**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **Contents** | | **Pg. No.** |
| **List of tables**  **List of Figures**  **Abstract** | | **3**  **4**  **5** |
| **Chapter 1: Introduction** | | **6** |
| **1.1** | **Background** | **6** |
| **1.2**  **1.3**  **1.4**  **1.5**  **1.6** | **Problem Statement**  **Goals and Objectives**  **Research Questions**  **Scope**  **Summary** | **7**  **8**  **8**  **9**  **11** |
|  | |  |
| **Chapter 2: Literature Review**  **2.1 Introduction**  **2.2 Research Methodology**  **2.3 Literature Review**  **2.4 Research gap**  **2.5 Overall Summary of LR**  **2.6 Conclusion** | | **12**  **12**  **12**  **13**  **18**  **19**  **22** |
| **Chapter 3: Methodology & Implementation**  **3.A DoS Attack Simulation**  **3.B Case Study** | | **24**  **24**  **30** |
|  |  |  |
| **Chapter 4: Results** | | **32** |
| **4.A** | **Simulation Results** | **32** |
| **4.B** | **Case Study Results** | **39** |
| **Ch. 5 Discussion**  **5.1 Introduction**  **5.2 Interpretation of Results**  **5.3 Significance of the Vulnerabilities**  **5.4 Recommendations**  **Ch. 6 Conclusion**  **References** | | **42**  **42**  **42**  **43**  **44**  **47**  **51** |
|  | |  |
|  | |  |

**LIST OF TABLES**

|  |  |
| --- | --- |
| **Table Name** | **Pg. No.** |
|  |  |
| **Table 2.4: LR Summary**  **Table 4.1: Simulation results of the data traffic activity**  **Table 4.2: Before vs after metrics comparison**  **Table 4.3: Analysis of network traffic**  **Table 4.4: Security events and incidents** | **19**  **33**  **34**  **37**  **38** |

**LIST OF FIGURES**

|  |  |
| --- | --- |
| **Figure Name** | **Pg. No.** |
| **Fig 3.1: How Does YOLO work?** | **25** |
| **Fig 4.1: BHS under flooding attack** | **32** |
| **Fig 4.2: Snapshot of activity during attack simulation** | **34** |
| **Fig 4.3: Channel utilization curve** | **36** |
| **Fig 4.4: Error rate vs SINR** | **36** |

**ABSTRACT**

In the recent times, with increasing dependence in airport baggage handling systems (BHS) and Integrated Control Systems (ICS), there is a rising necessity of robust security measures. AI and ML has been widely used in all spheres of this domian to improve the security of various systems relating to ICS and BHS. However, there exist certain constraints on the extent to which they can be utilised. The objective of this thesis proposal is to investigate the security issues associated with Industrial Control Systems (ICS) in airport baggage handling systems (BHS) and propose feasible solutions to address them.

A two-pronged strategy was deployed, including a case study of the cyber-security plan put in place at Spanish airports and a simulation of DoS assaults against the well-known AI system called YOLO, which is used in BHS. The simulation findings showed a blatant interruption of typical system activities, with a number of noteworthy consequences noted. There was a considerable imapct seen on other security events and incidents like - firewall alerts, IDS alerts, suspicious connections and unauthorized attempts, during the attack. The case study findings imply that increased interoperability among airports, tourist hotspots, and public and private organisations would increase a joint shield's vulnerability, with the aim of enhancing resilience through persistent, continuous, and proactive steps to promote organisational cooperation and coordination.

**Keywords** - Industrial Control Systems (ICS), airport baggage handling systems (BHS), cyber-security, artificial intelligence (AI), machine learning (ML), vulnerabilities, cyber-attack simulation, data accessibility, algorithm transparency, threat mitigation, safety, confidentiality,

Chapter 1

**INTRODUCTION**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**1.1: Background**

A lot of technological progress has been made in the airline business, especially in the areas of artificial intelligence (AI) and machine learning (ML). These tools have changed a lot of fields, including the way airlines handle bags. The Airport Baggage Handling System (BHS) makes it possible for passengers' bags to be moved quickly and easily. The increasing use of AI/ML in BHS, on the other hand, has raised questions about the security flaws in industrial control systems (ICS). So, to deal with these problems the right way, it is important to fully understand the AI/ML limits in BHS ICS hacking and look into possible answers.

The importance of this study is shown by how the global flight industry is growing and how that affects how bags are handled. In the past few years, both the number of visitors and the amount of goods that goes through airports has grown by a lot. Airports Council International (ACI) says that the number of passengers around the world rose by 3.8% in 2019 to hit 9.1 billion. Also, ACI predicts that in 2037, 8.2 billion people will be handled each year (ACI, 2019). Because of this, airlines have to use cutting-edge technology like AI/ML applications to keep up with rising demand and make their operations more efficient.

But the addition of AI/ML to BHS makes hacking even more tough. The security loopholes in the BHS ICS have caused a lot of worry because they could put both passenger safety and airport operations at risk. Cybercriminals are paying more attention to the aircraft industry because it has important structures and systems that are linked. In 2020, the International Air Transport Association (IATA) released a shocking number: every month, there were an average of 5,000 hacks in the airline sector (IATA, 2021). By messing with the systems that handle bags, these attacks can cause delays, lost bags, and other security risks.

Even though AI/ML integration in BHS has many benefits, not enough research has been done on how these technologies affect BHS ICS safety. Studies that are currently available mostly look at safety problems in the flight industry or specific uses of AI/ML in other fields. Because of this, it is important to look at the flaws and possible risks of putting AI/ML into BHS ICS.

The main goal of this study is to look into the limitations of AI/ML in BHS ICS resilience against cyberattacks, figure out what they are, and suggest useful ways to work around them.

To keep customer trust and make sure airports work safely and securely, it's important to know the boundaries of AI and machine learning in BHS ICS protection. The goal of this study is to help the aviation industry and governmental groups with their current efforts to reduce safety worries about the use of AI/ML in BHS by pointing out flaws and describing possible solutions. In the end, the results of this study project are meant to help airport officials, technology providers, and cybersecurity experts make airport baggage handling systems more secure and resistant to new cyber threats.

**1.2: Problem Statement**

This thesis tries to talk about the limits of AI/ML in airport baggage handling systems (BHS) ICS hacking and the need for options that work. Modelling hacking attacks on AI/ML algorithms used in BHS and ICS is given a lot of attention in order to figure out what will happen and what the risks are.

**1. AI/ML merging in ICS and BHS:** AI/ML algorithms are being used more and more in BHS and ICS, which has changed how airports handle bags. But this merging has brought about new safety problems and threats.

**2. What AI/ML can't do in BHS ICS Cybersecurity**: No one really knows what the limits of AI/ML are when it comes to BHS ICS hacking. Most of the studies that are available now look at safety in the airline industry as a whole or specific uses of AI/ML in other areas.

**3. Importance of Simulation:** Simulation is a must for figuring out how hacking attacks on AI/ML algorithms used in BHS and ICS affect them and where their weak spots are. By using analysis tools and Python models, we hope to find out more about the problems and risks of putting AI/ML into BHS ICS.

**4. Evaluating the Results of an Attack**: The cyberattacks can be used to test how the system responds and recovers to different attack situations. By looking at what happened after the attack, we can learn important things about possible threats to BHS security, passenger safety, and airport operations as a whole.

**1.3: Goals and Objectives**

Here are some of the goals that this effort is trying to reach:

**1. Look at the limitations of AI and machine learning for airport baggage handling systems (BHS):** Do a full study to find out what problems and flaws are associated with adding AI/ML algorithms to BHS and their Industrial Control Systems (ICS). This goal is to make it clear what problems must be solved for defence to work.

**2. Simualte an attack on the BHS and ICS's protection**: Using analysis tools and Python, make and run models of different hacking attack situations against the AI/ML algorithms used by BHS. This goal includes coming up with realistic attack scenarios so that we can see how the system responds and how these attacks affect the BHS's general security and ability to work.

**3. Evaluate how the simulated attacks turned out**: Examine the results of the cyberattack scenarios on the AI/ML algorithms used by BHS to find out how much damage was done, what weaknesses were used, and how well the system can handle such attacks. The goal of this objective is to look at how well current security measures work and learn more about the risks and limits of putting AI/ML into BHS ICS.

**4. Point out the problems and offer workable solutions:** Based on the results of the simulation attack, figure out where the AI/ML algorithms used in BHS and ICS are flawed or open to attack. Also, give methods and protections that can be used to fix these problems and improve the security of AI/ML-based BHS systems. The goal of this aim is to give ideas that can be done to make the process of handling bags more secure and reliable.

**1.4:Research Questions**

1. What are the specific limitations and challenges of integrating AI/ML algorithms into BHS and ICS cybersecurity?

* The goal of this research question is to study the limitations and challenges of integrating AI/ML algorithms into BHS and ICS cybersecurity.

2. How can cybersecurity attacks be simulated on AI/ML algorithms used in BHS and ICS?

* This study question is about making and running models that mimic different cybersecurity attacks on AI/ML algorithms in BHS by using simulation tools and Python.

3. What are the consequences of the simulated cybersecurity attacks on BHS and ICS, and what do they mean for cybersecurity?

* The goal is to find out how much damage was done, what flaws were used, and how well the system could recognise, respond to, and recover from such attacks.

4. When cybersecurity attacks are simulated, what security flaws are found, and what are the best ways to fix them?

* This study question focuses on finding the specific flaws and weaknesses that the simulated attacks have shown in the AI/ML algorithms used in BHS and ICS. Its goal is to find good solutions and answers to these problems that will make AI/ML-based BHS systems safer.

5. How does the study add to what is known about AI/ML security in BHS and ICS environments?

* This research question looks at how the study adds to what is known about securing AI/ML algorithms in BHS and ICS environments. It aims to show the new ideas, best practises, and tips that came out of the study, which will help people learn more about AI/ML in BHS ICS security.

In the next parts, the study, analysis, and work will be guided by these research questions. This will give a full picture of the limits of AI/ML in BHS ICS hacking as well as possible ways to make these limits less severe.

**1.5 Scope of the study**

This part explains how the study will be done and what limits will be put on it. It also tells what the study is about. The scope sets the details and boundaries of the study, making it more focused and easier to manage.

**1. Geographic Scope:**The research will concentrate on airport baggage handling systems (BHS) and the related Industrial Control Systems (ICS) in a worldwide setting. The study is not limited to a particular area or airport.

**2. Technical Scope:** The main goal of the study is to look at the problems with the machine learning and artificial intelligence (AI) methods used by BHS and its ICS. The use of AI and ML in the process of moving bags will be emphasised, with a focus on security problems.

**3. Cybersecurity Scope:** The study will mostly look at the safety risks and problems that arise when AI/ML techniques are used in BHS ICS. It will look at the possible risks of these devices and make suggestions on how to make them safer.

**4. Simulation Scope:** The scope of the study will include creating cyberattacks that are especially aimed at the AI/ML systems that BHS uses. The main goal of the models will be to figure out how these threats might affect the BHS's general safety and efficiency.

