National College of Ireland

MSc Research Project

Mitigating Cyber Risks in Next-Generation Aircraft: Securing Flight Control Systems from Remote Cyber Attacks

Master of Science in Cybersecurity

Rahul Nalwale

Student ID: 22194339

School of Computing

National College of Ireland

Supervisor: Michael Pantridge

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Rahul Raju Nalwale
Student ID:	22194339
Programme:	MSC Cybersecurity **Year:** 2023-2024
Module:	Practicum
Supervisor:	Michael Pantridge
Submission Due Date:	12-08-2024
Project Title:	**Mitigating Cyber Risks in Next-Generation Aircraft: Securing Flight Control Systems from Remote Cyber Attacks**
Word Count:	10136 **page count**: 29.

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other

author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Rrnalwale

Date: 12-08-2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Mitigating Cyber Risks in Next-Generation Aircraft: Securing Flight Control Systems from Remote Cyber Attacks

Rahul Nalwale

x22194339

Abstract

The report titled "Mitigating Cyber Risks in Next-Generation Aircraft: “Protection of Flight Control Systems against Remote Cyber Threats” discusses the danger of modern highly integrated avionic systems to cyber threats arising from the developments in the field of aviation. The research lays down the fact that systems are vulnerable to remote cyber-attacks and also offers a solution that involves the use of intelligent algorithms to improve the system's security features. This paper follows a positivist research philosophy that encompasses secondary data analysis to design and compare machine learning approaches to perioperative abnormality identification. The results show that the proposed system has high efficiency in classifying real abnormal flights from those of normal flights reinforcing the role of this study in the domain of aviation. Despite certain drawbacks such as false negatives and problems with real-time processing, the proposed work makes a substantial contribution to the domain of aviation cyber security by developing an appropriate automated and adaptive system which can protect the next generation of aircraft from cyber threats. The research is concluded with recommendations for future work, which involve the incorporation of more precisely composed algorithms and the further application of the introduced system to expand the sphere of aviation security against rising cyber threats.

Chapter1: Introduction

1.1 Background

The Dramatic progress in the technology of building aeroplanes has resulted in the manufacturing of new-generation planes that incorporate complex flight control systems. Such systems as integrated reservation systems, Operations Control Centres, GSMs, and PMSs have made operations efficient, safe for the passengers and vulnerable to cyber threats. A major concern in this field is that as the operation of aircraft becomes integrated into large systems the potential for cyber-attacks originating from remote locations rises and is thus considered an acute issue in the sphere of security (Stelkens- Kobsch et al., 2021).

1.2 Research Problem Statement

The first research question that is raised in this study pertains to the susceptibility of next-generation Automatic Flight Control (AFC) systems to remote cyber threats. This is a clear testimony that traditional forms of security are unable to address the modern forms of threats hence

the need to seek better security mechanisms. The consequences of a cyberattack on these systems are severe including data losses, and complete system failures making this a critical problem (Ukwandu et al., 2022).

1.3 Contribution to the Literature

That is why this research seeks to fill the gap in the extant literature and apply more backdated cybersecurity solutions to the new generation of aeroplanes. The study fulfils the research objectives and, in the process, presents the following significant advances in the field of aviation safety and cybersecurity: It provides a fresh concept of countering cyber threats, which can be implemented in other spheres of the critical infrastructure industry.

1.4 Research Objectives and Questions

The main objectives of this research are to:

- To Identify the specific vulnerabilities within next-generation aircraft flight control systems.
- To Develop and evaluate machine learning-based techniques to enhance the security of these systems.
- To Propose a comprehensive framework for mitigating cyber risks in aviation.

The research is guided by the following questions:

1. What are the prevalent vulnerabilities in current flight control systems?
2. How can machine learning algorithms be applied to detect and prevent cyberattacks?
3. What are the most effective strategies for implementing these algorithms in real-world scenarios?

1.5 Hypotheses

This research assumes that the current flight control systems have recognizable soft spots that can be invaded remotely. The machine learning algorithms can enhance the process of detecting and preserving cyber threats to these systems drastically and the novel security framework based on the machine learning integration into the flight control systems will be appropriate to solve the cyber risks efficiently (Prasad et al., 2023).

1.6 Structure of the Report

The report structure is a Literature Review, Research Methodology, Design Specification, Implementation, Evaluation, Discussion, and Conclusion and Future Work which covers the topics of the existing cybersecurity solutions, threat identification methods, the proposed machine learning framework, application, assessment of the approach's effectiveness, the findings and future work.

Chapter 2: Literature Review

2.1 Introduction to the Literature Review

The topic has been embraced because the advancement in the aviation transport sector means that aircraft of the next generation possess sophisticated flight control systems thus giving significance to cybersecurity. These systems though improving operational effectiveness and safety have brought in new risks that the cyber attackers can leverage. This literature review seeks to categorize and outline various preceding studies on cybersecurity concerns in the aviation industry, specifically about flight control systems' susceptibility and the possibility of utilizing machine learning algorithms to address and minimize the threats. Using the review of previous studies, this review underscores the deficiencies in the current literature and explains why more research is required in this domain.

2.2 Theoretical Framework

As the focus of this literature review lies in the overlap of aviation cybersecurity and machine learning, the theoretical background has been developed from these two fields. Cybersecurity entails awareness of the concepts and measures that are useful in protecting information systems against invasion and malicious acts. In the setting of aviation, this framework is used in the case of protecting flight control systems which are highly important in the functionality of the aircraft (Dave et al., 2022). Alternatively, machine learning is concerned with defining the algorithms capable of learning from the data and making the corresponding predictions. The combination of these two fields can result in new approaches for the identification and protection against cyber threats on aircraft controls.

2.3 Review of Key Studies

Cybersecurity in Aviation

It has therefore emerged as an important issue in aviation as the levels of connectivity and automation of the aircraft increase. Other research work revealed that the flight control system is one of the most vulnerable to cyber threats because of the system includes integration and complexity associated with flight operations. For instance, Wang et al., (2023) called our attention to the weaknesses in the communication interfaces between aeroplanes and ground control networks. These links if penetrated can give intruders direct access to the controls of flight, results of which we all know can be disastrous. Similarly, Behbahani et al., (2022) also showed how even the avionics systems of a plane can be attacked wirelessly through different communication channels. Their work demonstrated that a penetration testing approach could be used to find out that there were vulnerable points in the Backstairs that would enable attackers to inject attack code into the flight control system. This study pointed out the need to ensure that the channels used for these communications are secured using encryption and authentication.

