangers. These IoT-based security applications that monitor the perimeter of an airport and detect unauthorised entry to high-risk areas, rely on networked systems that can be accessed either from the airport's intranet or from the Internet. Thus, attackers can launch a number of diverse attacks to affect the functionality of the security systems. Perimeter sensors can be compromised by gaining access to the the airport's intranet and either be deactivated, thus allowing unauthorised access to the runway and hangers, or cause excessive false alarms, which can be used as a distraction in more elaborate physical intrusions. IP cameras and other network-enabled IoT sensors can also be compromised, leading to DoS attacks through deactivation, spoofing attacks, video loop attacks and bypassing electronic locks.
- **Janitorial optimisation** [55]: Through the use of sensors, that count the number of people that tread through an area, and combining this information with flight arrival schedules, smart airports are able to predict when large flows of passengers will arrive and at which part of the ariport they are more concentrated. One example of such an application, is the use of sensors to count the number of people that utilise the restrooms. Such existing systems are pre-programmed to count up to a particular threshold, after which the counter is reset and janitorial staff that are stationed nearby are automatically informed through IoT wearable devices which restroom they need to be cleaned and sanitised. This application further optimises the airport operations, specifically those operations related to the janitorial staff, as they are instantly informed about when and where their services are required. Furthermore, additional IoT sensors and actuators have been outfitted to airport restrooms, allowing for automatic flushing, contactless faucets and hand driers and environmental humidity and temperature control. Additionally, sensors

can detect and inform janitorial staff of damages to restroom equipment and the various smart sensors, enabling swifter repairs and thus a better experience for passengers. However, smart restroom systems can be targeted by cyber-attackers. Attacks that target smart restroom systems can result in false activations of devices, causing toilets and faucets to unnecessarily waste water, hand dryers to turn on and waist electricity or even disable the functions of these devices, in a form of DoS attack. Furthermore, attackers can tamper with the sensors and counters that inform the janitorial staff when their services are required, wasting their time and thus affecting the optimisation of the system. In addition, if these smart devices are not secured properly, and due to the fact that passengers can spend time in the restroom without arousing suspicion, they can compromise the smart devices, and use them to spread malware infections to other IoT devices in smart airprot.

- **Runway structural integrity monitoring** [12], [14]: It is imperative to ensure that the runway is free of obstructions and to swiftly detect and repair any structural damages, as they may cause accidents during landing and takeoff. Traditionally, airports ensured the integrity of their runways by relying on visual inspections conducted by airport personnel. Such inspections were susceptible to human error which prompted the need for an automated, dynamic and reliable inspection process. For this purpose, contemporary smart airports have thus resorted to the use of automated equipment, such as heat sensors embedded in the runway and terrain-bound drones that utilise light-based detection technology. Several network protocols can be in effect in such applications, such as RFID chips for tarmac heat measurements [12], or ZigBee, Bluetooth and LoRA for the communication between the automated drones and a command and control platform. Attacks that target these structural integrity monitoring systems can have dire consequences. Drones can be employed by attackers, to come into close proximity to the monitoring rovers and utilise wireless protocols to connect and thus compromise them. Disabling the devices will delay the routine inspections that are regularly scheduled, however, more serious attacks can be launched, such as MiTM and data spoofing. By spoofing the data that the rover records, attackers can force the personnel responsible for maintaining the structural integrity of the runway, to perform unnecessary checks, thus wasting manpower. One, more considerable effects of such an attack would be to force the monitoring rover to falsely report that the runway is intact, when in actuality, its structural integrity is compromised or its covered with debris. Thus, compromising the runway structural integrity monitoring rovers can lead to aircraft sustaining damage during landing and takeoff, or even cause severe accidents.
- **Smart lighting** [56]: One other important application of the IoT in smart cities, smart homes and smart airports are the smart lighting systems. Through such systems, the lights on entire sections of the airport are controlled through a web-based platform or a smartphone application, and their status monitored, instantly informing the airport staff in the event of a malfunction. Furthermore, IoT-based systems have been developed that connect runway lighting to the control tower, alerting about hardware failures. This application is crucial to maintaining operational integrity, as runway lights are utilised during landing by aircraft. However, it has been shown that attacks can be launched that target smart lighting systems with a variety of consequences. First, due to hardware constraints and weaknesses in security protocols, it is possible to gain access to a smart lightbulb, force it to download a malware and execute it, by utilising mechanics meant for close-range firmware update [15]. This results in the malware utilising the smart lightbulb's network capabilities to spread to nearby lightbulbs and other devices, either bricking the devices or bringing them under an attacker's control. Furthermore, attackers can potentially force the devices to spend excessive amounts of electric power, disable them or block any signals that the lights transmit to the legitimate users about their status, delaying repairs and affecting the airport's efficiency, productivity and QoS towards passengers. In addition, tampering with the runway lights is a considerable threat to flight operations.
- **Airport asset tracking** [57]: Contemporary airports are comprised of multiple sections, each designed to handle a specific task. In these airport sections, often specialised assets (tools) are employed, for example baggage trollies are used for transporting passengers' luggage from the parking lot to the belt conveyors or the baggage drop-off zone. Other examples include ground support equipment that are utilised prior to takeoff or after an aircraft has landed, assisting in loading and unloading luggage, refueling the aircraft and assisting with general maintenance. Thus, the ability to swiftly locate these assets, organize them and make them available for re-use is imperative for the continued efficient operations of an airport. As such, sensors based on RFID, Zigbee, Bluetooth and other such lightweight network protocols are attached to these assets, the signal of which is gathered by a sensor bridge and transmitted to a server, through which administrative personnel are able to locate it (by overlapping positional data with digital maps). Such sensors can be attached assets used to service aircraft, in order to track their location, the frequency with which they are utilised and moved around the airport, with the intended outcome being to maximise and optimize their utilization, in order to shorten aircraft turnaround time. Attacking these systems can cause a decline of service quality, especially related to aircraft maintenance. By disabling the IoT-based trackers or spoofing the position that they are transmitting (within airport grounds), assets can become entirely unavailable or require time and effort

to be located. This can cause flights to be delayed and a reduction to the efficiency and optimisation of asset deployment.

- **Air quality and environmental conditions tracking** [58], [59]: A priority for airports, is to ensure the safety of both passengers and airport personnel. For the multitude of threats that exist, a contemporary smart airport needs to include monitoring and mitigation mechanisms. The degradation of environmental conditions is one such threat that needs to be handled. To that effect, IoT-based sensors have been developed, that monitor the air quality (radiation, toxicity,...), detect fire and smoke and measure. Aside from the security applications (to avoid chemical attacks,...), these sensors can be coupled with air conditioners, to automatically adjust the temperature in different areas of the airport and enhance passenger experience. Furthermore, environmental sensors that are deployed on the outside of an airport can be configured to provide regular weather-condition reports, which is an important source of information for control towers, as weather conditions may have serious impact to flights. Network bridges can be used in such applications to coordinate different sensor types that utilise diverse network protocols. Attacks that target these systems can have a number of consequences, ranging from disruption of airport services to potential life-threatening scenarios. By hacking into environmental condition monitoring sensors, attackers can alter their recording and cause them to incorrectly report hazardous conditions, which in turn can result in halting all processes, and forcing everyone to evacuate the airport as per security protocols and regulations. This can cause unnecessary panic, flights can be delayed and the reputation of the airport can be affected. Alternatively, the attackers can cause these sensors to display excessive false negative rates, which can function as one aspect of a physical attack intending to compromise the health of passengers and airport personnel.

By design, IoT sensors and actuators are intended to be distributed in remote areas of a building, complex or city, and at the same time, maintain communication through a sensor bridge or a router with their cloud backend infrastructure, through which users can monitor their status and issue commands. The hardware constraints, and deployment location affect the effectiveness of protocols and technologies to be used in smart airports. Several network and communication protocols power the aforementioned IoT smart airport applications.

- **RFID** [44], [60], [61]: The first instance of Radio Frequency Identification (RFID) technology appeared in 1945, and was intended as a spying tool developed by the Soviet Union [62]. RFID is a technology that has seen much use in short-range wireless communication systems. RFID application are typically comprised of three main components, a reader, a tag, and an application component that manages the collected data, often utilising a backend database. The reader transmits electromagnetic signals of specific frequency depending on the application of the system. The tags can either be active, where a small battery is used to power a constrained processing unit inside the tag with some storage capacity, or passive, where the chip utilises ambient electromagnetic energy to power itself and transmit data back to the reader, with very constrained storage capacity. Communication frequencies vary from 125 kHz to over 10 GHz, with several frequency ranges defined within these limits [62], [63]. The distance range of RFID applications, depends on the utilised frequency range, with Low Frequency (LF RFID) operating in the frequency range 125-150 kHz having an effective distance range of less than 10 cm and the Ultra High Frequency (UHF RFID) operating in the range 433-928 MHz with an effective distance range of up to 20 m. RFID technology has been linked with the IoT, as it provides a low-cost, power-efficient, wireless method of communication, with existing applications primarily focusing in asset, animal and people status tracking in industry, agriculture, healthcare and the aviation sectors, access control container tracking in maritime sector, health monitoring, toll tags and no-contact payments [62].Some systems have been developed, where active RFID chips have been outfitted with limited sensors that collect environmental data such as humidity and temperature.
  From a cybersecurity perspective, the RFID technology introduces some risks to IoT applications. To begin with, RFID chips have very constrained processing and storage resources, and as such introducing security mechanisms over RFID chips is difficult. Several types of attacks can target RFID systems, seeking to compromise the three principles of cybersecurity, the Confidentiality, Integrity and Availability (CIA) of the system [64]. Attacks targeting the Confidentiality of RFID systems include cloning, where RFID data is duplicated to a blank chip, eavesdropping, where an attacker reads data from a tag due to a lack of encryption in RFID tags. Attacks targeting the Integrity of RFID systems, include replay attacks, where attackers duplicates valid requests/responses from either the reader or a tag allowing them to mimic either device, spoofing attacks, where attackers attempt to interact with the RFID system by using false/forged data. An attack targeting the Availability of RFID systems, includes the deactivation attack, where an attacker disables an RFID tag by issuing specially crafted commands that force the tag to delete its data. Thus, developing power-efficient security mechanisms for RFID systems is crucial, however, existing proposed solutions are either expensive, inapplicable due to resource requirements, or vulnerable to attacks [65].
- **Bluetooth** [66], [67]: Invented in 1994 as a novel wireless technology, Bluetooth was initially designed

to replace RS-232 data cables. Bluetooth solutions utilise Ultra High Frequency (UHF) radio waves and are designed to function between 2.4 and 2.58 GHz, exchanging data in the form of packets, with each packet transmitted on one of the 79 channels that the protocol defines, each of which has a bandwidth of 1MHz [68]. Bluetooth is a short-range wireless communication protocol that has been used in various pre-IoT applications over the years (wireless keyboards, mouse, headsets,...). To enable various services to function over Bluetooth, several specifications, called "profiles" have been developed [69]. Each profile defines several parameters before any communication takes place, and indicates what actions are supported for a particular task. Over the years, different versions of Bluetooth emerged, with versions differing in their topology, throughput, power consumption and range. The first version of Bluetooth (Bluetooth classic) relied on a topology where multiple servant devices connected to a master device, with the configuration often called piconet and following a star topology. This topology, however had several drawbacks, such as a lack of resilience, as by disabling the master node, the entire network is disabled, limited range and connectivity, as the devices are connected in a 1-to-1 format (master,servant). With the emergence of the IoT, a new version of this protocol was promoted, the Bluetooth Low Energy (BLE). BLE, unlike Bluetooth classic, utilises 40 channels with a bandwidth of 2 MHz [68]. The original version of BLE supported only a star topology, however later versions (4.1 and above) introduced mechanics to simulate mesh topologies, which are commonly found in IoT applications, and preferred since they allow for a device to communicate with multiple other local devices (one to many communication) [70], [71]. Depending on the version and location where it is found, Bluetooth's effective range varies. In indoor settings, its range is less than 10 m, while in open areas it has been reported that it can reach 100 m, which is ideal for both close-range IoT applicaitons for smart buildings and long-range open-field solutions. Transmission speeds vary from 1 to 3 Mbps.

From a cybersecurity perspective, Bluetooth has faced several security threats throughout its many versions. The expected outcome of the security threats that target Bluetooth varies, from information stealing to device takeover, affecting either one of the three principles of cybersecurity (CIA) [72]. An attacker targeting the Confidentiality of Bluetooth systems can eavesdrop during the paring process, and attempt to generate the keys that two devices employ to encrypt their communication and to authenticate one another, through brute forcing. An attacker targeting both the Confidentiality and Integrity of Bluetooth systems can employ Man-in-the-Middle (MITM) attacks, where the attacker intercepts the communication between two devices and modifies it in order to appear as if it is coming from either of the authenticated ends. Similar to a MITM attack, a relay attack uses two impersonator devices to two legitimate Bluetooth devices, retransmitting the incoming traffic of one of the legitimate devices to the other, effectively breaching confidentiality. Denial of Service (DoS) attacks are one possibility for attackers to affect the Availability of Bluetooth systems, with some prominent examples being the Big NAK (Negative Acknowledgement) attack where the attacker initiates data exchange and then requests constant retransmissions, effectively locking the target in a constant loop of re-transmissions, and the battery exhaustion attack, where the attacker forces the target's processor to increase its power consumption and thus depletes the target devices power capacity, an attack that is very effective against IoT devices and their reduced resources. The BLE version of Bluetooth, which is found in IoT applications, has also displayed weaknesses to such attacks [73].

- **LoRAWAN** [74]: The Long Range Wide Area Network (LoRaWAN) protocol is a Network layer protocol, which bases its functionality on spectrum modulation techniques. LoRaWAN is a type of Low Power Wide Area Network (LPWAN) technology, that achieves very long range compared to other similar protocols (Bluetooth, RFID, ZigBee) with low transmission speeds. LoRaWAN uses a star topology where multiple sensors connect to a gateway that aggregates the collected data and transmits it to a cloud backend [75]. To increase a LoRaWAN-based system's range and enhance its versatility, a star-of-stars topology is often implemented, multiple intermediary gateways receiving incoming data from sensors, and bridging LoRaWAN-powered devices to the cloud backend. The star-of-stars topology, along with the low transmission speeds, and the use of base stations to forward node data streams, promotes a longer battery life in the IoT sensors that utilise this network protocol, while maintaining a simple network architecture. On the physical layer, LoRaWAN utilises the LoRa protocol, maintained by Semtech and which functions in sub-gigahertz frequency ranges (under 1GHz), and enables effective, low-power transmissions with a range that exceeds 10 Km. The maximum transmission bandwidth of this protocol is 50kbps, however it depends on LoRa's spreading factor, with increases in the spreading factor resulting in increases in effective range and decreases in data rate speeds. The maximum supported message payload size is 243 bytes [76].

  LoRaWAN employs an end-to-end encryption, using AES and a 128bit encryption key. Three classes are defined for LoRaWAN, each differentiating the way which nodes communicate with the base station, namely Class A, B and C [77]. Class A communication is asynchronous, with nodes transmitting data independently at random times. Class B defines specific time periods of

fixed length, where the cloud server transmits messages to the nodes, enabling synchronization and allowing the cloud server to wake the nodes at certain intervals. In Class C, the nodes are in constant communication with the gateway and thus the cloud server. Between the three classes of LoRaWAN, Class C can only be implemented by IoT devices that do not have limited power capacities, with Class A being the best choice for extending battery life, however, Class C enables bidirectional communication while Class A does not. LoRaWAN is employed in IoT applications that are not designed for real-time sensing and do not require constant communication between the nodes and the cloud backend. Examples of such applications include smart farming, livestock tracking, smart parking, environmental and building sensors [78], [79].