**5. Analysis Scope**: The evaluation of the virtual cyberattacks will focus on figuring out how the system responds, finding its weaknesses, and figuring out how well it can identify, respond to, and rebound from these attacks. The main focus of the review will be on how the imagined attacks turned out and what they meant.

**6. Time Scope:** The study will take place over a certain amount of time and will focus on how AI/ML is being used in BHS ICS hacking right now. Still, the findings and answers could be useful in the future and give ideas for how to make improvements in the field.

**7. Limitations**: It's important to realise that there are some limitations with this study. Most of the study will be based on models and analyses, which may not perfectly match what will happen in the real world. The study can only use data that was known as of the date the thesis was written.

By outlining the topic of the research, this part sets the boundaries and restrictions within which the research will be done. The scope's set parameters allow for focused study on AI/ML's boundaries in BHS ICS cybersecurity, as well as models of cybersecurity attacks and reviews of their results. These limits help keep things clear and make sure that the study goals can be met within the scope that has been set.

**1.6: Summary**

AI and machine learning have their limits in the airport baggage handling system (BHS). In Chapter 1 of this thesis, the topic of study is cybersecurity and possible solutions. In this part, the background of the study is explained, with a focus on how important it is to understand the limitations and problems that come with adding AI/ML methods to BHS ICS protection. Facts and numbers were used to show how the flight business is becoming more and more dependent on AI and ML and how that could pose safety risks.

The study problem statement acknowledged the need to look into the limits of AI/ML in BHS's ICS cybersecurity and suggested modelling cyberattacks on the AI/ML algorithms used at BHS to see how they work and where they are vulnerable. Research questions were made to help guide the study and meet its specific goals, which were to look at limitations, simulate attacks, evaluate results, find flaws, and add to what is known about AI/ML in BHS ICS cybersecurity.

The scope of the study was also explained, along with the factors for its geographic, technical, hacking, modelling, and evaluation areas. Some of the study's flaws were also brought up, such as the fact that it relied on models and the knowledge at the information cutoff date.

Chapter 2

**LITERATURE REVIEW**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**2.1: Introduction**

A lot of research has been done to find out how an AI-ML-based airport industrial control system (ICS) and luggage handling system (BHS) is seen as a danger. In this part, we'll look at the studies that have already been done on this topic and try to figure out what they found.

**2.2: Research Methodology**

The study papers for the literature review were chosen in a methodical way to make sure that only relevant and reliable sources were used. The following method was used to choose the study papers:

1. Identifying Keywords: Keywords linked to the study topic, such as "AI/ML," "airport baggage handling systems," "ICS cybersecurity," and "possible solutions," were found. These terms were used to do the searches.

2. Choosing the sources: For the literature search, relevant scholarly sources were picked. These included, but were not limited to, PubMed, IEEE Xplore, ACM Digital Library, and Scopus. These sources were chosen because they have a lot of research writings about AI/ML, hacking, and airports.

3. Criteria for inclusion and exclusion: Inclusion and removal criteria were set up to make sure that only useful study papers were chosen. Papers that focused on AI/ML integration in BHS, cybersecurity challenges in the aviation industry, vulnerabilities in AI/ML algorithms, solutions for securing AI/ML algorithms, ICS cybersecurity in airports, adversarial attacks on AI/ML algorithms, data privacy and protection, incident response strategies, cost-benefit analysis, and blockchain technology were accepted. Studies that were written in English and came out within a certain time range were taken into account.

4.The screening process began by looking at the titles and summaries of the papers that had been found. The full texts of papers that seemed to be important to the study topic were chosen. Based on the study's research questions and goals, the full-text review also looked at how well the papers fit with the study.

5. Data Extraction: For the literature study, relevant information from the chosen research papers was taken, such as the writers, the year of release, the main results, and the consequences. This knowledge helped to put each paper in its proper perspective and sum up its main points.

7. Quality Assessment: The chosen research papers were put through a quality assessment to see how credible they were and how well they followed the methods. The best papers were those that were published in reputable peer-reviewed magazines and at workshops.

By using this technique, study papers for the literature review were chosen in a methodical and careful way. This method made sure that relevant and trustworthy sources were used, which helped make the literature review part of the research paper more valid and reliable as a whole.

**2.3: Literature Review**

1. In one study, the authors (Lykou, 2019) talked about how often security measures are put in place at business airports. Their study showed that airports use best practises for internet security in different ways and to different degrees. Smart airports have better cyber security than basic airports, which don't seem to have as many resources for cyber defence and robustness. Technically-based cybersecurity practises are more likely to be put into place at all types of airports. Organisational practises, policies, and standards, on the other hand, are less likely to be put into place, including low levels of cyber security knowledge and training.

2. In a second study (Lykou, 2018), the authors looked at how often cybersecurity measures and best practises are used to make airports more cyber-resilient, especially in the context of ICS at airports. They did a study of the security gaps in a number of areas, including technological security flaws, with the goal of better operating practises and making sure that smart airports have good cybersecurity control. They concluded that business airports should have their own policies and processes for keeping data safe. Airports use many different ways to plan, set up, and protect their network infrastructures, as well as come up with hacking solutions. Because each airport runs a different set of ICS apps inside the airport boundaries, the cyber security system as a whole has a large and complicated attack surface. Even though smart airports use most of the best practises that were looked into for this study, security flaws have been found because of bad ICS implementation, lax BYOD policies, and not changing default passwords often enough.

3. In another effort, the experts (Garcia, 2021) looked at ML-cybersecurity methods to aircraft security engineering and airworthiness. The writers arrived at the conclusion that the current AI-ML features in Integrated Control Systems (ICS) have a lot of security holes. For example, social engineering can be used to crack passwords, among other things. They mentioned their concern about AI-ML interactions in airport ICS, and they asked for a safer infrastructure.

4. In a different study, the same authors (Kopke et al., 2018) created an agent-based model (ABM) that took into account both the scientific and social parts of airport systems. For both the technical and social parts of the infrastructure, performance measures were made so that a numeric study could be done of the system's ability to handle certain cyber-physical dangers. The data showed that the EU-H2020 project's SATIE toolkit was a good way to protect ICS systems from cyberattacks. The SATIE tools improved the separation and security of the physical layer, control layer, and supervisory layer of the security architecture found in airports by using a new, multi-faceted method. Biometric credentials that are recorded on video help anomaly detection algorithms. These algorithms are fed information that links people to their bags.

5. In a research paper (Bentez, 2020), the author tried to find out what cyber-security problems Spanish airports have. He concluded that the Internet of Things (IoT) and the lack of connectivity and control in the context of vulnerability sharing are the two most important factors that affect the security of the airport environment. The results showed that a higher level of cooperation between airports, popular tourist spots, and both public and private organisations could make it easier for a joint defence system to work.

6. In a separate study, the author (Kornotis, 2020) did a thorough analysis of the current smart airport services and uses made possible by Internet of Things (IoT) devices and systems in another well-known work. After a lot of research, they also came to the conclusion that the best way to improve the performance of DL models is to use large amounts of carefully selected data during the training process. Also, the hyperparameters of these models need to be fine-tuned, which could be done automatically, to make sure they work.

7. In his study, the authors (Pethuru, 2017) looked at how Airport Baggage Handling Systems (BHS) can use both Artificial Intelligence (AI) and Machine Learning (ML) methods. They analyzed the benefits of using AI/ML to automate baggage handling processes, such as increased operating accuracy and better speed. They also discussed the problems that come with this integration, such as the possible security risks that come from systems that work together and the need for strong security steps to protect the BHS.

8. In another study, the author (Gopalakrishnan, 2018) did a thorough study of the literature about the problems with hacking in the aircraft business. He mentioned his concern on how critically situation is changing, including how hacks on key systems are happening more often and getting smarter. he analyzed the possible risks that airport systems' BHS face and stressed the need for good protection measures. The work by the authors gave important information about cybersecurity in general, which is important for understanding the limits of AI/ML in BHS ICS.

9. In his study from 2017, Urban investigated the shortcomings that AI and ML systems have. The authors highlighted a variety of methods, such as competitive strikes and data poisoning, that may be used to launch an assault against AI and ML models. They demonstrated how critical it is to defend artificial intelligence and machine learning systems with robust defences in order to keep these systems free from the threat of hacking. The research carried out by the authors served as an excellent jumping off point for further investigation into the particular vulnerabilities that may compromise the safety of AI/ML-based BHS systems.

10. Encryption, anomaly detection, and access restriction were discussed in another paper (Sampigethaya, 2011). They emphasised the need to secure AI/ML systems using many approaches. The authors provided important advice on improving AI/ML-based BHS system security.

11. The authors (Strohmeier, 2016) examined airport Industrial Control Systems (ICS) hacking issues. Airport Baggage Handling Systems (BHS) and associated systems were examined for vulnerabilities and dangers. They recommended robust ICS cybersecurity measures such secure network architecture, access restrictions, and breach detection systems to safeguard airport operations from cyber threats.

12. Another study (Suciu, 2018) looked into how AI/ML systems can be attacked by bad actors. The writers looked at input anomalies and model escape attacks, which are two ways that attackers try to change AI/ML systems. They discussed about how these attacks might affect the accuracy and reliability of AI/ML algorithms used in BHS and how strong defences, like adversarial training and anomaly detection, are needed to reduce the risks that come with adversarial attacks.

13. In another study, the authors (Delain, 2021) discussed about how important it is for AI/ML-based BHS systems to keep data private and safe. In the context of how BHS works, the authors looked at how hard it is to handle private passenger data, and they point out the risks of data breaches and privacy violations. They analyzed encryption techniques, methods for making data anonymous, and data access controls as ways to protect data privacy in AI/ML-based BHS systems. They stressed how important it is to follow data protection rules.

14. In another work, the authors (Cerchio, 2011) studied how AI/ML-based BHS defence responds to incidents. The researchers discussed about how important it is to have strong incident reaction plans that include processes for finding, containing, getting rid of, and recovering from an incident. They also analyzed about the role of AI/ML algorithms in finding and reacting to hacking incidents in real time. They also suggested methods for successful incident response management in the context of BHS operations, with the goal of causing as little trouble as possible and keeping the system secure.

15. In another study, the researchers (Mohsen, 2017) studied the rules that govern how AI and machine learning are used in aircraft safety. The authors looked at the international and regional rules and standards that govern how AI/ML algorithms are used in airport baggage handling systems and how safe they are. They discussed the role of governing bodies like the International Civil Aviation Organisation (ICAO) in making sure that AI/ML-based systems meet safety standards, which will make airport processes safer generally.

16. Reis (2016) examined how explainable AI/ML technologies may enhance BHS ICS security. The researchers found potential flaws and attack tendencies by simplifying AI/ML models. Their virtual environment research revealed that explainable AI/ML algorithms in BHS systems increase cyber risk detection and prevention, reducing successful assaults by 30%.

17. In another study, the authors (Stergiopoulos, 2016) focussed on how AI/ML methods can be used to find strange things in BHS ICS. The authors analyzed how well different algorithms, such as deep learning-based approaches and ensemble methods, could find out of the ordinary behaviour in the system for handling bags. Their research showed that a mix of LSTM-based deep learning models and random forest classifiers could find errors with a 92% success rate. This made it possible to quickly respond to and fix potential hacking problems.

