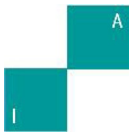
Inteligencia Artificial 28(75) (2025), 199-219
doi: 10.4114/intartif.vol28iss75pp199-219



INTELIGENCIA ARTIFICIAL

http://journal.iberamia.org/

A Review of Cyber Security Challenges and Solutions in Unmanned Aerial Vehicles (UAVs)

Yuvaraj Renu[1],Velliangiri Sarveshwaran[2]

[1][2] Department of Computational Intelligence, School of Computing, SRM Institute of Science and Technology, Kattankulathur Campus, Chengalpattu, India

[1] yr8525@srmist.edu.in
[2] vellians@srmist.edu.in

Abstract The widespread use of unmanned aerial vehicles in a variety of sectors poses major challenges to these issues of cyber security and data protection. In this paper, a detailed study of the security vulnerabilities in UAV-based systems was conducted and analytically categorized into three types: Software, hardware and communication links. These vulnerabilities include access rights without authentication, control channel tampering, data breaches and spoofing of the global positioning system. These vulnerabilities jeopardize the security, integrity of the data and privacy of not only the drone but also the users. The study analyzes some of the security protocols that aim to mitigate these risks. They range from advanced encryption techniques to authentication mechanisms and intrusion detection systems that can use classification models based on machine learning. The study also provides a context in which emerging technologies such as blockchain, machine learning and deep learning can make a greater contribution to securing drones. The detailed and in-depth discussion on the development of the security solution that the work provides emphasizes the importance of securing UAV operations and their data integrity aspects alongside securing public trust for autonomous systems.

Keywords: UAV security, cybersecurity vulnerabilities, data integrity, GPS spoofing, blockchain, machine learning, deep learning, encryption, authentication, intrusion detection systems.

1 Introduction

The rapid rise of UAVs, also known as drones, has remarkably changed the way this technology is used in various industries. There is no doubt that UAVs are perfecting search and rescue missions with their amazing versatility and efficiency. They can also be used for aerial photography and cargo transportation. However, there is one important aspect that is often overlooked in these developments: safety. Raising awareness: It is important to educate and sensitize students, teachers, parents and caregivers about cyberbullying. This includes providing clear and age-appropriate definitions, signs and consequences of cyberbullying. Building empathy and understanding of the impact of digital disruption can help with taking on bullying. A comprehensive network of safety measures is a must to ensure the safety and flight stability of drones [1]. Let us think of a recipe where a hacker could take control of the drone used to transport medicine. Another reason to prevent interference is to change the flight route, which could cause many people to lose their lives or property. On the contrary, compromised drones used to inspect critical structures could provide untrue data, leading to major security concerns. As a countermeasure to the threat of drones from unauthorized access or modification, comprehensive security protocols such as encryption and access control should be employed. Different types of UAVs are equipped with powerful cameras and sensors that can receive information remotely while providing their services. This may be privacy invading data, sensitive infrastructure details or confidential business data above. If there are no security measures in place, this data is likely to be easily accessible to other unauthorised parties, even paving the way for integrity and

ISSN: 1137-3601 (print), 1988-3064 (on-line)

confidentiality breaches [2]. Establishing a secure communication link and encrypting the data are critical to protecting the sensitive information that drones collect. Global trust is a prerequisite for the widespread use of drones. Serious safety issues related to drones that lead to accidents or privacy violations can quickly erode trust between businesses and consumers. These stringent safety measures are not only a sign of companies' commitment, but also give society a sense of confidence that all necessary steps have been taken to protect cyberspace and consumer privacy. This contributes to a more positive attitude towards drone technology and its development and integration into society. Example sentence: It is an area that is constantly evolving and challenging scientists to come up with new and innovative ideas [3].

Through the efficiency and flexibility of operations in critical areas such as search and rescue, aerial photography and cargo transportation, UAVs have transformed various industries. Their rapid coverage of large areas and provision of real-time data make them invaluable for emergencies and even time-critical tasks. However, amidst the rapid development and increasing reliance on UAV technology, one of the most overlooked issues is safety. This is mainly related to cybersecurity and privacy when UAVs become an integral part of everyday transactions and are exposed to significant cyber threats that impact operators and the general public [4]. For example, when drones are used to transport life-saving resources such as medicine, nefarious characters can exploit the drones, leading to horrific results. A hacked medical drone can divert or delay vital supplies and even alter the route, resulting in catastrophic loss of property and human life. This demonstrates the urgent need for a robust security measure to prevent unauthorized access and disruption.

Drones are even equipped with better cameras and sensors, especially when it comes to inspecting critical infrastructure such as bridges, power plants or pipelines. Such systems could therefore intercept sensitive information and pass on false information to operators, which can lead to an incorrect assessment, which in turn can lead to operational disruptions and significant security breaches. All these vulnerabilities have far-reaching implications for public safety and national security [5]. Privacy is another major concern with UAVs. In most cases, the devices collect information from individuals or private properties, causing issues related to surveillance and unauthorized access to personal data. If left unsecured, this type of data can be misused and manipulated to violate privacy or compromise infrastructure security [6].

Behind all of this is an awareness of the potential dangers that can be encountered with drones. Likewise, students, teachers, parents and caregivers need to familiarize themselves with the problems of cyberbullying in today's digital age. Educating people about empathy and creating a sense of digital disruption helps communities understand why cyber safety is important. All of these security measures through encryption, access controls, as well as intrusion detection systems should ensure that not only is drone operation consistent, but also safe. Such preventive measures ensure that the UAVs remain intact, thus ensuring the safety and privacy of individuals and institutions involved in the use of such devices [9].

The extensive use of UAVs, commonly referred to as drones, in a number of industries has indeed contributed tremendously to technological improvements and operational efficiency [11]. Nowadays, the use of UAVs is indispensable in many areas of our society, such as military platforms and surveillance or reconnaissance tasks, industrial supply industries and disaster response. On the other hand, the widespread use of UAVs in conjunction with the security problem shows that the issue of security is imperative. UAVs have a wide range of cyber threats and physical attacks. These types of threats can compromise the security of UAV operations and the confidentiality of UAVI flight control data [15]. To control themselves, UAVs rely on a high level of computer systems and wireless communication infrastructure, creating the possibility of unauthorized access, hijacking, or interference. Furthermore, the changing nature of cybersecurity challenges, as well as insufficient digital capabilities and the pitfalls of physics, pose additional problems for UAV security. It is therefore very important to produce safe and stable drones while ensuring that they are fully trusted by the public and continue to operate safely and efficiently. This requires the adoption of strong safety programs that must be tailored to the specifics of the nature of drone systems and their existing limitations [20]. This analysis is conducted to explore the factual notion of cyber threats, which are multifaceted and consist of hacking, tampering and data exfiltration, and also emphasizes the need for organizations to adopt comprehensive security protocols. Through a case study looking at a range of defense tactics and technologies such as encryption, authentication and IDS, this report highlights how cyber threats to drones can be mitigated.

- It aims to classify the key security vulnerabilities of UAVs based on the vulnerability of software, hardware and communication links, primarily addressing unauthorized access, data breaches and GPS tampering.
- Evaluate the applicability of existing defense technologies to control the risks associated with UAVs, including encryption, authentication mechanisms and intrusion detection systems.

- Discuss privacy issues related to the operation of UAVs, particularly with regard to the collection and sharing of sensitive information, and assess the effectiveness of the legal framework for protecting individual privacy.
- Whether emerging technologies such as blockchain, machine learning and artificial intelligence can help create a secure UAV ecosystem while providing adaptable and scalable solutions to evolving threats.

Given the various applications of unmanned aerial vehicles in almost every other industries, there appear to be glaring risks to cybersecurity and data protection. UAVs can be exposed to various threats in this regard, such as unauthorised access to their systems and the resulting data breach. Currently, existing security measures, which include encryption and authentication protocols, cannot address the emerging threats and contain insufficient data protection provisions related to data collection under current regulations. The rapid development of UAV technologies is leading to an increase in the attack surface, which in turn is exposing the systems to sophisticated cyberattacks [21]. This review provides a holistic assessment of the vulnerabilities of UAVs in the area of cybersecurity and data protection. It analyses the effectiveness of currently available defence technologies and discusses the emergence of new technologies such as blockchain and machine learning in addressing such challenges. In addition, this paper identifies research gaps and provides recommendations for further studies that could be used to improve UAV security and privacy protection.

2 Literature Survey

This study is a comprehensive study on the security and privacy limitations of UAVs. To be comprehensive, the study must cover all major topics, from risk assessment to privacy issues, defense technologies, regulatory compliance, alternative views, and blogging, all of which equip a security fanatic with the necessary information about UAV security. The material is evaluated to create a security plan that includes encryption, authentication and intrusion detection systems, as well as the ever-changing nature of cyber and physical threats. This article highlights the importance of addressing the above issues to ensure the safe and responsible use of drones for a variety of applications. Therefore, further studies in this area are urgently needed. The main cybersecurity challenges related to drones are presented along with the required solutions. In their comprehensive analysis, the author and her co-authors conclude that drone cybersecurity encompasses the vulnerabilities, threats, attack vectors and defense mechanisms. This assessment points the finger at the cybersecurity issues that should be considered when using UAVs in aviation to ensure safe and accurate use for various applications. By defining the core of cybersecurity and exploring novel defense strategies, this paper provides important details for researchers and other stakeholders dealing with unmanned aerial vehicles (UAV) [2]. Yang Wenzheng and others discuss the security issues related to the Internet of Drones (IoD) and the possible solutions that can be used as preventive mechanisms. This topic is about awareness and protection of privacy and confidentiality in a network that is highly vulnerable and used by the military, emergency services and the entertainment industry. The author's critical assessment reports on some key security premises and how IoD security research has gone from strength to strength with blockchain-based authorization and authentication methods as its foundation. This article emphasizes the need for security prosthetics capable of walking the fine line between optimal protection and savings, and discusses the future directions of existing research to combat the ever-growing IoD threats [3].

