ISSN 2616-5767 Vol.5, Issue 13: 55-61, DOI: 10.25236/AJETS.2022.051309

Using Digital Twins to Integrate Cyber Security with Physical Security at Smart Airports

Hao Su[1,a], Weijun Pan[1,b], Keyu Liu[2,c]

[1]Air Traffic Management Institute, Civil Aviation Flight University of China, Sichuan, China
[2]Information Service Department, Chengdu Tianfu International Airport, Sichuan, China
[a]clintsu97@icloud.com, [b]675702767@qq.com, [c]976864209@qq.com

Abstract: *Emerging digital twin technology is still at the stage of diverse standards and implementations, and its potential has not been widely validated. Digital twins allow systems to be fully digital from design time, even when combined with today's physical systems and can increase efficiency, validate ideas, and provide additional security. Digital twin technology has already highlighted its potential in industries such as construction, manufacturing, automotive, and agriculture. In this paper, the application of digital twin technology to smart airports is discussed, focusing on the physical and cyber security of airport subsystems. The advantages of adopting digital twin systems are discussed and recommendations are provided by sorting out the current cyber threats to smart airports, and countermeasures.*

Keywords: *smart airport, IoT, cybersecurity, digital twin*

1. Introduction

Airports play an important role in the global economy by bringing people around the world, expanding business prospects, promoting international tourism, generating revenue from business and tax revenues, and providing jobs. In some studies, there is a link between airports and regional economic growth, as ease of access is an important factor in promoting tourism and establishing cooperation between businesses in different regions, as well as facilitating the rapid movement of goods, which in turn accelerates trade. Therefore, airports must progressively modernize to keep up with the increasing passenger traffic and improve service quality through the application of emerging technologies.

Airport operations and business models have changed dramatically over the past few decades to support the explosive growth of the global aviation industry. The new changes have resulted in tremendous traffic growth and greater diversity of passenger choices. As airlines continue to refine their operating models to match growth with efficiency, airports have evolved in tandem, creating vast networks of hubs and intelligent systems that together create an efficient air transportation ecosystem. Along with this growth come threats and challenges, as emerging technologies bring efficiency while increasing instability, which increases with the total economic volume and strategic position of the airport.

1.1. Smart airports facing challenges

Airports have undergone significant changes in their operations and service offerings, from simply providing transportation to improving the quality of service and ensuring passengers enjoy a comfortable and entertaining experience. These airports employ a unified network of entities, including airports, aircraft, and airlines, with multiple sensors and IoT endpoint entities deployed throughout the airport to further enhance the passenger experience, while further enhancing it through the seamless collaboration of multiple subsystems and real-time data-sharing and analysis to enhance airport operations. Powerful technologies, including big data, biometrics, and artificial intelligence, power contemporary smart airports.

Like IoT, smart airports are an emerging trend, with the introduction of IoT devices dramatically changing the dynamics of traditional airports and introducing new subsystems of sensors and IoT terminals that are often interconnected, enabling systems and airport personnel to respond to events quickly and in an automated manner[1]. The regional nature of the IoT transforms the cybersecurity of

ISSN 2616-5767 Vol.5, Issue 13: 55-61, DOI: 10.25236/AJETS.2022.051309

smart airports from the traditional web-oriented applications and services to a subsystem that applies to a medium range of devices, sensors, antennas, LAN systems, CCTV systems, etc. combined in different areas divided to provide different services. According to the proposed architecture of international smart airports, both internal and external, it is emphasized that intelligence and automation are often combined to provide complex services. Depending on the area of the airport where the IoT application is deployed and its core functions, different network protocols and technologies will be used. For example, RFID technology is used for baggage handling processes where airport personnel manually or using robotic arms sort, load, or unload the correct cargo onto the aircraft.

However, the incorporation of IoT devices into industrial sectors, such as airports and their critical infrastructure, poses cyber risks. Various studies have demonstrated that various IoT devices are not properly protected against cyber-attacks. This insecurity can be attributed to many reasons, from users not changing the default credentials required to log in to the device and configure it, to software design flaws and hardware limitations. As a result, the reliability of services provided by IoT devices in smart airports and critical infrastructures is at risk from cyber-attacks that can tamper with data, cause sensors to report error messages, or make devices and systems completely unavailable through denial-of-service attacks.