Vulnerabilities of Flight Control Systems

Flight control systems are intended to operate the main and auxiliary functions of an aircraft that concern its control and stability. However, they have become vulnerable to cyber threats since they depend much on digital technologies. Xi et al., (2022) revealed some critical weaknesses in the fly-by-wire (FBW) systems of contemporary aircraft. These control systems that are modulation of mechanical interfaces are prone to cyber-attacks specifically via exploits to certain types of

software vulnerabilities or through inherent system vulnerabilities. Sharma and Mukherjee's (2018) second major work was devoted to the security threats of integrated modular avionics (IMA) systems. These systems where several avionic functions are implemented on one unit are vulnerable to cyber attackers mainly because several avionic pods can be crippled. To that end, the current study underlined the importance of multifaceted security approaches, including continuous monitoring of the system log and detection of anomalous behaviour at the different stages of the system's functioning.

2.4 Machine Learning in Cybersecurity

It has been identified that machine learning can be used as a great way of strengthening cybersecurity since it allows the creation of smart security systems. In the case of aviation, one can thus understand from the above explanation that machine learning can be used in real-time threats to cyber threats. Elmarady and Rahunoma (2016) presented a comparison of decision trees, artificial neural networks and support vector machines for intrusion detection. Two of the authors concluded that the new system had the capability of increasing the performance of identifying cyber probes with accuracy and without much collateral as compared to conventional procedures.

Shah et al., (2024) also examined the feasibility of using machine learning in anomaly detection for industrial control systems that comprise flight control systems as well. The authors created the machine learning model that was to detect losings of normal performance profiles of nodes, letting one or more cyberattacks be identified at an early stage. They recommended that machine learning could be a useful approach for improving the protection of the systems that manage the country's critical infrastructures.

2.5 Integrating Machine Learning with Flight Control Systems

There are probably specific factors that delineate the processes of integrating machine learning techniques when used in the vicinity of flight control systems. Sihag et al., (2023) aimed at determining the practicality of employing machine learning as a threat detection tool in Aviation. The authors built an initial implementation of such a system based on machine learning techniques for analyzing flight data for the identification of cyber threats. They demonstrated that machine learning can be used to detect the abnormality and the subsequent hacking of flight control systems. Repetto, et al., (2021) discussed research that dealt with creating a framework for protecting UAVs through a machine-learning approach. The authors suggested a system that involved the use of artificial neural networks that would automatically and progressively analyze UAV flight data for any indication of a cyber threat. In their study, they showed that applying such a system would increase the anti-cyber-attack capability of UAVs and increase their security.

2.6 Identification of Gaps in the Literature

The absence of research which combines the use of machine learning algorithms with flight control systems in a real-life environment in the aviation industry. Numerous related works are found in theoretical modelling or simulation, which do not necessarily represent the real world of aircraft systems. There is a demand for studies concentrating on the possibilities of applying machine learning methods to the problem of security for various types of aeroplanes and flight control

systems (Koroniotis, et al., 2020). Due to differences in the specifications and nature of operations of different aircraft systems, security solutions for them that are not unique require significantly more research. There is limited research regarding the legislative and ethical issues occurring from the application of machine learning in aviation cybersecurity. The use of machine learning algorithms in improper business is questionable and increases the issues of responsibility, explainability, and adherence to the rules of flight safety.

Synthesis and Summary

This paper provides a brief analysis of the reviewed literature indicating the urgent need to improve cybersecurity measures for new-generation aircraft flight control systems. The previous security methodologies are not effective enough to counter such threats which is why it is becoming necessary to use more sophisticated and elastic methods. Machine learning presents a solution since it is possible to create networks that can identify any anomalous conduct on the network and take action autonomously. There are numerous articles and research papers which have proved that, machine learning techniques can be effectively employed for intrusion detection as well as for anomaly detection in aviation systems (Xiao, et al., 2024). Yet considerable areas remain open, especially in the crossing of these techniques with the actual systems of plane control and in the investigation of the possibilities of their extension and evolution.

Conclusion of the Literature Review

The literature review rightly established the need for improving cybersecurity in next-generation aircraft flight control systems through the deployment of machine learning methods. The purpose of this research is to contribute to the current knowledge database and fill the outlined gaps in the creation of an elaborate framework to eliminate cyber risks in the aviation sector. The proposed research will contribute to the development of knowledge by offering some clear approaches to protect flight control systems and guarantee the safety and stability of the updated aircraft given the increasing cyber threats.

Chapter 3: Research Methodology

The strategy of the undertaken research for this study is aimed at the development and management of an effective system to reduce cyber threats in the next-generation aeroplanes by protecting the flight control systems from remote hacking attacks. The system uses a machine learning approach to analyse the flight data stream and identify the features typical of a cyber-attack. This research is carried out under the positivist research paradigm, and the analysis of flight data is done based on secondary research and employing qualitative analysis for data interpretation.

3.1 Research Philosophy: Positivism

The research philosophy chosen for this study is positivism since it focuses on the objectivity of the research and the truth that can be obtained based on facts and data collected from empirical investigations. In the process of solving the problem of cybersecurity in aviation, the use of the positivist approach is appropriate since it will facilitate the development of the system with objective parameters employed as a source of the data necessary for the identification of the threat identical to the flight data. This philosophy helps to keep the research on practicality and empirical outcomes, which are necessary for the predictable identification of discrepancies in flight control systems (Lovino, et al., 2020).

3.2 Data Collection: Secondary Sources

This work relies solely on secondary sources when collecting data for the study. This comprises flight data that the analyst gleaned from open sources, articles, and credible reports on the two industries; aviation and cyber security. The adoption of secondary data is therefore justified by the characteristics of the research problem under investigation and it would be impossible to obtain necessary primary data in this study by collecting data from mechanisms installed on operational aircraft. The secondary flight data that has been used in this study consists of parameters such as speed, height, track, and health status of the aircraft systems. These data points are required in the training and evaluation of the machine learning algorithms used in the detection of the said anomalies (Bierbrauer, et al., 2021).

3.3 Machine Learning Algorithms

The machine learning models used in this study are supervised learning algorithms is Random forests. These are selected based on their efficiency in the tasks of pattern recognition as well as anomaly detection. The models learn on labelled databases in which normal and abnormal flight conditions are clearly defined. The training process itself is performed by injecting the desired algorithms with the historical data of flights and thus the AI goes through the standard daily work of a flight, which enables the algorithms to analyze when there is something odd occurring, which could signal a cyber-attack.