From a cybersecurity perspective, LoRaWAN has some cybersecurity weaknesses and threats that target it on multiple levels [80]. By gaining physical access to sensor nodes, attackers can extract cryptographic keys used on the application and network layers, as these keys are stored locally inside the nodes and are transferred from the microcontroller unit to the LoRa radio module in plaintext format. Attackers can launch a type of denial-of-service attack, by utilising hardware that has LoRa connection capabilities and transmitting a flood of messages, effectively jamming LoRa communications in a chosen frequency. Another effective attacks against LoRaWAN systems is the replay attack, where an attacker monitors traffic in a particular channel and frequency, collects data that devices use to authenticate (part of a handshake process) and attempts to fool a server or device by retransmitting the same data and thus authenticate as a legitimate entity. An extension of the jamming and replay attacks is the wormhole attack, where an attacker utilises both a collector and a jammer device to capture legitimate LoRaWAN traffic and jams the traffic from reaching the gateway, thus being able to retransmit the legitimate traffic at a later time as the protocol does not specify time of transmission features. Finally, this protocol is susceptible to power-draining attacks, as forcing retransitions can lead to extra power consumption [81].

- **ZigBee** [15], [82]: ZigBee is a protocol used for short-range low-power IoT applications, often found in smart home, healthcare and other systems that require Machine to Machine (M2M) communication. It utilises a frequency of 2.4 GHz, similar to Bluetooth, with an effective transmission range between 10 and 100 meters and often requiring line of sight. Unlike Bluetooth, ZigBee supports star as-well-as tree and mesh network topologies, the latter allowing all devices in a local network to communicate with each other, and thus removing the single point of failure that can be targeted to disable the network. By using this mesh topology, and intermediate nodes as relay points, ZigBee networks can increase their effective range past the 100 m limit. To be ideal for IoT devices with limited power capacity, ZigBee utilises low data rates, at 250 kbps, however a good portion of that transmission capacity is used for other functionalities (mesh protocol, transmission cryptographic security and acknowledgements) [83], [84]. To secure communications and for authentication purposes, ZigBee uses AES-128bit similar to LoRaWAN.

  The devices, or nodes, that make up a ZigBee network are categorized in three groups, ZigBee Network Coordinator, ZigBee Router and ZigBee End device [83], [85]. A ZigBee Network Coordinator (ZC), is an essential entity which initiates the formation of a ZigBee networks, forms the root of the network and also carries out routing after the network has been established. ZCs decide if a new ZigBee device is allowed to join or leave an existing network securely, a process which relies on the Trust Center that these devices maintain. After a ZC has initiated the establishment of a network, ZigBee Routers (ZRs) and Zigbee End devices (ZEDs) join the network. Aside from the ZC, ZRs manage routing inside a ZigBee network, thus they are functioning constantly (increased power consumption), connecting the coordinator to routers and routers to end devices. The ZEDs are devices that have limited power capacity, and can only transmit data to a ZR, relying on it and the ZC to rout the transmitted traffic to the intended recipient inside the network. Depending on the power supply of devices and their purpose, they may assume any one of the three aforementioned roles in the network.

  From a cybersecurity perspective, ZigBee has been shown to have some weaknesses that allow attackers to exploit it [15], [86]–[88]. Several DoS attacks have been reported, where attackers force ZEDs to be constantly active and responding to maliciously-crafted messages, thus depleting their limited power capacities. Another attack, called ghost-in-the-ZigBee works in a similar way, by forcing a node to perform security operations as a result of receiving a forged message. Additional attacks that have been seen to affect ZigBee networks, include Sinkhole attacks, where an adversary attacks the integrity of the routing process by drawing messages away from their intended destination, and Wormhole attacks, that rely on recording legitimate traffic on one area of the network, and retransmitting it at another area. Further attacks have been demonstrated against particular versions of ZigBee, such as ZigBee Light Link. One particular attack against smart lightbulbs that function as part of a ZigBee network exploited the Touchlink's proximity check and the over the air (OTA) feature of the device, to install custom firmware that functioned as a worm, spreading to other lightbulbs in close proximity and infecting entire buildings. Additionally, as in LoRaWAN, signal jamming attacks can be launched, effectively causing a DoS.

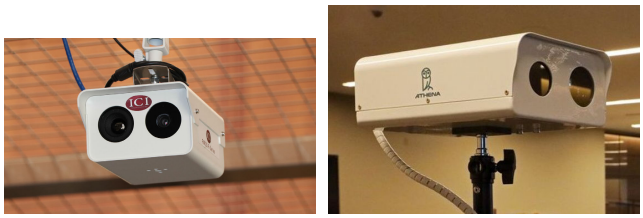
- **MQTT** [89]–[91]: The Message Queuing Telemetry Transport (MQTT) Protocol is a light-weight communication protocol, often utilised in systems with constrained resources. The protocol functions in a publish-subscribe mode, where clients subscribe to a topic housed in an MQTT broker, and publish data which can be read by all subscribed clients. The format in which the data is publish depends on the sender, however in IoT it tends to be a semi-structured format such as XML or JSON.
- **PROFINET** [92]: The Process Field Net (PROFINET) is a communication standard that works over Industrial Ethernet and is utilised to connect controllers with devices and collect data in an industrial environment. It supports transmissions at regular intervals, in ?real-time? and utilises data structures such as XML for device communication and device monitoring. It leverages three communication channels, a standard TCP/IP channel for configuration and not-regular asset accessing, a Real Time channel for alarms and regular device communication, and an Isochronous channel for high-speed communication.
- **XMPP** [93]: The Extensible Messaging and Presence Protocol (XMPP) is an open communication protocol based on XML, that can be used in a publish-subscribe mode, similar to MQTT. It has been utilised in a diverse range of applications, including chatting, audio or video calls and middleware communication. The protocol is designed to be extensible, flexible and decentralised.

The suitability of one of these wireless protocols for an IoT setting, depends mostly on the application in question. IoT systems that do not require regular transmissions from their sensors/actuators and prioritise battery life while requiring a large effective range can employ LoRaWAN. With regards to robustness, ZigBee would be the better choice for a wireless protocol in an IoT setting, due to its support of multiple topologies, and the versatility of its nodes. The RFID protocol is mostly suited to asset tracking and applications that require close-range contact. The Bluetooth protocol can be employed in small to mid-range applications, like building Personal Area Networks (PANs) or small-scale sensor networks. Generally, due to the field of application being the IoT, with such devices often prioritising extended battery life rather than processing power and memory stores, the wireless network protocols that enable it on a local level will not incorporate powerful cryptographic algorithms and excessive security protocols, as by including such mechanisms, a device's battery life would be diminished. Table 3 depicts several smart airport IoT applications, and the network protocols they utilise for device-to-bridge communication.

D. SECURITY AND SAFETY HEALTH SYSTEMS IN SMART AIRPORTS

One of the key aspects of contemporary airports, is to function as a hub for recreational, touristic and business travel while also connecting remote geographic areas for commerce. As such, airports are a place of high mobility, with passengers from all around the globe arriving and interacting with local airport personnel, often on a physical level, for example during the security screening process, which can facilitate the transmission of viruses and affect public health. The COVID-19 pandemic has made apparent the need to introduce biometric sensors at specific areas where crowd interaction, and thus the probability of transmission, is high such as airports. As such, contemporary smart airports have been encouraged to consider the development of *Security and Safety Health Systems*, in order to detect and stop the transmission of the virus, both globally by passengers, as-well-as locally by the airport personnel.

(a) Left: BTM-T5 [102]. Right: FevIR Scan 2 [103]



(b) Left: ICI FM320 [104]. Right: Athena fever camera [105].

FIGURE 4. Thermal cameras used for human temperature screenings.

Such screening Biometric IoT sensors have already been implemented in several airports around the world, and unlike previous biometric systems that were used primarily for the secure validation of passengers' credentials, they are now focusing on recording detecting data features that can be used to distinguish between healthy and infected passengers. Thermal cameras have been the primary type of biometric IoT sensor that has been chosen by many airports for such detection scenarios [100], [101], as they enable the rapid detection of passengers with high fever without slowing down the screening process, avoiding physical contact which can further spread viruses or requiring more intrusive measures that the passengers may object to. An example of such a camera with thermal capabilities can be seen in Figure 4.

Cybersecurity weaknesses could expose these cameras to attacks by hackers, causing increased false positive rates, that can affect airport processes and cause delays, or in a more severe scenario, cause false negative rates to increase, effectively allowing detectable cases of the virus to spread, causing a bio-cyber-attack. As such, the cybersecurity of thermal cameras needs to be examined, and potential flaws detected, in order to protect these systems from cyberattackers.

TABLE 3. Common smart airport applications and corresponding protocols.

Smart device	Network Protocol(s)	Limitations
Luggage tagging and tracking [50]	RFID	Small-range, very restricted power supply, vulnerable to attacks
Indoor navigation [94]	Bluetooth (BLE), WiFi	Topology star-of-stars vulnerable, vulnerable to takeover and power depletion attacks
Lights [95]	ZigBee	Vulnerable to attacks, low data rates
Runway integrity scanner rover [14]	Bluetooth	Topology star-of-stars vulnerable, Vulnerable to MITM attack, vulnerable to takeover and power depletion attacks
Environmental condition tracking scanners [59], [96], [97]	WiFi, Ethernet, Bluetooth, LoRa	Topology star-of-stars vulnerable, vulnerable to data spoofing attacks, vulnerable to takeover and power depletion attacks
Smart restroom [98]	Bluetooth (BLE), Ethernet	Topology star-of-stars vulnerable, vulnerable to data spoofing and manipulation attacks, vulnerable to takeover and power depletion attacks
Airport asset tracking [57]	Bluetooth, RFID, ZigBee, LoRaWAN	Topology star-of-stars vulnerable, vulnerable to takeover and power depletion attacks
eGates [99]	RFID, NFC	Small-range, very restricted power supply, vulnerable to attacks

TABLE 4. Classes of smart airport devices and services.

Class	Most Common Devices and Services
Operational-maintenance	Runway health scanner [12], [14], Smart smoke and fire detectors [106], Perimeter Intrusion Detection System [107].
Operational-efficiency	Self-check-in systems [108], eGates [45], [46].
Operational-management	Trolley RFID locator [109], video surveillance systems [110], electronically controlled doors [111].
Services-augmentation	Indoor navigation [112], [113], Parking lot car tracking service [13].

E. A CATEGORISATION OF AIRPORT SUBSYSTEMS

From a technological perspective, a smart airport is a network of interconnected smart devices, each specialised in performing a specific task, while the data collected by sensors that are deployed in the airport are often used to power secondary services that enhance the experience of travelers. These smart devices that lie at the core of a smart airport can be logically categorized based on their deployment task and purpose into the following distinct classes: 1) Operational-maintenance, 2) Operational-efficiency, 3) Operational-management, and 4) Services-augmentation. In Table 4, the four classes and examples of devices that belong to these classes are given.

Operational-maintenance refers to devices that are tasked with supporting the maintenance procedures of the airport. Such devices can monitor the state of various areas of the airport, such as the runway, and raise an alarm if some sort of malfunction is detected. An example of such a device would be a runway health scanner, a device which automates the detection of damages or foreign objects in a runway instead of relying on manual inspection [12], [14] thus enhancing reliability while minimizing human error. Other devices that are classified in this category, include smart sensors like smoke and fire detectors [106], which are network enabled sensors that are connected to a centralized platform where alarms can be viewed and dangerous incidents better managed. More related to security, IoT-based systems have been proposed for securing the perimeter of an airport, detecting and preventing unauthorized entry [107].

The Operational-efficiency group includes devices and subsystems that promote efficiency in the day-to-day processes of the airport. For example, self-check-in systems [108] are one such subsystem that has become an integral part of most contemporary airports. By accessing dedicated kiosks or by using their smart phones, passengers are able to check-in, drop off their luggage and receive their boarding passes easier and quicker than waiting in line for manual check-in, saving time in the process. The use of biometrics in eGates [45], [46] is another subsystem that promotes efficiency. It eliminates the need for airport personnel to manually check a passengers identity, thus automating the passport control process by utilising the passenger's biometric data that is kept in the passport's chip, reducing the processing time.

Operational-management devices are tasked with supporting management of areas and other secondary services in the airport. By using these devices, it becomes possible to track the location and status of resources of an airport, thus limiting unnecessary replacement expenses and maximizing their usability. For example, RFID Transmitters for the detection of luggage trolleys [109] in parking lots or inside the airport is such an application, as often travelers will not return the trolleys they used to its proper location. Further applications include, the video surveillance systems [110] and electronically controlled doors [111] that monitor the passengers in order to swiftly detect suspicious behavior and controlling access to certain restricted and possibly high-risk areas of the airport.

Services-augmentation refers to smart things and applications that enhance the traveler's experience in the airport or during a flight. An example of such a subsystem is indoor airport navigation [112], [113] through the use of smartphone

applications and technologies like WiFi, Bluetooth and ZigBee, which enables passengers to easily navigate the interior of an airport, often incorporating translation capabilities to the applications to help passengers that may not speak the local language. Another application is the smart airport parking lot car tracking service [13], which enables users to remotely view the position of their car inside the parking lot of an airport.

IV. CYBER SECURITY MECHANISMS EMPLOYED IN SMART AIRPORT NETWORKS

In a smart airport, multiple devices are interconnected, forming various and often technologically diverse networks that coexist throughout multiple buildings, in order to build the services that qualify an airport as being ''Smart''. Additionally, such airports maintain at least one Internet connection for various operational and scheduling purposes. However, these networks can be targeted by cyber-attackers, who wish to identify a weakness, exploit, gain access to an airports inner systems and cause damage. Such security weaknesses can manifest either due to hardware misconfiguration, software bugs or inherent network protocol weaknesses. It is important for smart airport network managers to deploy tools that can detect such weaknesses, active campaign attacks or successful intrusions, in order to detect them swiftly and effectively combat or mitigate them, ensuring the integrity of the services provided by the airport and the safety of both passengers and personnel.

Firewalls [114]: are typically placed on the edge of a network and monitor inbound and outbound traffic for known patterns of attack, blocking traffic from hosts that exhibit attack-like patterns. A firewall utilises pre-defined rules that describe attack patterns, blocking any host that displays such behaviour, and allowing all other traffic.

Intrusion management systems: are deployed in a network to detect, assess, respond, and prevent intrusions. The most common intrusion-related systems are as follows:

- **Intrusion Detection System (IDS)** [115], [116]: are tasked with detecting the unauthorised access of assets in a protected network. It can be either a dedicated hardware device, or a software, and depending on the locations where it is deployed, it can either be a Network-based IDS (NIDS) or a Host-based IDS (HIDS). The two primary types of IDS depending on the detection method are Signature-based IDS, where an up-to-date database of attack signatures is maintained and utilised for attack detection, and Anomaly-based, where the normal activity of legitimate devices is learned and any deviation is detected as an attack.
- **Intrusion Intention (IIS) System and Intrusion Prediction System (IPS)** [115], [117], [118]: are supporting systems to IDSs and to security experts. The task of an Intrusion Intention System is to identify the goal of an attack by assessing the value of the protected networked assets, while an Intrusion Prediction System assesses historical events (attacks) that have targeted the network, in an attempt to estimate the predict future attacks.
- **Intrusion Prevention System (IPS) and Intrusion Response System (IRS)** [115], [119], [120]: function as secondary measures that are invoked, after an IDS has detected an attack. The task of an Intrusion Prevention System is to proactively monitor a network and attempt to counter attacks before they occur, based on pre-defined profiles, by dropping malicious traffic and blocking the attacker's source IP. An Intrusion Response System on the other hand, is a reactive measure that is invoked after an attack (intrusion) has been detected, employing either an expert-system rule-based approach or an adaptive feed-back approach to guide the system's mitigating actions.