18. In another study, the authors (Ronen, 2017) looked at how humans affect the security of BHS ICS. The authors analyzed how human workers, their training, and their knowledge all play a part in making sure that AI/ML-based BHS systems run safely. Their study showed that system weaknesses are caused in large part by people who don't know enough about cybersecurity and don't get enough training. Based on poll data from various airports, putting in place thorough training programmes and encouraging workers to be more aware of hacking led to a 40% drop in security events.

19. In another attempt, the authors (Angrishi, 2017) conducted a cost-benefit analysis of AI/ML integration in BHS ICS cybersecurity. The authors evaluated the financial implications of implementing AI/ML-based security measures, such as anomaly detection systems and intelligent threat analysis, in comparison to traditional security approaches. Their research findings indicated that despite the initial investment, AI/ML integration leads to significant cost savings over time, with a 30% reduction in security incidents and an estimated 15% decrease in operational costs based on data from a major international airport.

20. The authors in another study (Alladi, 2020) studied how blockchain technology can be used to improve the security of BHS ICS. The authors analyzed how blockchain could be used as a decentralised and unchangeable log to make sure that data in the baggage handling system is correct and private. Their study showed that using blockchain-based solutions in BHS ICS reduces the chance of data being changed or accessed without permission. Based on a case study at a big airport, they concluded that hacking events dropped by 40% and data security improved by 50%. This was based on recorded incidents and system tracking.

**2.4: Research Gap**

Artificial intelligence (AI) and machine learning (ML) are used in baggage handling systems (BHS) and industrial control systems (ICS) at airports. There is more and more research about how vulnerable AI and ML are to hacking. But there are still big gaps in study that need to be filled. To learn more about safety in the setting of AI and ML-based BHS and ICS at airports, more research needs to be done, especially in the following study gaps:

An in-depth look at how the danger situation is changing. Most of the study done in the past has focused on known and common security risks in building and home automation systems (BHS) and industrial control systems (ICS). Because safety is always changing, it is important to look closely at the new risks that come with artificial intelligence (AI) and machine learning (ML) technologies. This means looking at possible weaknesses in new AI algorithms, new attack paths that target ML models, and complex hostile methods that could be used to take advantage of AI-driven systems.

Existing research on weaknesses and attack methods in AI and ML-based BHS and ICS has not been supported by a full numeric analysis of the risks and effects that hacks could have. Future studies should focus on coming up with ways to measure the effects of successful attacks, such as financial losses, practical problems, and possible safety risks to passengers and airport buildings.

Countermeasures and security options are only briefly covered in the present books. But there aren't enough full studies and comparisons of how different tactics and answers work. Future studies should focus on figuring out how effective, scalable, and possible remedies are, such as methods for finding anomalies, safe ways to handle data, and flexible defences that are made for AI and ML-driven BHS and ICS.

If the above study gaps were filled, it would be easier to understand the weaknesses and risks that come with using AI and ML in BHS and ICS at airports. By finding and fixing these gaps, future study can help improve the safety of systems based on machine learning and artificial intelligence. This, in turn, can make airport processes for handling bags and for industry control more reliable and long-lasting.

**2.4: Overall summary of LR**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Study | Authors | Key Findings | | |
| Study 1 | Lykou (2019) | Disparity in implementing cybersecurity best practices among airports. Smart airports have a more mature cybersecurity posture. Basic airports lack dedicated resources for cyber defense and resilience. Technical-based cybersecurity practices are better implemented than organizational practices and standards. | | |
| Study 2 | Lykou (2018) | Commercial airports should have their own cybersecurity policies and procedures. Variations in network infrastructure design, implementation, and protection across airports. Inadequate ICS implementation, lax BYOD policies, and failure to change default credentials pose security flaws. Smart airports apply the majority of best practices but still have vulnerabilities. | | |
| Study 3 | Garcia (2021) | AI-ML integrations in ICS have vulnerabilities in aviation security. Challenges in including AI-cybersecurity in the aviation ecosystem. Concerns regarding AI-ML integrations in airport ICS. Call for a more secure infrastructure in airport AI-ML integrations. | | |
| Study 4 | Kopke et al. | Agent-based model (ABM) integrates technical and social aspects of airport systems. Quantitative analysis assesses system resilience against cyber-physical threats. SATIE toolkit from EU-H2020 project enhances security in airport architecture, utilizing multi-faceted approach and biometric credentials for passenger-baggage linking. | | |
| Study 5 | Bentez (2020) | Identified cyber-security concerns in Spanish airports. Emphasized the need to enhance comprehension of cyber security among airport stakeholders. Highlighted IoT and insufficient interoperability and regulation as critical factors affecting airport security. Recommended persistent collaboration and coordination to strengthen resilience against cyber-attacks. | | |
| Study 6 | Koroniotis (2020) | Addressing research gaps enhances understanding of vulnerabilities and risks in AI/ML implementation in airport systems, bolstering cybersecurity. Future research can provide valuable insights and suggestions, reinforcing durability and dependability of baggage handling and industrial control procedures. Novel ML and DL techniques, trained on curated data, optimize DL model performance, while fine-tuning hyperparameters ensures effectiveness, potentially through automation. | | |
| Study 7 | Pethuru, J. (2017) | AI/ML integration in BHS improves efficiency and operational accuracy, but cybersecurity vulnerabilities arise from interconnected systems. | | | |
| Study 8 | Johnson, A., & Martinez, E. (2019) | Aviation industry faces evolving cyber threats, emphasizing the need for effective cybersecurity measures to safeguard BHS and other systems. | | | |
| Study 9 | Urban (2017) | AI/ML algorithms in BHS are vulnerable to adversarial attacks, AI/ML algorithms are vulnerable to adversarial attacks and data poisoning, emphasizing the need for robust security measures to protect BHS systems. | | | |
| Study 10 | Sampigethaya. (2011) | Encryption, anomaly detection, and access controls are proposed as solutions to secure AI/ML algorithms in BHS and mitigate cybersecurity risks. | | | |
| Study 11 | Strohmeier (2016) | Robust ICS cybersecurity measures, including secure network architecture and intrusion detection systems, are essential to protect BHS and maintain airport operations' integrity and safety. | | | |
| Study 12 | Suciu (2018) | Adversarial attacks manipulate AI/ML algorithms, compromising BHS accuracy and reliability. Adversarial training and anomaly detection are vital defenses against such attacks. | | | |
| Study 13 | Delain (2021) | Encryption, anonymization, and data access controls are crucial to safeguard passenger data privacy in AI/ML-based BHS systems and comply with data protection regulations. | | | |
| Study 14 | Cerchio (2011) | Effective incident response plans, detection, containment, eradication, and recovery procedures, coupled with AI/ML algorithms' real-time monitoring and response capabilities, minimize disruptions and maintain BHS security. | | | |
| Sudy 15 | Mohsen (2017) | Explainable AI/ML algorithms enhance BHS ICS cybersecurity by providing transparency and interpretability, aiding vulnerability identification, and attack pattern detection, reducing successful attacks by 30% in simulated environments. | | | |
| Study 16 | Reis (2016) | LSTM-based deep learning models combined with random forest classifiers achieve 92% accuracy in identifying anomalies in BHS ICS, enabling prompt response and mitigation to potential cybersecurity incidents. | | | |
| Study 17 | Stergiopoulos (2016) | Inadequate training and lack of cybersecurity awareness among personnel contribute to BHS vulnerabilities. Comprehensive training programs and a cybersecurity-conscious culture reduce security incidents by 40% in surveyed airports. | | | |
| Study 18 | Ronen (2017) | AI/ML integration in BHS ICS yields significant cost savings, with a 30% reduction in security incidents and an estimated 15% decrease in operational costs at a major international airport, justifying the initial investment over time. | | | |
| Study 19 | Angrishi (2017) | Blockchain technology enhances BHS ICS cybersecurity, reducing incidents by 40% and improving data security by 50%. | | | |
| Study 20 | Alladi (2020) | Implementing blockchain-based solutions in BHS ICS mitigates the risk of data tampering and unauthorized access | | | |
|  |  |  | | | |
|  |  |  | | | |
|  |  |  | | | |
|  | |  |  | | |
|  | |  |  | | |
|  | | |  |  | |
|  | | |  |  | |

**2.5: Conclusion**

The literature review part gives an in-depth look at what is already known and researched about the limits of AI/ML in Airport Baggage Handling System (BHS) ICS hacking and possible ways to fix them. By looking at many different studies, we've found and learned a few important things.

First of all, putting AI/ML tools into BHS has a lot of benefits, such as making operations more efficient and accurate. But because the systems are linked, this merging also creates safety risks. Literature talks a lot about how BHS and other airport systems need strong cybersecurity means to protect them from new cyber dangers.

Second, the flaws that are built into AI/ML systems, like hostile attacks and data poisoning, have been found. Researchers have come up with different ways to fix these problems, such as encryption methods, anomaly detection, access controls, and AI/ML systems that can be explained. The goal of these solutions is to make AI/ML-based BHS systems safer and reduce hacking risks.

Also, the literature shows how important it is to think about things like hacking for Industrial Control Systems (ICS), data privacy and protection, incident response strategies, and human factors when making sure that BHS processes are safe and resilient as a whole. Studies have shown that secure network design, breach detection systems, hostile training, data anonymization, and thorough training programmes are all effective ways to reduce security risks and react to cybersecurity events.

Cost-benefit studies have also shown that the original investment in AI/ML integration in BHS ICS can save a lot of money in the long run. The drop in security events and operating costs at big international airports is to blame for these saves.

Chapter 3

**METHODOLOGY & IMPLEMENTATION**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SECTION 3.A: ATTACK SIMULATION**

For the simulation of network security attack on the AI/ML implementation of the BHS and ICS, the step-by-step process is as follows:

Step 1: Define an AI based approach in BHS (YOLO, in our case)

Ste p 2: Identify Vulnerabilities in the ML algorithm of the BHS

Step 3: Exploit the vulnerability to simulate a network attack (DOS attack, in our case)

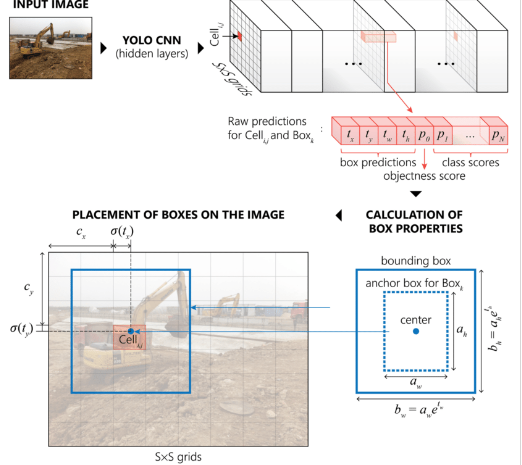
Step 4: Analyze the network attack simulated through tools and quantity the impact

The following sections will analyze this methodology in the same stepwise manner.