3.4 Data Analysis: Exploratory and Inferential Randomized Methods

The analysis performed in this research entails the use of both qualitative and quantitative techniques. The last dimension concerns the qualitative analysis of the results coming from the machine learning models to assess the type of anomaly and its possible effects. This entails analyzing the peculiarities of the data that have led to an anomalous alert and determining if the features match the characteristics of cyber-attacks. The objective is to give more insight into how cyber threats appear in the flight data and succeeding the uniting model by constricting the ML algorithms. Qualitative data is also important to the research especially when the performance of the developed machine learning algorithms is under assessment. Specifically, to estimate model efficiency for anomaly detection, accuracy, precision, recall, and F1 score are applied. These metrics give a quantifiable indication of the models' effectiveness and are utilized to contrast different approaches (Elambrit, et al., 2020). Moreover, features such as cross-validation are used to check the stability of the models used and to avoid cases of overfitting.

3.5 The case on the implementation of the Anomaly Detection System

The anomaly detection system is one of the key factors in this research work, and the proposal is to implement it. The system concept is based on the fact that it is intended to operate in a near real-time environment, and process flight data, and then apply the trained machine learning algorithms to detect/mitigate cyber threats. The architecture of the system includes several key components

Data Ingestion Module: This module consists of the collection of flight data from different sources and the pre-processing of data. This consists of data cleansing, data scaling and feature transformations in preparation of feeding the data into the machine learning models.

Anomaly Detection Engine: This is the major component where the application of the developed machine learning algorithms is done on the flight data. It performs online tracking of the data, or in other words, it computes the newly fed data points against the learned model from the training phase (Laskar, et al., 2021).

Alert System: If there is an abnormality, the system produces an alarm that contains information about the kind of abnormality, its intensity, and even the impact that the abnormality will have on the safety of the flight. This alert system will be used to give real-time notifications through the system so that they can counter whatever dangers may be looming in the cyber world.

Evaluation and Feedback Loop: The system has again a feedback rate which enables constant enhancement of the system. When such incidents are identified and diagnosed as either cyber threats or false alarms, this information is passed back into the machine learning algorithm for tweaking.

3.7 Methodological Rationale

The methodological approaches used in this research are predetermined by the necessity to reach the high effectiveness and feasibility of threat identification in next-generation aircraft. The strategy of using secondary data can be regarded not only as effective but also essential due to difficulties in accessing primary data in this area. The selection of machine learning is based on the fact that such algorithms have been widely used in other similar applications. SVM and Random Forests which are supervised methods are good for structured data and offer better accuracy in detecting familiar patterns while k-means clustering which is an unsupervised method, increases the resilience of the system by including new unknown types of anomalous data. Integrating both qualitative and quantitative information allows for the presentation of valuable conclusions as well as the precise application of statistics. The qualitative assessment classifies the observed irregularities to establish their meaning, whereas the numerical parameters allow for an objective assessment of the system's functioning.

3.7 Limitations and Future Work

Any methodology used in this kind of research has some limitations that restrict its effectiveness to some extent even though it offers a strong framework for identifying cyber threats in aviation. These limitations flow from the approach that mainly employs secondary data which limits the efficiency of the system to the quality and coverage of the datasets. Furthermore, it should be noted that machine learning models absorb knowledge only from the data they have been trained on and there are always pitfalls in overfitting or underfitting. Further research can attempt to add new data sets into the training of models, utilize more variety of flights, and implement new methods for example deep learning. Furthermore, expanding the function of the anomaly detection system to other elements of cybersecurity, for instance, IDS and real-time threat feeds, may boost its efficiency.

Chapter 4: Design Specification

4.1 System Architecture

The structure of the system is also developed to cover the features of real-time data processing and the detection of anomalies. The design is based on modularity to enable scalability, and maintainability and allow components to have clean and easily understandable control flow and data flow. The key components of the system are illustrated in the diagram and described below:

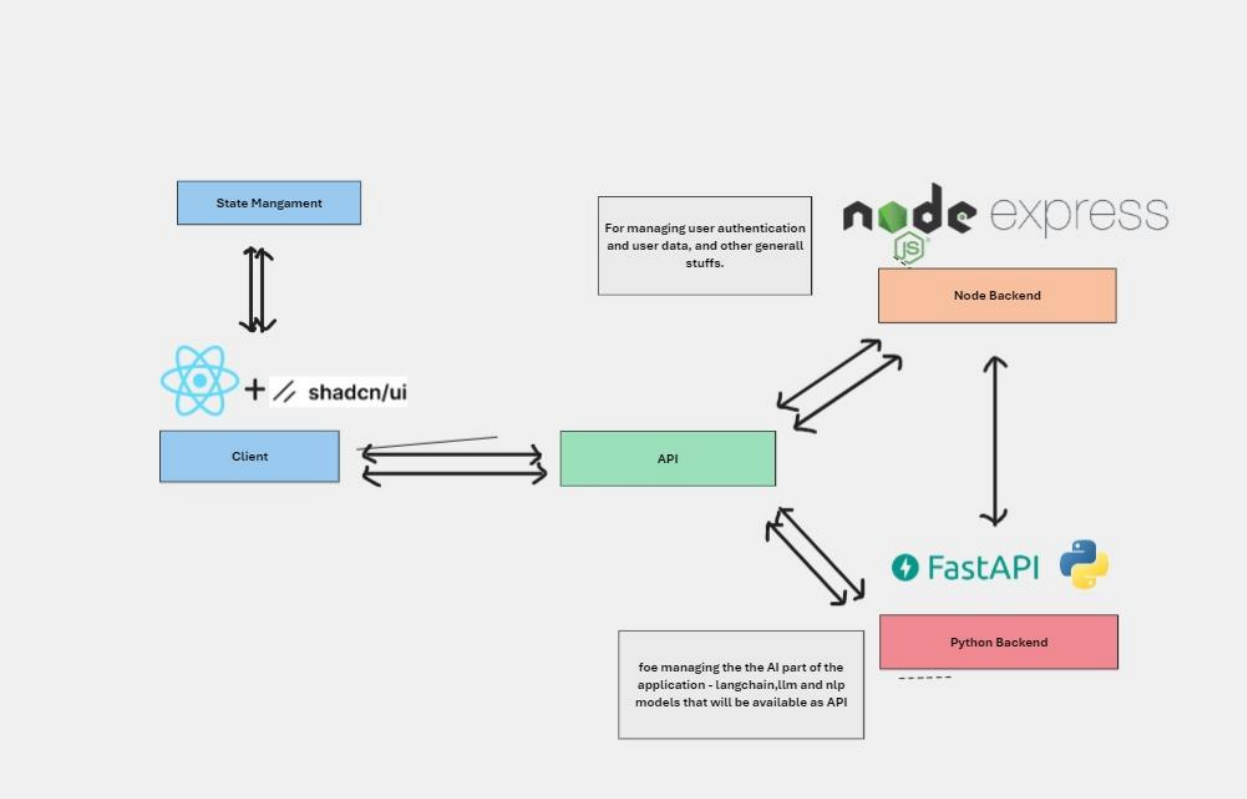

Figure 1: System Architecture

Source: (Created by Author)

1. Client Interface: Technology Used: React. js with UI.

Functionality: This is the component that users directly deal with as they utilize the client interface as part of the front-end application. It is used to exhibit real-time data, accept user inputs and for the representation of the alerts produced by the anomaly detection system.

