A Systematic Literature Review on the security of Unmanned Aerial Vehicle System

Tirth Patel *
*School of Engineering,
University of Guelph, Ontario, Canada
tpatel04@uoguelph.ca
Niyatiben Salot †
†School of Engineering,
University of Guelph, Ontario, Canada
nsalot@uoguelph.ca
Vrusha Parikh ‡
‡School of Engineering,
University of Guelph, Ontario, Canada
parikhv@uoguelph.ca

Abstract—Unmanned aerial vehicles (UAVs) are becoming more common, and their operational range is expanding tremendously, making the security aspect of the inquiry essential. This study does a thorough assessment of the literature to determine the most common cyberattacks and the effects they have on UAV assaults on civilian targets. The STRIDE assault paradigm, the challenge they present, and the proper tools for the attack are used to categorize the cyber dangers discussed in this paper. Spoofing and denial of service assaults are the most prevalent types of UAV cyberattacks and have the best results. No attack style demands the employment of a hard-to-reach gadget, indicating that the security environment currently necessitates improvements to UAV use in civilian applications.

Index Terms—SLR, Cyber Security, Cyber Attacks, UAV, Unmanned Aerial Vehicle, Drone, Security.

1 Introduction

The Unmanned Aerial Vehicle is an acronym for UAV, an air vehicle without any onboard pilot. The aircraft is controlled remotely by a controller which is on the ground or the UAV can fly autonomously with the complex pre-programmed model [1]. It is also called a Remotely Piloted Vehicle (RPV) when pilotless aircraft are operated from the ground via electronically controlled equipment. UAVs are used for observatory and tactic planning. UAVs are capable of maintaining the flight level which is powered by jet propellers or reciprocating engines. UAVs can be categorized into use for government, commercial and hobby purposes. [2] There are a plethora of functional uses for UAVs like military training by providing both sky and ground coverage of arms with a specific target and also helping in simulating enemies' air vehicles, reconnaissance, combating, for logistics: delivering cargo, improving technologies with research and development in UAVs and commercial/civil purpose of taking agriculture information and aerial photography. Unmanned Aerial vehicles have a great use to a certain level easing the work of humankind with economical financial cost [3].

Modern-day UAVs are helpful for tracking wildfires, observing the evolution of the hurricane, a survey of landscaping, and disaster relief. Several regions worldwide have put in a joint effort with innovators and have discovered ingenious ways of use [4]. A wireless network controls the device in the air [3]. The directions given to the drone and the data collected must be supported via a network [5], [6]. Encryption of the data collected through UAV must be checked for the security performance of the network [7]. The data collected through the drones vary on the purpose of the application and the device used. Data collected for agriculture has information on humidity, dampness of the soil, etc. while the data collected from the health department has information on heartbeats, disease type, etc. Data collected is not always private and confidential but data obtained should be secured when transmitted with the network and further as well [8].

Due to the escalating worries over the security of UAV software, there has been very little exploratory work. The existing drone security environment has been thoroughly examined as part of this research [9]. [10] The Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) threat model is used to categorize the cyberattacks in the research and identify the dangers they represent as well as the tools required to carry them out.

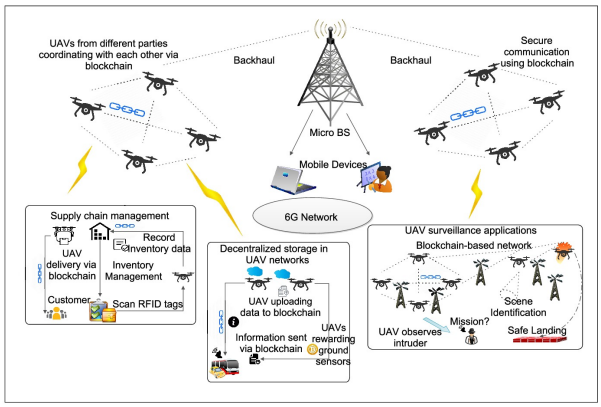

Fig. 1. Drones Applications

1.1 Prior research

Unmanned aircraft are seen as a new and developing category of "flying IoT" gadgets [11]. They include a number of applications. As stated by Alladi et al. [3] Unmanned Aerial Vehicle is more susceptible to being lost, hijacked, or destroyed since it is deployed in open-air space. Many network problems need to be taken into consideration like intra-communication, surveillance, protection of data in the air, data storage, and management because drone technology is now omnivorous. Blockchain, for instance, is a distributed ledger that uses encryption techniques like the hash function and public keys cryptography to protect shared data [12]. Additionally, it may be used to confirm the accuracy of the data that has been processed and to increase the safety and openness of UAVs. Flaws in security systems have many severe implications.

However, the upsurge in manufacturing to meet the rising demand has created a number of security flaws or vulnerabilities [13]. A number of issues make it feasible for an enemy to crash the device, causing the drone to malfunction and hurting network users. Significant flaws allow the hacker to totally control the control system and seize the UAV or anything it is holding [14]. Drones are often deployed for recording or monitoring in both private and commercial settings, and any cyberattack may frequently entail worries about privacy and other hazards.

Challenges of drones as security and privacy: Shakhatreh et al. [11] discussed the civil uses of Drones and their main difficulties. A study of the UAVs' cybersecurity vulnerabilities was done by Krishna et al. [15]. The authors suggested a taxonomy to categorize various UAV cyberattack types.

Privacy and Security issues in the communication of drones: The significant security concerns of Aircraft wireless connectivity were reviewed by Fotouhi et l. [16]. According to Mishra et al. [17], the incorporation of Drones into cellular networks like 5G introduces security problems that must be adequately addressed and analyzed by the scientific community. Hayat and co. addressed the UAV's privacy, security, and safety concerns networks from the perspective of communication. then offered UAV networks' standard communication requirements for a UAV deployment that is safe, secure, and protects privacy.

1.2 Research Goals

The objective of this research is to review earlier research, synthesize its conclusions, and focus on the security of Unmanned Aerial vehicles. To make the work more focused, we developed three research questions, as shown in Table. 1.

TABLE 1
Research questions.