Risk assessment [121]: are generally employed proactively by organisations, to assess their assets, identify any associated risks, determine the possibility of and circumstances under which an asset may be affected by a risk and the impact of such an event to the organisation. Cybersecurity risk assessment tools are applied to digital devices (hardware, software, PCs, laptops) and data, to detect the existence, likelihood, severity, and impact of risks to organisations, their operations, assets and to individuals. These tools often provide a high-level view of the cybersecurity state of an organisation, in the form of a report, where assets are identified, a scaled value indicates the severity of the risk and a short description addresses the ways this risk may be exploited. The functionality of existing cybersecurity risk assessment tools varies, depending on the sophistication of the tool. Some tools simply assist users in performing a risk assessment of an organisation, guiding them through the following steps: identify importance of assets, identify threats, identify asset vulnerabilities and impact, analyse existing preventive controls, assess the probability of an incident to occur and determine the threat level of the risk. Other automated tools monitor networks, computers, servers and other connected devices to detect known vulnerabilities. Yet other automated tools, known as breach and attack simulation software, are employed to continuously attack a company's infrastructure, attempting to breach its security using well-established methods and provide insights about potential vulnerabilities, the associated attack surfaces and the resulting risks.

Threat intelligence [122]: also known as cyber-threat intelligence, is data collected through tools that organisations employ to identify past, present, and future threats that target important assets that the organisation owns and utilises. The main purpose of cyber-threat intelligence is to provide organisations with insights into cyber threats and how they may be exploited, as a way of enhancing cyber-defences and designing prevention and mitigation strategies. These tools remain up to date, by acquiring unformatted data related to security breaches, zero-day threats and other exploits from a variety of sources. The data is then processed and analysed, with the results then either forwarded to other security

solutions such as IPS or parsed into reports that can be used by experts to better understand and patch the weaknesses of an organisations systems. Threat intelligence seeks to determine certain factors about a potential security incident, such as the identity of the attacker(s), their technical capabilities, their target and the potential attack vectors that they may apply. Threat intelligence is comprised of two main components, threat intelligence feeds and threat intelligence platforms (TIP). Threat intelligence feeds are real-time flows of data that represent information about ongoing cyber threats, such as malware hashes, known compromised IP addresses and potentially compromised domains. Threat intelligence platforms are connected to threat intelligence feeds, enabling organisations to collect data, transform it from its original format, correlate it and gain insights on prolonged cyber-attack campaigns, integrate it to the organisations existing security tools and further analyse it, in the process converting data into information and knowledge through contextualisation. Threat intelligence is designed to be a cyclical repeating process, as threats are constantly appearing and evolving.

Vulnerability analysis [123]: is an important step in risk assessment and a standalone continuous process that helps protect systems from potential future intrusions and exploitations. Vulnerability analysis tools critically and systematically assess an organisation's Information Technology infrastructure in order to detect known weaknesses in software, misconfigurations in hardware and generally ascertain to what extent these vulnerabilities can be exploited, while assigning a severity level to it. Vulnerability analysis tools can be connected to Threat Intelligence platforms, to receive updated information about existing security threats, improving their effectiveness. This process produces a number of results. To begin with, it detects vulnerabilities in the code of software, configuration of servers and devices or network protocols. Second, it provides the source of the vulnerability, its potential impact and suggested remediation methods. Furthermore, the detected vulnerabilities are sorted based on their importance, so that they are addressed based on their severity. Vulnerability analysis can be performed through the use of automated tools, that usually rely on well-maintained databases of known vulnerabilities and signature-based scanning.

Contemporary cyber-threats that exist, utilise and propagate through the Internet, render the adoption of one or more of the aforementioned security measures a necessity for ensuring the security of an airport's network. Smart airports that have incorporated IoT devices in their networks face an even greater threat, as new attack surfaces are introduced due to the vulnerability that the IoT has exhibited over the years. In a survey conducted by Lykou *et al.* [29] during 2018, and addressed to the IT personnel of airports around the world, it was discovered that the prompt incorporation of IoT devices in the smart airports networks does not coincide with a diligent consideration of the security flaws and weaknesses that these devices introduce. It was shown that the most popular security measure that was applied was a firewall, however what mechanisms these firewalls utilised was not discussed.

The researchers attribute the inconsistency in the level of sophistication and the security measures chosen by contemporary smart airports to the lack of commonly accepted security policies and standards. Additionally, a study by Cui *et al.* [124] published in 2018 showed that existing IDS/IPS solutions for smart systems have several challenges. To begin with, existing IPS systems exhibited large false negative rates, thus were ineffective at predicting, detecting or deterring attacks. Furthermore, the researchers stressed the need for light-weight IDS/IPS systems, as most IoT devices that constitute these smart systems, are power-constrained and incompatible with existing IDS/IPS that are designed to work continuously and thus require more power to operate.

V. RISK PROFILING

The term ''risk profile'' has been broadly used in multi-disciplinary fields, such as finance, software engineering, supply chain, risk management, cybersecurity and the IoT. Every domain has its own definition, reflecting their unique risks and the nature of the environment. For example, in finance and risk management domains, a risk profile is defined as an assisting tool employed by advisers to optimise decision making related to investment risks, on behalf of their clients, basing the decision on three parameters, the risk capacity, the tolerance to risk and meeting the desired investment objectives [125]. Before a clear definition of a ''risk profile'' for smart IoT environments, focusing specifically on smart airports, can be given, it is first essential to define what the meaning of ''risk'' and then proceed to describing the process of risk management.

From a security perspective, risk is defined as the likelihood of loss, damage, or disruption of assets and the services that they provide, such as the infrastructure of smart airports and its IoT networks, which is brought about by cyber threats that exploiting assets' vulnerabilities [126]. The difficulty of defining the term ''risk'' in the context of cyber security stems from the uncertainty related to quantifying the impact of attack surfaces and their associated attack vectors. In order to provide a satisfactory solution to this uncertainty, it is imperative to first define the term ''risk management'' and then link it to existing security standards, such as the ISO 31000 standard [127] and the 2019 Australian Government Information Security Manual (ACSC) [128]. A definition from the ISO standard [127] identifies risk management as the process of identifying, assessing, mitigating threats and monitoring, which take the form of cyber threats in the context of cybersecurity. In the ACSC, due to the increased frequency of cyber-attacks and their rising impact on business operations, it is recommended that organisations apply a risk management framework, to protect their systems, information and other assets from cyber threats.

There are various theoretical risk management frameworks and strategies that have been proposed in the literature [128]–[130]. By reviewing the literature, it is observed that several steps/stages are shared between the existing risk management frameworks or standards, which are described as follows:

- **Understand the environment and its context (e.g. airports and their assets)-** it is significant to scope the environment that we interact with to define its risks. For instance, smart airports contain multi-domain networks and IoT devices, such as explosive sensors, CCTV cameras, smart monitors and weather sensors, controlled by different operators.
- **Identify risk-** it is a procedure of discovering vulnerabilities, i.e., weaknesses of the network and IoT devices. This identification could be the first stage of implementing ''risk profiling'', which depends on collecting data, aggregating, and labelling them for further analysis. Artificial Intelligence algorithms could be the technology that allows the automation of risk identification in the era of IoT and its big data.
- **Analyse risk-** once attack surfaces and their vectors have been defined using analytics tools, it is important to assess the possibility of occurrence of those attack vectors and examine their consequences on the environment.
- **Evaluate risk-** after the cyber threats have been analysed, they are further assessed to examine their impact and likelihood of occurrence. Then, a decision-making process should be considered to take appropriate actions against those threats based on their effects on the environment assets.
- **Mitigate risk -** after assessing the cyber threats and their impacts, reactive and proactive security solutions should be applied such as intrusion detection and prevention systems along with patching and management tools.
- **Monitor risk-** is a continual and cyclic process that should be designed before identifying risk and after mitigating it. Before risk identification, there should be security solutions configured in the environment such as privacy-preserving techniques for protecting sensitive information from disclosure, blockchain technology for providing trust between communication elements in an environment. After mitigating risks, monitoring mechanics track existing and novel attack surfaces and vectors.

A. RISK PROFILING FOR SMART AIRPORTS

Airports are a vital aspect of society, which need to ensure the security and reliability of their operations. Contemporary airports, aside from enabling transportation, are central to trade and commerce. Therefore, the maintenance of airport operations within complex, dynamic and interconnected environments, which face numerous threats is a considerable challenge [7], [131]. In this case airport security and business continuity become significant challenge for the airport operation. Therefore, reduction of threats and risk management are not only critical for airports at the local level, but also for ensuring border protection and the national security for any country.

Identifying airport general risk management procedures are very important for risk and security mitigation as shown in Figure 5. The exogenous and endogenous factors influence the airport component, airport risk management strategy, risk management framework and the airport decision-making under risk. The results model provides airport components which include IoT-based control, integration and IoT-based communication that are influenced by exogenous and endogenous factors. In addition, the framework provides the airport's risk management strategy that is influenced by exogenous, endogenous factors and by airport components. Furthermore, the framework also provides the airport risk management framework which consists of risk identification, analysis, evaluation and monitoring.

An example of a generic risk management framework can be seen in Figure 6, while the framework depicted in Figure 5 provides the airport decision-making under risk polices that include risk identification and measurement methods. The International Civil Aviation Organization (ICAO) is responsible of creating safety and security polices and standards for the aviation industry throughout the world [8], [131], [132]. ICAO has response rules and polices for real airport environments to measure endogenous and exogenous factors. This could make a standard airport risk management strategy and a risk management framework. This framework describes the relationship between different elements inside the airport starting from different internal and external factors affect the operation of the airport, different airport components such as IoT communications and IoT control. Furthermore, it is in compliance with both ACSC and ICAO policies for airport policies and security procedures [128], [131], [132].

The security risk profile could be formulated as a combination of risk analysis and evaluation methods that integrate assets, threats and vulnerabilities and can be used for security factors analysis in endogenous factors. Today, there are many frameworks that can be used to analyse and manage risks in IoT environments of smart airport, such as the Factor Analysis of Information Risk (FAIR) framework [133], and Enterprise Architecture Management-Information System Security Risk Management (EAM-ISSRM) [130]. The FAIR is a stochastic approach that measures each factor against assets and threats, while the EAM-ISSRM is a conceptual model to provide the integration between different OT and IT services. Most of the existing risk management frameworks would be utilised to secure IoT architectures and assets of smart airports against cyber threats. In the next section, we will address the security risks that smart airport face, focusing on the network-side of their infrastructure, and then discuss the associated challenges.

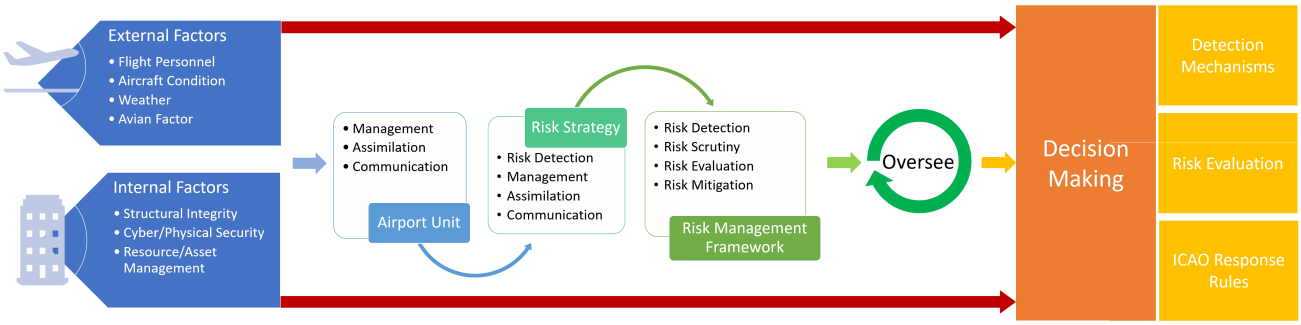


FIGURE 5. A risk profile decision making framework for smart airports.

VI. AI-BASED CYBER-DEFENCES IN SMART AIRPORTS

Prior to the development and augmentation of the machine learning field, cybersecurity scanning and audits were (and in some situations, still are) a manual process, relying on experts who reviewed every aspect of a system (including source code, logs, network ports), in order to identify security weaknesses and provide mitigations and solutions [134]–[136]. To eliminate the possibility of human error, automated security tools were developed, with the majority relying on expert-derived rules and signature-based scanning which use malware hashes. In recent works however, researchers have emphasised the value of machine learning (ML) and artificial intelligence (AI) in the development of cybersecurity tools [137]–[139]. In this section, we will discuss how AI can be employed in a cybersecurity setting, existing applications powered by AI and its strengths compared to signature and rule-based tools.

A. AI-BASED CYBER SECURITY APPLICATIONS

Essentially, AI is the discipline that studies algorithms that represent logic and solve problems. The main motivation behind AI development is to simulate human-like intelligence, through the use of mathematics, statistics and logic. AI spans multiple subdisciplines, including ML and rule-based expert systems, with each subdiscipline providing a different methodology to simulate intelligent behavior. An example of an AI system that preceded ML, would be a collection of if-then-else statements which are often crafted by an expert and are called expert systems (or rules engines) [140]. Expert rule-based systems are static representations of knowledge, that rely on experts (in the field where the system will be applied) to hard-code rules for the accomplishment of some task such as the detection of malicious network traffic or the processing of taxes.

A subset of AI, ML is a collection of models that are capable of "learning" dynamically from data and altering their inner state (values) that represents knowledge, in order to adapt to new data-based stimuli [140]. ML can be trained with supervision, where data has been curated and labeled, without supervision, where a ML model detects relationships and builds groups based on similarity, semi-supervised where a small number of labeled instances are combined with a larger number of unlabeled data or through reinforcement learning

FIGURE 6. An example of a generic risk management framework.

where the input data is not labeled and the learning process is formed as a game, where the model is rewarded or penalised based on its output [141], [142]. Furthermore, ML algorithms are separated, based on their data requirements, their output and use-cases into classification, clustering and regression [140], [143].

Classification algorithms rely on labeled data (where the output is known), to train models that assimilate relationships between input and output data, with the output being one of multiple possible and pre-determined classes. Classification algorithms include probabilistic classifiers such as Naïve Bayes that relies on the Bayes theorem, tree-based classification such as Decision Trees that relies on some measure of uncertainty (such as entropy) to decide the split condition in each branch and Artificial Neural Networks, that rely on multiple units, called neurons, that are organised in groups called layers, with neurons from one layer connecting to neurons of the next layer and the connections having weights the values of which, along with a bias value for each neuron, are assigned and corrected during training.

Clustering algorithms receive unlabeled data as input, and attempt to identify previously unknown classes, based on some measure of distance (such as Euclidean, Manhattan, Hamming) [144]. Essentially, a clustering algorithm seeks to detect groupings of similar data, where a datapoint in one cluster is more similar to other data points of the same cluster and less similar to those of other clusters. Clustering

algorithms include Centroid models such as K-means that uses imaginary centroids to calculate distance with other datapoints and form clusters and Hierarchical models which seek to build a hierarchy of clusters by either combining observations into increasingly larger groups (Agglomerative) or divide the whole data into increasingly smaller groups (Divisive). Regression models are similar to classification models, in that they predict a value based on input, however, unlike regular classification, where the output is one of multiple (two or more) pre-defined classes, regression is tasked with predicting a continuous value [145]. Regression algorithms include Linear regression, Logistic regression, LASSO and Support Vector Machines.