Bitas et al. present a study detailing how machine learning (ML) is used in UAV (unmanned aerial vehicle) communication systems. Given the growing importance of UAVs in next-generation wireless communication networks, this article explores the presumed advantages and disadvantages they bring. UAVs extend the coverage and spectral efficiency for the operation of cellular networks, but they also bring some integration limitations. Therefore, the paper addresses machine learning platforms that can be useful for solving various problems of UAV communication systems. The authors conduct a critical literature review, thus introducing readers to the potential areas for network operation and design using machine learning, such as channel modelling, resource management, positioning, and security. The results obtained demonstrate the benefits of machine learning solutions and contribute to the existing understanding of their ability to improve the reliability and efficiency of UAV communication systems in various application scenarios [4].

In our research, we deal with the security problems that are associated with the implementation of the latest artificial intelligence technologies into unmanned aerial vehicles. Although DL augments the capability of CSPs, they also expose CSPCs to risks, especially in SiucCyPc where the safety of the CSPS where safety is inferred may be an issue. The topic of attention in this article is adversarial attacks against UAVs based on DNNs and considers the risks involved, particularly those against the regression models. We suggest that the adversaries can exploit two attack strategies to abuse the regression models. There have been successful cases where they forced the UAVs to leave the intended routes and maneuvers. Moreover, this paper reviewed and examined adversarial

training and defensive distillation methods, which are critical to the reliability of DL models in the UAV environment. Through this work, which points to the necessity of concentrating on countermeasures possessing equal power against adversarial attacks [5].

Ghulam E. Mohammad Abro and Anis Lauiti explain the progress in terms of recognition, safety, and communications. RF and radar are mentioned in the article as improved detection methods, and different parameters are used for classifying the UAVs, while different movements can be tracked depending on the method. The sentence is a bit confusing and unclear. While these achievements seem promising, the key matter still pertains to cybersecurity and confidentiality during the flying operation. In this document, the main focus is on security hardening procedures such as control signal inhibition and signal redirection for managing such a threat. Part of this is finding ways to regulate drone operations with particular attention to privacy regulations and standardization. These purposes may be fulfilled through the provision of recent updates about laws and communication techniques that would help the reader adequately understand UAV security and privacy issues. To sum up the article, future studies are highlighted in an effort to secure UAVs and respect the end users' data privacy. At the same time, the quest for innovative ways to mitigate new threats and difficulties of technology use is warranted.

The growing application of Unmanned Aerial Vehicles (UAVs) has faced serious cybersecurity and privacy issues that must be confronted for safe and secure operations. A review of the existing literature, now done, reveals many dimensions of UAV security in which studies have taken some focus on risk assessment, privacy concerns, encryption, authentication, and intrusion detection systems. These play a critical role in UAVs' protection against malicious attacks, unauthorized access, and data breaches. Though UAVs have revolutionized industries that currently include surveillance, logistics, and so much more, their vulnerabilities, especially related to the communication link as well as dependency on GPS, make them prone to different cyberattacks, such as GPS spoofing, data manipulation, and unauthorized control. These vulnerabilities thus risk not only data integrity but also public safety and privacy.

Recent research focuses extensively on issues related to privacy concerning UAVs. Outfitted with high-definition cameras as well as advanced sensors, UAVs can surely collect vast amounts of sensitive data that include personal information as well as information on critical infrastructure. This raises the question of violations of privacy, particularly when UAVs are operated over or near densely populated regions or on critical infrastructure. The literature does highlight the need for a good encryption protocol and safe means of communication that will protect against data breaches and illegal access. Some research also includes the evaluation of supportive technologies including encryption and intrusion detection systems, which would be used to counter attacks like jamming for GPS, DoS, and malware infections. However, the pace of UAV technology development should not be outpaced by the advancement of its security implementation, thereby providing loopholes in its defense mechanism.

In their work, Abro and all offer a detailed picture of the evolution of UAVs. In their study, they concentrate on the following fields: detection, security, and communication. The authors discuss the progress in these areas, from the detection and classification of UAVs to tracking, which also enables us to generate meaningful insights. Although the priceless progress in the domain of UAV operations is highlighted in this paper, the relevance of maintaining security and privacy is still underscored. The review provides strategies for enhancing security, such as observation and sending signals for interferences in the area elsewhere, which reduces dangers. This field also explores privacy matters concerning drone control and regulations. The role of UAV security and the strategies for making flying objects safe are addressed in the closing section of the research paper. This develops research on creative approaches to successfully combat new threats and attempts to grasp the capabilities which a are not possible with UAV technology [7]. Mohsen et al.'s research analyzes the broad areas of economy, trade, defense, and education, among others, by focusing on the improvement of control systems, miniaturization, and specialized technologies of the computer. As a result, the industry of UAVs has continued to expand. Although they have good qualities such as ultrafast access to accident areas and high mobility, UAVs possess several difficulties that need to be overcome in terms of autonomous flight, path planning, battery life, and payload capacity. This paper concentrates on the broader issues of UAVs, depicting, among others, types, swarm capabilities, classification, charging methods, and regulatory frameworks. In addition, we will inquire into different use cases, roadblocks, and safety issues that may arise with UAV operation. The study ends with a set of recommendations for future work aimed at enhancing UAV flight characteristics and tackling other challenges inherent in this field as a step toward a better direction for research in this area [8].

The comparative analysis of various UAV security perspectives is discussed below in Table 1.

Table 1: Literature Review: Security Perspectives in Unmanned Aerial Vehicle (UAV) Networks

S. No.	Authors	Title	Focus Areas	Drawbacks
1	Hadi, H. J. et al [1]	Comprehensive Survey on UAV Security	Security, Privacy, Defense Technologies	Vulnerabilities in communication protocols
2	Shafik, W. et al [2]	Cybersecurity in UAVs	Cybersecurity Review	Inadequate protection against malware injection
3	Yang, W. et al [3]	Security Issues and Solutions in the Internet of Drones	Security Concerns, Countermeasures	Vulnerabilities in firmware or software
4	Bithas, P. S. et al [4]	Machine Learning for UAV Communications	Machine Learning Techniques	Insufficient encryption of data transmission
5	Tian, J. et al [5]	Adversarial Attacks and Defenses for Deep Learning in UAVs	Deep Learning Security	Limited protection against GPS spoofing attacks
6	Abro, G. E. M. et al [6]	UAV Detection, Security, and Communication Advancements	Multi-faceted Review	Lack of intrusion detection systems
7	Mohsan, S. A. H. et al [7]	UAVs: Practical Aspects, Applications, Security, and Future Trends	Broad Overview	Lack of secure authentication mechanisms
8	Ly, B. & Ly, R [8]	Cybersecurity in UAVs	Cybersecurity Analysis	Potential for denial-of-service (DoS) attacks
9	Krishna, C. L. & Murphy, R. R [9]	Cybersecurity Vulnerabilities for UAVs	Vulnerability Assessment	Risks associated with insider threats
10	Javaid, A. Y. et al [10]	Threat Analysis and Modeling for UAV Systems	Cybersecurity Threat Modeling	Difficulty in ensuring end-to-end encryption
11	Gudla, C. et al [11]	Defense Techniques Against UAV Cyber Attacks	Defense Mechanisms	Vulnerabilities in UAV control interfaces
12	Dahiya, S. & Garg, M [12]	UAV Vulnerability to Cyber Attacks	Vulnerability Exploration	Challenges in securing remote access to UAV systems
13	Rani, C. et al [13]	Security of UAV Systems Against Cyber-Physical Attacks	Cyber-Physical Security	Risks associated with physical tampering or sabotage
14	COSAR, M [14]	Cyber Attacks on UAVs and Security Measures	Attack Landscape and Countermeasures	Lack of secure storage for sensitive data
15	Shivers, M. et al [15]	Artificial Immune System for UAV Cybersecurity	Bio-inspired Defense Approach	Inadequate protection against cyber-physical attacks
16	Niyonsaba, S. et al [16]	Survey on UAV Cybersecurity	Comprehensive Review	Risks associated with physical tampering
17	Sethuraman, S. C. et al [17]	Cyber Attacks on Healthcare via UAVs	Emerging Threat Area	Challenges in securing UAV-to-UAV

				communication
18	Manesh, M. R. & Kaabouch, N [18]	Cyber Attacks on UAV Networks: Detection, Countermeasures, and Future Research	Network-centric Security Analysis	Potential for signal jamming attacks
19	Tomlin, C. J [19]	Secure Estimation for UAVs Against Adversarial Attacks	Resilient Control Systems	Risks associated with unauthorized firmware updates
20	Wiik, J. H [20]	Cybersecurity and Cryptography in Unmanned Systems	Cryptographic Methods for Security	Insufficient protection against side-channel attacks
21	Fotohi, R [21]	Securing UAS Against Security Threats using Human Immune System	Bio-inspired Security Approach	Challenges in ensuring secure payload delivery
22	Petnga, L. & Xu, H [22]	Security of UAVs: Dynamic State Estimation Under Cyber-Attacks	State Estimation Security	Vulnerabilities in ground control stations
23	Wang, Z. et al [23]	Survey on Cybersecurity for UAVs	Comprehensive Review	Lack of comprehensive security training for personnel
24	Tsao, K. Y. et al [24]	Cyber Security Threats and Solutions for UAV Communications	Communication Security Analysis	Risks associated with third-party integrations
25	Jeler, G. E. & Alexandrescu, .[25]	UAV Vulnerability Analysis to Cyber Attacks	Vulnerability Assessment	Challenges in ensuring regulatory compliance
26	Faughnan, M. S. et al [26]	Risk Analysis of UAV Hijacking and Detection Methods	Risk Analysis and Detection Techniques	Potential for reputation damage in case of security breaches
27	Farrukh, Y. A. & Khan, I [27]	Self-Incremental Learning for UAV Cyber Attack Detection	Machine Learning for Intrusion Detection	Lack of secure storage
28	Orhun, D. Ö. Ş. et al [28]	Hybrid Cyber Security of UAVs	Multi-layered Security Approach	DoS attacks
29	Haque, M. S. & Chowdhury, M. U [29]	Ad-hoc Framework for UAV Network Security	Efficient Network Security Design	GPS spoofing

The disjoint nature of the integration of technological and regulatory solutions is seen predominantly in the literature. While most studies see technical defenses of encryption and authentication protocols being discussed, few review the necessity of bringing regulatory compliance in with these technologies. Effective UAV security measures not only require robust technical means but also robust legal frameworks for the establishment of guidelines on the operation of UAVs so that privacy and security standards are met. Furthermore, the literature often fails to consider the long-term impacts of UAV security breaches in terms of public safety, critical infrastructures, and the environment.