Research Questions(RQ)	Discussion
RQ1: What are recent advances for pre-venting information loss of UAVs?	Routing protocols are necessary for multi-UAV networks to offer dependable end-to-end data transfer between UAV nodes. In the literature, a number of network applications have been presented with various classifications. One method divides these protocols into two categories: data forwarding and network architecture.
RQ2: Is any secured method available for communications the drones?	Communication methods vary from the use case of drones, thus we need a standard method for communication. In the papers, there are several methods proposed that are being used and can be used to mitigate the risk and have smooth communication.
RQ3: How is the security measured for overtaking attacks done at various types of stages like level of communication, hardware level, sensor level, and software level?	These stages are well structured for the best use of UAVs. In the papers, a very small number of studies have talked about all of the stages. We found that most of the studies have a level of communication and a few have hardware-level security measurements.

1.3 Contribution and Layouts

Current research is complemented by this SLR, which offers the For those interested in blockchain technology, the following contributions using cyber security to advance their work.

- We identify 30 primary studies during the search of IoT and UAV papers in the specific field.
- We analyze the data collected by the various studies and present the findings to provide an updated view of the UAV. Through the review, we hope to gain a deeper understanding of this subject.
- The goal of this review is to examine the several strategies that can be used to increase the safety of various cyber technologies.
- To encourage additional research in this field, we establish guidelines and make representations.

Table 1 summarizes the three relevant research questions and provides a discussion section where relevant topics can be discussed. The discussion section will also cover the various aspects of UAV Security.

2 Research Methodology

There are many studies have been carried out on Unmanned aerial vehicles. Rather than its speed, technology, safety, or its design. For the systematic review, we have taken guidance from the paper of Kitchen ham and Charters [18]. We have agreed to go through phases of Selection, Scanning, Prioritizing, and Extraction to get the best for our SLR.

2.1 Selection of primary studies

Research studies were found by passing the search keyword or string to the search engines or publications to get the primary studies. The keyword selection was done to proliferate research and can able to find the paper for answering the research questions. The search string was as below:
The data was extracted using the boolean operator AND and OR, which were used as search strings:
The boolean operators are as follows for IEEE: *"Unmanned Aerial Vehicle" OR "IoT" AND (" Cyber Security" OR "security")*.
Based on INSPEC the search strings are: *"IoT" AND "UAV" AND " communication" AND ("networking" OR "security")*.

The digital library platforms used during the research are as follows:
- IEEE Xplore Digital Library
- SpringerLink
- Google Scholar
- UOG Library
- ScienceDirect

The search was run through description, abstract, or title on the basis of the platforms. This search was done on 1st Oct 2022. After filtering from Inclusion and Exclusion criteria, which will be discussed further. The criterion enabled us to generate a set of outcomes that were then subjected to Wohlin's snowballing process [19].

2.2 Inclusion and Exclusion criteria

The goal of this article is to provide a review of the literature on cybersecurity in UAVs, with a particular focus on cybersecurity issues and solutions in this setting. The following research questions were posed for this study:
RQ1: What are recent advances for preventing information loss of UAVs?
RQ2: Is any secured method available for communications the drones?
RQ3: How is the security measured for overtaking attacks done at various types of stages like level of communication, hardware level, sensor level, and software level?
The study selection criteria were used to determine the most relevant papers for the review. The results of the search were then analyzed using Google scholar to find the most relevant papers. Table 2 illustrates the criteria for the inclusion and exclusion of the papers for the primary studies.

2.3 Selection results

Hundreds of research papers were searched under the above-mentioned search string related to UAV and Cyber Security. After removing duplicates and irrelevant studies, 450 research papers were there to analyze using Inclusion and exclusion criteria. After the criteria were applied a total of 25 papers remained. Snowballing both forward and backward revealed an additional 2 and 3 papers, bringing the total number of papers to be included in this SLR to 30

2.4 Quality assessment

In this section, we assess the research papers on the basis of their quality of writing, their ideas, and their experimental ideas based on guidance by Kitchenham and Charter [18]. This assessment gives us knowledge of the content of the primary studies. This assessment is followed by the assessment described by Hosseini et al. [20]. Randomly 4-5 papers will be tested on 4 stages of assessment, in each stage, we look for specific data, if the research paper passes all the stages, we would include those papers in our SLR, otherwise, we have to drop them. Those stages are as follows. After this assessment, it has been detected that there are 9 studies that do not meet the requirement, that's why removed from the SLR. Refer to table.

TABLE 2
Inclusion and exclusion for primary studies

Criteria for Inclusion	Criteria for exclusion
The paper must have information regarding UAVs.	Paper focusing mainly on the economic side of the UAV.
The paper must have cyber security or UAV security-related data.	Paper with just cyber security.
The paper must possess information regarding cyber attack and their prevention.	Any global blogs or internet source data.

The stages of finding the excluded studies, as seen in Table 3, are as follows:
Stage 1: **Unmanned Aerial Vehicle.** The studies must be on UAVs and their functions or have a case study on UAVs.
Stage 2:**Security.** The studies must have information on the security of UAVs.
Stage 3: **Cyber Attacks.** Studies must have data on the cyber attack that can be done on drones
Stage 4: **Data Context** The studies must have ample information on each stage and can be verified.

2.5 Data extraction

Now that we have our final research papers, we plan how to extract information from them. As our topic is related to security, the first thing we look for is security purposes. We want those papers, which has in-depth data regarding the security of the UAVs and we will use data on UAVs provided by other papers to examine it . We created two categories in which we divided the papers to conduct further research. Those categories are:
UAV: Use-case and Functions.
Security: Threats, attacks and possible solutions.

2.6 Data analysis

We gathered the information included in the qualitative and quantitative data categories in order to achieve the

goal of responding to the study questions. Additionally, we performed a meta-analysis on the studies that underwent the last step of data extraction.

2.6.1 Publications over time

The concept of the Unmanned Aerial Vehicle goes back to 1849. After that many researchers studied this concept and presented their ideas on this. However, there is a very inclination in field research after 2010. In 2010 there is 200 studies presented on Unmanned Aerial vehicles. As we see in the chart, there is the most upward trend in the use case and research of Unmanned Aerial Vehicle over the period of time.

