MITIGATION STRATEGIES FOR CYBER THREATS AGAINST SMART AIRPORTS

Jihan Jayanath Hewa Battage

A dissertation submitted in partial fulfillment of the requirements for
MSc in Cyber Security & Forensics

Department of Computing

Informatics Institute of Technology, Sri lanka
In Collaboration with
University of Westminster, UK

2021

Abstract

Smart airports have emerged as a combination of massive advancements in the IoT (Internet of Things) as well as the aviation industry. It has many benefits such as improved control, resilience, and efficiency in a smart airport as it uses IoT-powered systems and services that are regulated by real-time observing with analytics. In general, smart sensors provide powerful support for tasks such as regulating environmental conditions, automating passenger operations, and assisting airport security. Nevertheless, these enhancements and automation pose vast security risks to entire smart airport systems as well as networks.

Cyber-hackers often resort to IoT devices and network APTs (Advanced Persistent Threats) due to hardware or physical limitations, software vulnerabilities, or configuration issues of IoT. With the rising complexities of cyber-attacks or attack vectors, it is critical to protect IoT networks and systems of smart airports and maintain service dependability, since cyber-attacks may have devastating repercussions such as interrupting networks, canceling flights, or acquiring important information, etc.

Cybersecurity is rapidly becoming an essential facilitator of protection, which is a critical requirement in the aviation environment. By focusing on the fields of development, efficiency, security, safety, etc., the Smart airports seek to deliver optimal services in a dependable and sustainable approach. This research majorly emphasis the requirements for implementing cybersecurity procedures in Smart airports, malicious issues that emerge as a result of IoT as well as Smart appliances deployed, vulnerability situation analysis for IoT malicious assaults with mitigation activities of existing and emerging threats, and so on.

As a result, to improve policies, procedures and developing strong cybersecurity management, this study aims to conduct a methodical and detailed investigation of harmful assaults in Smart airports. Moreover, it is explicitly stated that applying cybersecurity best practices as well as resilience mechanisms would help the airport industry understand threats and respond proactively.

Keywords – Smart Airport, IoT, Cybersecurity, Mitigation Strategies