The existing research also lacks an investigation into emerging technologies such as blockchain, machine learning, and artificial intelligence for security improvement in UAVs. While some touch on the prospects of

these technologies in enhancing encryption and intrusion detection systems, empirical evidence that might be used in real-world scenarios to enhance security is lacking. These technologies, especially machine learning and AI, can be the core of adaptive security systems and may be able to identify and mitigate threats in real time. Further research would be necessary to understand them thoroughly regarding their effects and limits concerning securing UAV systems. With the steady and rapid advancement of UAV capabilities, it has brought along increased vulnerability; thus, scalable and cost-effective measures for security are vitally needed, which can keep up with the great changes.

This raises new dangers: since decision-making algorithms are increasingly important to the UAV, these can themselves be potential targets for powerful cyberattacks. Even less representation in the literature has focused on sufficient treatment of issues on how to secure these algorithms and against manipulation. Current studies fail to address any of these matters concerning the integration of AI-driven security measures and risks from AI-enabled attacks. The solution to all of the above issues will provide the key to the safe operation of UAVs in an increasingly complex and interwoven world.

3 Taxonomy of Cyber Attacks in UAV s

The classification of cyberattacks targeting Unmanned Aerial Vehicles (UAVs) serves as a foundational framework for categorizing the various threats that compromise the safety of these systems. This classification acts as a representation method that informs UAV operators, specialists, and cybersecurity researchers in developing their protective strategies, grounded in an understanding of the fundamental characteristics of cyberattacks, including data interception, manipulation, and disruption. Figure 1 illustrates notable cyberattacks that jeopardize the confidentiality, integrity, and availability of UAV systems. This representation enhances the visualization and comprehension of the risk landscape associated with unmanned aerial vehicle operations. As privacy-related threats in the cyber domain escalate, it becomes increasingly challenging to detect communications intercepted by attackers targeting private exchanges between UAVs and Internet of Things (IoT) devices. Research has identified specific vulnerabilities, such as active eavesdropping and jamming techniques, underscoring the urgent need for heightened awareness regarding information security. Additionally, the functionalities of keyloggers and malware that capture keystrokes and compromise data integrity present significant privacy concerns, illustrating the growing complexity of cyber threats within UAV systems. Integrity attacks, including man-in-the-middle attacks and GPS spoofing, represent a category of threats that undermine the authenticity and reliability of data exchanged among UAV systems.

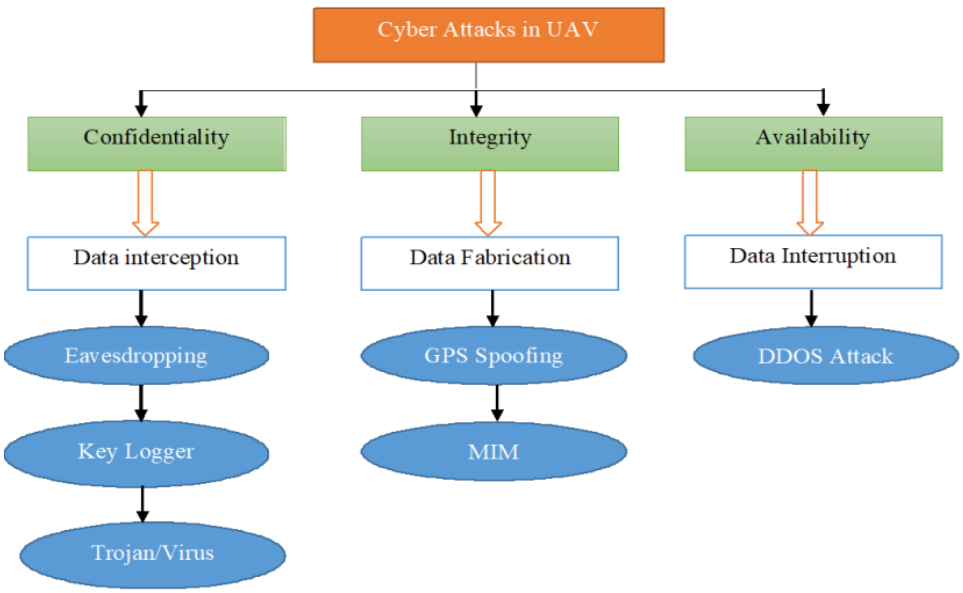


Figure 1: Taxonomy of cyber attacks

These vulnerabilities grant adversaries the opportunity to access the data exchange, alter, or even manipulate the information, which in certain instances could lead to the hijacking of UAV controls or interference with sensitive data. Notably, availability attacks, particularly Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, hold particular importance. They disrupt UAV services and communications, presenting significant challenges that underscore the need for strategic enhancements[35,36,37]. Nevertheless, the evolving landscape of cyber threats necessitates the refinement of existing research initiatives, which predominantly focus on developing innovative cybersecurity measures, including encryption, anomaly detection, and layered defense strategies, to protect UAV systems from malicious actions that could compromise their operational effectiveness[38,39,40].

Figure 1 illustrates a kind of cybersecurity attacks, severely affecting UAVs belonging to type. These attacks fall into three main types: data breach, data altering and also data blocking or manipulation. This categorisation will help to explain why cyber threats exist for UAV systems and affords for a much wider range [41,42]. It also adds on to the skill you possess in developing individual protection strategies that will work well to tolerate these hazards. Figure 1 elegantly illustrates the various ways UAVs are attacked – with these notches in confidentiality, integrity and availability removed. Therefore, it is a powerful tool for users of UAVs, cybersecurity experts and researchers. By this we shall be able to recognize possible those susceptible points and ensure that the available measures are robust enough to prevent cybercrimes.

As the main part, a security system set in Fig.2 that is confident to plan out the security of UAV systems with the data router to serve as the basic structural element. This framework is specifically designed to strengthen cyber security implemented on UAVs and deter data hacking incidents, including interception, manipulation, and much more. The purpose of this setup is to reinforce the communication, reliability and the availability of UAV networks by introducing routers as one of the components of the system, consequently reducing the chances of unauthorized access to the system, data tampering and service failures [46,47,48]. A multi-router network is essential for ensuring secure and uninterrupted communication across the UAV channel net and between the UAV and its Ground Control System [49]. Sophisticated security protocols and encryption mechanisms used by the router as a result provide a shield from eavesdropping attacks, keyloggers and viruses.

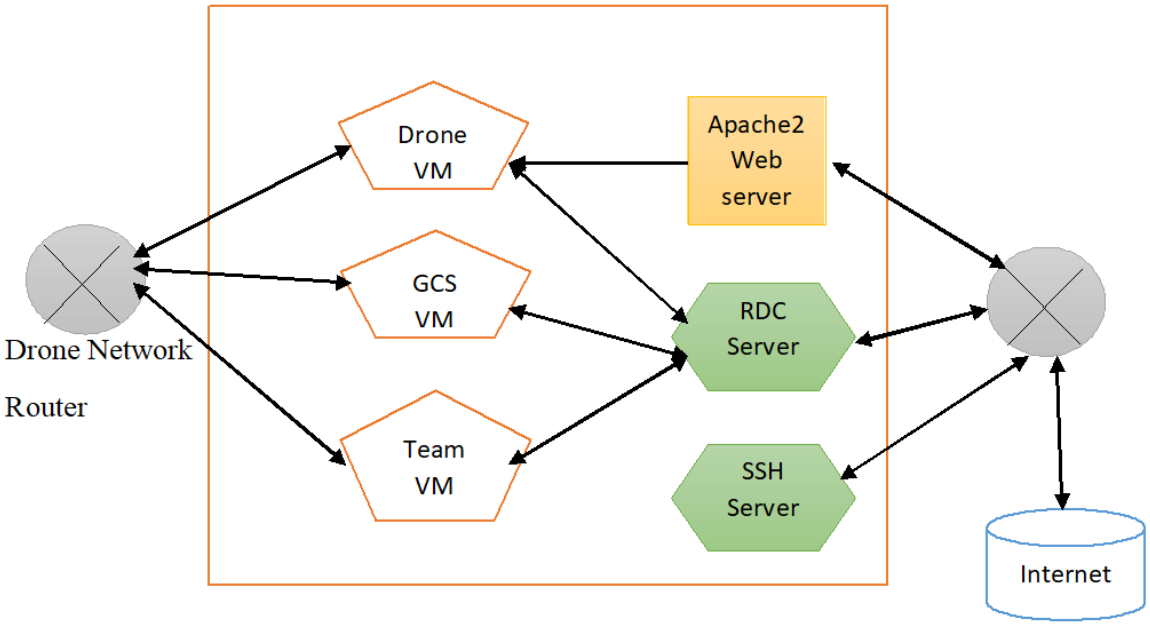


Figure 2: Defense framework for UAV systems

In addition, sensitivity of commands and control messages transmitted through the router is also guarded by it [50,51]. Furthermore, the architecture of the system is designed in a way that an intrusion and prevention system is installed inside of the router that is likely to enhance the resistance of the UAV system to new security risks by

discovering and averting cyber threats in a timely fashion [52]. In summary, Figure 2 brings into the limelight the main reason for the use of preventive measures in the cyber security and also shows the fact that the network router is the principal factor in the prevention of cyberattacks [53,54,55].