TABLE 3
Excluded studies

Checklist for the Criteria Stages	Excluded Studies
Stage 1: Unmanned Aerial Vehicles.	[21], [22]
Stage 2: Security	[23], [24]
Stage 3: Cyber Attacks	[22], [25], [23]
Stage 4: Data Context.	[26], [27]

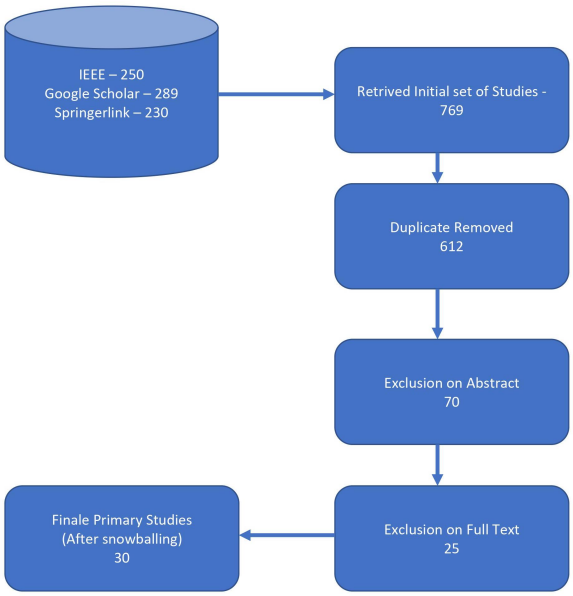

Fig. 2. Attrition of papers through processing

2.6.2 Significant keyword counts:

In order to identify the theme of the selected primary studies we have to summarize the keywords count in the table. Using this table we can determine how much a keyword inspires the topic of the paper. From the table, it can be seen that the word "UAV" and "Cyber-Security" were the most frequent, after that the third most frequent word was "Cyber-attack". So, it can be said that lately, everyone is focusing on cyber attacks over UAVs or any other IoT devices.

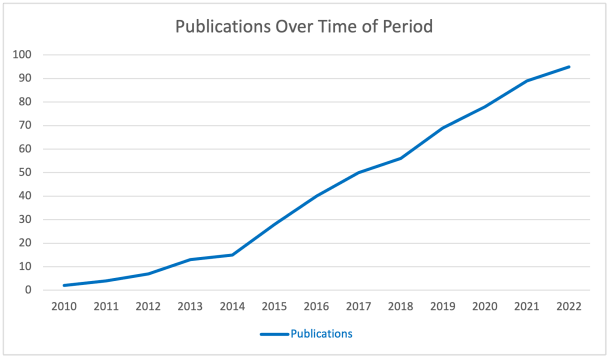

Fig. 3. Number of primary studies published over time.

3 Findings

Following a thorough reading of each primary research paper, pertinent qualitative and quantitative information was gathered, and then condensed in Table 5, Table 6 and Table 7. With respect to how Unmanned Aerial Vehicles was addressing a specific issue, all of the major studies had a focus or topic. Additionally, Table 5, Table 6 and Table 7 below lists each paper's focus. To make it easier to classify the primary studies' topics, each paper's focus was further divided into wider groups. In the area of the network between UAV and the base station, studies that focused on virtual machines, networking, and virtual network management were gathered. In the area of data storage and sharing, studies with an emphasis on peer-to-peer sharing, encrypted data storage, and search were compiled. fig 3. demonstrates the percentages of the 30 primary studies' various topics that met the criteria for inclusion in the data analysis. The themes found in the primary research show that the security and privacy of IoT devices account for nearly half (42 %) of all studies on applications for cyber security. The second most common subject, at a proportion of 20 %, is data sharing and storage. Networking for encrypted data and for avoiding tampering with file names and data within is included in the research. The third most prevalent subject, networks, accounts for 16 % of all themes and is mostly focused on how security and authenticity may be given for UAVs. The fourth most prevalent subject is data privacy and public key infrastructure, each with a proportion of 5 %. The fifth most prevalent subject is how Distributed Denial of Service (DDoS) and Internet of Drones (IoD) may successfully host records in a distributed environment to thwart malicious alterations and denial of service assaults. WiFi, GPS, and e-attacks make up the final three prevalent topics on our list, each of which accounts for 4 %.

Below are discussed in-depth the three research questions for better understanding and information for researchers gathered from the several primary studies listed above.

3.0.1 RQ1: What are recent advances for preventing information loss in UAVs?

It is necessary to answer the research question after the primary studies have been selected. With that in mind, it can be said that the most recent advancement in the prevention of information loss in UAVs is complete knowledge of cyber

TABLE 4
Number of keywords used in primary studies.

Keywords	Count
UAV	3426
Cyber-Security	2897
Cyber Attack	2490
IoT	2289
Network	2019
Drone	1892
Privacy	1625
Application	1545
Encryption	1278
Wireless Connectivity	1190
GPS	929
Ground Control	857

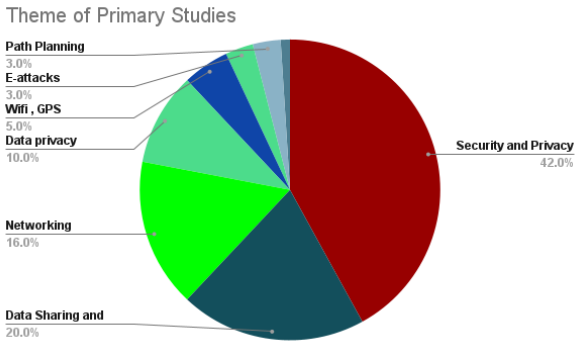

Fig. 4. Themes of the Primary Studies

attacks. At the current state, researchers have reviewed all primary studies and determined that all the possible attacks that can happen over an Unmanned Aerial Vehicle is classified into 2 different part and they are discussed as follows:

1) Physical - Potential eavesdropping is the most of attack that can happen over unmanned aerial vehicles [33], [36], [37]. The second most attack is traffic analysis [32], [35] followed by Interference [39], [40]
2) Electronic - this attack includes scanning, Man-in-the-middle, WiFi-jamming [49], [48], [42]. There are additional other attacks too such as, denial of service, Password Breaking, and Reconnaissance. [21] [49], [25], [30], [37], [24], [40].

3.0.2 RQ2: Is any secured method available for communications of the drones?

From our primary research, Today, UAVs have advanced significantly in both the military and defense sectors, such as security missions involving reconnaissance, surveillance, and monitoring of the environment, as well as in the civil sectors, including urban planning, search and rescue, law enforcement, traffic monitoring, accident management, agricultural assessment, and entertainment. environmental surveillance Rapid growth is being seen in photography, infrastructure monitoring, and rescue operations.
So, in both use cases, military and civil use, different communication system is used in drones. In military usage,

TABLE 5
Main findings and themes of the primary studies.

