IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 29, 2021, accepted April 6, 2021, date of publication April 9, 2021, date of current version April 20, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3072030

Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges

MUKTAR YAHUZA[1,2], (Graduate Student Member, IEEE), MOHD YAMANI IDNA IDRIS[1,3], (Member, IEEE), ISMAIL BIN AHMEDY[1], (Member, IEEE), AINUDDIN WAHID ABDUL WAHAB[1], TARAK NANDY[1], (Member, IEEE), NOORZAILY MOHAMED NOOR[1], AND ABUBAKAR BALA[4,5], (Student Member, IEEE)

[1]Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia
[2]Department of Computer Science, Faculty of Science, Yobe State University, Damaturu 620242, Nigeria
[3]Center for Research in Mobile Cloud Computing, University of Malaya, Kuala Lumpur 50603, Malaysia
[4]Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Technology PETRONAS, Seri Iskandar 32610, Malaysia
[5]Department of Electrical Engineering, Faculty of Engineering, Bayero University Kano, Kano 3011, Nigeria

Corresponding author: Mohd Yamani Idna Idris (yamani@um.edu.my)

This work was supported in part by the University of Malaya Impact Oriented Interdisciplinary Research Grant under Grant IIRG003A, B, C-19IISS, and in part by the Ministry of Higher Education Malaysia Fundamental Research Grant Scheme (FRGS) under Grant FP055-2019A.

ABSTRACT Internet of Drones (IoD) is a decentralized network and management framework that links drones' access to the controlled airspace and provides inter-location navigation services. The interconnection of drones in the IoD network is through the Internet of Things (IoT). Hence the IoD network is vulnerable to all the security and privacy threats that affect IoT networks. It is highly required to safeguard a good atmosphere free from security and privacy threats to get the desired performance from IoD applications. Security and privacy issues have significantly restricted the overall influence of the IoD paradigm. There are existing survey studies that helped lay a vital foundation for understanding the IoD security and privacy issues. However, not all have thoroughly investigated the level of security and privacy threats associated with the various drone categories. Besides, most existing review studies do not examine secured IoD architecture. This paper aims to assess the recent trends in the security and privacy issues that affect the IoD network. We investigate the level of security and privacy threats of the various drone categories. We then highlight the need for secured IoD architecture and propose one. We also give a comprehensive taxonomy of the attacks on the IoD network. Moreover, we review the recent IoD attack mitigating techniques. We also provide the performance evaluation methods and the performance metrics employed by the techniques. Finally, we give research future direction to help researchers identify the latest opportunities in IoD research.

INDEX TERMS Attacks, Internet of Drones, IoD architecture, localization error attacks, security and privacy, UAS, UAV, UUV.

I. INTRODUCTION

A drone is an aircraft or submarine operated remotely without a human pilot [1]. It has many other names. It is called Unmanned Aerial Vehicle (UAV) when used on land, Unmanned Aircraft System (UAS) when operated on air, and Unmanned Under-Water Vehicle (UUV) when employed underwater. The term drone originated from the military, while UAV and UAS were adopted by some regulators of the US Federal Aviation Administration (FAA) [2]. The history of the first drone named Torpedo can be traced back to World War I. It was invented by Dayton-Wright Airplane company for military applications [3]. However, large-scale drone production started during World War II by a company called Reginald Danny. They produced almost 15,000 drones for the US army [3]. They fitted the drones with different cameras that sent data to ground equipment [2]. The drones were also embedded with a Global Positioning System (GPS), equipment for accessing data from Google Earth and a sensor with a circuit board for data recording [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Ahmed Farouk.

The Internet of Drones (IoD) derives its name from IoT by putting "Drones" in place of "Things." Thus, IoDs have similar properties to IoT. Gharibi *et al.* [4] defined IoD as a layered network control architecture that helps coordinating drones [5]. IoD network paradigm could be applied in search and rescue operations, fleet monitoring, industrial inspections, infrastructure monitoring, delivery systems [6], agriculture [7], [8], supply chain mapping, disaster management [9], [10], and so forth. There is a strong expectation that IoD will take significant roles in the nearest future's advanced smart cities [11]. Advanced public services can now conduct critical natural and human-made risk operations with the IoD [12], [13]. However, the IoD network can become the target of many malicious security and privacy threats. The drones and other IoD entities may be hijacked for cyber-attack, data breaches, or payload value theft. According to authors in [14], a DJI Phantom drone, when hijacked, is sold through eBay online portal at the cost of $1000. The authors further stated that the drone cameras used in the film industries could cost almost $20,000, and a light detection and ranging (LIDAR) sensor can cost up to $50,000. Also, when a drone carrying valuable data is hijacked, it worth thousands of US dollars. More significant damages are done when a military drone is attacked. The result is not only compromising valuable data or the drone's physical components, but the attacked drone can be used as a weapon by the adversary [15]. The communication between drones in the IoD network is through the insecure internet (mainly wireless network and WiFi) and using navigational signals (e.g. the global positioning system (GPS)) [16]. This seriously affects their privacy and security. Malicious hackers can easily access the drone configuration and hijack it using the open-source drone-hijack applications (e.g. skyjack) and wirelessly take control over it. Most security and privacy threats on civilian drones occur due to the fault in their designs. Many drones are designed without internet security protection and authentication mechanism [17]. Although it is comparably difficult to attack military drones due to their security infrastructure, a well-trained hacker may use advanced techniques. An example is the CIA RQ-170 Sentinel US spy drone brought down by Iranian hackers in December 2011 [18].