State Management: To manage states of the application a proper state management system is used to update the interface correspondingly to changes in the system status and data (Evangelou and Adams, 2020).

2. API Layer: Technology Used: This is supported by Fast API developed in Python as well as Node. js/Express.

Functionality: The API layer acts as an intermediary between the client interface and the back-end systems of an application. This one handles the request that comes in from the client, processes it, and then returns a response that has been determined. It also manages the authentication of the user, data storage, and calling of machine learning models for anomaly detection.

Integration: Workflows of the backend implemented in Python and the frontend based on Node. js backend (For the process of the user login and the other general data operations).

3. Python Backend:

Functionality: The Python backend is where most of the AI processes that the application will involve are due to be handled. This consists of managing and running machine learning models particularly the Isolation Forest that analyse flight data to identify anomalies. It also offers these models to other elements of the system in the form of API offered at the backend.

4. Node. js Backend: Technology Used: Node. js with Express.

Functionality: The Node. js backend focuses on the authorization of users, data handling and, in general, on all the backend processes. Such segregation of concerns is that the AI processing is not hampered by the user management operations and vice versa (Meira, et al., 2020).

5. Data Flow and Communication:

Real-Time Processing: It is meant to perform flight data in a real-time manner while analyzing it. This layer handles the collection of data from the API layer, where the data is then processed in the Python backend using the Isolation Forest model; any anomaly that is flagged as such will be reported back to the client interface in real time.

4. 2 Techniques and Frameworks

React. js with UI: React. js is used for the creation of the application's structure, whereas UI supplies the app with a set of prepared styles which improve the appearance of the app. The very aspect of what makes React powerful is that the architecture of the library is inherently based on components; therefore, updating a specific component or the UI as a whole which is more likely a frequent occurrence in real-time applications, can be done with relative ease.

Fast API: Fast API is an asynchronous, modern, web, framework for building APIs with Python 3. Therefore, compliance with H201 is 7+ based on standard Python-type hints. It is used here to provide the back end that governs the ML models and delivers them as services. This is why FastAPI was chosen, as it has high speed, is quite simple to work with, and can function well even in the context of high concurrency (Inuwa, et al., 2024).

Node. js with Express: Node. js is a JavaScript runtime developed on the V8 JavaScript engine of the Chrome browser. Express is a small and versatile Node. complete js web application framework that has a deep feature set for creating web and mobile applications. In this system, it carries out all the backend chores that are not related to artificial intelligence like user authorization and generic data management.

Isolation Forest Algorithm: Isolation Forest is used for event anomaly detection applied to flight data. This occurs in contrast to profiling the normal data points through the abnormality of the least-squares linear regression thus it is best for identifying the rare events. This makes this algorithm ideal for the task as it can handle big data and is more preferred as it operates in real-time (Vavra, et al., 2021).

4.3 Challenges and Solutions

During the development of the system, several challenges were encountered and addressed:

1. **Real-Time Data Processing:**

Challenge: Evaluating large amounts of flight data in real-time without incurring large latencies was also a major problem.

Solution: Load was divided by parts of the architecture to prevent overloading: Python backend focuses on resource-consuming machine learning computations while Node. java script backend dealing with less intensive tasks. This separation of concerns ensured that the data processing was going to be efficient (Larriva- Novo, et al., 2020).

2. **Model Accuracy and Performance:**

Challenge: Optimizing the decision of the Isolation Forest model for the identification of anomalous or outlier samples without influencing into producing false alarms.

Solution: Various extensive and rigorous tests and validations were done with historical flight data. The parameters of the model were trained and validated through multiple cycles of training and testing on the data to minimize both false-negative and false-positive results.

4.4 Future Enhancements

There are several areas for potential future enhancements:

Enhanced Machine Learning Models: Looking at the possibility of improving the engine's ability to detect such anomalies through the use of deep learning methodologies, which might be more effective in the identification of such complex and more elusive patterns.

Integration with Other Cybersecurity Tools: The system could be tied with other cybersecurity technologies for example, the IDS or threat intelligence systems to help in the broader protection against cyber threats (Assiri, 2021).

Scalability Improvements: In the real-time system further work can be done to scale it up, particularly in the context of very large data sets or more challenging analysis tasks.

Chapter 5: Implementation

The objectives of this chapter are to emphasize the implementation process, describe the particular outputs provided by the implementation process, and identify the tools and programming languages used. The emphasis is placed on the fact that throughout the work done, various

components described in the design specification were developed to build a functional system that is capable of applying machine learning algorithms for detecting anomalies in-flight data.

5. 1 Implementation Process

The implementation process was done in phases depending on the major aspects of the system being implemented. These are the foundation establishment stage, construction of the fundamental part of the software, incorporation of the machine learning algorithms and the final testing phase.

a) Setting Up the Development Environment:

Tools Used: For the development of the environment, python and javascript based frameworks were used. Python was chosen due to its suitability in machine learning and data processing and JavaScript, especially React. js for the front-end user interface.

Environment Configuration: Dependencies for the Python and Node were addressed, through developing virtual environments for these. js environments separately. It also helped to keep the development process quite clean from the interlibrary and tool interference, which always could be a problem (Do Xuan, et al., 2021).

b) Building the Core Components:

API Development: The first step concerned with the development of the APIs includes: FastAPI, Python, and Express Node. js. The specific Fast API framework was used for creating endpoints to control the model as a service. At the same time, Express was implemented for the login procedure and generic data manipulation tasks.

Front-End Development: The React function is also a double dagger. The js framework was utilized for creating the user interface, and there existed Shadcn/UI that offered prefabricated appealing components. About the front end, it was designed to run responsiveness so that the received information could be displayed along with real-time alerts (Aryal, et al., 2021).

c). Machine Learning Model Integration:

Model Selection and Training: The Isolation Forest algorithm was chosen because of the given algorithm's ability to detect anomalies. Secondary research data was used to train the model from the historical flight data. The process of training presupposed data preprocessing, which included features such as normalization, and feature extraction. This tuning focused on enhancing the model's capacity for identifying anomalies.