4 Classification Methods for Detecting Cyber Attacks in UAVs

Sophisticated techniques are necessary to detect cyberattacks in Unmanned Aerial Vehicles (UAVs) because of the distinct challenges they present and the vulnerabilities they possess. Various classification methods, such as those utilizing machine learning, anomaly detection, and intrusion detection systems, can be employed for this task. Below are some commonly employed classification methods for identifying cyberattacks in UAVs.

4.1 Machine Learning-Based Intrusion Detection Systems (IDS)

Labeled datasets are used to train machine learning models by applying supervised learning techniques. In the approach, each data item is mapped to a particular category. This annotated data, used in this way, requires a clear labeling of normal and abnormal behavior in a dataset, respectively. These different supervised learning models, such as Support Vector Machines (SVM), Random Forests, Decision Trees, and Neural Networks, are capable of identifying patterns and connections between the system data extracted from UAV system data and their corresponding labels. Subsequently, these models may be utilized to keep a record of the new cycle of behavior as normal or the one linked to the cyber-attack solely based on the online courses previously conducted [62].

Semi-Supervised Learning becomes highly applicable while performing cybersecurity activities in those situations where properly labeled data is not available or is expensive. This strategy employs a blend of labeled and unlabeled data and proceeds to utilize the information from both sources to leverage the accuracy in detection. In UAV cybersecurity, semi-supervised learning methods can help systems make use of a limited amount of labeled data by merging additionally available unlabeled data for elite model predictions, reducing errors, and thus, the machine learns to forecast new types of attacks and adapt to dynamically developing threats.

Learning without supervision, here are the types of machine learning that can be used to identify or discover anomalies or patterns in data without the need for labeled examples. Utilizing unsupervised learning methodologies such as cluster algorithms or autoencoders in UAV cybersecurity contexts can be beneficial to us in detecting any anomalous behavior based on the data structure alone. The approaches that are effective when data is labeled with scarcity of any kind or even unavailability still assist in the detection of new attacks or those previously unseen in UAV systems by means of identifying peculiar patterns or outliers in system logs, sensor readings, or network traffic.

The reinforcement learning way of computing cyber-attacks in UAVs is of another kind where the access problem can be considered in the context of the sequential act of decision-making. By employing reinforcement learning algorithms, the drone can optimize its defense techniques under dynamic forces to confront ever-changing strategies, as well as the evolving nature of threats. When their endless learning of reinforcement learning is used, UAV systems can gradually absorb a lot of knowledge about both successful and unsuccessful attacks in real environments and make them capable of recognizing and combating cyberattacks. Therefore, this gives them an advantage over all the sneaky modern adversaries who are slick [63].

4.2 Anomaly Detection Techniques:

Statistical Methods is the method that is based on the exponential statistical characteristics like average, variance, or higher-order moments through which the data can be described. The drawing of profiles is feasible for cyber attack detection in UAVs. The method is based on the utilization of the statistical approach to revealing the normal behavior via analyzing historical data. By crunching numbers that settle across different attributes, targets are on areas such as network traffic, system resource utilization, or sensor readings; things that are not similar to the pattern can be picked out. Observations that exceed the defined statistical thresholds should alert the system to potential cyberattacks, which should trigger further investigations or actions to mitigate the risk of perceived risk [64].

Machine Learning-Based Anomaly Detection may be applied to utilize supervised, semi-supervised, or unsupervised learning techniques that can pinpoint the outliers or anomalies in data, capable of suggesting cyber attacks. The ensemble algorithms like One-Class SVM, Isolation Forests, or Gaussian Mixture Models are usually used for classifying anomalies in supervised learning. Applying such techniques to the field of UAV cybersecurity, these methods can develop to discriminate between the patterns associated with normal and abnormal behaviors from system logs, network traffic, or sensor data. Through the practice of training models on

either variably annotated or unlabeled datasets, the machine learning anomaly detection can be adjustable whenever new attack strategies inevitably appear and can detect previously unknown threats in UAV systems.

Using Time-Series Analysis, we can view data generated over time chronologically and identify patterns or changes that can create suspicions about cyber attacks. In the case of UAVs, data streams might feature flight trajectories, sensor data, records of communications, and system performance metrics that have been captured during operation. Using techniques like moving averages, auto correlation, or Fourier transforms, it is possible to detect irregular trends or any departures from the standard change pattern. Time-series analysis is highly useful in recognizing very delicate but temporal-dependent phenomena in UAV systems, so these threats can potentially be detected before they evolve into adverse consequences [65].

4.3 Deep Learning Approaches:

The DL Approaches involve a robust computing system that enables the detection of cyber attacks targeting UAVs through the automatic assimilation of intricate interpatterns and the interpretation of raw data. Deep Neural Networks (DNNs) excel particularly in data analysis, which is essential for aerial systems utilizing UAVs that generate a wide array of dynamic data streams overwhelming the systems. The DNNs employed by UAV operators will facilitate the development of advanced models for cyber attack detection, adept at identifying subtle indicators of cyber threats within sensor data, communication logs, and system variables through thorough examination.

Systems that utilize Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Graph Neural Networks (GNNs) are well-equipped to address the specific challenges associated with predicting cyber attacks in Unmanned Aerial Vehicles (UAVs). CNNs are adept at processing spatial data, including images and sensor data with spatial orientation, making them suitable for tasks such as detecting anomalies in image records or analyzing spatial patterns in data derived from UAV footage. RNNs, which are capable of modeling sequences, can effectively analyze time-series data generated by UAVs, enabling the identification of temporal patterns that may signal cyber threats. Additionally, GNNs can be employed to model relational data, which may encompass communication networks or interactions between UAVs and ground control systems, thereby facilitating the observation of deviations in network behavior that could indicate potential attacks[65].

The DL Approaches involve a robust computing system that enables the detection of cyber attacks targeting UAVs through the automatic assimilation of intricate interpatterns and the interpretation of raw data. Deep Neural Networks (DNNs) excel particularly in data analysis, which is essential for aerial systems utilizing UAVs that generate a wide array of dynamic data streams overwhelming the systems. The DNNs employed by UAV operators will facilitate the development of advanced models for cyber attack detection, adept at identifying subtle indicators of cyber threats within sensor data, communication logs, and system variables through thorough examination[66].

4.4 Real-time Monitoring and Response:

Instantaneous surveillance and reaction have an imperative part in cyber-threat detecting for UAVs and operators themselves can prevent the attacks in a minute. Sensor data, TVs, transmission channels and gadget logs are continuously monitored for suspicious activities and abnormal behavior. This monitoring covers aspects as network patterns of the traffic, metrics of performance system, sensor readings and communication protocols. Therefore, among the most critical action in this field include fast motions made from the use of sensors and equipment which enables operators recognize abnormal behavior almost immediately enabling them to prevent or minimize possible cyber-attacks [67]. Once a threat is spotted, the system goes into action to facilitate fast and precise actions. This results in a quick and specific response to the problem and the effect of the cyber attack will be lessened if not averted. These procedures could include a deactivation of affected components, and whatever service appears vulnerable; or they may even entail the deployment of active defense tools to restrict further taunting of infrastructure undermining efforts. Moreover, the\ human operators can be alerted to take a look at the incident in more detail, get more information, and manually respond to the situation once they deem it necessary [68].

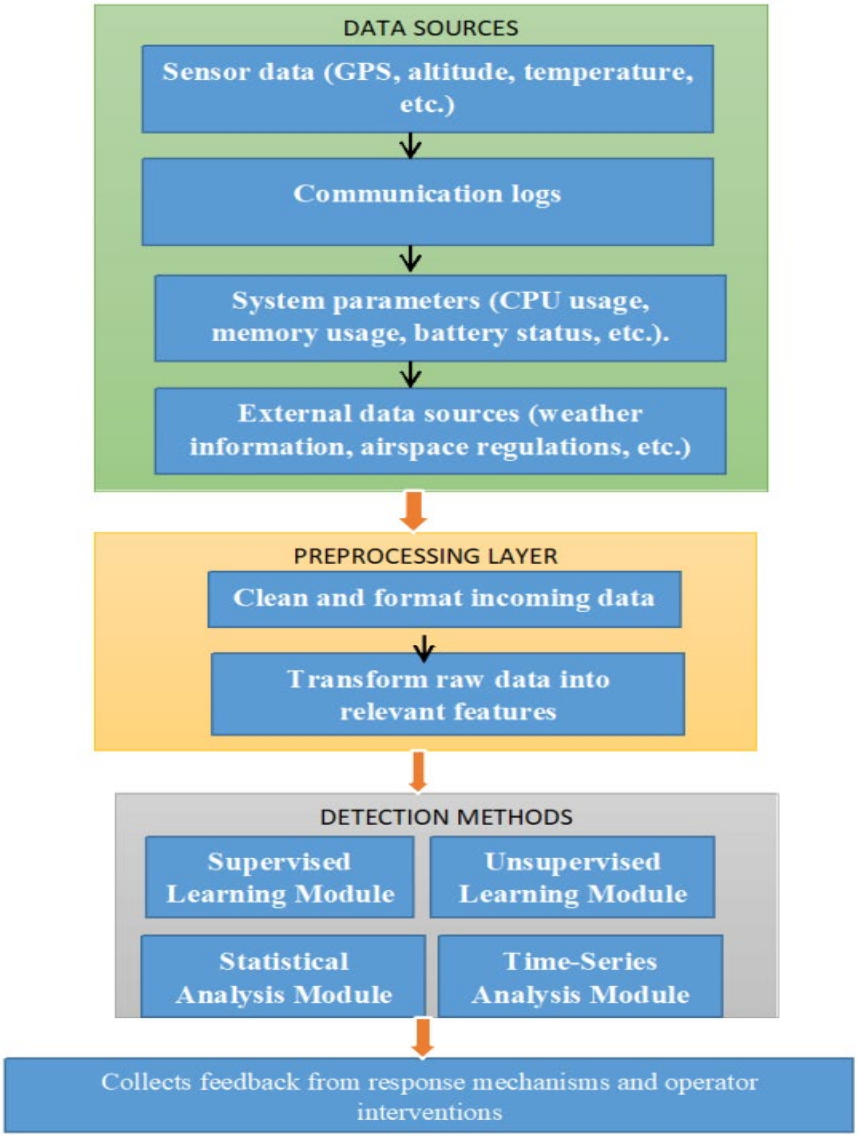


Figure 3: Classification models in identifying cyber-attacks in UAV

In the field of cyber attacks detection in UAVs, a complex approach which comprise of a diversity of tools including those that are UAV attack-specific is vital, as UAV operation have their own challenges. There are supervised learning methods, which use labeled datasets to train classifiers such as Support Vector Machines, Random Forests, and neural networks. These classifiers have been trained to distinguish between normal and anomalous behavior by the way they identify and define abnormal behavior in a given area. On top of this supervised learning, semi-supervised learning uses partially labeled data mainly in the processes that add a bonus to labeling when the obtaining of fully labeled datasets is costly or impractical, thus enabling detection with fewer labeling resources. Unsupervised learning algorithms, including clustering and autoencoders, provide means for spotting failings without labeled data, which becomes extremely helpful for the process of discovering novel attacker techniques or discreet deviations from standard behavior. The total architecture of model is illustrated in Figure 3 as well.