Primary Studies	Key Qualitative and Quantitative Data Reported	Types of Security Applications
[23]	A path is created in the first stage by building and searching a graph based on Voronoi polygons. The graph is used as a starting condition in the second stage, which simulates nonlinear ordinary differential equations. The dynamics of a group of virtual masses situated in a force field are described by the ODEs.	Path planning of UAV
[21]	Any company that lacks comprehensive security measures and security procedures is in significant danger. Cyber crimes are on the rise in the modern period, which has increased the need for system security or even network-wide security.	Firm Data Security
[28]	The next major advancement in UAV technology , known as smart UAVs, promises to open up new possibilities in a variety of applications, particularly in civil infrastructure. Over $45 billion in UAV utilization is predicted to be dominated by civil infrastructure. We discuss UAV civil applications and their difficulties in this study.	UAV as civil infrastructure
[25]	Unmanned aerial vehicles (UAVs) are used increasingly more often. Within a cellular network, UAVs can function as mobile terminals or aerial base stations. Key principles for the analysis, optimization and design of UAV-based wireless communication systems are presented in this lesson.	Cellular network
[22]	Autonomous UAVs can be used in search and rescue efforts to scan the area and gather information about a missing person's whereabouts. Some important factors must be taken into consideration while designing the search algorithms in order to reduce the amount of time it takes to discover the victim. We examine how these elements may influence the search task and outline some of the directions for further study.	Search Algorithm
[29]	Drone technology has new applications because of the Internet of Things (IoT), but it also faces new risks due to its quick development. Small drones have design problems as well as security and safety definition problems. These little drones still need a design that is developed enough to meet domain criteria.	Issues in IoT applications
[30]	Drone security and privacy issues are becoming more and more of a worry. This essay offers a succinct explanation of the privacy and security issues surrounding unmanned aerial vehicles. Additionally, it talks about related constraints, vulnerabilities, and current defenses against various assaults. The study ends with a discussion of open research areas and suggestions for how to deal with these issues.	Security and Privacy issue
[31]	Provide the first approach to a UAV-specific risk assessment based on the provided services and communication infrastructures.	Risk Assessment
[13]	UAVs carry, collect, or communicate sensitive information which becomes a target for cyber-attacks. Securing the communication network between the operator and the UAV is crucial. MTD technique changes the static nature of the systems to increase the difficulty and cost of mounting attacks.	MTD Techniques
[26]	Global Navigation Satellite System (GNSS) is widely used for locating drones. This is because of the simplicity and low cost of this technology. There are many security threats to GPS navigation. These are primarily related to the nature of the GPS signal. We discuss methods of protection against this type of attack.	Safe navigation
[32]	UAV systems may collaborate with one another to carry out a variety of functions. UAVs can be used for business purposes including transportation of commodities, military surveillance, and search and rescue operations. Such attacks have become more frequent, and they can have terrible consequences. Security measures for UAV systems and networks are being investigated by industry and standardization organizations. Our investigation focuses on risks to the Internet of Drones architecture as well as security and privacy concerns for UAVs while constructing flying ad-hoc networks (FANETs).	Ad-Hoc Network
[27]	Paper will analyze the legal and ethical issues on using drones as a weapon. Unmanned aerial vehicles, (UAVs), called drones, have recently increased their role from simple surveillance and reconnaissance to increasingly controversial targeted killings. Autonomy refers to respect for human autonomy (in contrast with the autonomy of a drone) and includes the free choice of individuals and groups.	Ethical Issues
[33]	Drones' access to regulated airspace is linked via the Internet of Drones (IoD), a decentralized network and management architecture that also offers inter-location navigation services. All security and privacy risks that are present for IoT networks also exist for the IoD network. The total impact of the IoD paradigm has been considerably constrained by security and privacy concerns. This essay tries to evaluate current trends in network security, privacy, and data protection concerns. Then, we emphasize the demand for a secure IoD architecture and create one.	IoD and Privacy Threat

TABLE 6
Main findings and themes of the primary studies.

Primary Studies	Key Qualitative and Quantitative Data Reported	Types of Security Applications
[34]	Especially DDoS and Distributed Denial of Service (DDoS) assaults, the Internet of Flying Things (IoT) is susceptible to cyberattacks. In order to remedy the security flaw, this paper suggests a deep learning system based on experience that can handle DoS, D-DoS, and ping-of-death assaults. The suggested plan makes use of the idea of an intrusion detection system (IDS).	DDoS
[35]	Unmanned aerial vehicles (UAVs) have the potential to revolutionize a wide range of industries, including the military, security, healthcare, surveillance, and traffic monitoring. UAVs with cameras, sensors, and GPS receivers have a lot of promise when using emerging technologies like 4G/5G networks. Before UAVs may be used effectively, a number of problems, including those relating to administration, security, and privacy must be overcome.	Traffic Monitoring and GPS
[36]	Unmanned aerial vehicles, or drones, are examples of cyber-physical systems (CPS), which combine physical, networking, and computational processes. Systems used by drones to fly are dependent on embedded computing power and virtual cyber networks to function. Because of the drone's distinctive network and distributed physical systems that are situated in far-off locations, it has been determined that they are susceptible to cyberattacks.	Cyber-Physical Systems.
[37]	It is possible to take advantage of flaws in the Wi-Fi access point utilized by the Parrot Bebop UAV and the usual ARDiscovery Connection procedure. The UAV's rotors might be catastrophically and instantly disabled in midflight if these vulnerabilities are exploited. We claim that Wi-fi-based commercial UAVs need a robust security architecture that employs a defense-in-depth strategy based on the literature and our own penetration tests.	WiFi vulnerabilities
[38]	The assault, danger, and vulnerabilities of cyberinfrastructure—including networks, business networks, and intranets—are examined in this article. It goes through the significance of network intrusions, cybercrime, and the causes of its rapid expansion. The research comes to the conclusion that while technology can help lessen the effects of cyberattacks, people are nonetheless vulnerable because of their actions and psychological tendencies.	Cyber issues
[24]	Cybercrime is estimated to have cost the global economy just under USD 1 trillion in 2020. The average cyber insurance claim will rise from USD 145,000 in 2019 to USD 359,000 by 2020. The lack of available data on cyber risk poses a serious problem for stakeholders seeking to tackle this issue. We posit that the lack of available data on cyber risk poses a serious problem for stakeholders seeking to tackle this issue.	Cyber data crime
[39]	Threat modeling can be extremely important in realizing the idea of "secure by design" for Multi-UAV systems, which are still in the early phases of design. In order to investigate and identify dangers affecting the Internet of Drones (IoD) architecture, we use a threat modeling approach known as threat trees in this article.	Threat Modelling
[40]	Although there are many applications for UAVs, security has always been a top priority. UAV transports private information that is sensitive and poses serious risks if unscrupulous attackers utilize it to their advantage. This study suggests a method for preventing unidentified attackers from controlling commercial UAV hardware or network channels. In the article, it was suggested that a Raspberry Pi-based DoS assault, an extra encrypted communication channel, and authentication algorithms be used to keep control of the UAV in a hijacking situation.	Authen-tication algorithm

TABLE 7
Main findings and themes of the primary studies.