Many security and privacy techniques have been developed by researchers for ensuring security on the internet of drones (IoD) network. The techniques aimed at either mitigating issues that affect the secure localization of drones or security and privacy requirements associated with the IoD network. Localization error attacks hinder the reliable positioning of drones which resulted in devastating consequences on the overall performances of the IoD network. Moreover, security and privacy requirements are the goals that determine the capabilities and functions of the IoD network achieved in mitigating certain security and privacy threats [19]. The security and privacy requirements on the IoD network include integrity, availability, authenticity, confidentiality, and privacy preservation.

Most of the techniques developed for the mitigation of drone localization errors attacks aimed at detecting the attacks before their effects. Mostly, the schemes are based on machine learning, deep learning, and artificial intelligence approaches. Moreover, conventional cryptographic based intrusion detection schemes involved complex computation that may result in changes been made to the structure of the localization signals generating devices. Details of these techniques are explored in section III. Besides, cryptographic-based techniques are employed for mitigating the threats to integrity requirements on the IoD network. Likewise, blockchain-based techniques are employed for ensuring integrity requirement on the IoD network. Considering the techniques employed for ensuring the availability requirements on the IoD network, they are incorporated with mechanisms that sense the presence of denials of service (DOS), distributed denial of service (DDOS), and physical attacks. The mechanisms detect large and small objects that may collide with the drones while on flight mode. The mechanisms are also capable of detecting the flight status of the drones and check the flight limit for allowing the flight control systems to detect drones malfunctions that may affect the availability requirements.

On the other hand, among the techniques employed for ensuring authenticity requirements, cryptographic-based techniques are quite common. Cryptographic-based authenticated key agreement (AKA) techniques allow the IoD communicating entities to generate and share a common session key before message exchange for ensuring reliable authentication. Also, blockchain-based schemes are developed for ensuring authentication requirement on the IoD network. Likewise, for ensuring confidentiality on the IoD network, cryptographic-based protocols are used. The identity-based encryption and advanced encryption standard (AES) algorithms are among the prominent protocols employed. Furthermore, blockchain-based access control schemes are deployed to the IoD network for ensuring the confidential exchange of information. The secured information from the various IoD entities form a transaction, and the numerous transactions build together into blocks. The blocks are then incorporated into the blockchain. This guarantees that the transactions added to the blockchain are kept confidential.

Besides, the techniques deployed for ensuring privacy preservation on the IoD network utilized a check module that assures safer operations of drones by mitigating the adverse effects of the attacks affecting the privacy preservation requirements on the network. Moreover, blockchain-based techniques are deployed to the IoD network for ensuring privacy preservation requirements as will be explored in section III.

Many review studies have discussed the security and privacy issues on the internet of drones (IoD) networks. These existing survey studies have helped to lay a solid foundation for understanding the issues. Table 1 illustrates a brief description of the existing survey studies on IoD

TABLE 1. The description of the existing survey studies including the proposed review work.

Review	Focus Area	Survey Years
Chang V. *et al.* 2017 [20]	Laboratory survey to discover the user perception of drones security and privacy issues	From 2007 to 2017
Wazid M. *et al.* 2018 [21]	Investigation of the security and functionality requirements of the IoD environment	From 1983 to 2018
Choudhary G. *et al.* 2018 [5]	Survey on the critical threats and vulnerabilities of IoD over radio space, and attacks categorization	From 2004 to 2018
IIgi G. S. and Y. K. Ever, 2020 [22]	A critical review of the security and privacy challenges of the IoD network	From 2008 to 2020
Yaacoub and Salman O., 2020 [23]	Review on the use of drones for mischievous intents and the existing detection methods	From 1987 to 2020
Lin C. *et al.* 2018 [24]	Survey on the various existing IoD architectures and the security and privacy requirements of IoD network	From 2008 to 2017
Laccadito M. *et al.* 2018 [25]	Review on the architecture and state of the art vulnerabilities of drones against cyber-attacks as well as the mitigation, countermeasures, and defence strategy	From 1993 to 2017
Our proposed work	A comprehensive review of the level of security and privacy threats associated with the IoD network, including the various drone classes and the general architecture	From 2004 to 2021

security and privacy issues compare with our proposed work. To the best of the authors' knowledge, however, the level of security and privacy vulnerability associated with the different categories of drones is missing in the existing reviews. Additionally, most works provide limited information on the issues or performed the study early when the IoD paradigm emerged. The researchers in [20] conducted a laboratory survey with twenty experienced drone users to discover their perception of drones security and privacy issues. At the end of the study, the authors recommended geofencing, creating designated spaces for drones, and enhancing drones' design for mitigating security and privacy issues in the IoD network. However, a thorough exploration of the attacks affecting the IoD network is missing in the study. In [21], the authors investigated the IoD environment's security and functionality requirements and the challenges of designing authentication schemes for secure IoD communication. Additionally, a taxonomy of security protocols deployable in the IoD environment was developed. However, the study discussed only the techniques that ensure authentication requirements, while other securities and privacy requirements were ignored. A survey on the critical threats and vulnerabilities of IoD over radio space is given in [5]. The authors developed a taxonomy of attacks. However, the latest technological schemes for mitigating the identified attacks were not discovered.