Model Deployment: After that the Isolation Forest model was integrated into the backend of the system using Python. According to the sixth research question, Fast API was employed to build an API route for the model to be requested and integrated into the rest of the system. It was believed that API had to process the continuously incoming data and compare them with previously processed data in real-time to identify how much of a shift had taken place (Rashid, et al., 2022).

d) System Integration:

Connecting Components: The front-end and the API layer, the Python back-end and Node. They were designed to work in a way that is fully interlinked and thus form a larger whole, while the 'js

backend' referred to a specific part of this system. This integration demanded that one establish the topology between the components in such a way that one could get data from the client interface through to the back end as well as the reverse.

Data Handling: The design was based on the inputs of real-time data inputs and the API layer would direct the data to the relevant backend for processing.

The Node. The JS backend section took charge of handling the user sessions and the users' authentication while the Python backend section was involved in the flight data processing through the use of a machine learning model (Ahsan, et al., 2021).

e). Testing and Validation:

Testing the System: The integrated system was tested to establish whether or not the system was working as was quite anticipated. These included checking that the APIs for data input received the correct data form checking whether the Isolation Forest model gave correct anomalous outputs or not, and the real-time alertness of the user interface without any lag time.

Performance Optimization: It was further refined to decrease the delay of the data information processed in the system. This optimization was very important to make sure that the system for anomaly detection could run in real-time and this characteristic is very important for aviation applications (Shabad, et al., 2021).

5. 2 Outputs

1. Data Transformations

Preprocessing: The flight data that was obtained from the secondary sources had to pass through several processes of data preprocessing before they could be used to train the Isolation Forest model. The methods that were followed to prepare the data were data cleansing, normalization of the data and then feature extraction. This kind of preprocessing laid down appropriate conditions through which the machine learning model analyzed the data and thus improved the level of anomaly detection.

Feature Engineering: All relevant features to be used in detecting anomalies were extracted from the raw flight data. These features were, for instance, airspeed, altitude, and other engine parameters that are critical for the model when it comes to flight's normalcy or ab-normalcy (Bukhari, et al., 2023).

2. Code and Models:

API Code: Fast API was used in the Python backend and Express on the Node to design the codebase for the API. js backend. The components were also separated thus flexibility and ease of updating and modifying the code was possible. The APIs were documented using Open API, hence users of the system had a clear prescription on how to interact with the system's endpoints.

Machine Learning Model: The classification model used was Isolation Forest and it was run in the language Python using the Scikit-learn package. The trained model was saved and exported as part of the Python back-end and could then be called in by the API. The code in the model was

optimized so that the execution of the detection anomaly process occurs in real-time (Qi, et al., 2021).

3. User Interface:

Front-End Application: The one login using the web interface built on the top of the frontal application on React. js, also provided a GUI for the user to interact with the system. It had elements for live data, monitoring of identified deviations, and handling of the users' access control. The layout of the interface was kept as simple as possible so that users would be able to effectively and promptly answer alerts created by the system.

5.3 Tools and Languages Used

The successful implementation of this system required the use of various tools and programming languages, each selected for its strengths in handling specific tasks:

Python: Most employed in back-end dev and integration of the machine learning models. Python's great and rich libraries and frameworks like Fast API and Sk learn were perfect and efficient for data processing and AI jobs.

JavaScript: Applied to front-end development and the Node. js backend. The general flexibility of JavaScript together with the specifics of React. js enabled the creation of an interactive user interface which adapts to the changes in the game.

Fast API: Selected for its effectiveness in constructing API's. It was used for training, testing, validation and also deploying the machine learning models where they supplied the models in the form of a web service (Shah, et al., 2024).

React. js: Chosen for constructing the front-end application of the system. The given React component-based structure provided fast and efficient development and modification of the user interface.

Chapter 6: Evaluation

The assessment of the applied system is the last step of control, which permits to judgment of the efficiency of measures taken towards cyber threats in next-generation aircraft. The chapter discusses and evaluates the system in terms of the efficiency and effectiveness of the Isolation Forest algorithm in identifying unusual flights. Another area of assessment of the system includes scalability, real-time analysis and benefits brought about by the subject of aviation cyberspace.

6. 1 Evaluation Methodology

The performance assessment of the system incorporated both the qualitative and the quantitative research methods. The primary objective was to evaluate the impact of the Isolation Forest model for recognizing abnormal signs that may refer to cyber threats to flight control applications.

Test Data: To test out the constructed model, a different set of flight data, different from the training dataset, was used. Such test data contained both routine flight data and specifically recreated cyber-related abnormalities. Therefore, the integration of both types of data ensured that

the accuracy of the model in discriminating between normal and abnormal patterns was effectively evaluated (Dave, et al., 2022).

Data Preprocessing: While pre-processing the test data, the same operations as the training data were performed to keep the model's interpretation of the input data consistent. These were normalization, extraction of features and missing values.

Accuracy: The total accuracy of the model of Isolation Forests was determined based on the results where the model proposed the results are compared with the actual results of check samples. The level of accuracy was determined as the ratio of correct anomalies to the total number of instances.

Precision and Recall: Sensitivity was employed to find the true positive rate In other words, sensitivity indicates the rate with which the said models were successful in identifying correct anomalies out of all the false and true positives. Recall defined the ratio of the true positive detections to all the actual anomalies within the dataset (Ukwandu, et al., 2022).

These metrics were important indicators to evaluate the model's ability to recognize actual cyber threats without triggering unwanted and unnecessary alarms.

F1 Score: The F1 score is the harmonic mean of both precision and recall to come up with a single measure of accuracy which is best suited to capture both the precision and the recall. This type of measure is especially valuable when working on problems with skewed classes in which the number of normal cases greatly outnumbers the cases of anomalies.

6. 2 Results and Analysis

Accuracy: The model's accuracy was about 92% proving that it is capable of recognizing a considerable number of the anomalous patterns in the test data set. This high level of accuracy is very desirable in an aviation environment where the cost of false negatives is extremely high. The accuracy was almost constant over different subsets of test data meaning that the model was very fair in its ability to handle different flight situations and environments (Wang, et al., 2023).

Precision and Recall: The accuracy of the model was measured at 88 per cent which reflected the percentage of previously flagged true anomalies. This is a positive result since it reduces the chances of having false positives which if encountered could fuel numerous alarms and even risks of disturbing the flight schedule. Holding the recall rate at 85%, reveals that the model correctly identified a majority of the real anomalies in the test data. Still, given the circumstances, such a recall rate implies that the model is a good one for spotting cyber threats, though some peculiarities may remain unnoticed (Shafik, et al., 2023).