Primary Studies	Key Qualitative and Quantitative Data Reported	Types of Security Applications
[41]	Numerous obstacles must be overcome in order to provide UAVs with the secure operation and dependable wireless communication. These encompass authentication, mobility management and handover, cyber-physical threats, and interference management. Such problems are addressed using ANN-based solution strategies. The strategies that have been presented allow UAVs to utilize wireless system resources in a flexible manner while yet maintaining real-time operational security.	ML for Wireless Connectivity
[42]	Networked virtual machine security settings that use private block-chain; IBM's Hyper-ledger Fabric served as an example. sufficient characteristics to enable the researchers' suggestions	Block-chain
[43]	The GPS signal is weakly received by devices on the ground and is open and unencrypted. GPS transmissions are hence susceptible to jamming and spoofing. UAVs might go out of control or even be hijacked as a result of GPS spoofing. Our approach was tested on the DJI Phantom 4 UAV.	GPS based on spoofing
[44]	Unmanned aerial vehicles are a fast-evolving cyber-physical platform, and as their capabilities and use improve, so do the security risks they face. In this study, we want to create a general security framework called Blue Box that can recognize and respond to such attacks. The results of the experiments proved that Blue-Box was capable of both identifying different cyber-physical threats and offering a way to recover from them.	Method against cyber attack
[45]	Insecure mobile and wireless networks, as well as smart gadgets, provide a risk of unintended data sharing and UAV control loss to adversaries. When it comes to identifying cyber security risks and ensuring the right security countermeasures are in place, the Department of Defense has failed to create a threat model and risk assessment. This essay will examine the hardware, software, and communication channels that make up smart devices' cyber security vulnerabilities.	Ground control of UAV
[46]	An open-source UAV simulator called Air Sim contains characteristics including simplicity in construction, effective motion capture, effective collision and obstacle recognition, and physics models. IoD communication frameworks must be created securely while minimizing performance compromises due to the huge volume of data that is currently being sent between IoD devices.	Open Air space issue
[47]	Concerns about electronic attacks, hacking, and hijacking on civilian UAVs are all made much more complicated by the lack of attribution and security procedures to prevent these actions. The public's careless usage of drones raises a variety of problems, from privacy infractions to potentially very dangerous circumstances like failing to avoid regulated airspace.	Electro-nics Attacks
[48]	Many UAV-related security incidents are reported nowadays. Governments around the world have started to regulate the use of UAVs. In this paper, we investigate the security of existing operating systems used in consumer and commercial UAVs. We discuss several research challenges for developing a secure operating system for UAVs.	Operating System Security
[49]	UAV control systems should be built to be as secure and resistant to assaults as feasible, including fault data injection (FDI) attacks. In this research, a novel technique is presented to identify malicious flaws and cyber-attacks in UAVs. To find the inserted errors in a UAV's sensor, an adaptive neural network is employed.	Fault Data Injection

the communication protocols have to be secured, because if a communication breach occurs, many important military security-related data might be compromised. Whilst, In Civil Sectors, more focus is on data leaks rather than communications. There are several methods of communication in drones and they are discussed below: Most UAV communication is based on three types and they are as below:

Radio Frequency - As we know, all communication for UAVs is wireless. So, the controller sends a radio signal of the next action for the drone. The radio frequency has to be between 2.4 GHz and 5.8 GHz as it is a normal frequency bandwidth in which UAV communications work. [45], [41], [40], [34]

WiFi Controls - WiFi-enabled drones are typically used to stream footage to a tablet, PC, or smartphone. These gadgets can also be used by a controller to remotely control the drone, [37], [34]. For this type of communication, first, one WiFi network has to be created and deployed, so that tests over drones can take place. There are several WiFi nodes in this Aerial WiFi network, the connectivity of drones jumps from one node to another and that brings us a continuous connection to the UAV devices. However, it is not efficient as the Ad-hoc method. [34], [32], [29]

GPS - A GPS drone is equipped with a GPS module that allows it to know its position relative to a network of orbiting satellites. By connecting to signals from these satellites, drones can perform functions such as position-keeping, autonomous flight, homecoming, and waypoint navigation, [35]. There are different factors that affect the use of this communication type, they are higher cost, battery drainage, GPS-Denied Scenario, and others. [35], [42], [44]

3.0.3 RQ3: How is the security measured for overtaking attacks done at various types of stages like level of communication, hardware level, sensor level, and software level?

As described in the research question itself the measurement for preventing the cyber attack happens over several stages, any vulnerable leaks in each stage can result in overtaking control of drones. Each stage is described below:

- **Communication Level** - At the communication level, attacks that could happen are eavesdropping, network collision, and others. To prevent this advanced Machine Learning algorithms are used to secure communication. GPS is suggested to use for communication, as it is worldwide and it communicates through satellite. [27]
- **Hardware Level** - We can consider this as ground level, from where all the communications and orders are relayed to UAVs. For this level, a multi-factor authentication system is established to secure communication. In addition, strong and periodic passwords are used. The hash key can be used to secure the password. [40]
- **Sensor Level** - Mostly 4 types of sensors are being used in UAVs, Optical Cameras, Ground Penetrating Radar, Lightweight Portable Radiometer, and Lidar (Light Detection and Ranging) sensors. To protect this sensor, some changes to hardware equipment are required. We can use an extra layer of protected glass over a sensor to protect it from potential threat. As per the logical threats, a multi-factor authentication system and a Hash-key password system are being used. For the ground Penetration radar, encryption of the frequency is required to secure the communication. [42], [44]
- **Software level** - At the software level, many attacks can be done using MALWARE. Protection against blocking by calculating position by drift measurements using odometer techniques. We can use blockchain and Machine Learning algorithms to protect the software that communicates with the drone. The drone collects all kinds of data text, images, location, and videos. To transfer this data there is software that works behind this. So, we can embed that software with security levels to prevent it from leaking data. [47], [49], [21]

4 Discussion

There is a considerable number of research papers available for the keyword UAV or Unmanned Aerial Vehicle. The technologies for UAV and multi-UAV systems have been developed in the past 7 years and can be told as the beginning level of development in the field.