In [22], the authors critically reviewed the security and privacy challenges of the IoD network. Moreover, they proposed a solution to the identified challenges. However, the IoD architecture incorporated with security and privacy mechanism was not explored. Yacoub, J. P., and Salman, O. [23] reviewed the use of drones for mischievous intents and the existing detection methods. The authors also examined the usage of various drones in different domains and applications. Simulation of attacks on a given drone is also carried out to help ethical hackers understand drones existing vulnerabilities in both military and commercial applications. However, the level of attack vulnerability on each class of the categorized drones is not given. Lin *et al.* [24] surveyed the various existing IoD architecture and their security and privacy requirements. The authors proposed protection against the identified challenges using a lightweight cryptography approach. However, the IoD architecture incorporated with the security and privacy mechanism was not explored. In [25], the authors reviewed the architecture and state of the art vulnerabilities of drones against cyber-attacks and the mitigation, countermeasures, and defence strategy. Additionally, the areas that require an urgent emphasis on securing drones were recommended by the authors. These include encrypting the wireless communication channel, provision of mischievous free firmware, detection, eliminating corrupt sensors, and securing the drones at the hardware level. However, a classification of drones is missing in the study.

Motivated by these observations, this review work aims to thoroughly investigate the current security and privacy issues affecting the IoD networks. The IoD architecture will be explored to see how security features will be incorporated into it for ensuring secured communication in the network. A comprehensive taxonomy of drones with the level of security and privacy vulnerability associated with each class will be given. Moreover, a comprehensive taxonomy of attacks on the IoD network will be given. The study will also explore the latest security and privacy requirements of the IoD network and the technological schemes employed to mitigate the threats affecting the identified requirements. Furthermore, the evaluation methods and the metrics used for the evaluation of the proposed mitigation techniques will be explored. In the end, open research issues on the IoD model will be discussed. We believe that these will serve as a guide for new and experienced researchers in the field.

The paper's remaining part is listed as follows: the background of the IoD paradigm is presented in Section II. Section III highlights the safety and attacks on the IoD network. Future research directions are discussed in Section IV. Finally, Section V concludes the paper.

II. BACKGROUND

This section discusses the existing architectures of the internet of drones (IoD) networks. It also proposes a secured

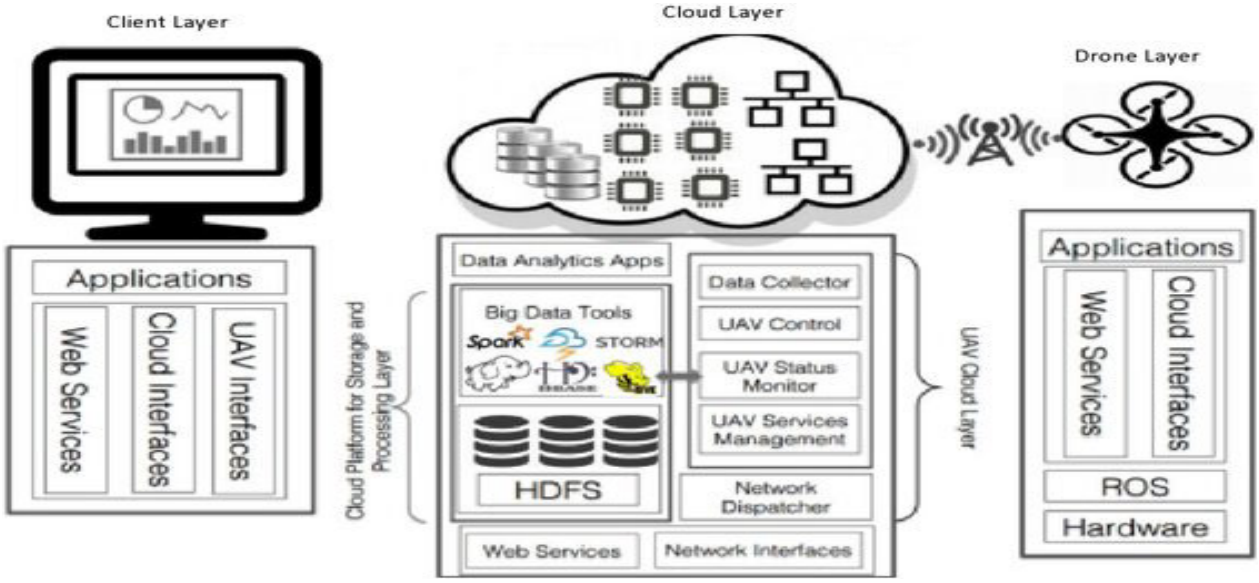

FIGURE 1. Typical cloud-based IoD architecture (Source: [29]).

architecture that ensures the security and privacy of IoD network components and their payload data. The technological advancement that led to the IoD paradigm development is also presented. Moreover, drones' taxonomy with the respective level of security threats is presented. This taxonomy will help select the right drones for a given application.