Deep Learning (DL) is a subcategory of AI and ML, and more specifically, a particular subset of ANNs. The original inspiration for neural networks (NN) comes from the human brain, and specifically, the neuron cells that are comprised of multiple inbound connections called synapses (found on dendrites) and a single outbound connection called axon [146]. Multiple neurons connect to each other, axons to synapses, thus forming a complex network where information is represented, stored and processed by neurons ''firing'' an electric current (value equivalent of 1) or remaining dormant (value equivalent of 0). What differentiates simple NNs from DL, is the architecture. Specifically, NNs that have a ''deep'' architecture, that is, that are comprised of numerous neurons and multiple layers can be considered to fall under the DL category, although there exists no strict rule for determining how many layers or neurons a NN needs, in order to be considered ''deep'' [147].

Each neuron in a deep NN (DNN), receives some input from previous layers (or the original input), applies a linear transformation, multiplying the input with weights and adding a bias factor, parses this linear transformation through an activation function and delivers this last output to the next layer. DNNs are powerful models that usually require huge datasets (Big Data) to improve the performance of the model, and a lot of memory and processing resources (usually depending on the number of connections between neurons) [148], [149]. Popular DNN models include Recurrent Neural Networks (RNN) and Long-Short Term Memory RNN (LSTM/RNN) that utilise memory of previous data input points to make future predictions, Deep Belief Networks (DBN), Convolutional Neural Networks that are primarily employed for image recognition and classification and Deep Multi-layered Perceptrons (MLP). The relationship of AI, ML and DL can be seen in Figure 7.

B. CYBER-DEFENCE TOOLS BASED ON AI TECHNIQUES

The automated mechanics that AI, ML and DL offer, have been applied in a number of fields to great success, one of which is cybersecurity and, in this case, cyber-defences. In general, AI and its subcategories can be employed in cyber-defences, as an automated decision-making engine, prepared on pre-acquired data that can be either labeled or unlabeled. In this subsection we will discuss some types of cyber-defence tools and address their underline mechanics.

- IDS [150]–[154]: Traditionally, IDS were based on AI models, as an automated and intelligent method was required to process multiple files and network traffic. Older IDS implementations, also known as misuse-IDS employed rules-based engines, similar to firewalls and anti-virus software, and relied on a database of known rules or patterns, to detect a threat. Contemporary research has lead to the development of anomaly-based IDS that utilise NN and DL. An anomaly-based IDS is a ML or DL model that has been trained and evaluated on data instances that are considered normal, allowing the model to ''learn'' to detect the normal behaviour of the users in a system. Anything that deviates from this normal behaviour is automatically flagged as an attack. Previous research has applied several models, such as: CNN, DBN, RNN, DNN, SVM, Naïve Bayes.
- Firewalls and Anti-Malware [155]: Originally, firewalls and anti-malware software relied on rule-based engines. Recent developments have lead to firewalls that, at their core, rely on ANN with one example being FortiWeb [156] a firewall for web applications. Anti-malware software based on NN have also emerged such as Deep Armor [157], which is a cloud-based service that protects computers from malware and zero-day exploits, utilising ML models that are kept up-to-date through re-training on newer malware instances.
- Threat Intelligence [158]–[161]: The purpose of threat intelligence is to provide insights into potential security threats, by processing various and diverse data threads that networked sensors produce, often in real time. However, this can not be a manual task for a number of reasons, such as the possibility of human error, the need for near real-time processing of vast collections of data, originating from multiple sources. As such, automated methods based on both ML and DL models have been incorporated into threat intelligence platforms, providing reliable classification of security events, or seeking to identify new patterns through clustering. The output of threat intelligence platforms can then be forwarded into other tools such as IDS/IPS, thus orchestrating a more robust cyber-defence. Existing research has utilised DL and ML models, such as LSTM and CNN to differentiate between known strains of malware [161], SVM to classify malicious source code obtained from forums and combine the results with metadata to enrich the model's output [158], [159]. Furthermore, a system based on honeypots of varying levels of interaction and installed on different platforms (IoT, embedded devices, PCs, Servers) with a DL model such as CNN applied to the obtained data to identify the presence of malware. An example of a real-world cybersecurity platform that provides threat intelligence and utilises DL models is Deep Instinct [162].

FIGURE 7. The relationship of AI, ML and DL.

- Vulnerability Analysis [163]: Vulnerability analysis is the proactive process of detecting weaknesses and vulnerabilities in an organisation's cyber-defences, evaluating their significance and assigning some severity marker, which is used to prioritise fixes for the more impactful vulnerabilities. This process involves the thorough investigation of networks, devices and software that is owned by an organisaiton. To that effect, automated methods based on ML and DL have been proposed and employed for the detection and categorization of vulnerabilities, reducing processing times and minimizing the human error factor which appears in such complex and repetitive activities. Depending on the area of application, automated vulnerability scanner tools, can be considered cloud-based, host-based, network-based and database-based. Research has produced vulnerability scanning solutions that scan source code based on Concatenated CNNs [164], distributed network-based vulnerability scanners based on Multi-layer Perceptrons (MLPs) [165], and other vulnerability assessment tools based on Naïve Bayes, Fuzzy Logic, DNN, Regression and Rule-based Engines [166].
- Risk Assessment [167]: Risk assessment refers to the identification of risks that can potentially harm the systems of an entity or organization. The impact of such risks in critical infrastructure environments, such as smart airports, if left unchecked can range from loss of service, to severe sabotage and threat to human life. Existing research has produced both ML and DL methods to automate the process of detection, enhance efficiency and reduce false alarm rates, with the latter resulting in either unnecessary disruptions in the operations of the airport, or failure to detect risks. A review by Hegde *et al.* [167], identified that machine learning methods are utilised in risk assessment in a number of fields, one of which was cybersecurity. A risk assessment tool that was trained on a large dastaset containing instances of past security events and was based on RNN was developed by Shen *et al.* [168].
- AI-enabled cognitive security [169]: This field of cybersecurity focuses primarily on the utilisaiton of ML or DL models for the processing of sensory data, such as video and sound streams. AI-enabled cognitive security are employed to assess potential risks related to physical attacks that may threaten an airport and its infrastructure, by assessing incoming data for suspicious activities. One application would be facial recognition, where camera feeds are constantly parsed by DL models such as RNN,

LSTM and CNN, focusing on the detection of faces. The identified faces can then be cross-referenced with law enforcement databases that maintain images of wanted terrorists and criminals, informing authorities in the case of a positive match [169], [170]. Another application is behaviour and intention analysis, where DL models are trained to scan video streams and detect irregular or suspicious movements of individuals, unusual poses, facial expressions and concealed weaponry [110], [171]–[174]. Such systems can be deployed in critical infrastructure like airports, where irregular movement of a passenger could signify a potential threat.

- Network Forensics [175]–[178]: Usually employed as a reactive measure, after an attack or breach has been detected and data has been collected, network forensic frameworks can be combined with other security mechanisms, to speed-up the analysis of network-derived traces and produce results faster. Several network forensic frameworks have been proposed, that utilise ML or DL for the detection of illegitimate network flows or packets. These frameworks can either scan the contents of packets in what is known as deep packet inspection (DPI) or focus on the header of packets and other descriptive data (timing data) which is known as network flow analysis. Such work, is mostly based on some form of DNN, where a model such as a deep MLP, or an RNN/LSTM model that includes the benefit of memory, is trained on some pre-acquired, representative data.

C. WEAKNESSES OF AI-BASED CYBER-DEFENCE MECHANISMS

The cyber-defence tools that were previously discussed can be separated into two types, either rules-based expert systems or ML/DL systems. Each type has its strengths and is best suited to different applications, however, they also have weaknesses. To begin with, signature/rules-based systems, are static representations of knowledge, and can not detect unknown (zero-day, previously unseen or processed) security threats [179]. They rely on a database of signatures, which has to be kept up-to-date by experts. Furthermore, they are susceptible to malware mutations, as they are unable to detect them if the binary (and thus the signature/hash) is altered in any way. Traditional pre-ML rules-based engines required thousands of rules to be effective [140].

ML and DL models rely heavily on data. That means that low quality or incorrectly prepared data can have a negative impact on the model's performance. Furthermore, the selection of hyperparameters is an important task, which can greatly affect the model. No clear rules exist for selecting the best hyperparameter values for a model in any particular field of application, with experts often calling it more of an ''art'' than a science. Essentially, most often it is a trial and error process, although existing research has addressed and proposed methods for automatic hyperparameter selection/tuning [176], [180]. Another threat that can target ML and DL models is an adversarial attack, during which, an attacker prepares a malicious input for a trained model, aiming to force it to misclassify the fake input, or to otherwise manipulate the model's output [181]. Unlike adversarial attacks, that target a trained model, other attacks, called poisoning attacks [182], [183], can target the training process, crafting fake data points to affect the resulting model's predictive capabilities.

TABLE 5. Risks associated with compromising devices, according to smart airport device classes.

Smart Airport sub-systems	Consequences
Operational-maintenance	Degradation of services. Unauthorised entry. Escalation of intrusion. Cause accident, potential loss of life.
Operational-efficiency	Degradation of services.
Operational-management	Degradation of services. Unauthorised entry.
Services-augmentation	Degradation of services.

VII. SMART AIRPORT-SECURITY RISKS AND CHALLENGES

The process of augmenting airports with IoT-powered automations has substantial benefits from an operational and efficiency standpoint, improving the QoS for passengers and increasing financial returns for all the relevant stakeholders. In a smart airport, IoT devices can be found almost anywhere, from the restrooms to the runway and the air traffic control tower, often interacting with each other through bridged networks. However, the incorporation of IoT devices in the networks of a smart airport introduces a number of risks that can be exploited by attackers, to cause disruptions and affect the normal operations of the airport. These risks, in turn, introduce challenges for researchers that seek to develop new cyber-defence methods and tools that can effectively detect risks, analyse them and provide mitigation steps.

A. CYBER SECURITY RISKS

Although exposing systems to the Internet can promote interoperability, and enables remote accessing of services, imposes risks to these systems, due to the malware, botnets, hackers and other threats that often scan the Internet for vulnerable devices [184]. Through empirical studies, the IoT has been shown to be insecure in many instances [2], [185]. Shielding smart things against cyber-attacks is hard due to hardware constraints [186], as often these devices have limited computational and power capacities, and thus adding security mechanisms could deplete the devices resources.

Additionally, the security of IoT devices is hindered due to design flaws and users often neglecting to change the default credentials [15], [187]–[189]. As smart airports are outfitted with ubiquitous smart things comprised of both sensors and actuators, the possibility that they might not be secured properly introduces considerable risks. In Table 5 a smart airport sub-systems and the associated consequences in the event they are compromised.

- Operational-maintenance: Compromising devices in the operational-maintenance sub-system category imposes a plethora of consequences, depending on the kind of device that is affected. For example, compromising a runway health scanner, causing it to produce incorrect data, may result in an accident for an aircraft, possibly by damaging a tire during take-off or landing. Another scenario involves setting off the smart fire and smoke detectors, causing chaos and delays.
- Operational-efficiency: Compromising operational-efficiency devices may result in financial loss and degradation of services. By compromising and disabling the self check-in and eGates, can result in increased workload for the manual passport check kiosks.
- Operational-management: Attacking devices in the operational-management category introduces both degradation of services, reduction of productivity and possible unauthorised entry to sensitive or high-risk areas of the airport. Compromising the RFID locators of luggage trollies for instance, in effect invalidates the purpose of the system, as it forces airport personnel to waist time retrieving and returning the trollies to their designated position. Furthermore, compromising video surveillance and electronically controlled doors may allow unauthorised, malicious individuals to gain access to restricted areas of the airport and allow them to access otherwise inaccessible parts of the airport's network, further compromising it and even setting up a back-door system to allow remote access.
- Services-augmentation: Attacking the self-augmentation devices can further degrade services for passengers, disabling features that are designed to augment their experience.

In the following, some important smart airport subsystems are discussed, along with potential consequences for attacking and jeopardising their security.

1) THE AIR TRAFFIC CONTROL

Air traffic control (ATC) towers are the command center for managing flights at each airport, ensuring the safety of commercial and private aircraft flights. ATC towers, among other things, review weather conditions, receive a flight plan from the aircraft's captain and manage ground traffic including takeoff landing and taxiing [190]. During a flight, an aircraft will communicate with multiple ATC stations along its rout, transmitting a signal that carries the flight's number, altitude, airspeed and destination. Attackers can affect an aircraft' s environmental control system [191], spoofing fire or smoke alarms and altering the air temperature, causing discomfort or even emergency landings.

2) DRONES

Drones are another security risk for airports [192]. They can be outfitted with portable computers and antenna and flown around an airport, compromising the security of IoT devices inside the airport, either disabling the devices, making their functionality irregular or use them as a bridge to propagate malware and further compromise other subsystems of the airport [15], [192].

3) E-ENABLED AIRCRAFT

E-enabled aircraft [193] are also at risk, as they incorporate systems that handle regular communication between the aircraft and ground control. Such aircraft incorporate systems such as Electronic Flight Bags, where flight plans, weather patterns and maps are stored and updated regularly, even during flight, while contemporary aircraft communication, addressing and reporting systems (ACARS) which play the role of the central communication link with ground control are being designed to work over IP. Further applications include credit card authorization for on-flight purchases and damage reports for the aircraft's subsystems which can be sent to maintenance crews at the flight's destination before it arrives.

4) HEALTH SAFETY SYSTEMS

With the proliferation of COVID-19, the threat of world-scale pandemics has become apparent. As a result, added measures of safety and security have been scheduled and implemented in some airports, to detect any cases of infected passengers and reduce the spread of the virus [100]. The primary methods used to screen passengers, prior to boarding is the utilisation of biometric smart sensors, specifically thermal cameras that are configured to raise alarms if the temperature of a passenger exceeds a pre-determined threshold. Malicious actors can target these thermal cameras, that may or may not be connected to an extended intranet and affect their functionality in many ways, which is a risk for the airport and for the public. In one scenario, an attacker could compromise the thermal cameras, and force them to output false (spoofed) temperatures or disable them by performing a DoS, which can be considered a combined bio-cyber-attack. This can result in extended delays brought about by increasing the false positives of the system which, in turn, results in the airport management invoking their secondary measures that may include retaking the flagged passenger's temperature. Alternatively, the attackers could force the cameras to falsely record all incoming passengers as healthy, thus increasing the false negative measurements, which in turn can result in increases in infection cases in the local or foreign communities' depending on where the compromised camera is situated.

5) SMART LIGHTS, ENVIRONMENTAL SENSORS AND SURVEILLANCE SYSTEMS

Smart lights and environmental sensors can also be a source of risks for smart airports, as indicated by previous research [15]. Attackers can target these smart devices and launch DoS attacks by disabling them temporarily or permanently (bricking). Furthermore, by compromising one such smart light device, it is possible to propagate malware to other

devices within range that utilise the same wireless protocol, which will eventually infect most if not all the smart light devices, bringing them under the attacker 's control. Attacks on the environmental sensors can result in false alarms by tampering with the fire, smoke and air quality and toxicity sensors, or resulting in unnecessary evacuations and thus disrupt operations.

Surveillance systems include CCTVs, perimeter intrusion sensors and other such devices that are used to monitor and restrict access to certain areas of the airport. Security weaknesses in these systems can pose significant risk for both the cybersecurity and the physical security of an airport [29], [194]. First, cameras can be compromised by attackers, who can then gain unauthorised remote access to them, and in turn monitor the movement of airport personnel and extract security patterns such as the habits of guards, as an initial reconnaissance stage. Furthermore, attackers can block the live feed of the cameras, replacing it with false video footage, to cover illegal actions or unauthorised entry to restricted areas of the airport. Perimeter intrusion sensors can be similarly affected.