The majority of those listed in primary research are experimental hypotheses or notions with limited quantitative information and few real-world implications for the challenges of today. Many of the more useful security options provided in the subsequent primary studies demonstrate creative methods for addressing a variety of issues relating to data security, mutability, and networking. The solutions delivered in the studies highly depend on the number of the system environments and surrounding and various factors like weather, labor, and attacks. Due to the reasons mentioned [46] open-air space, and practical experiments of a certain length have shown the effectiveness of UAV applications in today's world over conventional security. Notable work in [21] is seen for data security to secure data networking and communication. This study discovers that while creativity has a role to play in decreasing the effect of digital assaults, threats, and weaknesses, cyber security threats and approaches have a role to play in minimizing the impact of digital attacks, risk, and vulnerability. Although cyberattacks can be mitigated, there does not currently seem to be a conclusive way to defeat such network security risks.

The researchers used the current [30] network security methods like ML-based IDS, which is considered to be a successful implementation. There are various IDS like rule-based, signature-based, and anomaly-based. This study finds that while cyber security threats and techniques have a role to play in limiting the impact of digital attacks, risk, and vulnerability, creativity also has a role to play in reducing the effect of digital assaults, danger, and weakness. [49] Although assaults can be lessened, there doesn't appear to be a definitive solution to eliminate such network security vulnerabilities at the moment. Both performance measurements and security aspects (authentication, forward secrecy, reverse secrecy, etc.) have been considered in the analysis of the frameworks (communication cost, computation cost, storage cost, signature generation time, signature verification time, etc.). The review study concludes with difficulties and recommendations for the foreseeable future for the researchers.

[46]. The fault data injection [49] helps the data to be safe in the electronic attack [47] which is like privacy

infractions to circumstances in the airspace. [43] Regular network structure swapping makes it challenging to implement the flying-AntHocNet routing control scheme, which was inspired by a systematic environment-based approach and exhibits optimal simulation results for metrics like end-to-end delay, packet loss [21], data-packet drop-count, and throughput analysis in comparison to traditional routing techniques like DSDV, DSR, AOMDV, M-DART, and Z-R-P, which are introduced in aerial networks [22]. In order to protect society from cyberattacks, smart cities are technologically implementing internet-of-everything abstraction.

5 Future Research Directions of UAV Cyber Security

Based on the outcomes of this survey along with our own observations, we suggest the following blockchain research areas that need further study:

5.1 UAV: Deep and Machine Learning:

[50] Recently, a lot of support has been given to machine learning and deep learning techniques in a variety of UAV-related applications, including allocation of resources, obstacle detection, tracking, trajectory planning, and battery scheduling. In order to complete the help device accurately and without the risk of collision, it will be necessary to design nano UAVs that are much smaller, lighter, and smarter than existing UAV models. [51] This will be facilitated by the creation of more accurate algorithms and an increase in onboard computational power. Furthermore, reliable data availability can help UAVs execute precise control, path planning, and vision jobs.

The mission route of UAVs should be optimized while the energy usage of flights with emergency braking is reduced by using better tracking and path planning algorithms. [52]While path planning of complicated paths to avoid obstacles and identify the shortest path to spend minimal energy may be carried out by employing a multi-objective optimization algorithm, recent work on the issue of tracking is mostly based on heuristic techniques. [53] The review included a number of deep-learning applications for UAVs, including feature extraction. The UAV may be equipped with numerous cameras to capture a range of picture types for further processing. As the UAV searches the surroundings for an appropriate path, planning for path motion, tracking, and manipulation were given. Deep learning-based UAV motion control is another use.

5.2 UAV: Security and Privacy

Due to their cellular networking and limited processing capabilities, UAV security and safety are crucial factors. [50] They might be threatened by intrusion attempts, which would jeopardize the acquired data's security and privacy. It may be replaced or stolen. New onboard methods are thus needed to ensure privacy during the voyage. Recent technologies like blockchain technology and physical layer protection need further study and development to reach the necessary security level with the necessary quality and dependability [53].

The effectiveness of optical wireless communications (OWCs) in 4th Generation or, 5th Generation, and beyond 5G mobile networks has been established. [54]They are frequently utilized in UAV communication, and the 6G mobile network is anticipated to employ them. However, a number of issues with this technology still need to be resolved, including the high likelihood of signal blocking, power consumption, and weather conditions. There are some practical issues that need to be answered or future investigations and understandings like:

1) What development can be made for high end-to-end delay for non-delay tolerant UAVs when the link between the control and data panel is affected?
2) While being energy-efficient UAVs how will it make sure about the confidentiality of the data?

5.3 UAV: Detection System for Intrusion

Real-time network traffic analysis is needed to find intrusions against UAVs while they are in flight. In order to do this, employing an IDS for Drones allows the detection of many intrusion types, including assaults that alter signals, malware, attack routing, and message forging [55]. Anomaly detection framework development to track malicious actions also plays a significant part in identifying attack patterns [56]. Additionally, the use of honey pots and honey nets in conjunction with IDS can aid in shielding the flying mission from nefarious actors [57].

However, having additional sources of information can also result in higher communication costs and higher overhead costs for processing. Creating such solutions is difficult since security and performance are currently tradeoffs. To monitor UAV communications and identify threats, lightweight IDSs must be put into use. In this regard, several systems make use of the flight's behavioral profile to find unusual activity and malicious intrusions [58]. However, such methods cannot identify cyber assaults that compromise UAVs while guaranteeing that the flying pattern remains constant.

6 Conclusion

This study has uncovered previous studies that examine how Unmanned Aerial Vehicle solutions might exacerbate cyber security issues. This study examined a UAV system's overall security hazard. The thorough threat analysis of the system is intended to assist both the system's designers and users in recognizing potential vulnerabilities and putting appropriate mitigation and recovery mechanisms in place. It is still difficult to pinpoint which risks could have the greatest impact on UAV systems because the majority of the information about the current safeguards is classified. Working on a few of these dangers and utilizing mission data to better precisely simulate them will be part of future development.

6.1 Potential research agenda 1: Fuzzing UAV

To accomplish the goal of a wide coverage and depth test, the fuzzing is guided by the information gathered about the program execution. The technological issues brought on by the uniqueness of UAV systems, such as the inapplicability of standard fuzzing testing methodologies, secret communication protocols, and difficulties in monitoring

the running state must be resolved. An innovation would be to accomplish generation-based fuzzing by extracting syntactic information from the proprietary protocols of UAV systems.