A. THE ARCHITECTURE OF THE INTERNET OF DRONES

The existing architectures of the internet of drones (IoD) network are presented in this section. The architecture is mainly designed to provide navigational services and manage the access of drones to the controlled airspace [21], [26]. As highlighted in section I, a mechanism for ensuring the security and privacy requirement needs to be incorporated into the internet of drones (IoD) architecture. In line with this requirement, a secured IoD architecture is proposed in this section.

1) EXISTING ARCHITECTURES

According to Yao and Ansari [27], the first IoD architecture is designed by Gharibi *et al.* [4]. The architecture consists of five conceptual layers (air space layer, node-to-node layer, end-to-end layer, services layer, and, application layer). Each layer can access the services rendered by a layer below it. Authors in [24] further studied Gharibi's architecture and presented its advantages and otherwise. The architecture can offer airborne collision avoidance and greater control of spaces where the drone can or cannot access. However, the disadvantages include lack of effective routing, congestion control, and security and privacy challenges (insecure data sharing). The authors proposed a potential solution to the highlighted problems that will suit the IoD architecture's nature. Moreover, authors in [28] proposed the addition of blockchain technology to IoD's layered architecture to make it more secure, secret, and tamperproof. Qureshi *et al.* [29] proposed a cloud-based IoD architecture to provide virtualization access of drones through the cloud and upload heavy computation to the cloud with limited resource constraints. The architecture consists of three layers. The first layer is the drone layer representing a set of resources/services to be delivered to the end-users. In contrast, the second layer is referred to as a cloud service layer. It comprises three components (storage components for storing a stream of data originated from the drones, the computation part, and, interface component). Finally, the third layer is referred to as a client layer. This layer has interfaces with both the drone layer and the cloud layer. The typical cloud-based IoD architecture is depicted in Figure 1.

An IoT-based IoD architecture is proposed in [30]. The authors considered the various IoT smart devices (sensors) miniaturized into drones, which are obliquely matched into IoT technology. The architecture enabled the communication between drones in the flying zone, drones and Ground Station Server (GSS), and between the GSS and Control Room (CR), as depicted in Figure 2.

Authors in [31] proposed a centralized multi-layered virtual network mapping architecture. It uses the virtualization of network functions that promote earlier researchers' traditional IoD architecture's technological progress. Additionally, an internet-based IoD architecture is found in [21] (as shown in Figure 3). In the proposed architecture, five distinct entities are considered. These include drone flying zones, a central server that coordinates all the IoD functionalities, a control room, an internet communication channel, and an external user. On the other hand, a multi-drone network IoD architecture that considered Flying Ad Hoc Networks (FANETs), which is a contrast to Mobile Ad Hoc Networks

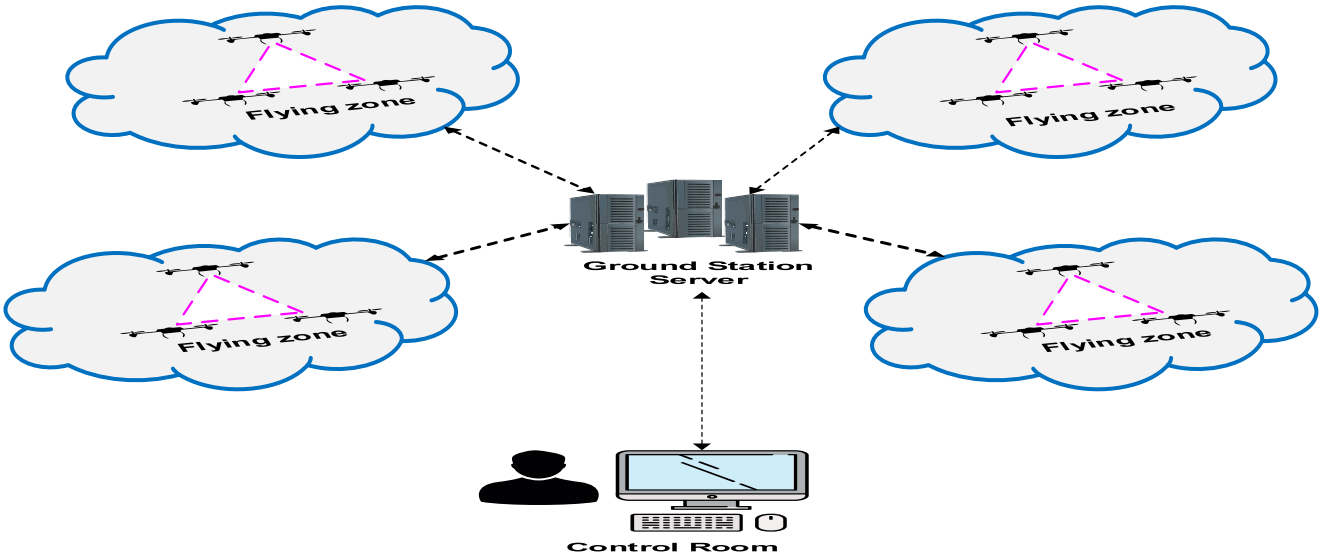

FIGURE 2. IoT-based IoD architecture (Source: [30]).