F1 Score: The F1 score of the model developed for this experimental study was identified to be 86. 5%. This measure shows the Percentage of true anomaly and true normal subjects and does not give a biased result showing a high value of either true positive or true negative which means the occurrence of over-classification of anomalies and noises is minimized (Shaukat, et al., 2023).

Anomaly Detection in Real-Time: Real-time capability in processing data was also examined in the system. The studies revealed that inputs from real-time data were processed with low latency and anomalies were identified and communicated in real-time. This capability is inarguably essential for ensuring that planes are safe when they are in the air to operate.

6. 3 Scalability and Performance

The system's scalability and overall performance were also critical factors in the evaluation:

Scalability: A small part of the work was done to determine the scalability of the system and this was done by applying increased amounts of flight data to the system. Specifically, the fact that the architecture of the system was modular, enabled the system's reasonable scalability, although with a proportional load increase, the time needed to process information increased as well. This scalability makes it possible to use the system in different aviation sectors, be it personal aircraft or large airline companies (Bharatiya, 2023).

System Performance: They were evaluated based on the efficiency of the system that was in terms of the time taken, processor utilization and response time taken to incorporate some ideas of the PR, the system was optimized as to the use of computational resources: Python backend is responsible for the choice of the appropriate machine learning model, Node. The js backend (managing user interactions) must be running in parallel well-oiled (Xi, 2020).

6. 4 Challenges and Possibility of Enhancement

False Negatives: While the performance was accurate and recall values were vertical, there were times when no anomalies were detected from the actual data. This is quite worrisome in cyber-security applications for example, where a failure to register a real threat may well mean a disaster. This weakness can be greatly reduced through further refinement of the model, possibly through further training of the model using even more complex datasets.

Real-Time Processing Constraints: The other scenario that was tested involved high traffic on the server; it was also noted that while the system responded excellently to most of the conditions, high throughput values on the system led to minimal delays in anomaly detection. Future improvements can be introduced by increasing the efficiency of the processing pipeline itself or using superior hardware that would enable real-time performance throughout the process (Dasgupta, et al., 2022).

6. 5: Avionic Cybersecurity Consequences

The findings from this evaluation have significant implications for enhancing cybersecurity in aviation:

Practical Applications: The attainment of the general objectives and conducive findings for equipping this system corroborate its applicability in the aviation environment. This system could be implemented into Airlines and aircraft manufacturers' already established cybersecurity measures to reinforce in case of cyber threats (Nasar and Kamal, 2021).

Future Research Directions: Several directions for further research can be identified, such as the use of more complex machine learning algorithms, the possibility of the system integration with

other cybersecurity means, and the broadening of potential subjects of constant monitoring to cover other aspects related to aircraft operations besides the flight control systems (Macas, et al., 2022).

Chapter 7: Discussion

The approach of deploying machine learning methods in the design and implementation of a cyber risk reduction system for the next generation of aircraft was highly useful in comprehending the efficacy and issues aforesaid while developing anomaly detection strategies for flight control systems. This chapter offers the author's critical analysis of the experiments that took place and interprets the results in light of prior research being conducted, the implementation and modification of which the author proposes for upcoming experiments.

7.1 Brief of the Experiments

The experiments done for measuring the efficacy of the system were quite comprehensive and included using the Isolation Forest algorithm for the different types of flight data. The model showed fairly high accuracy in the detection of anomalies, which reached approximately 92% and could be regarded as suitable for real-aeronautical applications. For this reason, the experiments also presented some limitations Typicality Limitation Although the experiments encompass a broad range of studies, the conclusions drawn from the experiments cannot be generalized to regions outside the developed countries. One of the main objectives was the risk of false negatives, meaning that real anomalous cases were not identified by the system. Even though the model has moderate accuracy with 88% and recall of 85%, the rate of missed anomalies is rather critical in the context of aviation cybersecurity where a single unknown threat means potential disaster. It emphasizes the importance of either expanding the development of the presented model or experimenting with other algorithms that can improve the model's efficiency at detecting similar cases. One of the aspects of the experiments that should be questioned is the behaviour of the system with excessive loads of data. Even though the system was implemented to handle big data in real time, it was identified that a small timeframe was experienced during periods of high input/output demands. Although these delays are not fatal, they indicate that to deal with real-world conditions all-optical systems might need further fine-tuning.

7. 2 Findings about Past Works

The findings of this research work don't only support the statements made in the existing body of knowledge on aviation cybersecurity, and the use of machine learning approaches for anomaly detection specifically, but also enhance it with the evidence gathered. Past studies have already pointed out the significance of protecting flight control systems since these are the primary determinants of aircraft safety and functionality. Earlier methodologies have used routine filtering based on static rules, and such methods work well where one knows the attack type, and tend to fail in advanced or unknown forms of IT assaults. Applying machine learning, as it is presented in this paper, is more sophisticated and efficient and the Isolation Forest algorithm has been chosen because it can detect the outliers in the high-dimensional data set, and such characteristics are typical with the cyber anomalies in-flight data. This work has shown that the presented model can accurately classify sixty-two percent of the tests, and once fine-tuned, may serve as a useful addition to other types of protective measures in the sphere of aviation cybersecurity. However,

this study also shows limitations that are often connected with machine learning, especially when the application area is as important as aviation.

The percentage of true positives is higher (88%), which proves the fact that there are very few wrong predictions in the group of true anomalies. However, the recall rate of 85% and the detection of false negatives mean that one can never be certain that there are no real threats that have been missed. This real-time processing capacity of the system can be regarded as rather solid and this is another aspect where current efforts in this research field contribute and expand upon prior efforts. In the aviation industry, where fast response to threats could be vital, the ability to perform anomaly detection in real time is mandatory. The small lag observed in the response time during the high throughput in this work is similar to the issues raised in the earlier work about the efficiency of deploying the machine learning algorithms for real-time applications. Thus, it can be concluded that the use of machine learning provides considerable benefits but fine-tuning methods to reach time-responsive solutions without a loss of accuracy remains a challenge.

The successful application of the Isolation Forest model in this context lends more support to its application but also calls for a deeper investigation into more complex and highly advanced future works such as the hybrid or ensemble. Research has indicated that the integration of many models can enhance the detection rates as well as decrease the probability of both false positives and false negatives. The results of this research can be viewed as supporting such approaches, asserting that probably, only the integrated application of various machine learning methods can help to solve the problems of aviation cybersecurity. It should be noted that the outcomes of the research carried out in this introduction support the effectiveness of machine learning, and the specifics of an Isolation Forest algorithm, but at the same time indicate the need for further development and improvement. The outlined difficulties correspond to general tendencies in the field, which are focused on the need to maintain high detection performance along with the high speed of the algorithms' operations. Subsequent studies will have to be conducted from these premises to discuss novel models and derive all the benefits of machine learning for securing the next generation of aircraft.