Data analytic tools, ML modeling and storing historical data are able to work together to provide alternative procedures to detecting cyber attacks in unmanned aerial vehicles. Statistical methods are more suitable for establishing normal behavior baselines that use simple measures such as standard deviation and spatial patterns

fall under machine learning-based anomaly detection algorithms which are capable of identifying outliners a probable poison attacks. Time-series analysis provides with clues as to what those patterns are, increasingly important in tracking dynamic threats or complex tactics. These methods when properly integrated constitute proactive monitoring and detection systems that permit the UAV operators to respond quickly to cyber attacks and consistently protect their operations from the possible threats that come their way in dynamic environments. Furthermore, artificial intelligence capabilities like CNN, RNN, and GNN allow operators to discern the complex structures from raw data independently, leading to enhanced identification capabilities and rapid adaptability with the arising situation. Similarly, immediate detection and response systems are other toolsets that clearly define cyber resilience.

5 Discussion

This dataset was compiled by collecting standard and attack data from rural mobile vehicles using the UAVCAN v0 (Drone CAN) protocol. This serves as a valuable resource for improving safety measures in UAVs. By including scenarios involving Flooding, Fuzzy, and Replay attacks, the dataset provides a comprehensive overview of the potential security threats faced by UAVs operating on the UAVCAN protocol. Based on this dataset, a testbed built using PX4 was created to provide researchers with the tools necessary to develop and validate an intrusion detection system (IDS) specifically designed to reduce security risks and protect UAVs from malicious attacks. . This initiative promotes innovation in UAV cybersecurity, contributing to ongoing efforts to improve the resilience and security of UAV systems [60].

Various attacks on UAV systems reveal serious vulnerabilities that demand deep knowledge of both mechanisms of attack and defense strategies that can neutralize them. Among these attacks, there are two: GPS spoofing attack, which involves false GPS signals sent by the attacker to fool the UAV navigation system, letting the attacker control the flight path or even cause loss of UAV location. The spoofing device uses the unencrypted nature of the GPS signal, hence often inexpensive. Proposals include advanced encryption methods for GPS signals to protect UAVs from false signals. Multi-sensor fusion helps detect UAVs by combining data from varied onboard sensors, such as barometers and inertial measurement units, to correct the inconsistency associated with GPS data. These sensor inputs are compared with GPS readings by the UAVs in order to detect anomalies such as spoofing attempts and remedial measures can be taken accordingly. Machine learning models also enable detection of anomalous navigation patterns, which enables UAVs to switch to safer modes of operation after detecting suspicious behavior.

Another kind of well-known attack is jamming, wherein an attacker would transmit high-power signals on the UAV's communication frequencies that have the effect of blocking the control as well as navigation signals. This usually results in loss of responsiveness and airframe communication with the control station. Strategies adopted in defense against jamming include the use of frequency-hopping spread spectrum (FHSS), which is a technique whereby the channel of communication rapidly switches across several frequencies, thus confusing attackers who cannot at the same time jam all channels. Directional antennas are also used to focus the communication signals along a particular direction so that an unknown jamming is less likely. UAVs can also be equipped with anti-jamming algorithms that are used to identify the presence of a jamming attempt based on the signal-to-noise ratios or packet loss rates. The anti-jamming algorithms enable the UAV to switch over to the alternative communication protocols or frequencies so that it doesn't lose its control links.

MITM attacks are considered those in which an attacker places himself between the UAV and its ground control station to intercept or manipulate communications. Most often, these attacks occur as eavesdropping on sensitive data or alteration of UAV commands. To be able to prevent MITM attacks, the key aspect is that there should be end-to-end encryption in communication between the UAV and its controller. Finally, encryption is critical, where intercepted communication will be unreadable to an attacker if he or she does not have relevant decryption keys. Another defense component is PKI, under which the UAV and control station authenticate each other before exchanging any information using digital certificates; at least one party will then be illegitimate in such attacks, reducing the risk of MITM attacks. In addition to this, SSL or TLS protocols augment the security of communication. It ensures that intercepted data during an MITM attack are encrypted and hence useless for attackers.

Malware Infiltration-Another serious threat to UAVs is the malware infiltration, where attackers inject malicious software into the UAV onboard system or control station. Such malware could be introduced through rogue or infected software updates or vulnerable control systems, which would then lead to the unauthorized control, theft of data, or disruption of flight operations about the UAV. To prevent such malware infiltration, most UAVs are fitted with IDS's which monitor real-time data and communications for suspicious activities. If the IDS

detects an anomaly such as unauthorized accesses or abnormal patterns of data transmission, it can alert operators and trigger action against the threat. Periodic software audits and updates are also vital to ensure the vulnerability is patched, therefore lessening the exploitation of malware. With the introduction of sandbox environments in some UAV systems, critical processes are isolated from the other parts of the operating system, thereby denying malware access to critical system components.

The created dataset, which was built based on the extraction of standard and attacking data from the rural mobile vehicles by using UAVCAN v0, also known generally as Drone CAN, boosted the development of UAV cyber security, and hence, it was implemented in UAVs to collect real-time communication data both in standard and compromised scenarios. Currently, the most popular protocol for UAV component communication is UAVCAN. Such attacks were incorporated into this system, basically mimicking some attack scenarios in real life through the use of Flooding, Fuzzy, and Replay attacks. Flooding attacks simply swamp the UAV's communication system with an avalanche of messages that it cannot handle with the intention of either causing delays or denial of service. Fuzzy attacks can be used in sending malformed or unwanted messages to exploit existing vulnerabilities in the UAV protocol of communication. These replay attacks then intercept the legitimate messages and forward them for deception later to persuade the UAV to execute false commands.

The last threat is to unauthorized access and hijacking of UAVs. Threats arise when attackers use weak passwords or communication protocols to hijack an UAV. Once access is obtained, attackers can take UAVs off course, compromise safety mechanisms, or exfiltrate sensitive data. MFA provides a powerful layer of protection since users have to authenticate more than once with different means such as a password and a security token, in order to log into the system. It thus enhances security because it's quite challenging for the attacker to infiltrate this system despite the stolen login credentials. The security further enhances through role-based access control that limits the functionality that various users may perform since only authorized staff may have access to critical UAV operations. Also, periodic firmware integrity checks have to be done to detect unauthorized changes in the control software of the UAV. These ensure that any deviation of the trusted firmware is identified and appropriate action may be taken, such as reverting to a previous version.

Table 2: Cybersecurity Performance analysis for UAV Systems

S.No.	Type of Attack	Defence System	Number of Detected Cyber Attacks	Incident Response Time	System Downtime
1	Eavesdropping	Cryptography	15	2 hours	30 minutes
2	Keylogger	Anomaly Detection	8	4 hours	45 minutes
3	GPS Spoofing	Signal uthentication	12	3 hours	1 hour
4	DoS/DDoS Attacks	Intrusion Detection	20	1.5 hours	2 hours

Table 2 presents an evaluation of the cybersecurity effectiveness of UAV systems, concentrating on four categories of cyberattacks: espionage, serious keylogging, position falsification, and DoS/DDoS attacks. Each row corresponds to a specific type of attack and provides data such as the utilization of protective measures, the number of detected attacks, incident response times, as well as information regarding system failures and recovery [56, 57]. An example of encryption applied within the attack defense system is illustrated in the context of eavesdropping attacks, where the system itself is subject to eavesdropping. The table indicates that fifteen instances of shoofly sabotage were identified, with a response time of two hours and a system downtime of thirty minutes. In this scenario, the cryptocurrency security system demonstrates a high level of competence in detecting various types of attacks promptly, thereby minimizing system disruptions and reducing associated risks. However, for keylogging attacks, this unusual detection serves as a protective measure as well [58, 59]. The table reveals that keyloggers and screen scraping were employed in the attacks, with keyloggers occurring eight times. The response time was set at four hours, with system downtime recorded at forty-five minutes. Despite the longer response times, the system effectively detected keylogger attacks, resulting in only moderate system downtime. This assessment underscores the pressing need for robust defensive systems specifically designed to address diverse cyber threats to ensure the safety of UAV systems.