CYBER SECURITY RELIABILITY IMPLICATIONS

An important implication of cyber-attacks that target Smart Airport infrastructure, is that reliability can be greatly affected. Critical infrastructure such as Smart Airports relies on the accurate and consistent orchestration of services from various systems, including contemporary IoT-powered systems, to improve efficiency, accelerate production, locate resources and prioritise actions such as repairs [21]. However, cyber-attackers can compromise IoT devices, and cause disruptions to occur, by either manipulating the input/output data of IoT devices, or by disabling them as a result of DoS attacks [195]. Thus, to ensure reliability of services, it is imperative to develop robust cyber-defence methods that ensure the swift detection of security flaws in critical networks and connected systems [135].

OPEN GAPS AND FUTURE DIRECTIONS

After the discussion of risks that can affect the ability of a smart airport to defend their cyber-resources and services, it is important to address the challenges that experts face during the development of cyber-defence mechanisms for smart airports.

- **Zero-day vulnerability detection**: A key feature that enables multiple smart airport augmented services, is the incorporation of IoT devices. Studies have shown that IoT devices are generally not secured properly, and attackers regularly expose zero-day vulnerabilities [196]. The first challenge is to find a method to reliably detect zero-day vulnerabilities in IoT devices. Vulnerabilities are characterised as zero-day, if either their existence was unknown prior to them being exploited by attackers, or they are known but remain unpatched [195]. It is important to develop cyber-defence methods to identify and mitigate zero-day vulnerabilities, as they can prove to be a stealthy attack vector. One such methods would be to design a DL-based system to scan the network-side of IoT infrastructure in smart airports and perform behavioural assessment. The model can function as an anomaly detection system, which is first taught the normal behaviour of such devices and then marks any deviations as an attack. The confirmed zero-day vulnerabilities detected through this method can then be compiled into labelled data, and utilised to train ML/DL models to detect these attacks and propose mitigation methods.
- **Designing of secure network architecture**: The concept of the smart airport is relatively new and not defined by rigid rules and commonly accepted standards. As such, each airport that is making the transition from ''mundane'' and ''agile'' to ''smart'', is a unique case, and needs to decide on its own what IoT-powered applications it will incorporate into its infrastructure, which vendor to choose from and in-turn, what hardware will be used and what communication protocols these devices will employ [197]. Thus, another important challenge is to design a secure architecture for the smart airport, and specifically the various subsystems that need to be orchestrated harmoniously, to ensure that services are resilient and remain uninterrupted. One approach towards designing such a secure architecture, would be to utilise SDNs to build a network that is centrally controlled, can be easily programmed and promotes scalability [198], [199]. In addition, the security of smart airport networks can be further enhanced through NFVs, which allow the rapid deployment of software-versions of traditionally hardware-based network nodes such as firewalls, IDS and load balancers [200]. Furthermore, AI-based systems can be developed to automate and augment the management and security measures of networks. They would operate by providing recommendations to experts, based on recorded traffic and the network's state, with alarms raised in the event of a security incident.
- **Ensure high performance of AI-base cyber-defence solutions**: In one form or another, AI-based measures have been applied to the field of cybersecurity, with the most prevalent method being expert rule-based systems, where carefully crafted rules in the form of ''if then else'', are used to scan networks or processes and detect known patterns of attacks [201], [202]. However, new methods based on ML and DL are emerging, where a model is trained on data that is usually pre-processed, cleaned and tagged. Thus, when developing ML and DL-based cyber-defence solutions, a challenge that emerges is to ensure high accuracy with low false alarm rates (FAR). The problem with low accuracy and high FAR is twofold. First, a false alarm can cause secondary security measures to be invoked, negatively impacting the business processes of an airport, causing delays, cancelations and evacuations. On the other hand,

failing to detect a cyber-threat may have other significant consequences, causing sensitive information to be stolen, devices and services to malfunction, flight plans to be altered, with the potential of threat to life becoming substantial. To ensure the effectiveness of DL models, extensive collections of properly curated data need to be utilised for the training process, and their hyperparameters need to be tuned, potentially through automated methods, for optimal performance [176], [203].

- **Process heterogeneous systems, protocols and data**: One of the main driving forces behind smart airports and their augmented services are the interconnected networks of IoT systems. Simple services powered by IoT systems can be combined and enhanced through AI, building more complex applications, and enabling high-level analytics. However, due to a lack of standardisation in the IoT [189], smart devices with similar functionality can be implemented by using different technologies both on a hardware, as-well-as a software (firmware) level, as each IoT vendor provides their own implementation. This diversification extends to the communication protocols that devices use to connect to their local IoT gateway, which bridges all local communication protocols with the Internet and in turn the cloud backend [204]. It is not uncommon to see an IoT system where smart devices use different protocols to communicate with a bridge, a device which can translate inbound traffic and transmit it to other devices in the local network or forward it to the backend server [205]. As such, the heterogeneity in hardware, and communication protocols, results in a diverse range of data formats, which poses a challenge for the development of cyber-defence systems deployed in these environments. In order to overcome this challenge for the purpose of implementing AI-based cyber-defence solution, network data can be captured on the transport-layer, as most IoT implementations utilise the Internet to connect to a cloud backend platform, to store and process data. After the data has been captured and pre-processed, powerful DL models can then be trained to detect security incidents in the network.
- **Scan large quantities of data in real-time**: A key characteristic of IoT devices, is that they are intended, by design, to be constantly active, either awaiting a request from the user, periodically performing some task, or recording data from their environment. This is also true for IoT devices that are deployed in smart airports, with some examples being smart lightbulbs, that enable swift and easy management from a smart device and can inform management of a malfunction, smart restroom sensors, that enable the efficient utilisation of janitorial services and smart surveillance systems with cameras and motion sensors constantly monitoring several areas at once [56], [173]. However, this means that smart devices generate massive quantities of data, some of which is temporarily recorded in the device before it is forwarded to the backend database. As such, a challenge that arises is that cyber-defence mechanisms need to be able to rapidly (often real time) scan the generated data and detect instances of misuse or cyberattacks. To overcome this challenge, DL models can be applied to swiftly process data that collected from IoT sensors. It has been proven, through empirical studies, that DL models perform well when tasked with analysing Bid Data, displaying increased performance and small processing time [206].
- **Effective separation of attack and non-attack instances**: Providing a cyber-defence shield for an organisation such as a smart airport is an important task, which needs to consider all the potential attack surfaces and their vectors to be effective. However, attackers have in their disposal a wide range of attack methods, some more covert than others [207]. Some attacks can be mistaken for normal network traffic under certain circumstances, which can pose a challenge for the development of an effective cyber-defence system. For example, serious advanced persistent threat (APT) that have been the cause of several high-profile cyber-attacks in the last few decades are botnets [208]. Botnets provide a structured infrastructure for an attacker, separated in the command and control side from which an attacker can issue commands and receive updates and information from the rest of the botnet, and an army of infected machines, called bots, that receive instructions and carry out attacks.
  Certain attacks that botnets can launch may be similar to normal network traffic, for example DDoS attacks could be mistaken for periods of high demand (and vice versa), successful data manipulation attacks against IoT devices can also be undetected as these attacks slightly shift the data that the device records, within a legitimate threshold, attempting to manipulate the state of the IoT system. Additionally, ransomware attacks need to be considered, as their purpose is to either steal, encrypt or otherwise make unavailable sensitive and valuable documents of organisations. Furthermore, as most people are increasingly reliant on remote conferencing for their jobs, video conferencing attacks are emerging, with one example being Zoom-bombing [209], where individuals intrude into conferences attempting to disrupt them. With their small processing time, enhanced pattern detection, robustness and adaptability, DL-based cyber-defence solutions are ideal for the task of separating normal behaviour from attack instance, when the two are similar in characteristics.
- **Passenger owned smart devices as attack vectors**: People these days carry their smartphone, wear smart watches or health monitoring devices and bring their handheld gaming consoles wherever they go, as a way to pass the time and stay connected, with the airport being no exception. Contemporary airports provide several complimentary services to passengers, such as free WiFi or indoor navigation through augmented reality, which

they can access through their smart devices. However, either due to software weaknesses or due to a lack of cybersecurity awareness, often these devices become the target of cyberattacks and malware that seek to steal sensitive information (bank accounts, credit cards, biometric data). As such, smartphones and similar devices that passengers bring to the airport can function as a kind of Trojan Horse [210], [211], with malware carried into the airport and spreading to other systems and smart devices. Thus, an additional challenge would be to consider passengers' smart devices as an extra attack vector, when building cyber-defence systems for a smart airport's infrastructure. To combat this threat, AI-based IDS and firewalls can be designed and deployed inside the airport's network. To be able to detect stealthy cyber-attacks that can be launched at any time from passenger-owned devices that connect to the complementary WiFi, security solutions need to be able to adapt to new and unknown threats. For this purpose, DL-based IDS and firewalls can be deployed in and between publicly accessible airport networks and other more sensitive networks, to ensure that a potential attack does not reach any vital systems.

- **Effectiveness of rule-based cyber-defence tools**: A considerable portion of the commercially available cyber-defence tools rely on extensive databases of expert-derived rules [24], [166]. These databases need to be constantly updated, through considerable effort from experts, to keep up with newer cyber-attacks. Such systems that can be found in smart airports include inbound and outbound network cyber-defence solutions such as firewalls and IDS/IPS. Furthermore, by modifying the binaries of malware (mutation, polymorphic malware) or altering the attack patterns, attackers are able to circumvent rule-based systems [212]. As such, it is a challenge to effectively generate rules for new cyber-threats and develop ways to minimise or eliminate the evasiveness of polymorphic malware. Additionally, another challenge is how to enhance rule-based cyber-defence systems, in order to effectively detect zero-day exploits, considering that rule-based solutions use signatures to detect well-known threats. To address these challenges, a hybrid strategy can be selected, that will combine the advantageous near-perfect detection of known threats of rule-based solutions and combine it with the robustness and adaptability of DL-based solutions. Furthermore, the need for expert-derived knowledge is minimised, as DL solutions require limited pre-processing to achieve acceptable performance.

In the future, we will design a realistic testbed comprised of smart devices, coordinators and stations managed by popular OSs. The motivation for this work, is to generate, pre-process and enhance a realistic network-based dataset, that will represent several realistic scenarios where vulnerabilities are exploited. The dataset will then be utilised to train a deep learning-based tool that will be able to automatically scan a local network and detect potential, and previously unknown vulnerabilities present in the smart sensors/actuators, coordinators and other network-enabled devices that can be found in smart airports. This work will be adaptable to other smart environments.

VIII. CONCLUSION

In this paper, we investigated smart airports, their advantages over their mundane and agile counterparts and the cyber-defence tools that are employed to protect their networks. Initially, due to a lack of standardisation, we reviewed existing definitions of smart airports which led us to provide our own definition, through which we assert certain characteristics regarding what a smart airport should look like. Next, we listed several IoT-powered smart airport subsystems, including the technology and protocols that they utilise, and then provided a classification based on the tasks they perform and their importance/criticality. Because of to the ongoing COVID-19 pandemic and the measures that are considered globally to reduce its spread, we have addressed the need for smart airports to incorporate biometric sensors for the detection of infectious cases in both inbound and outbound passengers. Additionally, we reviewed the current landscape of cyber-defence tools that are employed to protect a smart airport's networks, including rule-based, ML and DL tools while listing their performance weaknesses. Furthermore, we reviewed the risk profiling process and adapted it to a smart airport setting, stating that a number of heterogeneous sub-systems need to be considered for risks. Finally, we reviewed several security risks and challenges that can hinder the performance of a smart airport's operations and even threaten lives, which need to be addressed by the research community.

REFERENCES

[1] H. Tahaei, F. Afifi, A. Asemi, F. Zaki, and N. B. Anuar, "The rise of traffic classification in IoT networks: A survey," *J. Netw. Comput. Appl.*, vol. 154, Mar. 2020, Art. no. 102538.

[2] N. Koroniotis, N. Moustafa, and E. Sitnikova, "Forensics and deep learning mechanisms for botnets in Internet of Things: A survey of challenges and solutions," *IEEE Access*, vol. 7, pp. 61764–61785, 2019.

[3] B. Dorsemaine, J.-P. Gaulier, J.-P. Wary, N. Kheir, and P. Urien, "Internet of Things: A definition & taxonomy," in *Proc. 9th Int. Conf. Next Gener. Mobile Appl., Services Technol.*, Sep. 2015, pp. 72–77.

[4] M. A. Rahman and A. T. Asyhari, "The emergence of Internet of Things (IoT): Connecting anything, anywhere," *Computers*, vol. 8, no. 2, 2019.

[5] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the Internet of Things," in *Proc. IEEE World Congr. Services*, Jun. 2015, pp. 21–28.

[6] A. Solanki and A. Nayyar, "Green Internet of Things (G-IoT): ICT technologies, principles, applications, projects, and challenges," in *Handbook of Research on Big Data and the IoT*. Hershey, PA, USA: IGI Global, 2019, pp. 379–405.

[7] V. Roblek, M. Meško, and A. Krapež, "A complex view of industry 4.0," *SAGE Open*, vol. 6, no. 2, pp. 1–11, 2016.

[8] D. Kiel, J. M. Müller, C. Arnold, and K.-I. Voigt, "Sustainable industrial value creation: Benefits and challenges of industry 4.0," *Int. J. Innov. Manage.*, vol. 21, no. 8, Dec. 2017, Art. no. 1740015.

[9] H. Tao, M. Z. A. Bhuiyan, M. A. Rahman, T. Wang, J. Wu, S. Q. Salih, Y. Li, and T. Hayajneh, "TrustData: Trustworthy and secured data collection for event detection in industrial cyber-physical system," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3311–3321, May 2020.

[10] M. A. Rahman, S. Azad, A. T. Asyhari, M. Z. A. Bhuiyan, and K. Anwar, "Collab-SAR: A collaborative avalanche search-and-rescue missions exploiting hostile alpine networks," *IEEE Access*, vol. 6, pp. 42094–42107, 2018.

[11] Z. Alansari, S. Soomro, and M. R. Belgaum, "Smart airports: Review and open research issues," in *Proc. Int. Conf. Emerg. Technol. Comput.* Cham, Switzerland: Springer, 2019, pp. 136–148.

[12] S. Yang, H. Ceylan, K. Gopalakrishnan, and S. Kim, "Smart airport pavement instrumentation and health monitoring," in *Proc. FAA Worldwide Airport Technol. Transf. Conf.*, vol. 8, 2014.

[13] M. Suresh, P. S. Kumar, and T. V. P. Sundararajan, "IoT based airport parking system," in *Proc. Int. Conf. Innov. Inf., Embedded Commun. Syst. (ICIIECS)*, Mar. 2015, pp. 1–5.

[14] A. Elrayes, M. H. Ali, A. Zakaria, and M. H. Ismail, "Smart airport foreign object debris detection rover using LiDAR technology," *Internet Things*, vol. 5, pp. 1–11, Mar. 2019.

[15] E. Ronen, A. Shamir, A.-O. Weingarten, and C. OFlynn, "IoT Goes nuclear: Creating a ZigBee chain reaction," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 195–212.

[16] K. Angrishi, "Turning Internet of Things(IoT) into Internet of vulnerabilities (IoV): IoT botnets," 2017, *arXiv:1702.03681*. [Online]. Available: http://arxiv.org/abs/1702.03681

[17] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019.

[18] A. Albataineh and I. Alsmadi, "IoT and the risk of Internet exposure: Risk assessment using shodan queries," in *Proc. IEEE 20th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2019, pp. 1–5.

[19] T. Alladi, V. Chamola, B. Sikdar, and K.-K.-R. Choo, "Consumer IoT: Security vulnerability case studies and solutions," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 17–25, Mar. 2020.

[20] M. N. Kurt, Y. Yilmaz, and X. Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 498–513, Feb. 2019.