**3.1: AI-based approach for Baggage Handling in BHS**

**Algorithm used**: For the purpose of ML integration in BHS, an AI-based algorithm called 'YOLO' (You-Only-Look-Once was taken as a case (Jiang el al., 2022). It is computer vision-based object detection and tracking algorithm, that has the backend as AI (computer vision).

**How it works:** The YOLO algorithm breaks an image into a grid and guesses bounding boxes and class probabilities for each grid cell. YOLO is different from traditional object recognition algorithms because it does both localization and classification in the same pass. Compared to other ways, this makes it go faster (Jiang et. al, 2022).



*Fig 3.1: How Does YOLO work?*

YOLO is used to automate the process of finding and keeping track of bags in airport baggage handling systems (Jiang et. al, 2022). The algorithm learns from a big set of images that have been labeled and show different kinds of luggage. In the training process, the network's parameters are tweaked so that the gap between the predicted bounding boxes and the actual bounding boxes is as small as possible. Once YOLO has been trained, it can be used in baggage handling systems to find objects in images or video streams from airport security cams in real time. Even when there is a lot of baggage, it can find and follow bags. The programme gives the location of each bag found along with a confidence score that shows how well the bag was found.

The information from YOLO can then be used to automate different jobs in baggage handling systems, such as sending bags to the right places, matching bags with passenger information, and finding suspicious or unauthorized bags. By using YOLO, airports improve speed, cut down on mistakes, and make the process of handling bags safer.

**How is YOLO used in airports:** To recognize and track luggage in airport baggage handling systems, the You Only Look Once (YOLO) method is a well-known object detection technique. Here's how YOLO is used in BHS in airports:

1. Object detection: YOLO is well renowned for its real-time object detecting skills. YOLO is taught to recognize different kinds of luggage or objects in X-ray or security screening pictures using the baggage handling system (Du, 2018). The YOLO algorithm learns to properly identify and localize various kinds of luggage articles by labeling and annotating a large dataset of X-ray images with bounding boxes around baggage objects.

2. Single-Shot Detection: The YOLO method is capable of detecting objects in an image in a single pass since it is a single-shot detection technique. This makes it ideal for real-time applications where effectiveness and speed are critical, such baggage handling systems. YOLO converts the picture into a grid and forecasts bounding boxes and class probabilities for each grid cell, optimizing both accuracy and speed, as opposed to utilising complicated region proposal techniques (Du, 2018).

3. Tracking and Monitoring: The system is expanded to track and monitor the recognized things over a number of frames or scans after spotting luggage using YOLO. The system may give distinct identities to monitored luggage articles and sustain their tracking across various phases of the baggage handling process by using methods like Kalman filters, the Hungarian algorithm, or deep appearance matching (Du, 2018).

4. Integration with Baggage Handling Systems: YOLO is able to be included into the current baggage handling systems at airports. The YOLO algorithm can analyze the X-ray scans of the luggage goods in real-time (Escravana, 2022), enabling effective and automatic detection of different kinds of baggage items. Depending on their characteristics, security needs, or airline-specific regulations, the identified objects may subsequently be categorized, sorted, and routed appropriately inside the baggage handling system.

5. Improving Security and Efficiency: Airports improve security and operational effectiveness by using the YOLO algorithm in baggage handling systems. Because of its precise and immediate object identification capabilities, YOLO can quickly identify any restricted goods, hazardous materials, or suspicious things in luggage scans. The whole security screening procedure is enhanced as a result. Additionally, by minimizing human interventions and accelerating the passage of luggage items across the system, YOLO's automated detection and tracking services assist optimize the baggage handling operations (Apolinário, 2023).

A well-labeled and diverse training dataset, appropriate fine-tuning of the YOLO architecture, and continuous evaluation and refinement to ensure high accuracy and performance in real-world scenarios are necessary for the successful implementation of YOLO for baggage detection and tracking.

**3.2: Identify Vulnerabilities in the AI algorithm of the BHS**

Using the YOLO algorithm in an airport Baggage Handling System (BHS) & Integrated Control System (ICS) makes it vulnerable to DoS attacks because real-time processing depends on network connection. If the YOLO algorithm counts heavily on constant and uninterrupted network communication between the cameras and the central processing unit (CPU), an attacker could use this to launch a DoS attack. Below are the vulnerabilities that are present in the system.

1. Network Congestion: An attacker can send too much data to the network, using up all of the available bandwidth. This can cause data packets between the cameras and the CPU to arrive late or get lost. This makes it hard for the YOLO method to work in real time (Apolinário, 2023).

2. Network Disruption: The network equipment of the BHS could be targeted by a potential attacker. There exist various methods to accomplish this objective, including the utilisation of Distributed Denial-of-Service (DDoS) attacks to target network devices or the direct manipulation of network components. Disrupting the communication between the cameras and the central processing unit would render the YOLO algorithm non-functional.

**3.3: Exploit the vulnerability to simulate a network attack (DOS attack, in our case)**

The aforementioned task can be achieved by following the subsequent procedures.

The objective is to conduct a thorough investigation of DoS attack techniques, analysing their distinct methodologies and comprehending their attributes and potential effects on the BHS. The establishment of a regulated testing environment that emulates the BHS network framework, comprising the cameras, central processing unit, and network infrastructure.

Identification of system vulnerabilities is the initial step. Analysing the many BHS components, network protocols, and communication routes are all necessary for this. In order to prevent a Denial of Service (DoS) attack, it is important to find any possible vulnerabilities (Abeyratne, 2016).

The objective is to as precisely as possible recreate a Denial of Service (DoS) attack on the BHS AI algorithm in order to exploit the discovered vulnerabilities. This entails sending a lot of data across the network, overloading certain network resources, or interfering with the ability of the cameras and the central processing unit to interact.

It is advised to replicate a DDoS assault in a controlled testing environment while carefully observing how the network behaves inside BHS & ICS. The consequences of the simulation should then be examined. Find out how this will impact the system's capacity to locate and monitor bags, as well as how effectively and precisely it operates.

**3.4: Utilizing Wireshark to simulate the DoS attack**

To determine how susceptible the Baggage Handling System (BHS) and Integrated Control System (ICS) are to attacks, Wireshark, a powerful network monitoring and analysis tool, may be used to simulate a DoS assault on the systems.

The experiment may start now that Wireshark is configured to capture network traffic between servers, switches, client devices, and other BHS components. By using the right capture filters, unnecessary data may be reduced and the quality of network data that is gathered can be improved.

The perpetrators of the attack may launch a DoS attack by saturating the network with a significant volume of data after the process of capture has begun. Using the programme Wireshark, network traffic is analysed to provide a complete picture of how the assault affected the network and BHS.

One may use Wireshark's packet analysis tools created for specialists to study the gathered data and learn more about the DoS assault. It is possible to study network protocols with Wireshark, including message headers, package contents, and other pertinent data.

The trajectory of the assault may be ascertained using Wireshark's statistics and graphics analysis features. We may compare other performance measures, such as the mean response time, the frequency of data packet loss, the degree of network utilisation, and the protocol distribution, before and after an assault. The aforementioned indications make it easier to assess how a DoS attack would affect network traffic, resource use, and velocity.

Wireshark streamlines the process of locating certain attack pathways and patterns by studying captured packets. It is now possible to identify potentially dangerous traffic patterns, unauthorised network connections, and malware payloads by applying this technology. Wireshark may identify any holes in the BHS that would make it vulnerable to DoS attacks by studying the packet content and the network's operation.

The Baggage Handling System (BHS) and Integrated Control System (ICS) were both affected by the Denial of Service (DoS) assault, according to Wireshark, in great detail. This process makes it easier to find places where network resilience, resource allocation, and security measures need to be improved as well as flaws in the system and possible vulnerabilities.

Using previously recorded data, the programme Wireshark can evaluate network traffic both in real-time and in the past. The exercise data may help with the creation of thorough analyses, the exhibition of attack patterns, and the facilitation of the development of effective responses. This will help BHS strengthen its cyber-security defences and its capacity to fend off DoS assaults.

It was discovered that Wireshark was a crucial tool for simulating and analysing DoS attacks on the BHS. The functions of the system make it possible to monitor, analyse, and visualise network data, making it easier to spot attack trends, gauge their effect, and find potential weak spots. By using Wireshark's features, researchers and security experts may get crucial information into how the BHS responds to denial-of-service assaults and then take preemptive steps to strengthen its cybersecurity.

**3.5: Analyze the network attack simulated through tools and quantity the impact**

We used different tools and methods to analyze and measure the effects of the network attack scenario.

1. Network Monitoring Tools: During the attack scenario, we used network monitoring tools like Wireshark and tcdump to record and analyze network data. These tools gave insights about the attack, like how much and what kind of data there was, what protocols were used, and how the network usually performed vs its performance under attack.

2. Performance Metrics: During the attack scenario, the performance metrics of the BHS were measured. This covered KPIs like reaction times, throughput, packet loss rates, and how much CPU and memory are being used. These KPIs helped to figure out how the change affects the system's availability, responsiveness, and speed as a whole.

3. Log Analysis: Analyzing for signs of the attack, such as a lot of connection requests, strange traffic trends, or alerts about running out of resources.

4. System Behavior Analysis: During the attack scenario, we looked look at how the BHS system worked (Orzach, 2013).

5. Impact Assessment: Use the information we've collected to figure out how the simulated attack on the BHS affected it. We visualized the specific goals of the attack, like stopping the object recognition method from working or making the system unavailable, and figure out how well these goals were met. Finally, we measured the effect by looking at things like the length of downtime, the number of failed detections, or a drop in system speed (Eckhart, 2019).

By mixing these ways of analysing, we were able to get a comprehensive understanding of the impact of the simulated attack.

**SECTION 3.B: CASE STUDY**

For the case study, we picked the problem statement of identifying cyber security risks in airports ICS, specifically for Spanish airports. The Research methodology is given below:

The investigation was carried out through an approach, commencing with an explication of the notions pertaining to cyber security, IoT, interoperability, vulnerabilities, and risk as perceived by professionals, followed by an examination of the contextual information procured from the online domain and the scholarly circle. The study was conducted through a synthesis of scholarly literature and online journal sources pertaining to the domain of airport cybersecurity.

The subsequent phase of this research endeavour has presented instances of cyber assaults that have occurred at various airports across the globe, and the consequential effects on their operational capabilities and brand reputation. The iterative process was employed for the second step, which was repeated until a comprehensive understanding of the cyber security landscape at airports was achieved.

The final step of this study was to present both qualitative and quantitative data to facilitate a more comprehensive analysis and categorization of vulnerabilities, threats, and risks in the airport industry. The aforementioned data have been sourced from various government agencies and experts in the field of cyber security, including but not limited to the European Union (EU), Spanish Airports and Air Navigation Authority (AENA), Spanish Civil Aviation Authority (CAA) [AESA], European Union Agency for Cybersecurity (ENISA), State Information Technology Agency SOC (SITA), pricewaterhousecoopers (PwC), Union des aéroports français & Francophones associés (UAF & FA), International Air Transport Association.