Table 3: UAV Security Defense Metrics

S.No.	Defense Method	False Positive Rate	Mean Time to Detect (MTTD)	Mean Time to Respond (MTTR)
1	Intrusion Detection System	0.05	1 hour	2 hours
2	Machine Learning Algorithms	0.08	1.5 hours	3 hours
3	Signature-Based Detection	0.03	45 minutes	1.5 hours
4	Behavior-Based Detection	0.06	2 hours	4 hours

Table 3 is designated as UAV Security Protection Indicators. It outlines the security technologies employed in the protection schemes against UAV cyber threats. The effectiveness of each protection method is assessed based on the false alarm rate, mean time to detection (MTTD), and mean time to respond (MTTR). The Intrusion Detection System (IDS) demonstrates a low false positive rate of 0 hours, with an average detection time (MTTD) of 1 hour and an average response time (MTTR) of 2 hours. In contrast, the machine learning algorithm exhibits a slightly elevated false positive rate of 0.08, requiring 1.5 hours for detection and 3 hours for response. The signature-based detection method, however, boasts a commendable false positive rate of 0.03, achieving detection in 45 minutes and a response time of 1.5 hours. In summary, the overall system achieves detection within 2 hours and a response time of 4 hours, resulting in a false positive rate of 0.06. These systems leverage historical data to enhance their learning capabilities, potentially increasing their resilience against increasingly complex cybersecurity threats. Signature-based detection methods represent another preventive strategy, utilizing known viruses or attack patterns to compare incoming data against established signatures, thereby facilitating the rapid identification of recognized threats. The detection methodologies can be categorized into two groups. The first group comprises behavioral-based methods, where machine learning algorithms identify anomalies associated with UAV systems and network traffic. By collecting data, a baseline of behavioral profiles can be established, enabling swift detection and response to anomalies that may indicate a targeted cyberattack. This approach embodies a multi-layered security strategy that integrates various security technologies to thwart all forms of cyberattacks against UAV systems, including intrusions, data breaches, and system failures.

Table 4: Machine Learning Model Performance in Detecting Cyber Attacks in UAV

Model	Accuracy	Precision	Recall	F1 Score	AUC-ROC
Support Vector Machines (SVM)	0.95	0.93	0.91	0.92	0.97
Random Forests	0.94	0.92	0.90	0.91	0.96
Decision Trees	0.88	0.85	0.82	0.83	0.90
Neural Networks	0.97	0.95	0.94	0.94	0.98
One-Class SVM	0.91	0.88	0.85	0.86	0.93
Isolation Forests	0.93	0.90	0.88	0.89	0.95
Gaussian Mixture Models (GMM)	0.90	0.87	0.84	0.85	0.92

The data presented in Table 4 clearly illustrates the performance of various machine learning models in identifying cyber threats within UAVs. The metrics highlighted include accuracy, precision, recall, F1 score, and AUC-ROC score, which are essential for evaluating model effectiveness. Each model, including SVM, showcases its ability to classify normal versus anomalous behavior. Additionally, models such as Random Forests, Decision

Trees, Neural Networks, One-Class SVM, Isolation Forests, and Gaussian Mixture Models demonstrate their capacity to differentiate similar phenomena. This research lays the groundwork for the incorporation of these models into cyber threat intelligence systems, where they rank highly with accuracy scores ranging from 0.88 to 0.97, consistently achieving strong results in precision, recall, F1 score, and AUC-ROC. Figure 4 provides a visual representation of the machine learning models.

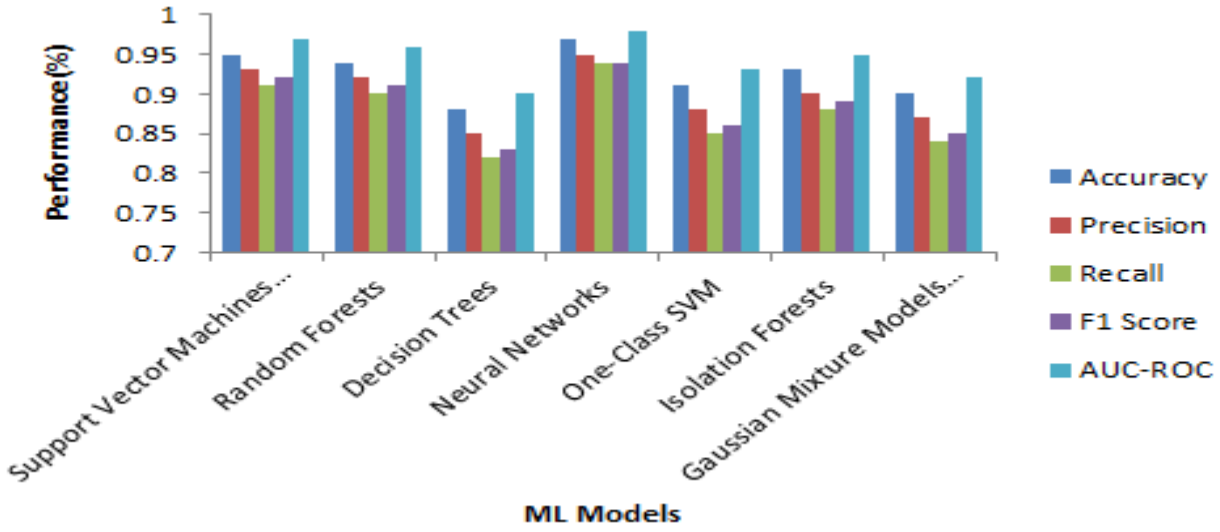


Figure 4: ML models and its performance for accuracy, precision, recall,F1 Score,AUC-ROC

Table 5: Deep learning Model Performance in Detecting Cyber Attacks in UAV

Model	Accuracy	Precision	Recall	F1 Score	AUC-ROC
Convolutional Neural Networks (CNN)	0.96	0.94	0.92	0.93	0.98
Recurrent Neural Networks (RNN)	0.93	0.91	0.89	0.90	0.96
Graph Neural Networks (GNN)	0.95	0.93	0.91	0.92	0.97

Table 5 illustrates the superiority and advancement of deep learning models in their effectiveness at detecting cyber attacks in unmanned aerial vehicles (UAVs). The capabilities of Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Graph Convolutional Networks (GCN) are highlighted, demonstrating their ability to differentiate between various behaviors of UAV systems, including both normal and anomalous activities. These models are particularly valuable in reinforcing UAV operations by addressing sensory overload and facilitating timely identification and mitigation of cyber threats. The accuracy rates for these models range from 0.93 to 0.96, and they consistently perform well across various metrics, including precision, recall, F1 score, and AUC-ROC. Consequently, they serve as effective tools for proactively and reliably enhancing the security of UAVs. The results of the deep learning models are visually represented in Figure 5.

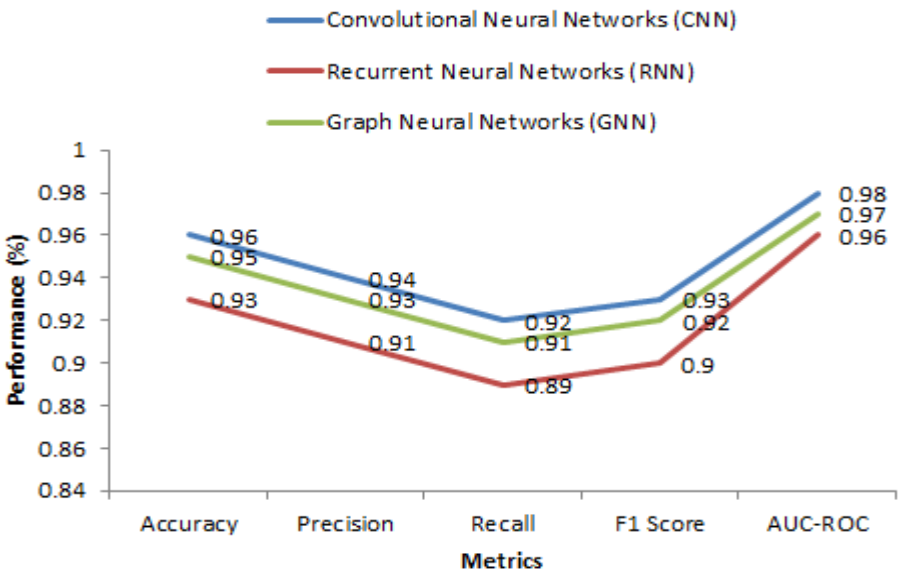


Figure 5: DL models and its performance analysis

Table 6: Analysis of Statistical Methods for Cyber Attack

Statistical Method	**Value**
Mean	15.2
Variance	25.6
Standard Deviation	5.1
Median	12.5
Mode	8
Correlation	0.75
Chi-Square Test	18.2
ANOVA	0.04
Regression Analysis	0.92
Time-Series Analysis	0.88

Table 6 offers an in-depth analysis of the statistical methods commonly utilized in the identification of cyber-attacks, along with specific metrics that demonstrate their real-world application. The techniques span from fundamental statistics such as mean, variance, and standard deviation to more sophisticated inferential approaches including correlation, the Chi-Square Test, and ANOVA. Each method presents unique insights into the data produced by UAV systems. Additionally, regression analysis and time-series analysis are essential for elucidating relationships between variables and recognizing temporal trends, thereby enhancing the capacity to detect anomalies that could signify cyber-attacks.

Figure 6 presents the annual distribution of research analyses carried out in the field. The bar chart displays the quantity of research analyses conducted each year, offering insights into the trends of academic activity over time. This visualization facilitates an understanding of the temporal dynamics of research endeavors, emphasizing possible areas of concentration or changes in interest within the discipline.