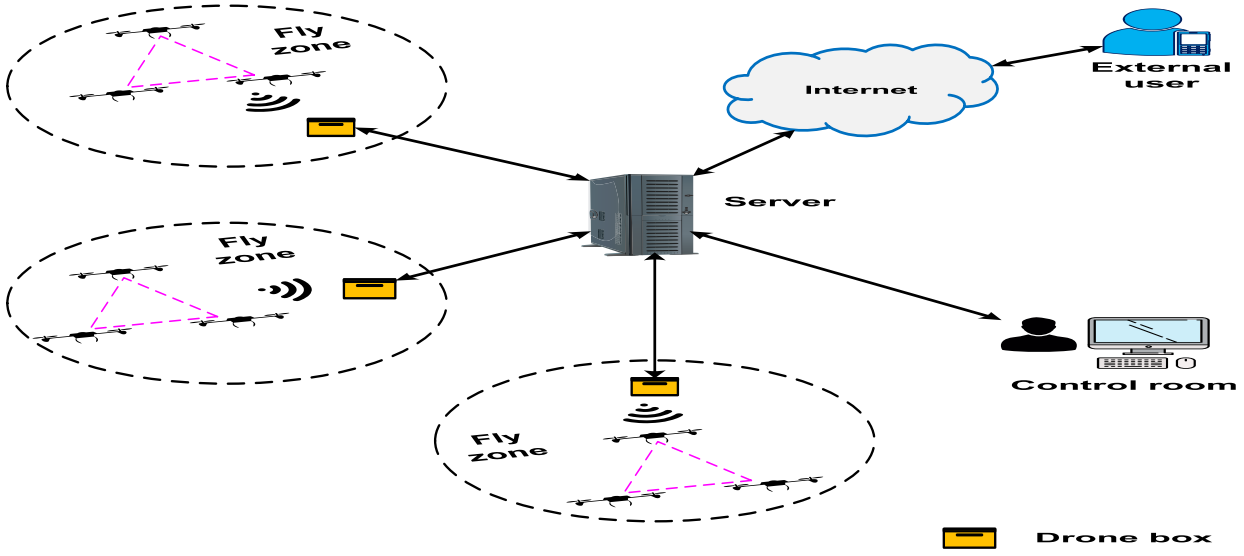

FIGURE 3. The internet-based IoD architecture (Source: [21]).

(MANETs) and Vehicular Ad Hoc Networks (VANETs) is elaborated in [32]. Depicted in Figure 4, groups of flying drones from the various FANETs zones are autonomously connected and coordinated to achieve the best services. The advantages of this multi-drone network architecture over the remaining single-drone architectures include scalability, improved survivability, improved transmission efficiency, and adaptability and self-organization.

Looking at the discussed IoD architectures, it is easy to see security and privacy flaws that arise from several angles. The security issues occurred due to the lack of safeguards in the communication channel and between IoD communicating entities. As such, various adversary attacks may occur. Therefore, there is a need for integrating the protection mechanisms into the IoD architecture. Moreover, most of the architectures ignore the mobility features of the drones. A flying drone at a particular zone may decide to communicate with another drone at a different flying zone, which leads to an increase in latency. Besides, drones are resource constraint devices with limited memory, power, computational and communication ability [33]. Therefore, if an edge device is placed between the flying zones of drones, the latency, computational and communication overhead will significantly be reduced. Motivated by these observations, a mobile edge computing assisted secured IoD architecture is proposed in this paper.

2) THE PROPOSED IOD ARCHITECTURE

The proposed architecture is illustrated in Figure 5. The network comprises four entities. The first entity is the central server that helps the communicating devices set up authentication before the communication process. It is assumed to be trusted and secured. The second entity is the mobile