Another area that merits investigation in order to help grey-box fuzzing is UAV simulation technology. One may properly extract execution information from simulation systems by using memory activity detection, program stack status, and hardware output to direct the process of fuzzing.

6.2 Potential research agenda 2: BlockChain

Blockchain is a brand-new way to use cloud computing including point-to-point transmission, consensus, encryption, and distributed data storage. Attackers find it challenging to change or remove the records that may be used to record, gather, and search information about UAV systems, such as where the UAV has been or what it has done, because of its decentralized and encrypted communication capabilities, notably the redundancy check of data. It may be used to spot unauthorized UAV systems or unusual operating modes, making it more challenging for attackers to get data from UAVs or alter flight plans. Although it is unclear what effect blockchain will have on UAV security, it will be a future technology and development pattern to be taken into account.

REFERENCES

[1] N. Hallermann and G. Morgenthal, "Visual inspection strategies for large bridges using unmanned aerial vehicles (uav)," in *Proc. of 7th IABMAS, International Conference on Bridge Maintenance, Safety and Management*, 2014, pp. 661–667.

[2] Y. Liu, H.-N. Dai, Q. Wang, M. K. Shukla, and M. Imran, "Unmanned aerial vehicle for internet of everything: Opportunities and challenges," *Computer communications*, vol. 155, pp. 66–83, 2020.

[3] Z. Lv, "The security of internet of drones," *Computer Communications*, vol. 148, pp. 208–214, 2019.

[4] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, "A comprehensive review of the covid-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact," *Ieee access*, vol. 8, pp. 90 225–90 265, 2020.

[5] F. Aftab, A. Khan, and Z. Zhang, "Hybrid self-organized clustering scheme for drone based cognitive internet of things," *IEEE Access*, vol. 7, pp. 56 217–56 227, 2019.

[6] Z. Lv, I. Mehmood, M. Vento, M.-S. Dao, K. Ota, and A. Saggese, "Ieee access special section editorial: Multimedia analysis for internet-of-things," *IEEE Access*, vol. 7, pp. 65 211–65 218, 2019.

[7] Y. Zhang, M. Chen, V. C. Leung, T. Xing, and G. Fortino, "Guest editorial special issue on cognitive internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2259–2262, 2018.

[8] T. Alladi, V. Chamola, B. Sikdar, and K.-K. R. Choo, "Consumer iot: Security vulnerability case studies and solutions," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17–25, 2020.

[9] K. Pärlin, M. M. Alam, and Y. Le Moullec, "Jamming of uav remote control systems using software defined radio," in *2018 International Conference on Military Communications and Information Systems (ICMCIS)*. IEEE, 2018, pp. 1–6.

[10] B. Ly and R. Ly, "Cybersecurity in unmanned aerial vehicles (uavs)," *Journal of Cyber Security Technology*, vol. 5, no. 2, pp. 120–137, 2021.

[11] H. Shakhatreh, A. H. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. S. Othman, A. Khreishah, and M. Guizani, "Unmanned aerial vehicles (uavs): A survey on civil applications and key research challenges," *Ieee Access*, vol. 7, pp. 48 572–48 634, 2019.

[12] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," *Vehicular Communications*, vol. 23, p. 100249, 2020.

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

[14] O. Westerlund and R. Asif, "Drone hacking with raspberry-pi 3 and wifi pineapple: Security and privacy threats for the internet-of-things," in *2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS)*. IEEE, 2019, pp. 1–10.

[15] C. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," in *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*. IEEE, 2017, pp. 194–199.

[16] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodriguez, and J. Yuan, "Survey on uav cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Communications surveys & tutorials*, vol. 21, no. 4, pp. 3417–3442, 2019.

[17] D. Mishra and E. Natalizio, "A survey on cellular-connected uavs: Design challenges, enabling 5g/b5g innovations, and experimental advancements," *Computer Networks*, vol. 182, p. 107451, 2020.

[18] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," 2007.

[19] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proceedings of the 18th international conference on evaluation and assessment in software engineering*, 2014, pp. 1–10.

[20] S. Hosseini, B. Turhan, and D. Gunarathna, "A systematic literature review and meta-analysis on cross project defect prediction," *IEEE Transactions on Software Engineering*, vol. 45, no. 2, pp. 111–147, 2019.

[21] K. Thakur, M. Qiu, K. Gai, and M. L. Ali, "An investigation on cyber security threats and security models," in *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*. IEEE, 2015, pp. 307–311.

[22] S. Waharte and N. Trigoni, "Supporting search and rescue operations with uavs," in *2010 international conference on emerging security technologies*. IEEE, 2010, pp. 142–147.

[23] S. A. Bortoff, "Path planning for uavs," in *Proceedings of the 2000 american control conference. ACC (IEEE Cat. No. 00CH36334)*, vol. 1, no. 6. IEEE, 2000, pp. 364–368.

[24] F. Cremer, B. Sheehan, M. Fortmann, A. N. Kia, M. Mullins, F. Murphy, and S. Materne, "Cyber risk and cybersecurity: a systematic review of data availability," *The Geneva Papers on Risk and Insurance-Issues and Practice*, pp. 1–39, 2022.

[25] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah, "A tutorial on uavs for wireless networks: Applications, challenges, and open problems," *IEEE communications surveys & tutorials*, vol. 21, no. 3, pp. 2334–2360, 2019.

[26] E. Basan, A. Basan, A. Nekrasov, C. Fidge, J. Gamec, and M. Gamcová, "A self-diagnosis method for detecting uav cyber attacks based on analysis of parameter changes," *Sensors*, vol. 21, no. 2, p. 509, 2021.

[27] A. Konert and T. Balcerzak, "Military autonomous drones (uavs) - from fantasy to reality. legal and ethical implications." *Transportation Research Procedia*, vol. 59, pp. 292–299, 2021, 10th International Conference on Air Transport – INAIR 2021, TOWARDS AVIATION REVIVAL. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352146521008838

[28] H. Shakhatreh, A. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. Othman, A. Khreishah, and M. Guizani, "Unmanned aerial vehicles: A survey on civil applications and key research challenges. arxiv 2018," *arXiv preprint arXiv:1805.00881*.

[29] R. Majeed, N. Abdullah, M. Mushtaq, and R. Kazmi, "Drone security: Issues and challenges," *International Journal of Advanced Computer Science and Applications*, vol. 12, 06 2021.