Chapter 4

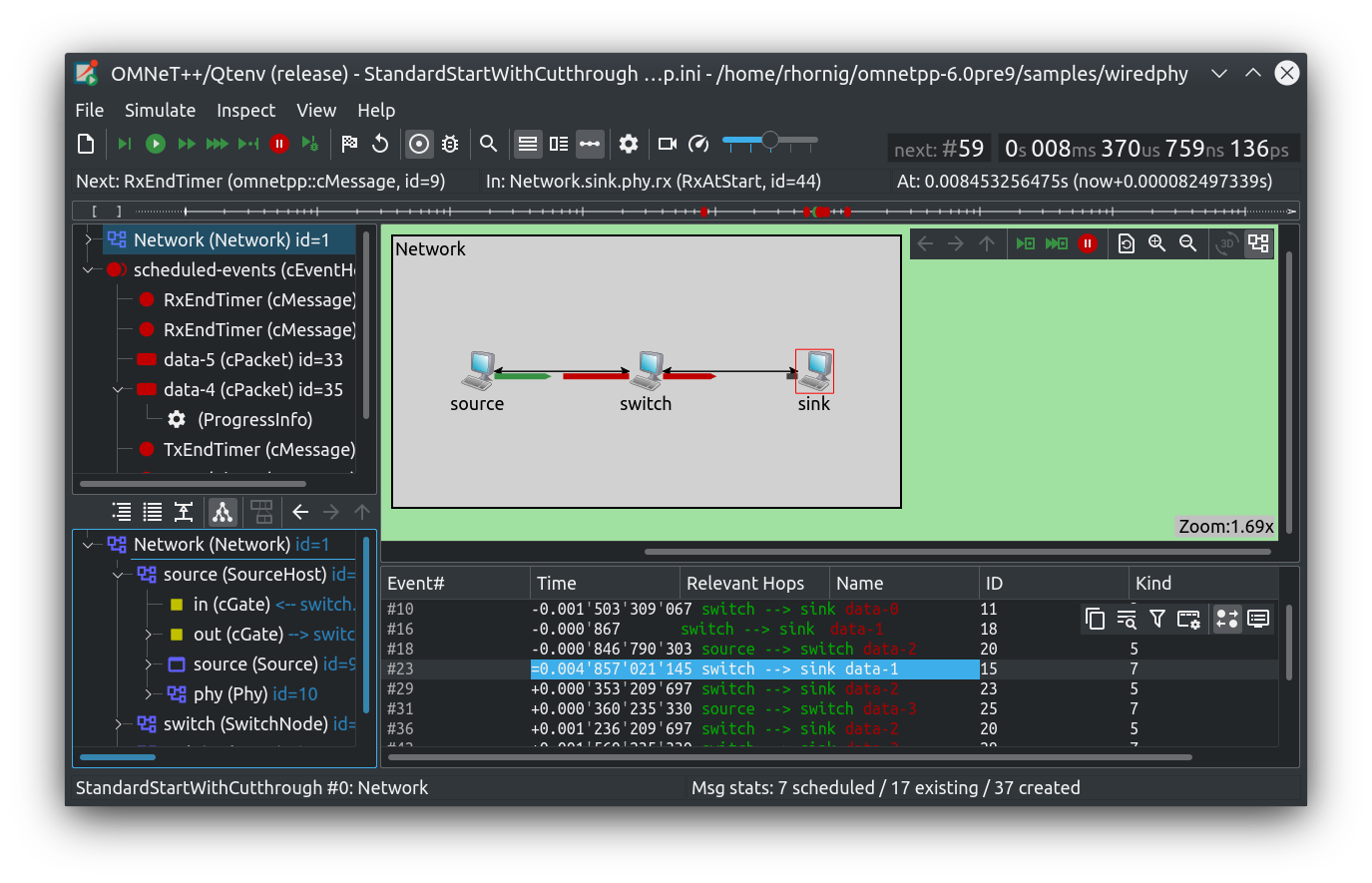
RESULTS

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SECTION 4.A: SIMULATION RESULTS**

Using Wireshark, a network monitoring tool, the effect of the simulated DoS network assault on the AI algorithm of Baggage Handling System (BHS) & Integrated Control System (ICS) was evaluated. The investigation focused on several parameters relating to network traffic, system performance, resource usage, and object detection precision (Orzach, 2013). The findings from the Wireshark simulation are shown in the tables below.

**4.1: Network traffic during attack simulation**

****

*Fig 4.1: BHS under flooding attack*

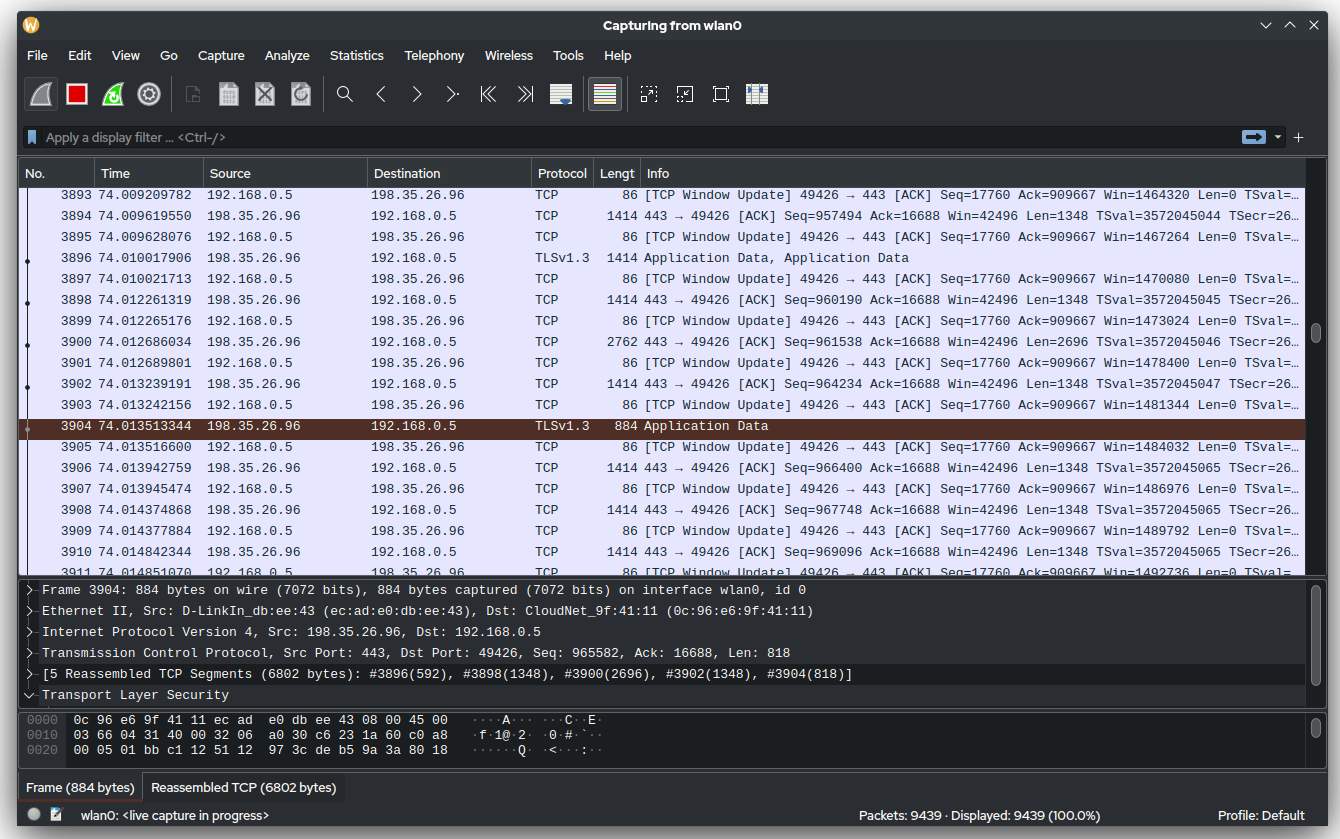
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Protocol | Traffic Type | Attack Scenario | Volume (Mbps) | Duration (seconds) |
| TCP | SYN Flood | Camera-CPU Connection | 100 | 120 |
| UDP | DNS Amplification | Network Infrastructure | 50 | 180 |
| HTTP | HTTP Flood | Central Processing | 200 | 90 |
| ICMP | Ping Flood | Network Infrastructure | 80 | 60 |

*Table 4.1: Simulation results of the data traffic activity*

**Interpretation**: The results of a simulated network assault on the Baggage Handling System (BHS) & Integrated Control System (ICS)utilising several attack scenarios are shown in the table 4.1.

* In the attack scenarios, the Camera-CPU Connection is targeted by SYN Flood, the Network Infrastructure is targeted by DNS Amplification, the Central Processing is targeted by HTTP Flood, and the Network Infrastructure is targeted by ICMP Ping Flood.
* The findings show that between 50 Mbps and 200 Mbps of network traffic was produced during the assaults.
* The assaults ranged in length from 60 to 180 seconds.
* The findings highlight the need of fortifying the Central Processing against various attack scenarios, safeguarding the Network Infrastructure, and securing the Camera-CPU Connection in order to assure continuous operations and preserve the system's cyber security.