[21] P. L. Gallegos-Segovia, J. F. Bravo-Torres, J. J. Argudo-Parra, E. J. Sacoto-Cabrera, and V. M. Larios-Rosillo, "Internet of Things as an attack vector to critical infrastructures of cities," in *Proc. Int. Caribbean Conf. Devices, Circuits Syst. (ICCDCS)*, Jun. 2017, pp. 117–120.

[22] G. George and S. M. Thampi, "Vulnerability-based risk assessment and mitigation strategies for edge devices in the Internet of Things," *Pervas. Mobile Comput.*, vol. 59, Oct. 2019, Art. no. 101068.

[23] G. Suciu, A. Scheianu, A. Vulpe, I. Petre, and V. Suciu, "Cyber-attacks—The impact over airports security and prevention modalities," in *Proc. World Conf. Inf. Syst. Technol.* Cham, Switzerland: Springer, 2018, pp. 154–162.

[24] L. Liu, O. De Vel, Q.-L. Han, J. Zhang, and Y. Xiang, "Detecting and preventing cyber insider threats: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1397–1417, 2nd Quart., 2018.

[25] A. Chiappetta and G. Cuozzo, "Critical infrastructure protection: Beyond the hybrid port and airport firmware security cybersecurity applications on transport," in *Proc. 5th IEEE Int. Conf. Models Technol. Intell. Transp. Syst. (MT-ITS)*, Jun. 2017, pp. 206–211.

[26] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, "Implementing cybersecurity measures in airports to improve cyber-resilience," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2018, pp. 1–6.

[27] B. Willemsen and M. Cadee, "Extending the airport boundary: Connecting physical security and cybersecurity," *J. Airport Manage.*, vol. 12, no. 3, pp. 236–247, 2018.

[28] F. Lekota and M. Coetzee, "Cybersecurity incident response for the sub-saharan African aviation industry," in *Proc. Int. Conf. Cyber Warfare Secur.* Gaithersburg, MD, USA: National Institute of Standards & Technology, Academic Conferences International Limited, 2019, pp. 536–545. [Online]. Available: https://search.proquest.com/docview/2198531213?accountid=12763

[29] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, "Smart airport cybersecurity: Threat mitigation and cyber resilience controls," *Sensors*, vol. 19, no. 1, p. 19, Dec. 2018.

[30] C. D. Aboti, "Survey on IoT: Challenges and cyber risks in commercial aviation," *IJRAR*, vol. 6, no. 2, pp. 1–9, Jun. 2019.

[31] G. Suciu, A. Scheianu, I. Petre, L. Chiva, and C. S. Bosoc, "Cybersecurity threats analysis for airports," in *New Knowledge in Information Systems and Technologies*, Á. Rocha, H. Adeli, L. P. Reis, and S. Costanzo, Eds. Cham, Switzerland: Springer, 2019, pp. 252–262.

[32] A. Rajapaksha and D. N. Jayasuriya, "Smart airport: A review on future of the airport operation," *Global J. Manage. Bus. Res.*, vol. 20, no. 3, pp. 25–34, 2020.

[33] M. Lehto, "Cyber security in aviation, maritime and automotive," in *Computation and Big Data for Transport*. Cham, Switzerland: Springer, 2020, pp. 19–32.

[34] D. K.-D. Feldman and E. Gross, "Cyber terrorism and civil aviation: Threats, standards and regulations," *J. Transnat'l L. Pol'y*, vol. 29, p. 131, 2019.

[35] R. Florida, C. Mellander, and T. Holgersson, "Up in the air: The role of airports for regional economic development," *Ann. Regional Sci.*, vol. 54, no. 1, pp. 197–214, Jan. 2015.

[36] D. Baker, R. Merkert, and M. Kamruzzaman, "Regional aviation and economic growth: Cointegration and causality analysis in Australia," *J. Transp. Geogr.*, vol. 43, pp. 140–150, Feb. 2015.

[37] A. Fattah, H. Lock, W. Buller, S. Kirby, and D. Gajda, "Smart airports: Transforming passenger experience to thrive in the new economy," Cisco Internet Bus. Solutions Group, Amsterdam, The Netherlands, Tech. Rep., 2009, pp. 1–16.

[38] J. B. Nau and F. Benoit, "Smart airport how technology is shaping the future of airports," Wavestone, Paris, France, Tech. Rep., 2017.

[39] E. Nagy and C. Csiszár, "Airport smartness index–evaluation method of airport information services," *Osterreichische Zeitschrift Fur Verkehr-swissenschaft*, vol. 63, no. 4, pp. 25–30, 2016.

[40] Q. Qi and Z. Pan, "Internet of Things, Internet, big data and airport services make smart airport based on O2O and humanism," in *Proc. Int. Conf. Mech., Electron., Control Automat. Eng. (MECAE)*, 2018, pp. 1–4.

[41] *Securing Smart Airports*, ENISA, Heraklion, Greece, Dec. 2016.

[42] V. Casola, A. De Benedictis, M. Rak, and U. Villano, "Toward the automation of threat modeling and risk assessment in IoT systems," *Internet Things*, vol. 7, Sep. 2019, Art. no. 100056.

[43] J. Hong, J. Oh, and H. Lee, "Smart airport and next generation security screening technology," *Electron. Telecommun. Trends*, vol. 34, no. 2, pp. 73–82, 2019.

[44] R. Baashirah and K. Elleithy, "Automation of the baggage check-in process using RFID system in airports," in *Proc. IEEE Long Island Syst., Appl. Technol. Conf. (LISAT)*, May 2019, pp. 1–4.

[45] A. Opitz and A. Kriechbaum-Zabini, "Evaluation of face recognition technologies for identity verification in an eGate based on operational data of an airport," in *Proc. 12th IEEE Int. Conf. Adv. Video Signal Based Surveill. (AVSS)*, Aug. 2015, pp. 1–5.

[46] J. S. del Rio, D. Moctezuma, C. Conde, I. M. de Diego, and E. Cabello, "Automated border control e-gates and facial recognition systems," *Comput. Secur.*, vol. 62, pp. 49–72, Sep. 2016.

[47] M. Mohamed, H. Gomaa, and N. El-Sherif, "Evaluation of current smart airport technologies implemented in cairo international airport," *Int. J. Heritage, Tourism Hospitality*, vol. 12, no. 2, pp. 130–140, Sep. 2018.

[48] D. Spaniel and P. Eftekhari, *Hacking Our Nation's Airports: Cyber-kinetic Threats to the Technologies Running Airport Operations*. Washington, DC, USA: Institute for Critical Infrastructure Technology, 2019. [Online]. Available: https://books.google.com.au/books?id=c6FFzQEACAAJ

[49] A. Yang and G. P. Hancke, "RFID and contactless technology," in *Smart Cards, Tokens, Security and Applications*. Boston, MA, USA: Springer, 2017, pp. 351–385.

[50] A. Singh, S. Meshram, T. Gujar, and P. R. Wankhede, "Baggage tracing and handling system using RFID and IoT for airports," in *Proc. Int. Conf. Comput., Analytics Secur. Trends (CAST)*, Dec. 2016, pp. 466–470.

[51] *Transport 2040: Automation in Airports: Automatic Baggage Handling Systems—Technology and Transformation*, World Maritime Univ., Malmö, Sweden, 2019.

[52] A. Davis and H. Chang, "Airport protection using wireless sensor networks," in *Proc. IEEE Conf. Technol. Homeland Secur. (HST)*, Nov. 2012, pp. 36–42.

[53] R. Baggett, C. Foster, and B. Simpkins, *Homeland Security Technologies for the 21st Century* (Praeger Security International). Santa Barbara, CA, USA: ABC-CLIO, 2017. [Online]. Available: https://books.google.com.au/books?id=YeBqDgAAQBAJ

[54] N. Lakshmanan, I. Bang, M. S. Kang, J. Han, and J. T. Lee, "SurFi: Detecting surveillance camera looping attacks with Wi-Fi channel state information," in *Proc. 12th Conf. Secur. Privacy Wireless Mobile Netw.*, May 2019, pp. 239–244.
[55] R. Silk, "Airports deploying smart tech to keep restrooms clean," Travel Weekly, 2018.
[56] Y. Gao, Y. Cheng, H. Zhang, and N. Zou, "Dynamic illuminance measurement and control used for smart lighting with LED," *Measurement*, vol. 139, pp. 380–386, Jun. 2019.
[57] A. Suresh, M. Nandagopal, P. Raj, E. Neeba, and J. Lin, *Industrial IoT Application Architectures and Use Cases*. Boca Raton, FL, USA: CRC Press, 2020. [Online]. Available: https://books.google.com.au/books?id=3eXkDwAAQBAJ
[58] S. Zanni, F. Lalli, E. Foschi, A. Bonoli, and L. Mantecchini, "Indoor air quality real-time monitoring in airport terminal areas: An opportunity for sustainable management of micro-climatic parameters," *Sensors*, vol. 18, no. 11, p. 3798, Nov. 2018.
[59] N. Rodríguez-Pérez, P. Caballero-Gil, J. Toledo-Castro, I. Santos-González, and C. Hernández-Goya, "Monitoring environmental conditions in airports with wireless sensor networks," *Multidisciplinary Digit. Publishing Inst.*, vol. 2, no. 19, p. 1260, 2018.
[60] D. Ley, "6-emerging technologies for learning," in *Web 2.0 and Libraries* (Chandos Information Professional Series), D. Parkes and G. Walton, Eds. Oxford, U.K.: Chandos Publishing, 2010, pp. 123–168. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9781843343462500065
[61] T. Wasson, T. Choudhury, S. Sharma, and P. Kumar, "Integration of RFID and sensor in agriculture using IoT," in *Proc. Int. Conf. Smart Technol. Smart Nation (SmartTechCon)*, Aug. 2017, pp. 217–222.
[62] Y. Duroc and S. Tedjini, "RFID: A key technology for humanity," *Comp. Rendus Phys.*, vol. 19, nos. 1–2, pp. 64–71, Jan. 2018.
[63] E. Valero, A. Adán, and C. Cerrada, "Evolution of RFID applications in construction: A literature review," *Sensors*, vol. 15, no. 7, pp. 15988–16008, Jul. 2015.
[64] D. Braganza and B. Tulasi, "RFID security issues in IoT: A comparative study," *Oriental J. Comput. Sci. Technol.*, vol. 10, no. 1, pp. 127–134, Mar. 2017.
[65] K. Mansoor, A. Ghani, S. Chaudhry, S. Shamshirband, S. Ghayyur, and A. Mosavi, "Securing IoT-based RFID systems: A robust authentication protocol using symmetric cryptography," *Sensors*, vol. 19, no. 21, p. 4752, Nov. 2019.
[66] B. D. Wassom, "Privacy," in *Augmented Reality Law, Privacy, and Ethics*, B. D. Wassom, Ed. Boston, MA, USA: Syngress, 2015, ch. 3, pp. 43–69. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B978012800208700003X
[67] P. Spachos and A. Mackey, "Energy efficiency and accuracy of solar powered BLE beacons," *Comput. Commun.*, vol. 119, pp. 94–100, Apr. 2018.
[68] A. Nikoukar, M. Abboud, B. Samadi, M. Güneş, and B. Dezfouli, "Empirical analysis and modeling of Bluetooth low-energy (BLE) advertisement channels," in *Proc. 17th Annu. Medit. Ad Hoc Netw. Workshop (Med-Hoc-Net)*, Jun. 2018, pp. 1–6.
[69] D. Gratton, *Bluetooth Profiles: The Definitive Guide* (Wireless Communications/Bluetooth). Upper Saddle River, NJ, USA: Prentice-Hall, 2003. [Online]. Available: https://books.google.com.au/books?id=08eByqhzJ3wC
[70] S. Darroudi and C. Gomez, "Bluetooth low energy mesh networks: A survey," *Sensors*, vol. 17, no. 7, p. 1467, Jun. 2017.
[71] M. Labib, A. Ghalwash, S. Abdulkader, and M. Elgazzar, "Networking solutions for connecting Bluetooth low energy devices—A comparison," in *Proc. MATEC Web Conf.*, vol. 292, 2019, Art. no. 02003.
[72] S. S. Hassan, S. D. Bibon, M. S. Hossain, and M. Atiquzzaman, "Security threats in Bluetooth technology," *Comput. Secur.*, vol. 74, pp. 308–322, May 2018.
[73] Y. Zhang, J. Weng, R. Dey, and X. Fu, *Bluetooth Low Energy (BLE) Security and Privacy*. Cham, Switzerland: Springer, 2019, pp. 1–12, doi: 10.1007/978-3-319-32903-1_298-1.
[74] D. Paret and P. Crego, "10-RF connectivity in wearables," in *Wearables, Smart Textiles Smart Apparel*, D. Paret and P. Crego, Eds. Amsterdam, The Netherlands: Elsevier, 2019, pp. 265–294. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9781785482939500155
[75] D. M. Ibrahim, "Internet of Things technology based on LoRaWAN revolution," in *Proc. 10th Int. Conf. Inf. Commun. Syst. (ICICS)*, Jun. 2019, pp. 234–237.
[76] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Express*, vol. 5, no. 1, pp. 1–7, Mar. 2019.
[77] N. Sornin, M. Luis, T. Eirich, T. Kramp, and O. Hersent, "Lorawan specification," in *Proc. LoRa*, Jan. 2015, pp. 1–5.
[78] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of LoRaWAN," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 34–40, 2017.
[79] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "Overview of cellular LPWAN technologies for IoT deployment: Sigfox, LoRaWAN, and NB-IoT," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2018, pp. 197–202.
[80] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes, "Exploring the security vulnerabilities of LoRa," in *Proc. 3rd IEEE Int. Conf. Cybern. (CYBCONF)*, Jun. 2017, pp. 1–6.
[81] V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, "Energy depletion attacks in low power wireless networks," *IEEE Access*, vol. 7, pp. 51915–51932, 2019.
[82] X. Fan, F. Susan, W. R. Long, and S. Li, "Security analysis of ZigBee," Massachusetts Inst. Technol., Cambridge, MA, USA, Tech. Rep., 2017.
[83] D. Gislason, *ZigBee Wireless Networking*. Amsterdam, The Netherlands: Elsevier Science, 2008. [Online]. Available: https://books.google.com.au/books?id=up8Oa7456I8C
[84] M. A. Rahman, M. M. Hasan, A. T. Asyhari, and M. Z. A. Bhuiyan, "A 3D-collaborative wireless network: Towards resilient communication for rescuing flood victims," in *Proc. IEEE 15th Int. Conf. Dependable, Autonomic Secure Comput., 15th Int. Conf. Pervas. Intell. Comput., 3rd Int. Conf. Big Data Intell. Comput. Cyber Sci. Technol. Congr. (DASC/PiCom/DataCom/CyberSciTech)*, Nov. 2017, pp. 385–390.
[85] T. Kumar and P. B. Mane, "ZigBee topology: A survey," in *Proc. Int. Conf. Control, Instrum., Commun. Comput. Technol. (ICCICCT)*, Dec. 2016, pp. 164–166.
[86] X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen, "Ghost-in-ZigBee: Energy depletion attack on ZigBee-based wireless networks," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 816–829, Oct. 2016.
[87] I. Vaccari, E. Cambiaso, and M. Aiello, "Remotely exploiting AT command attacks on ZigBee networks," *Secur. Commun. Netw.*, vol. 2017, pp. 1–9, Oct. 2017.
[88] S. Khanji, F. Iqbal, and P. Hung, "ZigBee security vulnerabilities: Exploration and evaluating," in *Proc. 10th Int. Conf. Inf. Commun. Syst. (ICICS)*, Jun. 2019, pp. 52–57.
[89] M. Kashyap, V. Sharma, and N. Gupta, "Taking MQTT and NodeMcu to IoT: Communication in Internet of Things," *Procedia Comput. Sci.*, vol. 132, pp. 1611–1618, Jan. 2018.
[90] M. A. Pradana, A. Rakhmatsyah, and A. A. Wardana, "Flatbuffers implementation on MQTT publish/subscribe communication as data delivery format," in *Proc. 6th Int. Conf. Electr. Eng., Comput. Sci. Informat. (EECSI)*, Sep. 2019, pp. 142–146.
[91] G. Suciu, I. Hussain, A. Badicu, L. Necula, and T. Uşurelu, "IoT services applied at the smart cities level," in *Proc. World Conf. Inf. Syst. Technol.* Cham, Switzerland: Springer, 2020, pp. 457–463.
[92] R. Zurawski, *Embedded Systems Handbook 2-Volume Set* (Industrial Information Technology). Boca Raton, FL, USA: CRC Press, 2018. [Online]. Available: https://books.google.com.au/books?id=wzhZDwAAQBAJ
[93] D. Serpanos and M. Wolf, *Internet-of-Things (IoT) Systems: Architectures, Algorithms, Methodologies*. Manhattan, NY, USA: Springer, 2017. [Online]. Available: https://books.google.com.au/books?id=ckRADwAAQBAJ
[94] V. P. Nigam, A. Kutvonen, B. Molina, P. B. Muñoz, and J.-N. Willing, "Dora: An experimental platform for smart cities," in *Intelligent Transport Systems. From Research and Development to the Market Uptake*, A. L. Martins, J. C. Ferreira, and A. Kocian, Eds. Cham, Switzerland: Springer, 2020, pp. 292–302.
[95] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, "Smart cities: A survey on data management, security, and enabling technologies," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2456–2501, 4th Quart., 2017.
[96] K. Tzortzakis, K. Papafotis, and P. P. Sotiriadis, "Wireless self powered environmental monitoring system for smart cities based on LoRa," in *Proc. Panhellenic Conf. Electron. Telecommun. (PACET)*, Nov. 2017, pp. 1–4.