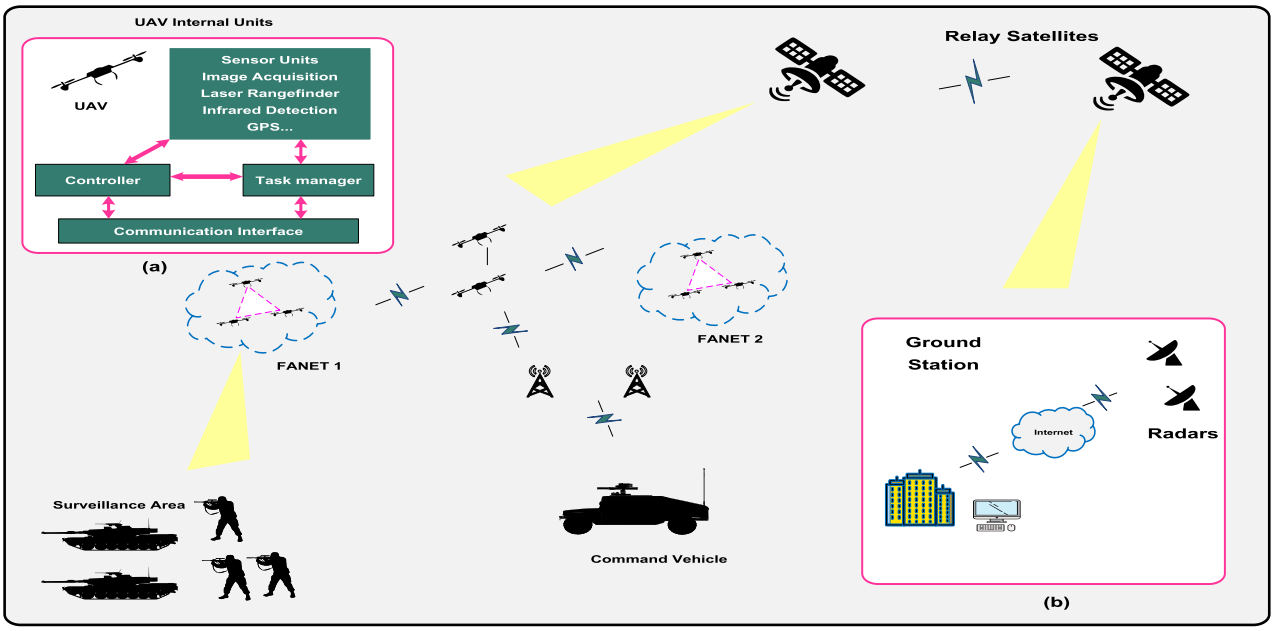

FIGURE 4. A multi-drone network IoD architecture (Source: [32]).

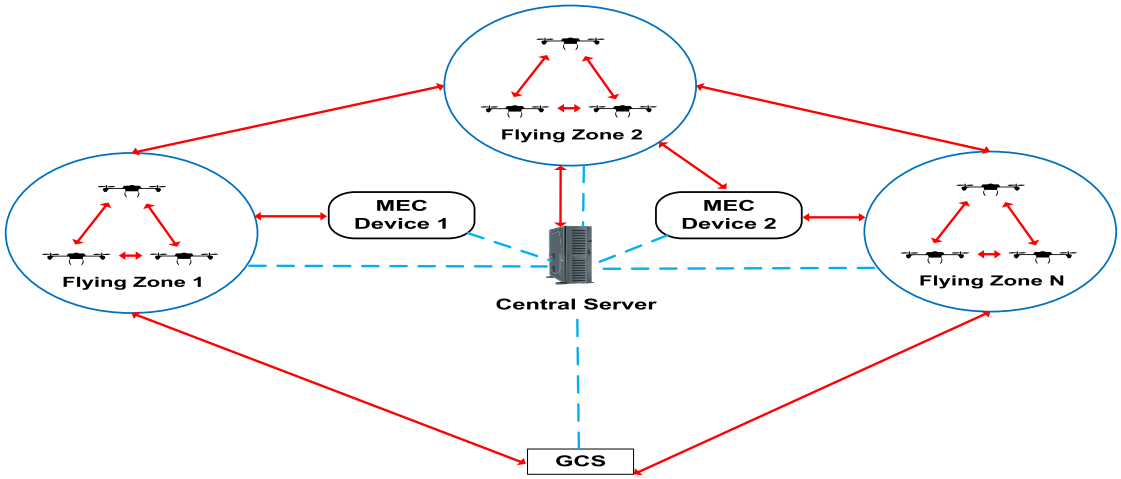

FIGURE 5. The proposed IoD architecture with MEC denoting mobile edge computing, GCS designating ground control station, and dashes blue line representing the registration of the IoD entities with the central server, while the red two-arrow head tick line representing the communication between the IoD entities.

edge computing (MEC) devices that help drones communicate faster with other drones outside their flying zones. The flying drones communicate with the MEC device closer to its vicinity. The MEC devices are mobile, which supports the flying drones' mobility features. They also have more computational ability and memory capacity than the drones, offering faster and efficient communication. The third entity is the Ground Control Station (GCS) that communicates with the flying drones corresponding MECs for control and other flight information. The fourth entities are the flying drones at the various flying zones. Each drone. MEC and GCS devices ask for permission from the central server before participating in the communication process. The drones, MEC, and GCS devices ask for permission from the central server before participating in the communication process. Moreover, each MEC device can communicate with other MEC devices and the central server through a faster and secure channel.

The proposed secured IoD architecture will ensure proper and reliable communication in the IoD network. All the network entities will fully trust each other and the communicated messages. This will ensure overall safety, security, and privacy on the IoD network.

B. TECHNOLOGICAL ADVANCEMENT OF THE INTERNET OF DRONES PARADIGM

Initially, drones were deployed only to the military world. Fortunately, the IoD's applications in various civilians are now evolving rapidly. This significant increase in applications is due to the rapid advancement in science and technology [26], [34], [35]. Moreover, advancement in technological

mechanisms such as the Global Positioning System (GPS), Global Navigational Satellite System (GNSS), Light Detection and Ranging (LIDAR), Synthetic Aperture Radars (SARs), Inertial Measurement Unit (IMU), Robotics, and Imaging Sensing (RIS) has much contributed to the rise of drones [3].