[30] M. Siddiqi, C. Iwendi, K. Jaroslava, and N. Anumbe, "Analysis on security-related concerns of unmanned aerial vehicle: attacks, limitations, and recommendations," *Mathematical biosciences and engineering: MBE*, vol. 19, pp. 2641–2670, 01 2022.

[31] K. Hartmann and C. Steup, "The vulnerability of uavs to cyber attacks-an approach to the risk assessment," in *2013 5th international conference on cyber conflict (CYCON 2013)*. IEEE, 2013, pp. 1–23.

[32] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, "A survey of cyber security threats and solutions for uav communications and flying ad-hoc networks," *Ad Hoc Networks*, p. 102894, 2022.

[33] M. Yahuza, M. Y. I. Idris, I. B. Ahmedy, A. W. A. Wahab, T. Nandy, N. M. Noor, and A. Bala, "Internet of drones security and privacy issues: Taxonomy and open challenges," *IEEE Access*, vol. 9, pp. 57 243–57 270, 2021.

[34] M. Albalawi and H. Song, "Data security and privacy issues in swarms of drones," in *2019 Integrated Communications, Navigation and Surveillance Conference (ICNS)*. IEEE, 2019, pp. 1–11.

[35] T. Lagkas, V. Argyriou, S. Bibi, and P. Sarigiannidis, "Uav iot framework views and challenges: Towards protecting drones as "things"," *Sensors*, vol. 18, no. 11, p. 4015, 2018.

[36] B. Siddappaji and K. Akhilesh, "Role of cyber security in drone technology," in *Smart Technologies*. Springer, 2020, pp. 169–178.

[37] M. Hooper, Y. Tian, R. Zhou, B. Cao, A. P. Lauf, L. Watkins, W. H. Robinson, and W. Alexis, "Securing commercial wifi-based uavs from common security attacks," in *MILCOM 2016-2016 IEEE Military Communications Conference*. IEEE, 2016, pp. 1213–1218.

[38] T. P. Parikh and A. R. Patel, "Cyber security: Study on attack, threat, vulnerability," *Int. J. Res. Mod. Eng. Emerg. Technol*, vol. 5, pp. 1–7, 2017.

[39] A. Almulhem, "Threat modeling of a multi-uav system," *Transportation Research Part A: Policy and Practice*, vol. 142, pp. 290–295, 2020.

[40] K. Yoon, D. Park, Y. Yim, K. Kim, S. K. Yang, and M. Robinson, "Security authentication system using encrypted channel on uav network," in *2017 First IEEE International Conference on Robotic Computing (IRC)*. IEEE, 2017, pp. 393–398.

[41] U. Challita, A. Ferdowsi, M. Chen, and W. Saad, "Machine learning for wireless connectivity and security of cellular-connected uavs," *IEEE Wireless Communications*, vol. 26, no. 1, pp. 28–35, 2019.

[42] Y. Qiao, Y. Zhang, and X. Du, "A vision-based gps-spoofing detection method for small uavs," in *2017 13th International Conference on Computational Intelligence and Security (CIS)*. IEEE, 2017, pp. 312–316.

[43] I. J. Jensen, D. F. Selvaraj, and P. Ranganathan, "Blockchain technology for networked swarms of unmanned aerial vehicles (uavs)," in *2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*. IEEE, 2019, pp. 1–7.

[44] F. Fei, Z. Tu, R. Yu, T. Kim, X. Zhang, D. Xu, and X. Deng, "Cross-layer retrofitting of uavs against cyber-physical attacks," in *2018 IEEE International Conference on Robotics and Automation (ICRA)*. IEEE, 2018, pp. 550–557.

[45] K. Mansfield, T. Eveleigh, T. H. Holzer, and S. Sarkani, "Unmanned aerial vehicle smart device ground control station cyber security threat model," in *2013 IEEE International Conference on Technologies for Homeland Security (HST)*. IEEE, 2013, pp. 722–728.

[46] Y.-J. Chen and L.-C. Wang, "Privacy protection for internet of drones: A network coding approach," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1719–1730, 2018.

[47] M. Strohmeier, M. Smith, M. Schäfer, V. Lenders, and I. Martinovic, "Assessing the impact of aviation security on cyber power," 05 2016.

[48] S. Iqbal, "A study on uav operating system security and future research challenges," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2021, pp. 0759–0765.

[49] A. Abbaspour, K. K. Yen, S. Noei, and A. Sargolzaei, "Detection of fault data injection attack on uav using adaptive neural network," *Procedia computer science*, vol. 95, pp. 193–200, 2016.

[50] J.-S. Lee and K.-H. Yu, "Optimal path planning of solar-powered uav using gravitational potential energy," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 53, no. 3, pp. 1442–1451, 2017.

[51] A. Noorwali, M. A. Javed, and M. Z. Khan, "Efficient uav communications: Recent trends and challenges," *CMC-Comput. Mater. Contin*, vol. 67, pp. 463–476, 2021.

[52] R. Shakeri, M. A. Al-Garadi, A. Badawy, A. Mohamed, T. Khattab, A. K. Al-Ali, K. A. Harras, and M. Guizani, "Design challenges of multi-uav systems in cyber-physical applications: A comprehensive survey and future directions," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3340–3385, 2019.

[53] A. Carrio, C. Sampedro, A. Rodriguez-Ramos, and P. Campoy, "A review of deep learning methods and applications for unmanned aerial vehicles," *Journal of Sensors*, vol. 2017, 2017.

[54] O. S. Oubbati, M. Atiquzzaman, T. A. Ahanger, and A. Ibrahim, "Softwarization of uav networks: A survey of applications and future trends," *IEEE Access*, vol. 8, pp. 98 073–98 125, 2020.

[55] G. Choudhary, V. Sharma, I. You, K. Yim, R. Chen, and J.-H. Cho, "Intrusion detection systems for networked unmanned aerial vehicles: a survey," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2018, pp. 560–565.

[56] J. Schumann, P. Moosbrugger, and K. Y. Rozier, "R2u2: monitoring and diagnosis of security threats for unmanned aerial systems," in *Runtime Verification*. Springer, 2015, pp. 233–249.

[57] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2351–2383, 2021.

[58] Z. Birnbaum, A. Dolgikh, V. Skormin, E. O'Brien, D. Muller, and C. Stracquodaine, "Unmanned aerial vehicle security using behavioral profiling," in *2015 International Conference on Unmanned Aircraft Systems (ICUAS)*. IEEE, 2015, pp. 1310–1319.