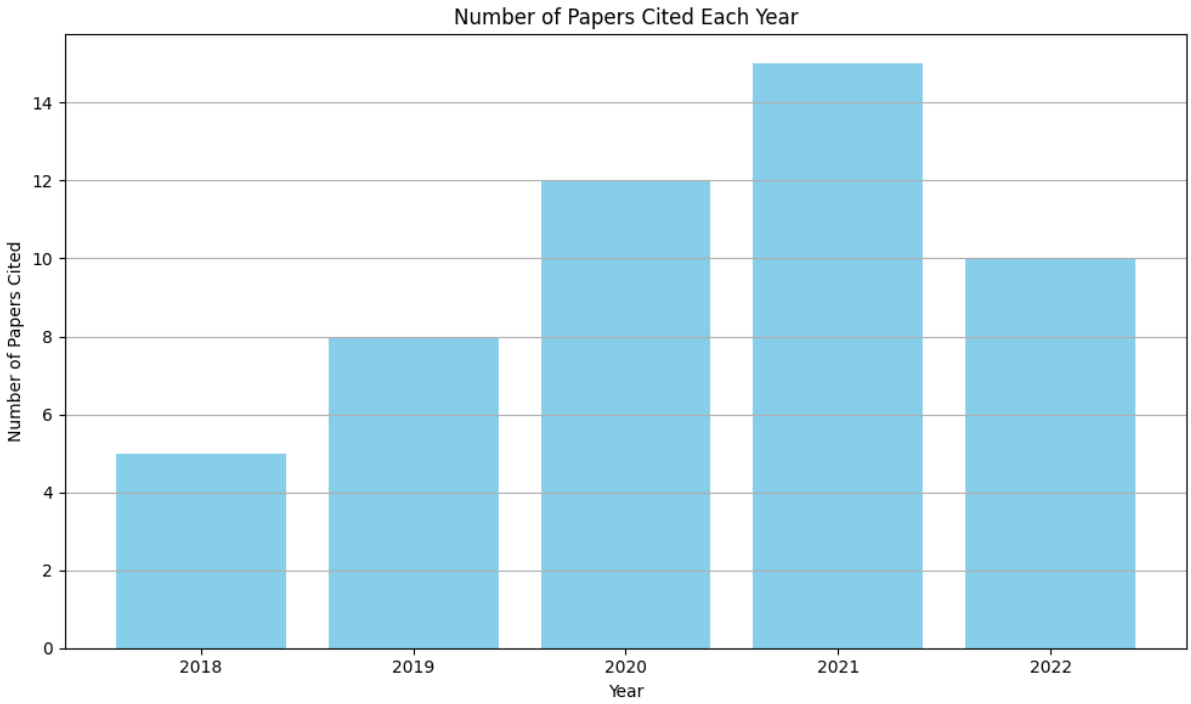


Figure 6: Number of research analysis (Year wise)

6 Research Gaps

In the field of cyberattack detection against UAVs, there are several areas that require attention in order to increase knowledge and develop effective defenses. First, the emergence of targeted attacks on UAV systems poses a major challenge. Current research has not yet fully explored the techniques to defend against these sophisticated attacks, highlighting the need for innovative strategies to strengthen detection models against the manipulation of UAV sensor data and communication channels.

Second, real-time adaptation of defense mechanisms is a critical area that needs to be further explored. As cyber threats evolve rapidly, it is crucial for UAV systems to dynamically adapt their defense strategies in response to emerging threats. Research in this area could focus on developing adaptive algorithms that continuously learn from new data and update detection models in real time to ensure a timely and effective response to evolving cyber threats.

Finally, while anomaly detection techniques show promise in detecting unusual behavior indicative of cyberattacks, there is a gap in interpretability. Current methods often lack transparency in explaining the nature and causes of detected anomalies. Future research efforts could explore methods to improve the interpretability of detected anomalies and provide actionable insights and explanations to human operators to facilitate informed decision making in cybersecurity operations for UAV systems. Addressing these research gaps is critical to improving the cyber resilience of UAVs and ensuring their safe operation in dynamic and hostile environments.

In the review paper presented here, we have attempted to provide the reader with a comprehensive overview of today's UAV cybersecurity by highlighting different types of attacks that can occur and defense mechanisms. Nevertheless, we have not conducted our own experiments, although we have discussed the dataset collected from land mobile vehicles using the UAVCAN v0, known as Drone CAN, and even mentioned the theoretical framework of a testbed that could be built using the PX4 autopilot framework. Our main interest was to synthesize the existing literature and potentially identify gaps in it.

Although the aspect of practical experimentation is crucial for the validation of a theoretical model, we have cited the PX4 framework as a recognized tool in the UAV research community and widely used for such purposes. Our review does not include empirical results or direct experiments. Future researchers in this field could use the findings we have presented here in our review, as well as the testbed we have discussed for conducting practical experiments to test some of the theoretical approaches we have discussed. We clarify this point to avoid any confusion about what exactly falls within the remit of our paper, as well as the context for the part of the PX4 framework mentioned here as a potential platform for further study.

7 Conclusion and Future Works

To summarize, it is important to protect UAV systems from cyber threats to ensure safe and efficient operations in various fields. Cyber attack classification provides a systematic approach to understanding and organizing potential risks so that individual defense strategies can be implemented. It highlights the wide range of threats that UAV systems face from a variety of actors, including nation states, cyber criminals, cyber terrorists and hacktivists. Addressing these challenges requires defense mechanisms such as intrusion detection systems, machine learning algorithms, signature-based detection and behavior-based detection to quickly identify and respond to cyber threats. Future advances in UAV cybersecurity could focus on several areas to further strengthen defense capabilities. First, continued research and development is needed to improve the sophistication and accuracy of detection algorithms, particularly in the detection of new and zero-day attacks. In addition, integrating threat information sharing and cooperative defense mechanisms can improve the overall resilience of the UAV ecosystem against coordinated cyber threats. Furthermore, improving the interoperability and compatibility of cybersecurity solutions with existing UAV platforms and communication protocols will facilitate integration and deployment in a variety of operational environments. Ultimately, maintaining a proactive cybersecurity posture through continuous awareness training and threat modeling exercises is critical to proactively respond to evolving cyber threats and protect the integrity, confidentiality and availability of UAV systems

Acknowledgements

We would like to express our gratitude to the experts whose valuable insights and feedback significantly contributed to the validation and improvement of our article.

References

[1] Hadi, H. J., Cao, Y., Nisa, K. U., Jamil, A. M., & Ni, Q. (2023). A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs. *Journal of Network and Computer Applications*, *213*, 103607.

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

[3] Yang, W., Wang, S., Yin, X., Wang, X., & Hu, J. (2022). A review on security issues and solutions of the internet of drones. *IEEE Open Journal of the Computer Society*, *3*, 96-110.

[4] Bithas, P. S., Michailidis, E. T., Nomikos, N., Vouyioukas, D., & Kanatas, A. G. (2019). A survey on machine-learning techniques for UAV-based communications. *Sensors*, *19*(23), 5170.

[5] Tian, J., Wang, B., Guo, R., Wang, Z., Cao, K., & Wang, X. (2021). Adversarial attacks and defenses for deep-learning-based unmanned aerial vehicles. *IEEE Internet of Things Journal*, *9*(22), 22399-22409.

[6] Abro, G. E. M., Zulkifli, S. A. B., Masood, R. J., Asirvadam, V. S., & Laouiti, A. (2022). Comprehensive review of UAV detection, security, and communication advancements to prevent threats. *Drones*, *6*(10), 284.

[7] Mohsan, S. A. H., Othman, N. Q. H., Li, Y., Alsharif, M. H., & Khan, M. A. (2023). Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. *Intelligent Service Robotics*, *16*(1), 109-137.

[8] Ly, B., & Ly, R. (2021). Cybersecurity in unmanned aerial vehicles (UAVs). *Journal of cyber security technology*, *5*(2), 120-137.

[9] Krishna, C. L., & Murphy, R. R. (2017, October). A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In *2017 IEEE international symposium on safety, security and rescue robotics (SSRR)* (pp. 194-199). IEEE.

[10] Javaid, A. Y., Sun, W., Devabhaktuni, V. K., & Alam, M. (2012, November). Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In *2012 IEEE conference on technologies for homeland security (HST)* (pp. 585-590). IEEE.

[11] Gudla, C., Rana, M. S., & Sung, A. H. (2018). Defense techniques against cyber attacks on unmanned aerial vehicles. In *Proceedings of the international conference on embedded systems, cyber-physical systems, and applications (ESCS)* (pp. 110-116). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[12] Dahiya, S., & Garg, M. (2020). Unmanned aerial vehicles: Vulnerability to cyber attacks. In *Proceedings of UASG 2019: Unmanned Aerial System in Geomatics 1* (pp. 201-211). Springer International Publishing.