Additionally, reduced weight of the drone, improved battery life, smart sensors incorporation, new camera integration, use of machine learning, deep learning, and artificial intelligence have much influenced the increase in drone applications. Besides, the recent increase in the IoD applications can be related to a decrease in the network entities' cost, most especially the drones [36]–[38]. The evolved drop in drones' price is supported by the miniaturization and cost reduction of the latest electronic components, such as microprocessors, sensors, batteries, imaging systems, and other communication gadgets. Some drones are now sold at the price of a smartphone.

From the past few years until now, drone technology has undergone a transformation series classified into seven groups. Table 2 illustrates the description of the seven groups of drone technology. The advent of the internet of things (IoT) has paved the way to the new face of drone technology, called the Internet of Drones (IoD). IoT allows devices to communicate with one another through a mutual communication network. IoD combined drone technology and IoT to coordinate and control its activities [39]. One of the most important technological models employed by the IoD is edge/fog computing. With this paradigm, IoD entities can process information in a smart/intelligent mode. Real-time processing in an area with minimal connectivity can be handled. The IoD applications can perform computation locally and offload complex computations to the edge/fog nodes, resulting in more accurate and reliable results. This significantly reduced latency, provide tremendous real-time data analysis, decreased computational cost, and increased scalability and overall quality of service [19].

Smart drones equipped with more advanced technological mechanisms will be deployed to the internet of drones (IoD) networks in the nearest future. The mechanisms include and are not limited to magnetometers, gyros, actuators, GPS modules, and advanced processors. The smart drones will have systematic board processors and software, better motors and rotors, more accurate sensors, built-in safe and effective flight control technology that may pave the ways for new transportation and logistics opportunities [40].

Additionally, the deployment of smart sensors on the future IoD network will enhance control and flight monitoring. Deployment of advanced algorithms in the future IoD paradigm will significantly increase its services. For example, researchers at the Massachusetts Institute of Technology (MIT) have developed an algorithm that will enable a drone to track its health condition and take all the necessary actions where applicable [40]. With the algorithm deployment, the drone can check its fuel capacity, damages to its propellers, cameras, sensors, and all other embedded devices.

TABLE 2. The classification of drones' technology [40], [41].

Drones Generation	Technology involved
Group 1	Kid drone toys and basic remote control aircraft of all forms.
Group 2	Static design, Fixed Camera Integration, Video/Still Images Photography, and Manual Pilot Control.
Group 3	Static Design, 2-axis Camera Gimbals, High Definition Video, Basic Safety and assisted Piloting.
Group 4	Transformative Design, 3-axis Camera Gimbals, 1080p High-Quality Video Recording, Improved Safety and Auto-Piloting, and Collision Avoidance.
Group 5	Transformative Design, All round 360^0 Camera Gimbals, 4K, or Higher Video Recording, Intelligent and Advanced Flight Control, and Collision avoidance.
Group 6	Safety and Regulatory standard-Based Design, Collision Avoidance, Control and Safety Landing, Face/Object Recognition, Machine and Deep learning integration, Artificial Intelligence integration, and Air-Space Awareness.
Group 7 (Future Drones)	Fully compliant Safety and Regulating Standard-Based Design, Commercial Suitability, Enhanced Intelligent Piloting and Automated Safety Models, Full Autonomy, Full Air-Space Awareness, Auto Takeoff, Landing, and Mission Execution.

The future IoD technology advancement may also include batteries with a better life, powerful cameras, surrounding-analysis software, advanced sensors for detecting and avoiding obstacles, and developed sense-and-avoid systems.

The past, present, and future technological advancement of the IoD paradigm is presented in this section. It is observed that the improvement in science and technology is the backbone of the overall development. The advancement in science and technology have also paved the ways for many other important aspects that improve the IoD network. These include the Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning (MI), Deep Learning (DL), etc. All these improvements contributed to the achievements attained by the IoD paradigm. Furthermore, there is every tendency that advancement will increase in the nearest future.

C. TAXONOMY OF DRONES

Varieties of drones have been developed in recent years, applicable to different areas [42], [43]. Therefore, a unique classification that will encompass all the available drones is hard to specify. A drone for a particular application can be selected from the lists of drones available with a well-developed classification. This section will, therefore, discuss the existing classification of drones. A comprehensive classification of the drones different from the existing classification will be proposed and relates each class with the level of security and privacy vulnerability associated with it.