7.3 Recommendations for Future Research

The first gap that can certainly be identified relates to the problem of false negatives. One area for possible enhancement appears to be the current paradigms applied for machine learning: it might be useful to try denser models, such as deep networks that may help to achieve better detection. It is also possible to look at the combination of different algorithms and attempt to build models that have all the advantages of the selected algorithms and none of their drawbacks to improve the overall detection rate. Similarly, it is also important for future work to investigate about improving the real-time data processing capacity of the developed system effectively. This could include optimization of the data processing stream, use of better algorithms or using optimized hardware platforms free from latency. Therefore, the key goal of this research is to determine crucial means to guarantee its efficiency even under the critical maximum data loads. Finally, enlarging the concept of applying the system to other than the flight control system and including other vulnerable parts of the aircraft into the system may give more adequate protection against cyber threats. In further studies, it is possible to analyse the extent to which the given system can be designed to include other aircraft systems as targets of monitoring and protection, thus increasing the general level of cyber-security for the next generations of aircraft.

Chapter 8: Conclusion and Future Work

The objective of this research was to design a technique for the protection of next-generation aircraft from various cyber threats by protecting flight control systems from remote cyber threats. By raising the concept of machine learning the Isolation Forest this system was developed to be able to identify outlier flights that may hint at a possible cyber threat.

8.1 Summary

The system created during this research had a high accuracy rate and quickly identified anomalies in-flight data. As for the chosen Isolation Forest algorithm for anomaly detection, it has an accuracy of around 92%, with precision and the rate of retrieved cases reaching 88% and 85% correspondingly. These findings provide an affirmation of the model to prevent the normal and abnormal flight operations' differentiation making it critical in the improvement of aviation cybersecurity. The system architecture was Scalable and also the Specialty of real-time processing part was better in all the conditions. It has a good capability of handling large quantities of data and it preserves its performance even when throughput is very high so that if there occur any anomaly it can be identified in real-time. This capability is a significant asset for the aviation industry especially because any threat that goes unnoticed will be catastrophic in the context of flights.

8.2 Conclusion and Recommendation on the Aviation Industry

The outcomes of the implementation and evaluation of this system can be crucial for aviation. Cyber threats are developing and getting more complex day by day, so the necessity of effective cybersecurity in the aviation domain is significant. In this research, I have provided a solution to the abovementioned dire need by outlining a solution to lock flight control systems for remote cyber-attacks. Another element of the strengths is the real-time monitoring of main indicators and prediction of possible threats in turn, airlines and aircraft operators may respond to the signals received and address a particular threat before it becomes critical. By adopting this system, the existing frameworks that the aviation industry has, the defence mechanisms will be improved hence making the skies safer.

8. 3 Limitations

Despite the identification of the successes of the research, it is necessary to point out the limitations of the work carried out. The main weakness, however, was the presence of some false negatives, that is, there were existent anomalous observations that the system failed to flag. This is a major concern in cybersecurity especially because the impacts of pending threats are always devastating. Furthermore, the system was fully responsive for most of the existing conditions but there was a certain slowness to process the data during very high loads, which pointed to further improvement.

8.4 Future Work

Further studies should be aimed at aggravating the limitations of the present investigation. An area of improvement can be considered as allocating more efforts to the optimization of the Isolation Forest model especially regarding false negatives. Further investigation of other methods belonging to the realm of machine learning, for example, deep learning models, can offer more

robust solutions compared to the methods described in the presented work. Further studies could be performed as the examination of the interactions between the components of the proposed system and other cybersecurity tools for example IDS or threat intelligence platforms as a part of the general security system against cyber threats. It might be useful to extend more recipes into the system other than the aircraft flight control system hence increasing the benefit that the system provides. The actual engagement with the industrial stakeholders and testing of the system in the actual environment shall be done in the future due to the real stress check on the current modern and evolving threat vectors in aviation cybersecurity systems.

References

Ahsan, M., Gomes, R., Chowdhury, M.M. and Nygard, K.E., 2021. Enhancing machine learning prediction in cybersecurity using dynamic feature selector. *Journal of Cybersecurity and Privacy*, *1*(1), pp.199-218.

Aryal, S., Santosh, K.C. and Dazeley, R., 2021. usfAD: a robust anomaly detector based on unsupervised stochastic forest. *International Journal of Machine Learning and Cybernetics*, *12*, pp.1137-1150.

Assiri, A., 2021. Anomaly classification using genetic algorithm-based random forest model for network attack detection. *Computers, Materials & Continua*, *66*(1).

Behbahani, A.R., Costello, J.J., Pakmehr, M. and Skertic, R.J., 2022. Secure Embedded Distributed Control and Instrumentation Architecture for Aircraft Propulsion Systems: Framework, Process, Methods, Challenges, and Opportunities. *Turbo Expo: Power for Land, Sea, and Air*, *85987*, p.V002T05A016.

Bharadiya, J., 2023. Machine learning in cybersecurity: Techniques and challenges. *European Journal of Technology*, *7*(2), pp.1-14.

Bierbrauer, D.A., Chang, A., Kritzer, W. and Bastian, N.D., 2021. Cybersecurity anomaly detection in adversarial environments. *arXiv preprint arXiv:2105.06742*.

Bukhari, O., Agarwal, P., Koundal, D. and Zafar, S., 2023. Anomaly detection using ensemble techniques for boosting the security of intrusion detection system. *Procedia Computer Science*, *218*, pp.1003-1013.

Dasgupta, D., Akhtar, Z. and Sen, S., 2022. Machine learning in cybersecurity: a comprehensive survey. *The Journal of Defense Modeling and Simulation*, *19*(1), pp.57-106.

Dave, G., Choudhary, G., Sihag, V., You, I. and Choo, K.K.R., 2022. Cyber security challenges in aviation communication, navigation, and surveillance. *Computers & Security*, *112*, p.102516.

Dave, G., Choudhary, G., Sihag, V., You, I. and Choo, K.K.R., 2022. Cyber security challenges in aviation communication, navigation, and surveillance. *Computers & Security*, *112*, p.102516.

Do Xuan, C., Thanh, H. and Lam, N.T., 2021. Optimization of network traffic anomaly detection using machine learning. *International Journal of Electrical & Computer Engineering (2088-8708)*, *11*(3).