[13] Rani, C., Modares, H., Sriram, R., Mikulski, D., & Lewis, F. L. (2016). Security of unmanned aerial vehicle systems against cyber-physical attacks. *The Journal of Defense Modeling and Simulation*, *13*(3), 331-342.
[14] COSAR, M. (2022). Cyber attacks on unmanned aerial vehicles and cyber security measures. *The Eurasia Proceedings of Science Technology Engineering and Mathematics*, *21*, 258-265.
[15] Shivers, M., Llanes, C., & Sherman, M. (2019, November). Implementation of an artificial immune system to mitigate cybersecurity threats in unmanned aerial systems. In *2019 IEEE International Conference on Industrial Internet (ICII)* (pp. 12-17). IEEE.
[16] Niyonsaba, S., Konate, K., & Soidridine, M. M. (2023). A Survey on Cybersecurity in Unmanned Aerial Vehicles: Cyberattacks, Defense Techniques and Future Research Directions. *International Journal of Computer Networks and Applications*, *10*(5), 688-701.
[17] Sethuraman, S. C., Vijayakumar, V., & Walczak, S. (2020). Cyber attacks on healthcare devices using unmanned aerial vehicles. *Journal of medical systems*, *44*(1), 29.
[18] Manesh, M. R., & Kaabouch, N. (2019). Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. *Computers & Security*, *85*, 386-401.
[19] Hu, Q., Chang, Y. H., & Tomlin, C. J. (2016). Secure estimation for unmanned aerial vehicles against adversarial cyber attacks. *arXiv preprint arXiv:1606.04176*.
[20] Wiik, J. H. (2020). Cybersecurity and cryptographic methods in unmanned systems-a study of the current state in unmanned aerial vehicles and similar systems.
[21] Fotohi, R. (2020). Securing of Unmanned Aerial Systems (UAS) against security threats using human immune system. *Reliability Engineering & System Safety*, *193*, 106675.
[22] Petnga, L., & Xu, H. (2016, June). Security of unmanned aerial vehicles: Dynamic state estimation under cyber-physical attacks. In *2016 International Conference on Unmanned Aircraft Systems (ICUAS)* (pp. 811-819). IEEE.
[23] Wang, Z., Li, Y., Wu, S., Zhou, Y., Yang, L., Xu, Y., ... & Pan, Q. (2023). A survey on cybersecurity attacks and defenses for unmanned aerial systems. *Journal of Systems Architecture*, *138*, 102870.
[24] Tsao, K. Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks*, *133*, 102894.
[25] Jeler, G. E., & Alexandrescu, G. (2020). Analysis of the vulnerabilities of unmanned aerial vehicles to cyber attacks. *Review of the Air Force Academy*, (2), 17-26.
[26] Faughnan, M. S., Hourican, B. J., MacDonald, G. C., Srivastava, M., Wright, J. P. A., Haimes, Y. Y., ... & White, J. C. (2013, April). Risk analysis of unmanned aerial vehicle hijacking and methods of its detection. In *2013 IEEE systems and information engineering design symposium* (pp. 145-150). IEEE.
[27] Farrukh, Y. A., & Khan, I. (2021). An autonomous self-incremental learning approach for detection of cyber attacks on unmanned aerial vehicles (UAVs). *arXiv preprint arXiv:2112.11219*.
[28] Orhun, D. Ö. Ş., KARAKOCA, Y. E., CAMADAN, E., & BAYKALI, F. (2023). Hybrid cyber security of unmanned aerial vehicles. *International Journal of Applied Methods in Electronics and Computers*, *11*(4), 179-185.
[29] Haque, M. S., & Chowdhury, M. U. (2019). Ad-hoc framework for efficient network security for unmanned aerial vehicles (UAV). In *Future Network Systems and Security: 5th International Conference, FNSS 2019, Melbourne, VIC, Australia, November 27–29, 2019, Proceedings 5* (pp. 23-36). Springer International Publishing.
[30] Lattimore, G. L. (2019). *Unmanned aerial system cybersecurity risk management decision matrix for tactical operators* (Doctoral dissertation, Monterey, CA; Naval Postgraduate School).
[31] Ippolito, C. A., & Krishnakumar, K. S. (2019). An Interface-based Cybersecurity Analysis Methodology for Untrusted Sub-Systems on Unmanned Aerial Systems. In *AIAA Scitech 2019 Forum* (p. 1459).
[32] Sathyamoorthy, D. (2015). A review of security threats of unmanned aerial vehicles and mitigation steps. *J. Def. Secur*, *6*(1), 81-97.
[33] Haider, M., Ahmed, I., & Rawat, D. B. (2022, July). Cyber threats and cybersecurity reassessed in uav-assisted cyber physical systems. In *2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN)* (pp. 222-227). IEEE.
[34] Tran, T. D., Thiriet, J. M., Marchand, N., & El Mrabti, A. (2022). A cybersecurity risk framework for unmanned aircraft systems under specific category. *Journal of Intelligent & Robotic Systems*, *104*(1), 4.
[35] Wang, L., Chen, Y., Wang, P., & Yan, Z. (2021). Security threats and countermeasures of unmanned aerial vehicle communications. *IEEE Communications Standards Magazine*, *5*(4), 41-47.

[36] Rahman, M. A., Rahman, M. T., Kisacikoglu, M., & Akkaya, K. (2020, October). Intrusion detection systems-enabled power electronics for unmanned aerial vehicles. In *2020 IEEE CyberPELS (CyberPELS)* (pp. 1-5). IEEE.
[37] Al-Dosari, K., & Fetais, N. (2023). A new shift in implementing unmanned aerial vehicles (UAVs) in the safety and security of smart cities: a systematic literature review. *Safety*, *9*(3), 64.
[38] Mansfield, K. M., Eveleigh, T. J., Holzer, T. H., & Sarkani, S. (2015). DoD comprehensive military unmanned aerial vehicle smart device ground control station threat model. *Defense Acquisition Res. J.*, *22*(2), 240-273.
[39] Kwon, C., Yantek, S., & Hwang, I. (2016). Real-time safety assessment of unmanned aircraft systems against stealthy cyber attacks. *Journal of Aerospace Information Systems*, *13*(1), 27-45.
[40] Keshavarz, M., Shamsoshoara, A., Afghah, F., & Ashdown, J. (2020, July). A real-time framework for trust monitoring in a network of unmanned aerial vehicles. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 677-682). IEEE.
[41] Shaikh, E., Mohammad, N., & Muhammad, S. (2021, March). Model checking based unmanned aerial vehicle (UAV) security analysis. In *2020 international conference on communications, signal processing, and their applications (ICCSPA)* (pp. 1-6). IEEE.
[42] Sachdeva, H., Gupta, S., Misra, A., Chauhan, K., & Dave, M. (2022). Improving privacy and security in unmanned aerial vehicles network using blockchain. *arXiv preprint arXiv:2201.06100*.
[43] Aldaej, A., Ahanger, T. A., Atiquzzaman, M., Ullah, I., & Yousufudin, M. (2022). Smart cybersecurity framework for IoT-empowered drones: Machine learning perspective. *Sensors*, *22*(7), 2630.
[44] Alexandre, R. C. J., Martins, L. E. G., & Gorschek, T. (2023). Cybersecurity Risk Assessment for Medium-Risk Drones: A Systematic Literature Review. *IEEE Aerospace and Electronic Systems Magazine*.
[45] Al-Bkree, M. (2023). Managing the cyber-physical security for unmanned aerial vehicles used in perimeter surveillance. *International Journal of Innovative Research and Scientific Studies*, *6*(1), 164-173.
[46] Podins, K., Stinissen, J., & Maybaum, M. (2013). The Vulnerability of UAVs to Cyber Attacks-An Approach to the Risk Assessment. In *5th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn* (Vol. 515).
[47] Fotohi, R., Nazemi, E., & Aliee, F. S. (2020). An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks. *Vehicular Communications*, *26*, 100267.
[48] French, R., & Ranganathan, P. (2017). Cyber attacks and defense framework for unmanned aerial systems (uas) environment. *J Unmanned Aerial Syst*, *3*, 37-58.
[49] Whelan, J., Sangarapillai, T., Minawi, O., Almehmadi, A., & El-Khatib, K. (2020, November). Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles. In *Proceedings of the 16th ACM symposium on QoS and security for wireless and mobile networks* (pp. 23-28).
[50] Negash, L., Kim, S. H., & Choi, H. L. (2017). Distributed observes for cyberattack detection and isolation in formation-flying unmanned aerial vehicles. *Journal of Aerospace Information Systems*, *14*(10), 551-565.
[51] Marinenkov, E. D., Viksnin Ilya, I., Zhukova, I. A., & Usova, M. A. (2018). Analysis of information interaction security within group of unmanned aerial vehicles. *Journal Scientific and Technical Of Information Technologies, Mechanics and Optics*, *117*(5), 817-825.
[52] Gnatyuk, S. (2019, October). Multilevel unified data model for critical aviation information systems cybersecurity. In *2019 IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD)* (pp. 242-247). IEEE.
[53] Tian, J., Wang, B., Guo, R., Wang, Z., Cao, K., & Wang, X. (2021). Adversarial attacks and defenses for deep-learning-based unmanned aerial vehicles. *IEEE Internet of Things Journal*, *9*(22), 22399-22409.
[54] Sandoval, S. (2018). Cyber security testing of the robot operating system in unmanned aerial systems. *Naval Postgraduate School Monterey United States*.
[55] Goppert, J., Shull, A., Sathyamoorthy, N., Liu, W., Hwang, I., & Aldridge, H. (2014). Software/hardware-in-the-loop analysis of cyberattacks on unmanned aerial systems. *Journal of Aerospace Information Systems*, *11*(5), 337-343.
[56] Majeed, R., Abdullah, N. A., Faheem Mushtaq, M., Umer, M., & Nappi, M. (2021). Intelligent cyber-security system for IOT-aided drones using voting classifier. *Electronics*, *10*(23), 2926.

[57] Molina, A. A. (2023). *Machine Learning for Intrusion Detection of Cyber-Attacks in Unmanned Aerial Vehicles* (Doctoral dissertation, The George Washington University).
[58] Whelan, J., Almehmadi, A., & El-Khatib, K. (2022). Artificial intelligence for intrusion detection systems in unmanned aerial vehicles. *Computers and Electrical Engineering*, *99*, 107784.
[59] Kateb, F., & Ragab, M. (2023). Archimedes Optimization with Deep Learning Based Aerial Image Classification for Cybersecurity Enabled UAV Networks. *Computer Systems Science & Engineering*, *47*(2).
[60] Dataset Collection: https://ocslab.hksecurity.net/Datasets/uavcan-attack-dataset
[61] Halimaa, A., & Sundarakantham, K. (2019, April). Machine learning based intrusion detection system. In 2019 3rd International conference on trends in electronics and informatics (ICOEI) (pp. 916-920). IEEE.
[62] Chriki, A., Touati, H., Snoussi, H., & Kamoun, F. (2020, July). Uav-based surveillance system: an anomaly detection approach. In 2020 IEEE Symposium on computers and communications (ISCC) (pp. 1-6). IEEE.
[63] Yuvaraj, R., Sarveshwaran, V.," Modified hunter prey optimization to enable secure communication for UAV", *International Journal of Information Technology (Singapore*,Springer, Jan 2024,16(3),pp. 1569-1579.
[64] Khan, S., Liew, C. F., Yairi, T., & McWilliam, R. (2019). Unsupervised anomaly detection in unmanned aerial vehicles. Applied Soft Computing, 83, 105650.
[65] Zeggada, A., Melgani, F., & Bazi, Y. (2017). A deep learning approach to UAV image multilabeling. IEEE Geoscience and Remote Sensing Letters, 14(5), 694-698.
[66] Osco, L. P., Junior, J. M., Ramos, A. P. M., de Castro Jorge, L. A., Fatholahi, S. N., de Andrade Silva, J., ... & Li, J. (2021). A review on deep learning in UAV remote sensing. International Journal of Applied Earth Observation and Geoinformation, 102, 102456.
[67] Choi, K., & Lee, I. (2012). A UAV based close-range rapid aerial monitoring system for emergency responses. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, 38, 247-252.
[68] Lin, F., Fu, C., He, Y., Xiong, W., & Li, F. (2021). ReCF: Exploiting response reasoning for correlation filters in real-time UAV tracking. IEEE Transactions on Intelligent Transportation Systems, 23(8), 10469-10480.