1.2. Digital twin

Digital twins are dynamic models constructed by experts, usually in data science or applied mathematics. These developers study the physics that mimics the basis of a physical object or system and use that data to develop a mathematical model that reflects and makes certain extrapolations to the real world in digital space. Construct the digital twin program so that it can receive input from sensors with data from the real world. This allows the program to simulate physical objects in real-time, thus providing an analysis of performance and potential problems. Existing digital twin frameworks are based more on GIS or CAD and other architectural early construction drawings translated over to mark critical infrastructure for its data, with higher-level simulation in the industry achieved through physical engines evolved from game engines that essentially reflect the simple composition of industrial IoT, but still do not speak to the accuracy of mathematical-level modeling[2]. The digital twin expects to fully simulate the real physical industrial system in the information system and to demonstrate and deduce the state of the system. The existing technology is still far from this point, but at the beginning of the work, the real physical parameters of the connected devices such as IoT terminal devices, web cameras, wireless network transmitters, self-service check-in counters, etc. are rather less important, what matters is the network connection running on them and the service information running on them. By combining network topology and digital twin, it is possible to better observe the network in effect at a certain scale and to complete the extrapolation of the network system work. By combining the network security process and the physical security process through digital twin, it will be clearer whether each node of the whole IoT is under threat and the trajectory of the attacker's actions compared to the traditional means of network protection, and whether it is even possible to simulate the consequences of possible future network threat situations on the system utilizing digital twin.

Digital twin technology offers a new potential outcome for physical information systems in terms of monitoring, simulating, optimizing, and predicting conditions. Thus, virtual copies of physical information systems are useful and can play an important role in ensuring that systems have continuous feedback to improve efficiency and complexity.

1.3. Related work

Due to the importance of smart airports to the local economy and strategy, smart airport cyber security has been at the center of many research concerns as cyber-attacks continue to increase, affecting not only the availability of digital systems but even compromising end devices and having an impact on physical security.

Suciu et al. briefly studied the impact of terrorist acts and cyber-attacks on the development of state-of-the-art cyber security detection, protection, and countermeasures[3]. In their work, the researchers initially presented the terrorist attacks that occurred in the United States in September 2011 as the main driving force behind several innovations in airport security and cybersecurity. They have demonstrated that by leveraging WIFI and malicious applications, critical systems at airports can be compromised. Examples include airport ventilation systems, security sensors, and aircraft navigation

ISSN 2616-5767 Vol.5, Issue 13: 55-61, DOI: 10.25236/AJETS.2022.051309

systems that could threaten human lives. Next, the researchers provide realistic attack scenarios against simulated airport infrastructure, its impact, and mitigation strategies.

Lykou et al. studied the extent of the threats that airports face by absorbing IoT devices in their business processes and gave cybersecurity countermeasures and related policies adopted by smart airports[4]. While airports have taken measures to defend against or otherwise mitigate isolated hacking incidents, a more collaborative approach with the various subsystems and stakeholders that coexist within the airport is lacking. Through a review of the literature, the researchers determined that there is a lack of work on cybersecurity for ground control and other smart airport subsystems that need to be addressed, as integrating smart things into sometimes outdated systems introduces new attack surfaces that can be exploited and lead to equipment damage, service degradation, and even loss of life. The authors identify best practices for smart airports and illustrate the importance of well-organized response systems through seven attack scenarios. They conclude that the perceived security issue for most survey respondents is building cybersecurity awareness, along with the need to define a trust framework that allows stakeholders to collaborate to protect the aviation industry from next-generation cyber-attacks.

Agapaki investigated the use of digital twins as a resilient data platform for airports[5], by importing multiple data sources to support the interaction between twins. The study reviewed the existing risks in the context of collecting available data sources, grouping them (geometric, financial, social, and environmental), and developing a unified risk assessment framework using multiple criteria. Special emphasis was also placed on environmental threats, providing metrics to assess these risks and open-source existing databases. agapaki will primarily integrate the underlying digital twin with existing infrastructure asset management (AM) software to predict parameters such as asset lifecycle, risk management, consequences of failure, and probability of failure through the capabilities of the digital twin. The research will shift from the traditional acquisition of data from a single data source to combining multiple data sources. The underlying digital twin is used to identify environmental threats and hazards, and the metrics are used to guide DT in developing the same integrated data framework.