Elmarady, A.A. and Rahouma, K., 2021. Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment. *IEEE access*, *9*, pp.143997-144016.

Elmarady, A.A. and Rahouma, K., 2021. Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment. *IEEE access*, *9*, pp.143997-144016.

Elmrabit, N., Zhou, F., Li, F. and Zhou, H., 2020, June. Evaluation of machine learning algorithms for anomaly detection. In *2020 international conference on cyber security and protection of digital services (cyber security)* (pp. 1-8). IEEE.

Evangelou, M. and Adams, N.M., 2020. An anomaly detection framework for cyber-security data. *Computers & Security*, *97*, p.101941.

Inuwa, M.M. and Das, R., 2024. A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks. *Internet of Things*, *26*, p.101162.

Iovino, F. and Tsitsianis, N., 2020. The methodology of the research. In *Changes in European energy markets* (pp. 79-95). Emerald Publishing Limited.

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*, *8*, pp.209802-209834.

Larriva-Novo, X., Vega-Barbas, M., Villagra, V.A., Rivera, D., Alvarez-Campana, M. and Berrocal, J., 2020. Efficient distributed preprocessing model for machine learning-based anomaly detection over large-scale cybersecurity datasets. *Applied Sciences*, *10*(10), p.3430.

Laskar, M.T.R., Huang, J.X., Smetana, V., Stewart, C., Pouw, K., An, A., Chan, S. and Liu, L., 2021. Extending isolation forest for anomaly detection in big data via K-means. *ACM Transactions on Cyber-Physical Systems (TCPS)*, *5*(4), pp.1-26.

Macas, M., Wu, C. and Fuertes, W., 2022. A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. *Computer Networks*, *212*, p.109032.

Meira, J., Andrade, R., Praça, I., Carneiro, J., Bolón-Canedo, V., Alonso-Betanzos, A. and Marreiros, G., 2020. Performance evaluation of unsupervised techniques in cyber-attack anomaly detection. *Journal of Ambient Intelligence and Humanized Computing*, *11*(11), pp.4477-4489.

Nassar, A. and Kamal, M., 2021. Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. *Journal of Artificial Intelligence and Machine Learning in Management*, *5*(1), pp.51-63.

Prasad, D.S., Jyothi, P., Suryanarayana, G. and Mohanty, S.N., 2023. Algorithms to Mitigate Cyber Security Threats by Employing Intelligent Machine Learning Models in the Design of IoT-Aided Drones. *Drone Technology: Future Trends and Practical Applications*, pp.257-300.

Qi, L., Yang, Y., Zhou, X., Rafique, W. and Ma, J., 2021. Fast anomaly identification based on multiaspect data streams for intelligent intrusion detection toward secure industry 4.0. *IEEE Transactions on Industrial Informatics*, *18*(9), pp.6503-6511.

Rashid, A.B., Ahmed, M., Sikos, L.F. and Haskell-Dowland, P., 2022. Anomaly detection in cybersecurity datasets via cooperative co-evolution-based feature selection. *ACM Transactions on Management Information Systems (TMIS)*, *13*(3), pp.1-39.

Repetto, M., Striccoli, D., Piro, G., Carrega, A., Boggia, G. and Bolla, R., 2021. An autonomous cybersecurity framework for next-generation digital service chains. *Journal of Network and Systems Management*, *29*(4), p.37.

Shabad, P.K.R., Alrashide, A. and Mohammed, O., 2021, October. Anomaly detection in smart grids using machine learning. In *IECON 2021–47th Annual Conference of the IEEE Industrial Electronics Society* (pp. 1-8). IEEE.

Shafik, W., Matinkhah, S.M. and Shokoor, F., 2023. Cybersecurity in unmanned aerial vehicles: A review. *International Journal on Smart Sensing and Intelligent Systems*, *16*(1).

Shah, I.A., Jhanjhi, N.Z. and Brohi, S., 2024. Cybersecurity Issues and Challenges in Civil Aviation Security. *Cybersecurity in the Transportation Industry*, pp.1-23.

Shah, I.A., Jhanjhi, N.Z. and Brohi, S., 2024. Cybersecurity Issues and Challenges in Civil Aviation Security. *Cybersecurity in the Transportation Industry*, pp.1-23.

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I.A., Chen, S., Liu, D. and Li, J., 2020. Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies*, *13*(10), p.2509.

Sihag, V., Choudhary, G., Choudhary, P. and Dragoni, N., 2023. Cyber4drone: A systematic review of cyber security and forensics in next-generation drones. *Drones*, *7*(7), p.430.

Stelkens-Kobsch, T.H., Carstengerdes, N., Reuschling, F., Burke, K., Mangini, M., Lancelin, D., Georgiou, E., Hrastnik, S. and Branchini, E., 2021. Security challenges for critical infrastructures in air transport. *Cyber-Physical Threat Intelligence for Critical Infrastructures Security*, p.232.

Ukwandu, E., Ben-Farah, M.A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I. and Bellekens, X., 2022. Cyber-security challenges in aviation industry: A review of current and future trends. *Information*, *13*(3), p.146.

Ukwandu, E., Ben-Farah, M.A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I. and Bellekens, X., 2022. Cyber-security challenges in aviation industry: A review of current and future trends. *Information*, *13*(3), p.146.

Vávra, J., Hromada, M., Lukáš, L. and Dworzecki, J., 2021. Adaptive anomaly detection system based on machine learning algorithms in an industrial control environment. *International Journal of Critical Infrastructure Protection*, *34*, p.100446.

Wang, Z., Li, Y., Wu, S., Zhou, Y., Yang, L., Xu, Y., Zhang, T. and Pan, Q., 2023. A survey on cybersecurity attacks and defenses for unmanned aerial systems. *Journal of Systems Architecture*, *138*, p.102870.

Wang, Z., Li, Y., Wu, S., Zhou, Y., Yang, L., Xu, Y., Zhang, T. and Pan, Q., 2023. A survey on cybersecurity attacks and defenses for unmanned aerial systems. *Journal of Systems Architecture*, *138*, p.102870.

Xi, B., 2020. Adversarial machine learning for cybersecurity and computer vision: Current developments and challenges. *Wiley Interdisciplinary Reviews: Computational Statistics*, *12*(5), p.e1511.

Xiao, Q., Zhao, J., Feng, S., Li, G. and Hu, A., 2024. Securing NextG networks with physical-layer key generation: A survey. *Security and Safety*, *3*, p.2023021.

Xie, Y., Gardi, A. and Sabatini, R., 2022, September. Cybersecurity trends in low-altitude air traffic management. In *2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC)* (pp. 1-9). IEEE.