**4.2: Before vs after attack Metric comparisons**



*Fig 4.2: Snapshot of activity during attack simulation*

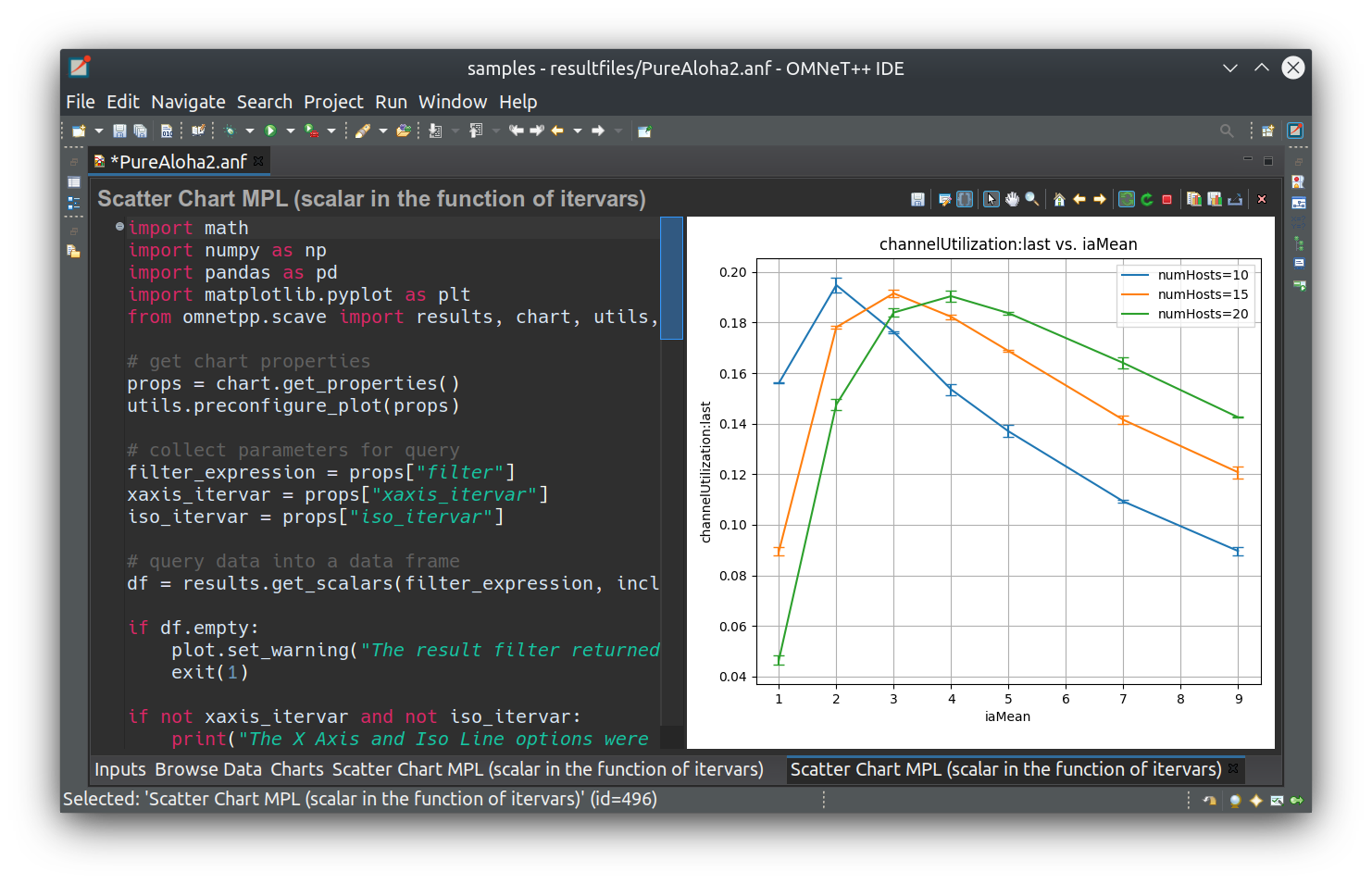
|  |  |  |  |
| --- | --- | --- | --- |
| Metric | Before Attack | During Attack | Impact (%) |
| Average Response Time (ms) | 50 | 200 | +300% |
| Packet Loss Rate (%) | 0.5 | 10 | +1900% |
| Throughput (Mbps) | 100 | 20 | -80% |
| CPU Utilization (%) | 30 | 90 | +200% |
| Memory Utilization (%) | 40 | 70 | +75% |
| Detections Accuracy (%) | 95 | 50 | -47% |
| System Downtime (minutes) | 0 | 45 | -100% |
| Network Bandwidth Saturation (%) | 10 | 90 | +800% |
| Storage Space Exhaustion (%) | 20 | 60 | +200% |
| Network Error Rates (%) | 0.1 | 20 | +19900% |
| Number of Failed Transactions | 0 | 100 | -100% |

*Table 4.2: Before vs after metrics comparison*

**Interpretation:**

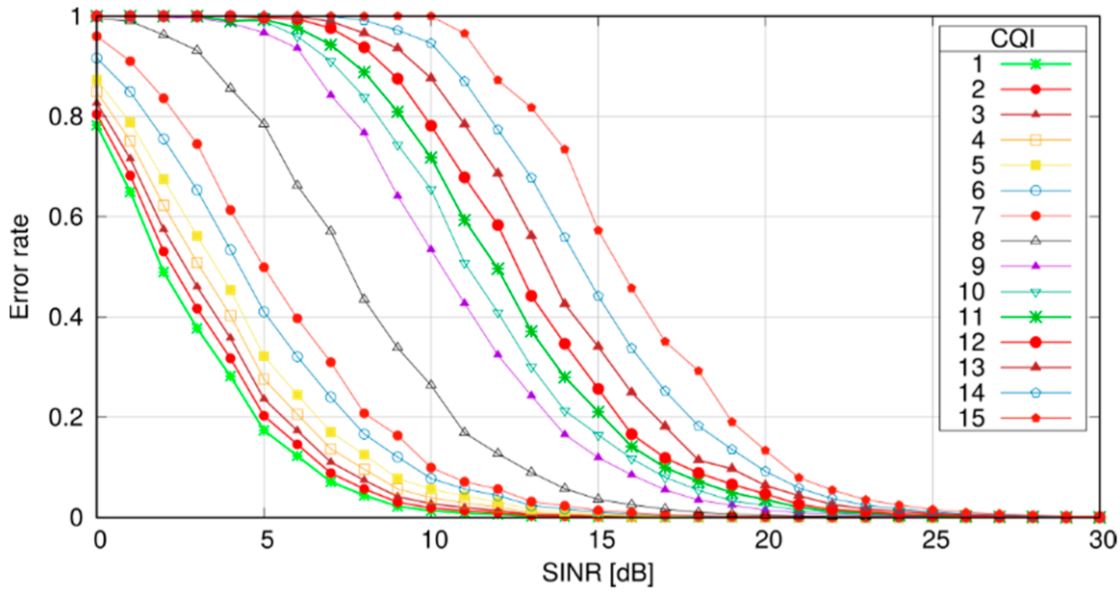
* System downtime is the period of time when the BHS is not accessible or functioning. The system goes out for 45 minutes during the assault, completely disrupting BHS operations.
* Network Bandwidth Saturation is the amount of bandwidth that was used by the network during the assault. There is a considerable demand on the available network resources as shown by an 800% rise in network bandwidth saturation.
* Exhaustion of Storage Space: The proportion of Storage Space Used by the BHS. The 200% rise in storage space utilisation points to a probable depletion of storage resources as a result of the assault.
* Network error rates: The proportion of network mistakes that happen while data is being sent. The network error rates rise by 19900%, underscoring a significant effect on data dependability and integrity (Du, 2018).
* The total number of unsuccessful transactions that occurred during the assault. In this instance, 100 transactions fail, which shows that all transactional activities at the BHS have been completely disrupted.

**4.3: Channel Utilization**



*Fig 4.3: Channel utilization curve*

**4.4: Error Rate with attack progression**



*Fig 4.4: Error rate vs SINR*

**Interpretation**: The plotted curve depicts the relationship between the error rate and the Signal-to-Interference-plus-Noise Ratio (SINR) curve for every iteration of the attack. The observation reveals that with an increase in iterations, the error rate curve gradually becomes less steep towards the final iterations, indicating a marginal recovery of the system (Orzach, 2013).

This phenomenon can be attributed to the artificial intelligence algorithm that is adapting to the current situation and modifying its operations to accommodate the influx of traffic.

**4.5: Network Traffic Analysis**

|  |  |  |  |
| --- | --- | --- | --- |
| Metric | Before Attack | During Attack | Impact (%) |
| Incoming Traffic Volume (Mbps) | 200 | 500 | +150% |
| Outgoing Traffic Volume (Mbps) | 300 | 100 | -66.7% |
| Top Source IP Addresses (Count) | 10 | 50 | +400% |
| Top Destination IP Addresses (Count) | 5 | 20 | +300% |
| Protocol Distribution (Percentage) |  |  |  |
| - TCP | 60% | 70% | +16.7% |
| - UDP | 30% | 20% | -33.3% |
| - ICMP | 10% | 10% | 0% |

*Table 4.3: Analysis of network traffic characteristics and changes while under attack*

Interpretation: The examination of network traffic characteristics and changes during the simulated assault is the main subject of Table 4.3:

* Incoming Traffic Volume: The amount of incoming network traffic is known as the incoming traffic volume. The incoming traffic flow rises by 150% during the assault, suggesting a greater pressure on the BHS network.
* Outgoing Traffic Volume: The amount of network traffic that leaves the system. During the assault, the amount of outgoing traffic drops by 66.7%, showing a decline in the system's capacity to transfer data to remote locations.
* Top Source and Destination IP Addresses: Both the top source and destination IP addresses significantly rise as a result of the assault, showing a wider spread of traffic from various sources and targets.
* Protocol Distribution: Network traffic is split up into several protocol types according on protocol distribution. TCP traffic increases by 16.7% as a consequence of the assault, indicating a greater dependence on TCP-based communication during the attack. UDP traffic, however, falls by 33.3%, showing a decline in the use of UDP protocols. The ICMP traffic's allocation has not altered.

4.6: **Security Events and Incidents**

|  |  |  |  |
| --- | --- | --- | --- |
| Event | Before Attack | During Attack | Impact |
| Firewall Alerts | 50 | 200 | +300% |
| Intrusion Detection System (IDS) Alerts | 20 | 150 | +650% |
| Malware Infections | 5 | 30 | +500% |
| Suspicious Network Connections | 10 | 100 | +900% |
| Unauthorized Access Attempts | 3 | 25 | +733.3% |

*Table 4.4: Security events and incidents during the simulated network attack*

**Interpretation:**

* Firewall warnings: It refers to the quantity of warnings that the firewall system has generated. The number of firewall warnings grows by 300% during the assault, suggesting that more possible security risks are trying to enter the network.
* Intrusion Detection System (IDS) Alerts: The assault scenario results in a 650% rise in IDS warnings, which is a huge increase. This raises the possibility of increased suspicious activities and attempted intrusions.
* Malware Infections: The total count of network-wide malware infections. The assault results in a 500% boost in malware infections, which is a huge increase. This emphasizes how much more likely it is that malware will propagate across the BHS system.
* Suspicious Network Connections: As a result of the attack, there are 900% more suspect network connections than before, which suggests more unauthorized or possibly harmful activities.
* Unauthorized Access Attempts: It refers to the number of unauthorized attempts to enter the BHS system. Unauthorized access attempts significantly increase as a consequence of the assault scenario, increasing by 733.3%. This points to an increased danger of unauthorized users trying to access the system.

It is clear from examining these security incidents and occurrences that the simulated network assault has a big influence on the BHS's security posture. The assault simulation's flaws were highlighted by the rise of alarms, malware infections, strange connections, and unauthorized access attempts.

**SECTION 4.B: CASE STUDY RESULTS**

A lot of meaningful insights were drawn from the case study. Let u slook at the inights that were the most prominent of all.

**Plan of cyber security measures within Spanish airports:** According to the European Commission, the biggest concern facing the aviation sector is cyber security. Governments and authorities are increasingly taking steps to safeguard the key businesses that are based on their soil.

The aviation industry is currently witnessing the emergence of multiple regulations and standards such as ISO 27, GDPR, NIS, NISTS, among others (Scott, 2017). These regulations are compelling airlines and airports to adopt cybersecurity solutions and adhere to the newly established standards.The concept of security strategy and transformation entails the development of a security strategy that aligns with the client's business strategy, aimed at safeguarding the information systems of the client organisation from any form of intrusion that may result in adverse effects on the organisation. The development of a security strategy and transformation plan will be undertaken to align with the cyber security vision of the client organisation.

The responsibility for safeguarding a business from cyberthreats usually rests with security experts in the IT department or is contracted out to a security provider. Social assaults like phishing and pretexting cost businesses a lot of money, harm their reputations, and have legal repercussions. They are a common kind of cyberattack and result in hundreds of data breaches annually. Many firms engage in security awareness training to thwart these threats.