Thus, in Chapter 2, we study the various devices that need to be networked in the different systems of a smart airport, the possible cyber threat scenarios, and consequences for these devices; Chapter 3 presents a scheme for building a network model of a smart airport using the digital twin and gives our conclusions in the last chapter.

2. Threats to The Airport Subsystem

The airport's network falls somewhat within the realm of the Industrial Internet but is not completely closed, and many network service interfaces are exposed to passengers, vendors, and the network as they operate. At the same time, IoT end devices and sensors introduce new risks while improving efficiency, and common cyber threats and threatened airport subsystems will be exemplified in this chapter.

2.1. Cyber-threats

2.1.1. Penetration from check-in service

Check-in services are one of the few services at airports that are directly exposed to the web. Airlines encourage the use of common passenger processing systems to facilitate 24/7 customer support and to expedite check-in and passenger control processes through automated smart devices. A large number of self-service check-in infrastructures are installed at the airport and are used and shared by multiple airlines. Most of these devices run common operating systems, firmware, or proprietary software. Although these devices use intranet connections to access only the contents of corporate servers, they often provide remote management capabilities and are subject to tampering attacks due to their exposure to public space.

2.1.2. DDoS attacks against network services

The key feature of a smart airport is networked, data-driven responsiveness through intelligent components and integrated IoT devices. Any smart device connected to the airport network can support the critical function of interoperability between aircraft, airport management, air traffic control, and other forms of communication. Distributed denial of service (DDoS) attacks are among the most common cyber-attacks in recent years. In a DDoS attack, a hacker sends requests for a specific service

ISSN 2616-5767 Vol.5, Issue 13: 55-61, DOI: 10.25236/AJETS.2022.051309

to a server or group of servers simultaneously from a large number of controlled networked devices, thereby overwhelming the server and causing it to ignore legitimate requests from end users. DDoS attacks can affect the availability of resources and services at smart airports.

2.1.3. Unauthorized abuse

Disgruntled employees, contractors, or business partners with access credentials may abuse their authorization privileges, posing an insider threat designed to steal information for personal gain or to benefit other organizations. In addition, an intruder may use APT to access an airport's network undetected for a while escalating authorized privileges. the purpose of an APT attack is usually to monitor network activity and steal data, rather than to cause damage to the network or organization. To maintain access to the target network without detection, threat actors use advanced methods, including the constant rewriting of malicious code to avoid detection and other sophisticated evasion techniques.

2.2. Airport subsystems that may be affected

The various IoT terminals and special devices in the smart airport are connected through the network but are divided into different subsystems according to the different operations. The sensors and specialized devices in the subsystems work together, so a problem in one of them may render the entire subsystem unusable. In a non-airport-specific cyber-attack, the different subsystems are affected only by their presence in the layer network of the airport campus, but an attack on one subsystem of the airport can easily cause the system to crash, thus causing the entire business process to lag. Table 1 shows the possible cyber-attacks on subsystems and their possible impact.

Table 1: Airport Subsystems Affected by Cyber Attacks

Subsystems	Cyber Attacks	Impact
Self-Check-in	DDoS, Network Penetration	Information Leakage, Reservation Failure
Boarding Check	DDoS, MiTM	Information Leakage, Escape Check
Luggage Handling	Unauthorized Abuse, Malware	Work Interruption
Physical Security	Malware	Asset Losses
Assets Tracking	MiTM	Work Interruption
CCTV	Botnet	Physical Security Failure

Self-check-in: Passengers can avoid long lines and obtain their boarding passes by checking in via smartphone before boarding and completing check-in via the Internet or at smart check-in kiosks at various airport locations[6]. Associated with these check-in methods is another trend, namely automated bag pick-up. By using one of the self-service kiosks, passengers can print the necessary barcode stickers, attach them to their bags and leave them in a designated place for further processing by the airport's system. The use of either the self-service check-in kiosk or the web interface implies an Internet connection and therefore allows for a variety of attacks on these systems.