[97] R. K. Kodali and S. Yerroju, "IoT based smart emergency response system for fire hazards," in *Proc. 3rd Int. Conf. Appl. Theor. Comput. Commun. Technol. (iCATccT)*, Dec. 2017, pp. 194–199.

[98] M. Collotta, G. Pau, T. Talty, and O. K. Tonguz, "Bluetooth 5: A concrete step forward toward the IoT," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 125–131, Jul. 2018.

[99] Q. Yang and L. Huang, "RFID/NFC security," in *Inside Radio: An Attack and Defense Guide*. Singapore: Springer, 2018, pp. 71–121.

[100] M. F. Alwashmi, "The use of digital health in the detection and management of COVID-19," *Int. J. Environ. Res. Public Health*, vol. 17, no. 8, p. 2906, Apr. 2020.

[101] *Management of Ill Travellers at Points of Entry–International Airports, Seaports and Ground Crossings–in the Context of COVID- 19 Outbreak: Interim Guidance, 16 February 2020*, World Health Org., Geneva, Switzerland, 2020.

[102] *EOS Australia BTM-T5*. Accessed: Aug. 9, 2020. [Online]. Available: https://www.eos.com.au/btm-t5.html

[103] *Thermoteknix FevIR Scan 2 Thermal Camera*. Accessed: Aug. 9, 2020. [Online]. Available: http://www.thermoteknix.com/products/oem-thermal-imaging/fevir-scan-fever-screening-system/

[104] *ICI FM320 P Series*. Accessed: Aug. 9, 2020. [Online]. Available: https://infraredcameras.com/product/fm-320-p-series-ir-camera/

[105] *Athena Security Temperature Detection*. Accessed: Aug. 9, 2020. [Online]. Available: https://athena-security.com/temperature-detection

[106] G. N. La Diega and I. Walden, "Contracting for the 'Internet of Things': Looking into the nest," *Eur. J. Law Technol.*, vol. 7, no. 2, 2016.

[107] C. X. Liu and K. Lu, "A perimeter intrusion detection system based on sensor network for airport application," *Appl. Mech. Mater.*, vol. 738, pp. 50–55, Mar. 2015.

[108] J. I. Castillo-Manzano and L. López-Valpuesta, "Check-in services and passenger behaviour: Self service technologies in airport systems," *Comput. Hum. Behav.*, vol. 29, no. 6, pp. 2431–2437, Nov. 2013.

[109] C.-H. Cheng and I. E. Olatunji, "Harnessing constrained resources in service industry via video analytics," 2018, *arXiv:1807.00139*. [Online]. Available: http://arxiv.org/abs/1807.00139

[110] S. C. Thomopoulos, S. Daveas, and A. Danelakis, "Automated real-time risk assessment for airport passengers using a deep learning architecture," *Proc. SPIE*, vol. 11018, May 2019, Art. no. 110180O.

[111] C. J. Wilkinson, "Airport staff access control: Biometrics at last?" in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2018, pp. 1–8.

[112] G. Gerstweiler, E. Vonach, and H. Kaufmann, "HyMoTrack: A mobile AR navigation system for complex indoor environments," *Sensors*, vol. 16, no. 1, p. 17, Dec. 2015.

[113] D. V. Gmar', K. I. Dyuldina, S. I. Snopko, K. J. Shakhgeldyan, and V. V. Kryukov, "Indoor navigation service based on Wi-Fi positioning," in *Proc. 2nd Russia Pacific Conf. Comput. Technol. Appl. (RPC)*, Sep. 2017, pp. 68–71.

[114] S. Sengupta, "Security," in *Practical Guide to Clinical Computing Systems*, T. H. Payne, Ed., 2nd ed. Oxford, U.K.: Academic, 2015, ch. 5, pp. 71–81. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780124202177000055

[115] Q. Chen, "Toward realizing self-protecting healthcare information systems: Design and security challenges," in *Advances in Computers*, vol. 114, A. R. Hurson, Ed. Amsterdam, The Netherlands: Elsevier, 2019, ch. 3, pp. 113–149. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0065245819300130

[116] A. K. Das and S. Zeadally, "Data security in the smart grid environment," in *Pathways to a Smarter Power System*, A. Tascikaraoglu and O. Erdinc, Eds. New York, NY, USA: Academic, 2019, ch. 13, pp. 371–395. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780081025925000132

[117] M. Abdlhamed, K. Kifayat, Q. Shi, and W. Hurst, *Intrusion Prediction Systems*. Cham, Switzerland: Springer, 2017, pp. 155–174, doi: 10.1007/978-3-319-44257-0_7.

[118] A. A. Ahmed and N. A. K. Zaman, "Attack intention recognition: A review," *IJ Netw. Secur.*, vol. 19, no. 2, pp. 244–250, 2017.

[119] S. Anwar, J. Mohamad Zain, M. F. Zolkipli, Z. Inayat, S. Khan, B. Anthony, and V. Chang, "From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions," *Algorithms*, vol. 10, no. 2, p. 39, Mar. 2017.

[120] A. Caballero, "Information security essentials for it managers: Protecting mission-critical systems," in *Managing Information Security*, J. R. Vacca, Ed., 2nd ed. Boston, MA, USA: Syngress, 2014, ch. 1, pp. 1–45. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780124166882000015

[121] K. Ruan, *Digital Asset Valuation and Cyber Risk Measurement: Principles of Cybernomics*. Amsterdam, The Netherlands: ElsevierScience, 2019. [Online]. Available: https://books.google.com.au/books?id=HxOaDwAAQBAJ

[122] W. Bautista, *Practical Cyber Intelligence: How Action-Based Intelligence Can be an Effective Response to Incidents*. Birmingham, U.K.: Packt, 2018. [Online]. Available: https://books.google.com.au/books?id=jrZTDwAAQBAJ

[123] S. Jetty and S. Rahalkar, *Securing Network Infrastructure: Discover Practical Network Security With Nmap and Nessus 7*. Birmingham, U.K.: Packt, 2019. [Online]. Available: https://books.google.com.au/books?id=BDqPDwAAQBAJ

[124] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: Challenges and opportunities," *IEEE Access*, vol. 6, pp. 46134–46145, 2018.

[125] R. W. Masenya, "Assessing the influence of South African investor well-being on risk tolerance," Ph.D. dissertation, North-West Univ., Potchefstroom, South Africa, 2020.

[126] M. Chapple, J. M. Stewart, and D. Gibson, *(ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide*. Hoboken, NJ, USA: Wiley, 2018.

[127] B. Barafort, A.-L. Mesquida, and A. Mas, "Integrating risk management in IT settings from ISO standards and management systems perspectives," *Comput. Standards Interfaces*, vol. 54, pp. 176–185, Nov. 2017.

[128] *Australian Government Information Security Manual*, D Solutions, Gurgaon, Haryana, 2019.

[129] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic security risk management using Bayesian attack graphs," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 1, pp. 61–74, Jan. 2012.

[130] N. Mayer, J. Aubert, E. Grandry, C. Feltus, E. Goettelmann, and R. Wieringa, "An integrated conceptual model for information system security risk management supported by enterprise architecture management," *Softw. Syst. Model.*, vol. 18, no. 3, pp. 2285–2312, Jun. 2019.

[131] H. Vogel, *Foundations of Airport Economics and Finance*. Amsterdam, The Netherlands: Elsevier Science, 2019. [Online]. Available: https://books.google.com.au/books?id=cx-ODwAAQBAJ

[132] L. Weber, *International Civil Aviation Organization*. South Holland, The Netherlands: Wolters Kluwer, 2017. [Online]. Available: https://books.google.com.au/books?id=5o2WDwAAQBAJ

[133] M. Park, H. Oh, and K. Lee, "Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective," *Sensors*, vol. 19, no. 9, p. 2148, May 2019.

[134] F. Liu, J. Xu, S. Xu, and M. Yung, *Science of Cyber Security: Second International Conference, SciSec 2019, Nanjing, China, August 9–11, 2019, Revised Selected Papers* (Lecture Notes in Computer Science). Nanjing, China: Springer, 2019. [Online]. Available: https://books.google.com.au/books?id=nxnCDwAAQBAJ

[135] P. Ackerman, *Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems*. Birmingham, U.K.: Packt, 2017. [Online]. Available: https://books.google.com.au/books?id=FhlKDwAAQBAJ

[136] T. McMillan, *CompTIA Cybersecurity Analyst (CySA+) Cert Guide* (Certification Guide). London, U.K.: Pearson, 2017. [Online]. Available: https://books.google.com.au/books?id=ZVgoDwAAQBAJ

[137] M. Stamp, *Introduction to Machine Learning With Applications in Information Security*. Boca Raton, FL, USA: CRC Press, 2017. [Online]. Available: https://books.google.com.au/books?id=CuM2DwAAQBAJ

[138] L. Batten, D. Kim, X. Zhang, and G. Li, *Applications and Techniques in Information Security: 8th International Conference, ATIS 2017, Auckland, New Zealand, July 6–7, 2017, Proceedings* (Communications in Computer and Information Science). Singapore: Springer, 2017. [Online]. Available: https://books.google.com.au/books?id=UWgpDwAAQBAJ

[139] H. Huang and H. Yu, *Compact and Fast Machine Learning Accelerator for IoT Devices* (Computer Architecture and Design Methodologies). Singapore: Springer, 2018. [Online]. Available: https://books.google.com.au/books?id=8RF-DwAAQBAJ

[140] O. Campesato, *Artificial Intelligence, Machine Learning, and Deep Learning*. Dulles, VA, USA: Mercury Learning & Information, 2020. [Online]. Available: https://books.google.com.au/books?id=pqnNDwAAQBAJ