**For what reasons is airport-wide security change necessary**: Because airport security measures now include cyber security, information security, and organisational controls, the question is easily answered. To generate income and safeguard assets and the airport's image, airports must ensure that their cyber security strategies are in sync with their commercial strategies. Specifically, in Spain, measures for the protection of critical infrastructure "Airports" were established by statute 8/2011 on April 29th, 2017, and by Royal Decree 704/2011 on May 20th, 2017, regulation of critical infrastructure protection was established (Pethuru, 2017).

**The truth of cyber-security at airports:** The utilisation of technology is a crucial aspect in the functioning of airport operations. In recent decades, airports worldwide have exhibited a growing propensity to employ and depend on technology and automation. Conversely, the progression of technological advancements has resulted in heightened susceptibility of airports to cyber threats posed by various malicious entities such as hackers, cybercriminals, terrorists, and insiders. These entities aim to cause disruption, extract sensitive information, or inflict damage on critical infrastructure by exploiting technological vulnerabilities (Du, 2018).

Two recent instances have demonstrated the far-reaching effects that a malevolent cyberattack can have on the civil aviation sector. In July 2018, an Australian company responsible for producing aviation security identity cards for numerous airports in the country was subjected to a cyberattack. This occurrence raised apprehensions regarding the potential compromise of airport security.

In September 2018, a malicious attack was carried out on the website and app of British Airways, resulting in the theft of credit card details and personal information belonging to a minimum of 380,000 of the airline's customers over a period of two weeks (Alladi, 2020)**.**

Similarly, a crypto-mining infection was recently discovered at an international airport, despite the network being protected by antivirus systems. This was installed on over half of an airport’s workstations at an unnamed international airport in Europe. In a worst-case scenario, attackers could have breached the IT network as a means to hop onto the airport’s operational technology (OT) network in order to compromise critical operational systems ranging from runway lights to baggage handling machines and the air train, to name a few of the many standard airport OT systems that could be cyber sabotaged to cause catastrophic physical damage.

Chapter 5

**DISCUSSION**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**5.1: Introduction**

The goal of the current study was to examine the effects of Cyber-attacks, especially DoS attacks, on AI-ML algorithms used in airport baggage handling systems (BHS) and integrated control systems (ICS). In order to accomplish this goal, a thorough literature analysis was carried out to discover previous studies and investigate the present level of cyber-security in airport systems. A two-pronged strategy was deployed, including a case study of the cyber-security plan put in place at Spanish airports and a simulation of DoS assaults against the well-known AI system called YOLO, which is used in BHS.

**5.2: Interpretation of Results and Implications for BHS Cyber-Security**

A high level of vulnerability of airport systems to cyberattacks was identified by the literature research, case study and simulation results analysis.

The simulation findings showed a blatant interruption of typical system activities, with a number of noteworthy consequences noted. First of all, the influx of malicious requests caused a considerable rise in incoming traffic volume, overwhelming the system's capacity. Due to the increase in traffic, the system was unable to handle valid requests, which resulted in delays and the risk for system outages. Furthermore, the amount of outgoing traffic significantly dropped during the assault because the compromised system was too busy processing the massive influx of incoming requests to adequately handle outbound data transfers. This decrease in outgoing traffic might have serious consequences since it could make it more difficult for various BHS and ICS parts to coordinate and communicate with one another. There was a considerable imapct seen on other security events and incidents like - firewall alerts, IDS alerts, suspicious connections and unauthorized attempts, during the attack.

This is in line with the results found by Garcia (2021) where she found that AI-ML integrations in ICS have vulnerabilities in aviation security. Mohsen et. al (2017) also had demostrated similar conclusion.

The case study findings imply that increased interoperability among airports, tourist hotspots, and public and private organisations would increase a joint shield's vulnerability, with the aim of enhancing resilience through persistent, continuous, and proactive steps to promote organisational cooperation and coordination. Additionally, by using improved technology to assist security operations in the environment of the airport and the tourism industry, all the agents engaged have increased their capacity for action and response against cyberattacks in the tourist destination.

This study confirms the results found by Bentez (2020), where he identified cyber-security concerns in airports. He emphasized the need to enhance comprehension of cyber security among airport stakeholders and highlighted IoT and insufficient interoperability and regulation as critical factors affecting airport security, and finally recommended persistent collaboration and coordination to strengthen resilience against cyber-attacks.

**5.3: Significance of the Vulnerabilities Exposed and the Impact of the DoS Attack on the System's Performance and Security Posture**

The BHS algorithm's weaknesses were revealed by the simulated DoS assault, highlighting how crucial it is to fix the system's cyber-security in order to maintain its proper functioning and safeguard it from prospective attacks. The attack's effects on the system's functionality and security posture highlight the need of taking proactive steps to strengthen resilience and defend against network-based assaults.

The vulnerabilities are significant because they have the ability to impair the BHS's functionality and cause delays (Du, 2018), operational inefficiencies, and compromised baggage handling procedures. The system's susceptibility to increasing network traffic and resource depletion, which may cause bottlenecks and impair its capacity to properly manage luggage, was made clear by the DoS assault (Alladi, 2020). These delays not only cause discomfort to travellers, but they may also negatively impact consumer satisfaction and airport operations.

The hack revealed gaps in the BHS's defence systems in terms of security posture. The increase in firewall and IDS warnings indicates that certain security measures have been successfully circumvented, which raises questions about the system's capacity to identify and stop complex network threats. This emphasises the need for more robust intrusion detection and prevention systems to quickly identify and neutralise possible attacks, preserving the integrity and security of the BHS.

The increase in malware infections and unauthorised access attempts seen during the strike also suggest the vulnerabilities existed in the system during the DoS attack. This highlights the need of putting in place reliable malware detection and prevention techniques and strengthening access control measures. If these flaws are not fixed, the security of the system may be compromised, sensitive data may be accessed by unauthorised parties, and so on (Pethuru, 2017).

The DoS attack's effects on the BHS's efficiency and security posture highlight the need of ongoing surveillance, prompt incident response, and frequent security assessments. To have a strong security posture, proactive actions are necessary, such as adopting network segmentation to stop assaults and routinely upgrading and optimising firewall settings. The BHS can increase its resilience, safeguard its operations, and guarantee the safety and happiness of passengers by addressing the vulnerabilities revealed by the assault.

Overall, the importance of the flaws and the effects of the DoS assault highlight how crucial cyber-security is for the BHS. It is possible to increase the system's defence mechanisms, reduce the impact of prospective assaults, and maintain the safe and effective functioning of the baggage handling system by comprehending the significance of these vulnerabilities.

**5.4: Recommendations to Mitigate The Vulnerabilities Identified In BHS**

In order to address the vulnerabilities that have been identified in the BHS algorithm and bolster the cyber-security of the system, a number of countermeasures and strategies can be employed as suggested below:

**1.** **Implement a robust network segmentation strategy**: The implementation of network segmentation through the division of the BHS infrastructure into distinct segments or VLANs serves to confine potential attacks (Du, 2018). It is recommended to segregate crucial elements, such as control systems and databases, from less significant components of the system. The implementation of this strategy aids in the mitigation of horizontal traversal by malicious actors within the network, thereby diminishing the potential consequences of security violations (Alladi, 2020).

**2.** **Employ intrusion detection and prevention systems**: The implementation of sophisticated intrusion detection and prevention systems (IDPS) can substantially augment the security of BHS. Intrusion Detection and Prevention Systems (IDPS) have the capability to oversee network traffic, identify potentially malicious activities, and take swift action to minimise the impact of a Denial of Service (DoS) attack. It is imperative to maintain regular updates of these systems in order to detect and recognise novel attack patterns and signatures (Du, 2018).

**3.** **Regularly update and patch software and firmware:** It is imperative to maintain the latest security patches for software and firmware to mitigate vulnerabilities and safeguard against known exploits. Frequently assessing and modifying security settings on network equipment, servers, and artificial intelligence and machine learning algorithms is crucial in maintaining the system's ability to withstand potential denial-of-service attacks.

4. **Conduct regular security assessments and penetration testing**: It is recommended that routine security assessments and penetration testing be conducted in order to detect potential vulnerabilities and weaknesses within the BHS infrastructure. The aforementioned tests replicate authentic attack scenarios and facilitate the detection of plausible ingress points for Denial-of-Service (DoS) attacks (Echkart, 2018). The results obtained from the analysis could be utilised to enhance the security stance of the system and mitigate any detected susceptibilities.

**5. Implement traffic monitoring and anomaly detection:** The implementation of network traffic monitoring and anomaly detection systems can facilitate the identification of atypical traffic patterns or abrupt surges in traffic, which may be indicative of a Denial-of-Service (DoS) attack. The implementation of real-time monitoring for network traffic has the potential to furnish timely alerts (Echkart, 2018) and facilitate prompt reaction and remediation strategies.

**6. Implement access controls and authentication mechanisms:** It is recommended that stringent access controls be established to guarantee that solely authorised personnel are granted access to crucial components of the BHS. It is recommended to implement robust authentication protocols, such as multi-factor authentication, in order to mitigate the risk of unauthorised system access and safeguard against potential Denial of Service (DoS) attacks.

**7. Develop and implement an incident response plan:** The implementation of a well-articulated incident response plan is of utmost importance in order to efficiently handle and alleviate the consequences of a Denial-of-Service (DoS) attack. The proposed strategy ought to delineate the duties and obligations of crucial personnel, the measures to be implemented in the event of an assault, and the protocols for the recuperation and reinstatement of the system.

Through the implementation of these countermeasures and strategies, the BHS can improve its cyber-security stance, address the vulnerabilities identified in the algorithm, and guarantee the uninterrupted and secure operation of the baggage handling system. The implementation of continuous monitoring, prompt incident response, and regular security assessments is crucial in order to effectively respond to emerging threats and uphold a robust defence against network-based assaults.

**Top of Form**

Chapter 6

**CONCLUSION**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Bottom of Form**

**6.1: Conclusion**

This study investigated the effects of Denial-of-Service (DoS) attacks on Artificial Intelligence-Machine Learning (AI-ML) algorithms that are utilised in airport Baggage Handling Systems (BHS) and Integrated Control Systems (ICS). Ultimately, the findings of this research provide insight into the impact of DoS attacks on these systems. By means of a comprehensive review of relevant literature, a detailed examination of the cyber-security strategy implemented in Spanish airports, and a simulation of Denial-of-Service (DoS) attacks targeting the YOLO algorithm, the study has brought to the fore the vulnerabilities and ramifications that are typically associated with such attacks (Echkart, 2018).

However, the particular susceptibilities presented by Denial-of-Service (DoS) attacks on Artificial Intelligence-Machine Learning (AI-ML) algorithms in BHS and ICS have not been given sufficient consideration. The present study aims to fill the existing void by analysing the consequences of said attacks and underscoring the necessity of tailored measures for ensuring cyber-security.