Boarding gate inspection: Passengers must go through border checks before boarding. Traditionally, this process required an office to manually check passengers' passports and verify their identity. In modern smart airports, an automated gate called an electronic gate is used instead of relying on this manual process. The boarding gate functions by scanning the microprocessor in the e-passport through the use of RF-enabled contactless smart card technology. Check-in at the gate relies heavily on obtaining biometric data on the passenger, such as facial recognition or fingerprint checks, and matching the information obtained with the data stored in the e-passport

Luggage handling: One of the problems facing contemporary airports is the misplacement and mishandling of baggage due to increased passenger traffic and human error. In recent years, one solution to this problem has been the application of RFID technology to tag and track baggage[7]. RFID tags store information about passengers and their baggage, as well as a unique ID created at check-in. during the flight, at the source, intermediate, and destination airports, the baggage's RFID tags are scanned and this information is shared between airports, allowing passengers to smartphone apps and online platforms to view the location of their luggage.

Airport asset tracking: Modern airports consist of multiple components, each designed to handle a specific task. In these airport areas, specialized assets (tools) are often used, such as baggage carts for transporting passengers' baggage from the parking lot to belt conveyors or baggage storage areas. Other examples include ground support equipment used before or after aircraft takeoff or landing, to assist in

ISSN 2616-5767 Vol.5, Issue 13: 55-61, DOI: 10.25236/AJETS.2022.051309

loading and unloading baggage, refueling aircraft, and assisting in general maintenance. Being able to quickly locate these assets, organize them and make them available for reuse is therefore essential to the continued efficient operation of an airport[8]. Therefore, RFID, Bluetooth, and other such lightweight network protocol-based sensors are attached to these assets, and their signals are collected by the sensor bridge and transmitted to a server through which managers can locate them (by overlaying location data with digital maps).

Physical security: As part of the physical security measures maintained at the airport, certain areas are only accessible to authorized personnel. To enforce these necessary restrictions, airports, like other institutions, make use of so-called electronic gates, combined with CCTV and motion sensors. By installing CCTV, webcams, thermal imaging cameras and motion sensors, the interior of the airport can be monitored, especially in high-risk areas. Restrictions on physical access can be achieved through the use of RFID, Near Field Communication (NFC) technology, smartphone apps, smart cards, or the use of alphanumeric codes and electronic locks.

3. Digital twin improves cybersecurity at smart airports

In the previous chapter, the common means of network protection for smart airports were introduced, using hardware and software that evolved based on commercial companies' requirements for security. The applicable scenario is a large computer cluster with a large number of servers under the same network bridge. It should be recognized that there is not only commercial Internet in smart airports, but also a larger part of industrial IoT, including subsystems such as security screening devices, self-check-in kiosks, and asset location using near-field communication, which often communicate with management services via RFID tags, NFC, Bluetooth, WIFI, or by connecting to nearby bridges or updating themselves via proximity firmware updates. This makes the attack scenario different from the traditional network service-based attack scenario. While the traditional network attack may come from anywhere in the network, through the service window of the smart airport service exposed to the extranet, the attack against the industrial IoT system of the smart airport occurs more within the scope of action of near-field communication, such as against the bridge deployed inside the airport, or the IoT end devices proximity firmware updates, or even insider threats via phishing emails or social engineering infiltration. In such cases, the benefits of monitoring the physical status of subsystems in real-time, collecting personnel information in critical areas through cameras and electronic gates, combing terminals connected to information exchange devices such as bridges through near-field communication means, and integrating this information employing digital twins to form a visual monitoring platform that unifies the physical security of airports and the industrial IoT security of subsystems.

3.1. Customized security

The beauty of the digital twin is that it allows organizations to build virtual, specific versions of their online infrastructure to do security analysis and attack prediction that fits their needs. It's a customized way to make security adaptable to different organizations. The benefits are twofold. Organizations can proactively develop countermeasures to defend against potential attacks and accurately calculate the cost of security based on their size. At the same time, organizations looking to introduce new systems or migrate old systems to the cloud can use the digital twin to improve their approach and test its viability through system application and data design. As part of a large and expanding operational entity, any organization should consider a practical solution that addresses the problem from a business perspective as well as a security perspective.