[141] J. C. Ang, A. Mirzal, H. Haron, and H. N. A. Hamed, "Supervised, unsupervised, and semi-supervised feature selection: A review on gene selection," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, vol. 13, no. 5, pp. 971–989, Sep. 2016.
[142] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*. Cambridge, MA, USA: MIT Press, 2018.
[143] P. Mallick, *Research Advances in the Integration of Big Data and Smart Computing* (Advances in Computational Intelligence and Robotics (2327-0411)). Hershey, PA, USA: IGI Global, 2015. [Online]. Available: https://books.google.com.au/books?id=BDi4CgAAQBAJ
[144] E. Alpaydin, *Introduction to Machine Learning* (Adaptive Computation and Machine Learning Series). Cambridge, MA, USA: MIT Press, 2020. [Online]. Available: https://books.google.com.au/books?id=tZnSDwAAQBAJ
[145] T. Hastie, R. Tibshirani, and M. Wainwright, *Statistical Learning With Sparsity: The Lasso and Generalizations* (Chapman & Hall/CRC Monographs on Statistics & Applied Probability). Boca Raton, FL, USA: CRC Press, 2015. [Online]. Available: https://books.google.com.au/books?id=f-A_CQAAQBAJ
[146] T. Sejnowski, *The Deep Learning Revolution* (The MIT Press). Cambridge, MA, USA: MIT Press, 2018. [Online]. Available: https://books.google.com.au/books?id=9xZxDwAAQBAJ
[147] J. Patterson and A. Gibson, *Deep Learning: A Practitioner's Approach*. Sebastopol, CA, USA: O'Reilly Media, 2017. [Online]. Available: https://books.google.com.au/books?id=rLcuDwAAQBAJ
[148] A. Galea and L. Capelo, *Applied Deep Learning With Python: Use Scikit-learn, TensorFlow, and Keras to Create Intelligent Systems and Machine Learning Solutions*. Birmingham, U.K.: Packt, 2018. [Online]. Available: https://books.google.com.au/books?id=dPFsDwAAQBAJ
[149] C. Perez, *DEEP Learning Using MATLAB. Neural Network Applications*. Abu Dhabi, United Arab Emirates: Lulu, 2019. [Online]. Available: https://books.google.com.au/books?id=ZyvJDwAAQBAJ
[150] A. Pathan, *The State of the Art in Intrusion Prevention and Detectio*. Boca Raton, FL, USA: CRC Press, 2014. [Online]. Available: https://books.google.com.au/books?id=MJrNBQAAQBAJ
[151] N. T. Van, T. N. Thinh, and L. T. Sach, "An anomaly-based network intrusion detection system using deep learning," in *Proc. Int. Conf. Syst. Sci. Eng. (ICSSE)*, Jul. 2017, pp. 210–214.
[152] E. Min, J. Long, Q. Liu, J. Cui, and W. Chen, "TR-IDS: Anomaly-based intrusion detection through text-convolutional neural network and random forest," *Secur. Commun. Netw.*, vol. 2018, pp. 1–9, Jul. 2018.
[153] S. A. Althubiti, E. M. Jones, and K. Roy, "LSTM for anomaly-based network intrusion detection," in *Proc. 28th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2018, pp. 1–3.
[154] N. Moustafa, B. Turnbull, and K.-K.-R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4815–4830, Jun. 2019.
[155] Y. Ji, B. Bowman, and H. H. Huang, "Securing malware cognitive systems against adversarial attacks," in *Proc. IEEE Int. Conf. Cognit. Comput. (ICCC)*, Jul. 2019, pp. 1–9.
[156] *Fortiweb Tool*. Accessed: Jul. 15, 2020. [Online]. Available: https://www.fortinet.com/products/web-application-firewall/fortiweb
[157] *Deeparmor Tool*. Accessed: Jul. 15, 2020. [Online]. Available: https://www.sparkcognition.com/products/deeparmor/
[158] I. Deliu, C. Leichter, and K. Franke, "Extracting cyber threat intelligence from hacker forums: Support vector machines versus convolutional neural networks," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017, pp. 3648–3656.
[159] S. Samtani, R. Chinn, H. Chen, and J. F. Nunamaker, "Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence," *J. Manage. Inf. Syst.*, vol. 34, no. 4, pp. 1023–1053, Oct. 2017.
[160] M. Conti, T. Dargahi, and A. Dehghantanha, "Cyber threat intelligence: Challenges and opportunities," in *Cyber Threat Intelligence*. Cham, Switzerland: Springer, 2018, pp. 1–6, doi: 10.1007/978-3-319-73951-9_1.
[161] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, R. Khayami, K.-K.-R. Choo, and D. E. Newton, "DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer," *Future Gener. Comput. Syst.*, vol. 90, pp. 94–104, Jan. 2019.
[162] *Deepinstinct Platform*. Accessed: Jul. 20, 2020. [Online]. Available: https://www.deepinstinct.com/
[163] Y. Wang and J. Yang, "Ethical hacking and network defense: Choose your best network vulnerability scanning tool," in *Proc. 31st Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, Mar. 2017, pp. 110–113.
[164] X. Li, L. Wang, Y. Xin, Y. Yang, and Y. Chen, "Automated vulnerability detection in source code using minimum intermediate representation learning," *Appl. Sci.*, vol. 10, no. 5, p. 1692, Mar. 2020.
[165] X. Tian and D. Tang, "A distributed vulnerability scanning on machine learning," in *Proc. 6th Int. Conf. Inf. Sci. Control Eng. (ICISCE)*, Dec. 2019, pp. 32–35.
[166] S. Khan and S. Parkinson, "Review into state of the art of vulnerability assessment using artificial intelligence," in *Guide to Vulnerability Analysis for Computer Networks and Systems*. Cham, Switzerland: Springer, 2018, pp. 3–32.
[167] J. Hegde and B. Rokseth, "Applications of machine learning methods for engineering risk assessment—A review," *Saf. Sci.*, vol. 122, Feb. 2020, Art. no. 104492.
[168] Y. Shen, E. Mariconti, P. A. Vervier, and G. Stringhini, "Tiresias: Predicting security events through deep learning," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Jan. 2018, pp. 592–605.
[169] A. Chaudhuri, "Deep learning models for face recognition: A comparative analysis," in *Deep Biometrics*. Cham, Switzerland: Springer, 2020, pp. 99–140.
[170] R. Watts, "Facial recognition as a force for good," *Biometric Technol. Today*, vol. 2019, no. 3, pp. 5–8, Mar. 2019.
[171] G. Tripathi, K. Singh, and D. K. Vishwakarma, "Convolutional neural networks for crowd behaviour analysis: A survey," *Vis. Comput.*, vol. 35, no. 5, pp. 753–776, May 2019.
[172] G. Sreenu and M. A. S. Durai, "Intelligent video surveillance: A review through deep learning techniques for crowd analysis," *J. Big Data*, vol. 6, no. 1, p. 48, Dec. 2019.
[173] F. Gelana and A. Yadav, "Firearm detection from surveillance cameras using image processing and machine learning techniques," in *Smart Innovations in Communication and Computational Sciences*. Singapore: Springer, 2019, pp. 25–34.
[174] G. Raturi, P. Rani, S. Madan, and S. Dosanjh, "ADoCW: An automated method for detection of concealed weapon," in *Proc. 5th Int. Conf. Image Inf. Process. (ICIIP)*, Nov. 2019, pp. 181–186.
[175] G. De La Torre Parra, P. Rad, and K.-K.-R. Choo, "Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 32–46, Jun. 2019.
[176] N. Koroniotis, N. Moustafa, and E. Sitnikova, "A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework," *Future Gener. Comput. Syst.*, vol. 110, pp. 91–106, Sep. 2020.
[177] G. S. Chhabra, V. P. Singh, and M. Singh, "Cyber forensics framework for big data analytics in IoT environment using machine learning," *Multimedia Tools Appl.*, vol. 79, nos. 23–24, pp. 15881–15900, Jun. 2020.
[178] L. F. Sikos, "Packet analysis for network forensics: A comprehensive survey," *Forensic Sci. Int., Digit. Invest.*, vol. 32, Mar. 2020, Art. no. 200892.
[179] D. Goyal, S. Balamurugan, S. Peng, and O. Verma, *Design and Analysis of Security Protocol for Communication*. Hoboken, NJ, USA: Wiley, 2020. [Online]. Available: https://books.google.com.au/books?id=O3LQDwAAQBAJ
[180] B. Veloso, J. Gama, and B. Malheiro, "Self hyper-parameter tuning for data streams," in *Proc. Int. Conf. Discovery Sci.* Cham, Switzerland: Springer, 2018, pp. 241–255.
[181] K. Ren, T. Zheng, Z. Qin, and X. Liu, "Adversarial attacks and defenses in deep learning," *Engineering*, vol. 6, no. 3, pp. 346–360, Mar. 2020.
[182] M. Jagielski, A. Oprea, B. Biggio, C. Liu, C. Nita-Rotaru, and B. Li, "Manipulating machine learning: Poisoning attacks and countermeasures for regression learning," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2018, pp. 19–35.
[183] S. Chen, M. Xue, L. Fan, S. Hao, L. Xu, H. Zhu, and B. Li, "Automated poisoning attacks and defenses in malware detection systems: An adversarial machine learning approach," *Comput. Secur.*, vol. 73, pp. 326–344, Mar. 2018.
[184] R. Singh, H. Kumar, R. K. Singla, and R. R. Ketti, "Internet attacks and intrusion detection system," *Online Inf. Rev.*, vol. 41, no. 2, pp. 171–184, Apr. 2017.
[185] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer Internet of Things devices," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2018, pp. 29–35.

[186] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.
[187] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things," in *Proc. 14th ACM Workshop Hot Topics Netw. (HotNets)*, 2015, pp. 1–7.
[188] M. B. Barcena and C. Wueest, "Insecurity in the Internet of Things, version: 1.0," *Secur. Response, Symantec*, p. 20, Mar. 2015.
[189] C.-K. Chen, Z.-K. Zhang, S.-H. Lee, and S. Shieh, "Penetration testing in the IoT age," *Computer*, vol. 51, no. 4, pp. 82–85, Apr. 2018.
[190] M. Nolan, *Fundamentals of Air Traffic Control*. Boston, MA, USA: Cengage Learning, 2010.
[191] M. Dechow and C. Nurcombe, *Aircraft Environmental Control Systems*. Berlin, Germany: Springer, 2005, pp. 3–24, doi: 10.1007/b107234.
[192] E. Vattapparamban, İ. Güvenc, A. İ. Yurekli, K. Akkaya, and S. Uluağaç, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Sep. 2016, pp. 216–221.
[193] M. Wolf, M. Minzlaff, and M. Moser, "Information technology security threats to modern e-Enabled aircraft: A cautionary note," *J. Aerosp. Inf. Syst.*, vol. 11, no. 7, pp. 447–457, Jul. 2014.
[194] M. B. and H. Sung Kim, "CCTV surveillance system, attacks and design goals," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 8, no. 4, p. 2072, Aug. 2018.
[195] C. Alcaraz, *Security and Privacy Trends in the Industrial Internet of Things*. Cham, Switzerland: Springer, 2019.
[196] D. Wang, J. Ming, T. Chen, X. Zhang, and C. Wang, "Cracking IoT device user account via brute-force attack to SMS authentication code," in *Proc. 1st Workshop Radical Experiential Secur. (RESEC)*, 2018, pp. 57–60.
[197] L. Jayashree and G. Selvakumar, *Getting Started With Enterprise Internet of Things: Design Approaches and Software Architecture Models*. Cham, Switzerland: Springer, 2020. [Online]. Available: https://books.google.com.au/books?id=wKrdDwAAQBAJ
[198] D. Huang, A. Chowdhary, and S. Pisharody, *Software-Defined Networking and Security: From Theory to Practice* (Data-Enabled Engineering). Boca Raton, FL, USA: CRC Press, 2018. [Online]. Available: https://books.google.com.au/books?id=_gF-DwAAQBAJ
[199] S. P. Singh, A. Nayyar, R. Kumar, and A. Sharma, "Fog computing: From architecture to edge computing and big data processing," *J. Supercomput.*, vol. 75, no. 4, pp. 2070–2105, Apr. 2019.
[200] Y. Zhang, *Network Function Virtualization: Concepts and Applicability in 5G Networks* (Wiley-IEEE). Hoboken, NJ, USA: Wiley, 2018. [Online]. Available: https://books.google.com.au/books?id=pqJFDwAAQBAJ
[201] M. Gregg, *CISSP Exam Cram: CISSP Exam Cram_4* (Exam Cram). London, U.K.: Pearson, 2016. [Online]. Available: https://books.google.com.au/books?id=2UzODAAAQBAJ
[202] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security," in *Proc. 10th Int. Conf. Cyber Conflict (CyCon)*, May 2018, pp. 371–390.
[203] P. Neary, "Automatic hyperparameter tuning in deep convolutional neural networks using asynchronous reinforcement learning," in *Proc. IEEE Int. Conf. Cognit. Comput. (ICCC)*, Jul. 2018, pp. 73–77.
[204] A. Khandelwal, I. Agrawal, I. Malaserene, S. S. Ganesh, and R. Karothia, "Design and implementation of an industrial gateway: Bridging sensor networks into IoT," in *Proc. 3rd Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, Jun. 2019, pp. 1–4.
[205] B. Donnellan, C. Klein, M. Helfert, and O. Gusikhin, *Smart Cities, Green Technologies and Intelligent Transport Systems: 7th International Conference, SMARTGREENS, and 4th International Conference, VEHITS 2018, Funchal-Madeira, Portugal, March 16–18, 2018, Revised Selected Papers* (Communications in Computer and Information Science). Cham, Switzerland: Springer, 2019. [Online]. Available: https://books.google.com.au/books?id=3PqlDwAAQBAJ
[206] B. Jan, H. Farman, M. Khan, M. Imran, I. U. Islam, A. Ahmad, S. Ali, and G. Jeon, "Deep learning in big data Analytics: A comparative study," *Comput. Electr. Eng.*, vol. 75, pp. 275–287, May 2019.
[207] M. Libicki, *Crisis and Escalation in Cyberspace* (Ciencia Militar y Naval). Santa Monica, CA, USA: RAND, 2012. [Online]. Available: https://books.google.com.au/books?id=D9YzsTx1mnMC
[208] J. Vacca, *Computer and Information Security Handbook*. Amsterdam, The Netherlands: Elsevier Science, 2017. [Online]. Available: https://books.google.com.au/books?id=05HUDQAAQBAJ
[209] T. Weil and S. Murugesan, "IT risk and resilience—Cybersecurity response to COVID-19," *IT Prof.*, vol. 22, no. 3, pp. 4–10, May 2020.
[210] V. Sivaraman, D. Chan, D. Earl, and R. Boreli, "Smart-phones attacking smart-homes," in *Proc. 9th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*, 2016, pp. 195–200.
[211] A. Furfaro, L. Argento, A. Parise, and A. Piccolo, "Using virtual environments for the assessment of cybersecurity issues in IoT scenarios," *Simul. Model. Pract. Theory*, vol. 73, pp. 43–54, Apr. 2017.
[212] R. Tahir, "A study on malware and malware detection techniques," *Int. J. Educ. Manage. Eng.*, vol. 8, no. 2, p. 20, 2018.

NICKOLAOS KORONIOTIS received the bachelor's degree in informatics and telematics in 2014, the master's degree in web engineering and applications in 2016, and the Ph.D. degree in the field of cyber security with a particular interest in network forensics and the IoT from UNSW Canberra at ADFA, in June 2020. He is currently a Research Associate with the School of Engineering and Information Technology (SEIT), University of New South Wales (UNSW) Canberra at ADFA, in February 2017.

NOUR MOUSTAFA (Senior Member, IEEE) received the bachelor's and master's degrees in computer science from Helwan University, Egypt, in 2009 and 2014, respectively, and the Ph.D. degree in the field of cyber security from UNSW Canberra, in 2017. He is currently a Lecturer and the Theme Lead of Intelligent Security with the School of Engineering and Information Technology, The University of New South Wales, Canberra, Australia, where he was a Postdoctoral Fellow, from June 2017 to December 2018. His areas of interests include cyber security, in particular, network security, big data analytics, service orchestration, host- and network-intrusion detection systems, statistics, and machine/deep learning algorithms. He is interested in designing and developing threat detection and forensic mechanisms to the industry 4.0 technology for identifying malicious activities from cloud computing, fog computing, the IoT, and industrial control systems. He serves as a Guest Associate Editor for IEEE Access and a reviewer of many high-tier journals and conferences in the domains of security and computing.

FRANCESCO (FRANK) SCHILIRO received the master's (by Research) degree in computing from Macquarie University, Australia, where he is currently pursuing the Ph.D. degree in "Linking Cognitive Technology to Policing Processes." He is also a Superintendent with the Australian Federal Police. His current research interests include improving the police officer's effectiveness and efficiency in crime response, detection, prevention, and disruption through the use of Information and Communication Technology (ICT). His research draws from a diverse background in policing, cyber security and information technology. He began his career, as a Police, with the New South Wales Police Force, in February 1988, having roughly spent 15 years, during which he pursued a role in criminal investigations and achieved his detective designation. In 2003, he joined the Australian Federal Police, where he moved up the ranks to become a Superintendent. He is the AI-enabled Policing—Stream Leader with the AI-enabled Processes Research Centre, Macquarie University, and a Senior Certified Professional with the Australian Computer Society (MACS Snr CP IP3P).

PRAVEEN GAURAVARAM received the Ph.D. degree in cryptology from the Queensland University of Technology, Brisbane, Australia.

He is currently a Senior Scientist with Tata Consultancy Services (TCS) Ltd., Australia and New Zealand (ANZ). He leads TCS's Research & Innovation portfolio in cyber security by engaging TCS business units, TCS Co-Innovation (COIN), TCS Research & Innovation, TCS Cyber Security Practice and Cyber Security Co-Operative Research Centre (Cyber Security CRC), a federal government cyber innovation establishment in Australia. As a TCS's lead at Cyber Security CRC, he works closely with the industry, academia, and government partners of Cyber Security CRC and presents TCS thought leadership and innovation in cyber security. He holds honorary academic title as an Adjunct Associate Professor with the Faculty of Engineering, School of Computer Science and Engineering, University of New South Wales (UNSW). He has published more than 50 scientific articles and consulting advisories in cryptology and cyber security. He has held scientific positions in India, Europe, and Australia, and was a recipient of research grants and awards whist his research fellowship at the Technical University of Denmark. Notably, he was a recipient of Young Elite Researcher Award from the Danish Agency for Science, Technology and Innovation, in 2010, for his contributions to cryptology research. He is a Co-Designer of Grøstl Cryptographic Hash Function Competition and a Finalist of the NIST's SHA-3 Hash Competition.

HELGE JANICKE (Member, IEEE) is currently the Research Director of the Cyber Security Cooperative Research Centre, Australia. He is also with Edith Cowan University, and holds a visiting professorship in cyber security with De Montfort University. He has also been the Head of the School of Computer Science, De Montfort University, before taking up his current position as a Research Director of the Cyber Security CRC. His research interests include the area of cyber security, in particular, with applications in critical infrastructures using cyber-physical systems, SCADA, and industrial control systems. His current research interests include the application of Agile techniques to cyber incident response in critical infrastructure, managing human errors that lead to cyber incidents, and research on cyberwarfare and cyberpeacekeeping. He established the DMU's Cyber Technology Institute and its Airbus Centre of Excellence in SCADA Cyber Security and Forensics Research. He founded the International Symposium on Industrial Control System Cyber Security Research (ICS-CSR) and contributed over 100 peer-reviewed articles and conference papers to the field that resulted from his collaborative research with industry partners, such as Airbus, BT, Deloitte, Rolls-Royce, QinetiQ, and General-Dynamics.