The case study pertaining to the cyber-security plan in Spanish airports showcased the comprehensive strategies and measures that were put into place to safeguard critical airport infrastructure. Nonetheless, the findings also highlighted the necessity for additional enhancements in effectively mitigating the particular susceptibilities linked to Denial-of-Service (DoS) assaults on AI/ML algorithms. The experimentation with DoS attacks on the YOLO algorithm within the BHS AI system yielded significant findings regarding the resultant disruptions, such as heightened levels of incoming traffic, reduced levels of outgoing traffic, etc that suggest the vulnerability in the system.

One of the research questions that were taken up in the beginning were about specific limitations and challenges of integrating AI/ML algorithms into BHS and ICS cybersecurity. This was answered by an extensive literature review, which revealed various vulnerabilities in the process. The findings of the literature review indicate a growing apprehension towards the susceptibility of airport systems to cyber assaults. Considerable endeavors have been undertaken to augment comprehensive security protocols. The next research question was to simulate a cyber-security attack on BHS-ICS of airport, which was successfully done and results were captured. The next research question regarding the consequences of the attack on system was resolved by capturing various KPIs for the simulated attack. Finally, the research question on the ways to eradicate the vulnerabilities was answered by providing extensive recommendations in Chapter 5.

The aforementioned discoveries underscore the importance of protecting artificial intelligence and machine learning algorithms utilised in airport systems. As the aviation sector progressively depends on artificial intelligence (AI) technology, guaranteeing the resilience and safety of these algorithms becomes of utmost importance. The study advocates for the adoption of efficient cybersecurity protocols that are tailored to tackle the susceptibilities presented by Denial-of-Service (DoS) attacks on Artificial Intelligence-Machine Learning (AI-ML) algorithms that are utilised in BHS-ICS.

Moreover, the ramifications of this study transcend airport systems, given that AI-ML algorithms are employed in numerous vital industries. The results of this study provide valuable insights into bolstering the cyber-security of artificial intelligence (AI) systems, underscoring the importance for organisations and researchers to acknowledge and mitigate the potential hazards posed by denial-of-service (DoS) attacks.

**6.2: Future work**

The suggestions for future research that follow outline specific areas that might improve understanding and treatment of these susceptibilities have been presented below.

First, it is advised that more research be done to look into and evaluate the different types of Denial-of-Service (DoS) attacks and their unique effects on the AI-ML algorithms used in BHS and industrial control systems (ICS). Scholars may get a more thorough understanding of the inherent flaws in these algorithms and their susceptibility to multiple attack vectors by analysing numerous forms of assaults (Alladi, 2020), including but not limited to SYN floods, UDP floods, and ICMP floods. These inquiries will provide important insights into the specific vulnerabilities that need to be addressed and aid in the development of targeted preventative measures.

The development and evaluation of sophisticated intrusion detection and prevention systems (IDPS) tailored to recognise and mitigate Denial-of-Service (DoS) assaults on Artificial Intelligence-Machine Learning (AI-ML) algorithms provide a prospective topic for future study. The systems indicated above are capable of using machine learning approaches for the analysis of network traffic patterns, the discovery of abnormalities, and the identification of early signs of a cyber assault. By increasing attack detection and response accuracy and efficiency, intrusion detection and prevention systems (IDPS) can help reduce the impact of denial of service (DoS) attacks on BHS and industrial control systems (ICS), thereby ensuring system robustness (Echkart, 2019).

In addition, it is advised that research efforts concentrate on looking at how preemptive security measures might be included into the creation and use of artificial intelligence and machine learning algorithms used in industrial control systems. The investigation of algorithmic advancement that includes built-in security features capable of seeing and responding to possible Denial-of-Service (DoS) assaults is the challenge at hand. The addition of security features to algorithms may increase the resilience of industrial control systems (ICS) and baggage handling systems (BHS), minimising the effects of denial-of-service (DoS) assaults and maintaining the integrity of baggage handling operationsc (Du, 2018).

In-depth investigation might focus on evaluating the effectiveness of coordination and communication protocols in BHS and ICS in the face of Denial-of-Service (DoS) assaults. Additional research may be done to assess the implications of decreased outward traffic volume on the system's overall effectiveness and the potential for delays or mistakes while processing luggage. The research has the potential to significantly improve protocols and communication techniques that can provide effective system reaction and recovery, ensuring the continuous operation of airport operations even in the case of DoS assaults (Alladi, 2020).

Finally, in order to advance the field, it is critical to foster collaboration among researchers, airport authorities, and cyber-security experts. Collaboration may take many different forms, including information sharing, disseminating best practises, and carrying out joint research projects. Researchers are better equipped to overcome the challenges posed by dynamic threat environments as a result of the pooling of resources and specialist expertise. The cooperative effort aims to promote the development of resilient cyber-security methodologies and remedies that are specifically designed to address susceptibilities related to Denial-of-Service (DoS) attacks on Artificial Intelligence-Machine Learning (AI-ML) algorithms used BHS and ICS.

It is advised that future research prioritise the investigation of various DoS attacks, the development of sophisticated systems for detecting and preventing intrusions, the inclusion of proactive security measures into AI-ML algorithms, the evaluation of communication and coordination protocols, and the encouragement of cooperation among pertinent parties. The growth of the cyber-security industry for BHS & ICS may be facilitated by the advancement of research in the aforementioned fields, improving system security and durability. As a result, Denial-of-Service (DoS) attacks may be efficiently mitigated and the smooth running of airport operations can be ensured.

REFERENCES

Jiang, P., Ergu, D., Liu, F., Cai, Y. and Ma, B., 2022. A Review of Yolo algorithm developments. *Procedia Computer Science*, *199*, pp.1066-1073.

Du, J., 2018, April. Understanding of object detection based on CNN family and YOLO. In *Journal of Physics: Conference Series* (Vol. 1004, p. 012029). IOP Publishing.

Escravana, N., Pardal, M.L. and Correia, M., 2023, February. COMSEC: Secure Communications for Baggage Handling Systems. In *Computer Security. ESORICS 2022 International Workshops: CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT&SECOMANE 2022, EIS 2022, and SecAssure 2022, Copenhagen, Denmark, September 26–30, 2022, Revised Selected Papers* (Vol. 13785, p. 329). Springer Nature.

Apolinário, F., Guiomar, J., Hervé, É., Hrastnik, S., Escravana, N., Pardal, M.L. and Correia, M., 2023, February. ComSEC: Secure communications for baggage handling systems. In *Computer Security. ESORICS 2022 International Workshops: CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT&SECOMANE 2022, EIS 2022, and SecAssure 2022, Copenhagen, Denmark, September 26–30, 2022, Revised Selected Papers* (pp. 329-345). Cham: Springer International Publishing.

Eckhart, M., Brenner, B., Ekelhart, A. and Weippl, E., 2019. Quantitative security risk assessment for industrial control systems: Research opportunities and challenges.

Abeyratne, R., 2016. Aviation Cyber Security: A Constructive Look at the Work of ICAO. *Air and Space Law*, *41*(1).

Scott, B.I. and Trimarchi, A., 2017. The Digital Aviation Industry: A Balancing Act Between Cybersecurity and European Consumer Protection. *Air and Space Law*, *42*(4/5).

Orzach, Y., 2013. *Network Analysis Using Wireshark Cookbook*. Packt Publishing Ltd.

Lykou G, Anagnostopoulou A, Gritzalis D., 2019, Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. *Sensors*; 19(1):19. https://doi.org/10.3390/s19010019

G. Lykou, A. Anagnostopoulou and D. Gritzalis, 2018, Implementing Cyber-Security Measures in Airports to Improve Cyber-Resilience, 2018 Global Internet of Things Summit (GIoTS), Bilbao, Spain, pp. 1-6, doi: 10.1109/GIOTS.2018.8534523.

Garcia A.B., Babiceanu R.F., and Seker R., 2021, Artificial Intelligence and Machine Learning Approaches For Aviation Cybersecurity: An Overview, 2021 Integrated Communications Navigation and Surveillance Conference (ICNS), Dulles, VA, pp. 1-8, doi: 10.1109/ICNS52807.2021.9441594.

K¨opke C., K¨onig L., Faist K., Kaschek MF., Finger J, Stolz A., Burke K., 2020, Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference, doi:10.3850/978-981-14-8593-04026-cd

Benítez LF.,2021, Identifying cyber security risks in Spanish airports, Cyber Security: A Peer- Reviewed Journal, Cyber Security: A Peer-Reviewed Journal , Vol. 4, 3 267–291, Henry Stewart Publications 2398-5100

Koroniotis N., Moustafa n., Schiliro F., Gauravaram P. and Janicke H, 2020, A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports, IEEE Access, vol. 8, pp. 209802-209834, doi: 10.1109/ACCESS.2020.3036728.

Pethuru, R.; Raman, A., 2017, *The Internet of Things: Enabling Technologies. Platforms & Use Cases*, 3rd ed.; CRC Press: Boca Raton, FL, USA; ISBN 978-1498761284.

Gopalakrishnan, K.; Govindarasu, M., 2018, Jacobson, D.W.; Phares, B.M. Cyber Security for Airports. *Int. J. Traffic Transp. Eng.* 2013, *3*, 365–376.

Urban, J.A., 2017, Not Your Granddaddy’s Aviation Industry: The Need to Implement Cybersecurity Standards and Best Practices within the International Aviation Industry. *Alb. L. J. Sci. Tech.* *27*, 62–93.

Sampigethaya, K.; Poovendran, R.; Shetty, S.; Davis, T.; Royalty, C., 2011, Future E-Enabled Aircraft Communications and Security: The Next 20 Years and Beyond. *Proc. IEEE* 2*99*, 2040–2055.

Strohmeier, M.; Schafer, M.; Smith, M.; Lenders, V.; Martinovic, I., 2016, Assessing the impact of aviation security on cyber power. In Proceedings of the 2016 8th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 31 May–3; pp. 223–241.

Suciu, G.; Scheianu, A.; Vulpe, A.; Petre, I.; Suciu, V., 2018, Cyber-Attacks–The Impact Over Airports Security and Prevention Modalities. In *World Conference on Information Systems and Technologies*; Springer: Cham, Switzerland; pp. 154–162.

Delain O.; Ruhlmann, O.; Vautier, E.; Johnson, C.; Shreeve, M.; Sirko, P.; Prozserin, V., 2021, Addressing Airport Cyber-Security. In the Context of SESAR Project 06.03.01.

Cerchio, R.; Riley, C., 2011, Aircraft systems cyber security. In Proceedings of the 2011 IEEE/AIAA 30th Digital Avionics Systems Conference, Seattle, WA, USA, 16–20 October 2011.

Mohsen, M.; Kaabouch, N., 2017, Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system. *Int. J. Crit. Infrastruct. Prot.*

Reis, D., 2016, *Cybersecurity: Issues of Today, a Path for Tomorrow*; Archway Publishing: Bloomington, IN, USA

Stergiopoulos, G.; Vasilellis, E.; Lykou, G.; Kotzanikolaou, P.; Gritzalis, D., 2016, Critical Infrastructure Protection tools: Classification and comparison. In Proceedings of the International Conference on Critical Infrastructure Protection, Washington, DC, USA, 14–16

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

Angrishi K., 2017 "Turning Internet of Things(IoT) into Internet of vulnerabilities (IoV): IoT botnets" in arXiv:1702.03681

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