3.2. Automated security

Security talent often works with third-party security companies in the form of providing consultants rather than IoT brick-and-mortar companies. As a result, critical infrastructures such as airports face the dilemma of not being able to proactively defend themselves. With the current manpower crunch in the cybersecurity industry, automated identification, alerting, and traceability software is iterating to a more advanced, smarter, and more visual approach, with digital twins being the next generation of automated response platforms. At a time when organizations are finding it difficult to figure out how to automate their response to threats, especially with a shortage of security-literate employees, digital twins alleviate this problem by allowing companies to quickly identify weaknesses in their systems and focus on addressing them with automated software. This prevents operations teams from dealing with potential troubles in a haphazard, time-consuming manner, maximizing staff efficiency and fortifying defenses

ISSN 2616-5767 Vol.5, Issue 13: 55-61, DOI: 10.25236/AJETS.2022.051309

where help is most urgently needed.

3.3. Simulating real security

Many current cybersecurity defenses are based on the assumption that the network is secure, but with the digital twin, you can determine if it is truly secure. The idea of building a copy of reality through a digital twin is feasible. Organizations are free to control and experiment with their cyber defenses at all levels. Even a cyber-attack that could bring down an entire industrial base would destroy a copy of the real system first. By repeatedly testing replicas, even the most unpredictable scenarios can be prepared for and ensure that all attacks are tested. With the digital twin, organizations can prevent cyber threats against their systems in advance. Capturing realistic data and visualizing it is a process that requires attention, and hidden security issues can only be realized when information such as physical and network copies of systems and the network traffic going through them are presented through the means of digital twins. For example, many companies are focused on meeting the compliance requirements of their superiors but are not actively managing risk. This gives them a false sense of security. Standing upgrades, network cleanups, and shutting down unneeded services were also not done properly.

4. Conclusion

Since smart airports are not only dotted with commercial networks, a large number of IoT sensors and terminals are used in various subsystems of airports, which together form the industrial IoT of smart airports. Since each airport has various network services and IoT terminals communicating around the airport, the resulting airport industrial IoT has a huge and complex attack surface. This paper composes the possible attacks implemented through external networks and the possible threats caused internally by the subsystems and investigates the cyber protection means used by airports. Airports vary greatly in how they design, implement and protect their cyber infrastructure and adopt cybersecurity solutions. What remains constant, however, are the underlying protocols employed by the IoT, and the research shows that these protocols typically act at a local scale and are distributed in closer proximity depending on the construction of airport subsystems. Securing smart airports and staying ahead of evolving cyber threats is a shared responsibility of airlines, airports, vendors, and regulators. Therefore, a collaborative cyber resilience model that defines an appropriate cybersecurity approach for airports is important today. Airport operators should prioritize cybersecurity to ensure operational safety, passenger safety, and public safety. Cyber threats and risks will continue to grow, driven by technological developments, and the relationship between safety and security will become increasingly intertwined. The digital twin, an emerging disruptive technology, is a digital environment where physical devices, software, firmware, and their interactions are replicated in digital form with precision. The digital twin is not only a promising technology for defining local physical and cyber security in smart airports but also for ensuring cooperation upstream and downstream in the IoT supply chain. The security benefits from digital twins are discussed in Chapter 4, using digital twins to augment traditional security techniques applied to the commercial Internet, giving organizations that struggle to develop security-qualified employees a visual security posture that not only reflects the reality of system damage but also gives them a head start on cyber threats by simulating cyber attacks on a copy of the data to find subsystem weaknesses.

References

[1] Abdullah Alghadeir, and Hasan Al- Sakran, "Smart Airport Architecture Using Internet of Things" International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN: 2347-5552, Volume-4, Issue-5, September 2016.

[2] Kaznah Alshammari, Thomas Beach, Dr., and Yacine Rezgui, "Cybersecurity for digital twins in the built environment: current research and future directions" Journal of Information Technology in Construction ITcon Vol. 26, pg. 159-173, April 2021

[3] 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.

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

[5] Eva Agapaki, "Airport Digital Twins for Resilient Disaster Management Response" arXiv: 2205.

ISSN 2616-5767 Vol.5, Issue 13: 55-61, DOI: 10.25236/AJETS.2022.051309

03739 7 May 2022.

[6] 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.

[7] 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.

[8] 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