1) THE EXISTING CLASSIFICATION OF DRONES

Drone classification has been essential, and its necessity is beyond the drone communities themselves. Researchers and

other governmental agencies have made many efforts to arrive at the most likely acceptable classification. The classifications that were in place are based on different criteria. Authors in [44] classified drones based on their application: civil scientific, and military. They considered drone features such as size, flight endurance, and capabilities. The classes of drones under the classification include Micro Air Vehicles (MAVs), Nano-Air Vehicles (NAVs), Vertical Take-Off and Landing (VTOL), Low Altitude Long Endurance (LALE), Medium Altitude Long Endurance (MALE), and High Altitude Long Endurance (HALE). With regards to the drones used by the UK military, the authors in [45] proposed drones classification by considering the least take-off weight, how the drone is expected to be used, and how they are expected to be operated. The categories of drones under this classification include Class I drones, divided into four sub-categories as Class I'a' (Nano drones), Class I'b' (Micro-drones), Class I'c' (Mini drones), Class I'd' (Small drones). The second group is Class II drones (Tactical drones). The third group is Class III drones (MALE, HALE, and Strike drone).

Authors in [46] classified drones as HALE which covers over 15,000m altitude, and with over 24 hours endurance, MALE that covers 5000-15,000m altitude, and 24 hours endurance, Tactical UAV (TUAV) that covers 100-300 km, Mini UAV (MUAV) that weights below 20kg, Micro UAV (MAV) with wing-span not greater than 150mm, and lastly Nano Air Vehicle (NAV) which are expected to be of the size of sycamore seeds. In [47], the author classified drones into four categories: micro, mini, tactical, and strategic drones. The drones' tactical class is further being classified into six sub-categories as close-range, short-range, medium-range, long-range, endurance, and MALE drones. Moreover, authors in [48] categorized drones as micro, mini, tactical, medium-altitude, high-altitude, and heavy drones.

A comprehensive classification of drones is given in [49]. The classification is based on different features: the mission capabilities, the materials used in manufacturing, wingspan, weight, size, configuration, complexity, and cost of the control system. The drones are categorized into Horizontal take-off landing (HTOL), Vertical take-off landing (VTOL), Hybrid model sub-categorized into Tilt-wing, Tilt-rotor, Tilt-body, and Ducted fan, the remaining categories are Helicopter, Heli-wing, and unconventional drones (those that cannot be under the previous categories). Recently, Tahir *et al.* [50] classified drones based on the number of propellers/rotors and their basic structures. The categories based on the number of propellers/rotors include Tricopter (3 propellers), Octocopter (4 propellers), Hexacopter (6 propellers), and Octocopter (8 propellers). On the order hand, drones' categories based on their basic structures include Fixed-wing, Fixed-wing hybrid, Single-rotor, and Multi-rotor.

According to the Australian Civil Aviation Safety Authorities (CASA), drones can be classified into micro weighing less than 0.1kg, small with a weight between 0.1-150kg, and large drones weighing more than 150kg for fixed-wing and more than 100kg for rotorcrafts drones [51]. Similarly, the United Kingdom Civil Aviation Authority classified drones into three categories: small drones weighing less than 20kg, light drones with a weight between 20kg-150kg, and heavy drones considering more than 150kg [52]. According to a technical report by Arjomandi *et al.* [53], drones are classified based on two major aspects that include their mission and specification. The drones under mission aspects are sub-categorized into six, including Combat, Multipurpose, Rader and communication relay, Vertical take-off and landing, Aerial delivery and supply, and (ISTAR) (Intelligence, Surveillance, Target Acquisition, and Reconnaissance). Furthermore, the drone class under specification aspect is further being classified into eight sub-categories, including Weight, Endurance and range, Speed, Payload, Wing loading, Power, Engine type, and Cost. Don Rassler, a researcher from United states military academy [54] classify drones into four categories: hobbyist drones, midsize military/commercial drones, large military-specific drones, and stealth drones.

Authors in [55] classified drones according to the sectors they are applied to. The sectors include emergency (search and rescue, natural disaster management, humanitarian, aid, ambulances), defence and security (traffic surveillance, drug monitoring, pipeline patrol, port security), environment (soil moisture, gas level, agriculture), infrastructure monitoring and inspection (real estate agents, power line inspection, logistics, insurances), earth observation (archaeology, GIS professionals, media business). Each drone is grouped under a sector based on its metric of performance. Similarly, according to researchers in [3], drones can be classified into six categories that include target and decoy, civil and commercial, military/combat, research and development, logistics, and exploration.

The classification of drones into various categories simplifies their selection for a particular application. As discussed earlier, various drones taxonomy exist. To the best of the authors' knowledge, however, a taxonomy that specifies the level of attacks on the various drones' categories is absent from the literature. This motivated the authors of the current survey to come up with a new taxonomy of drones that will examine the level of attack vulnerabilities associated with the various drones available.

2) THE PROPOSED CLASSIFICATION OF DRONES

In this work, drones are categorized based on four characteristics: the embedded mechanisms on drones, power, user capabilities, and the operating environment. Furthermore, the level of security and privacy of each class is highlighted. The proposed taxonomy of drones is illustrated in Figure 6. The major classes, their description and corresponding sub-categories are given in Table 3, Table 4, Table 5, and Table 6.

A new taxonomy of drones different from the existing classification has been proposed in this study. The different vulnerabilities associated with the drones' categories were given. It is observed that the computational capability of drones is directly proportional to the drones' sizes. Hence, bigger drones with higher computational capability

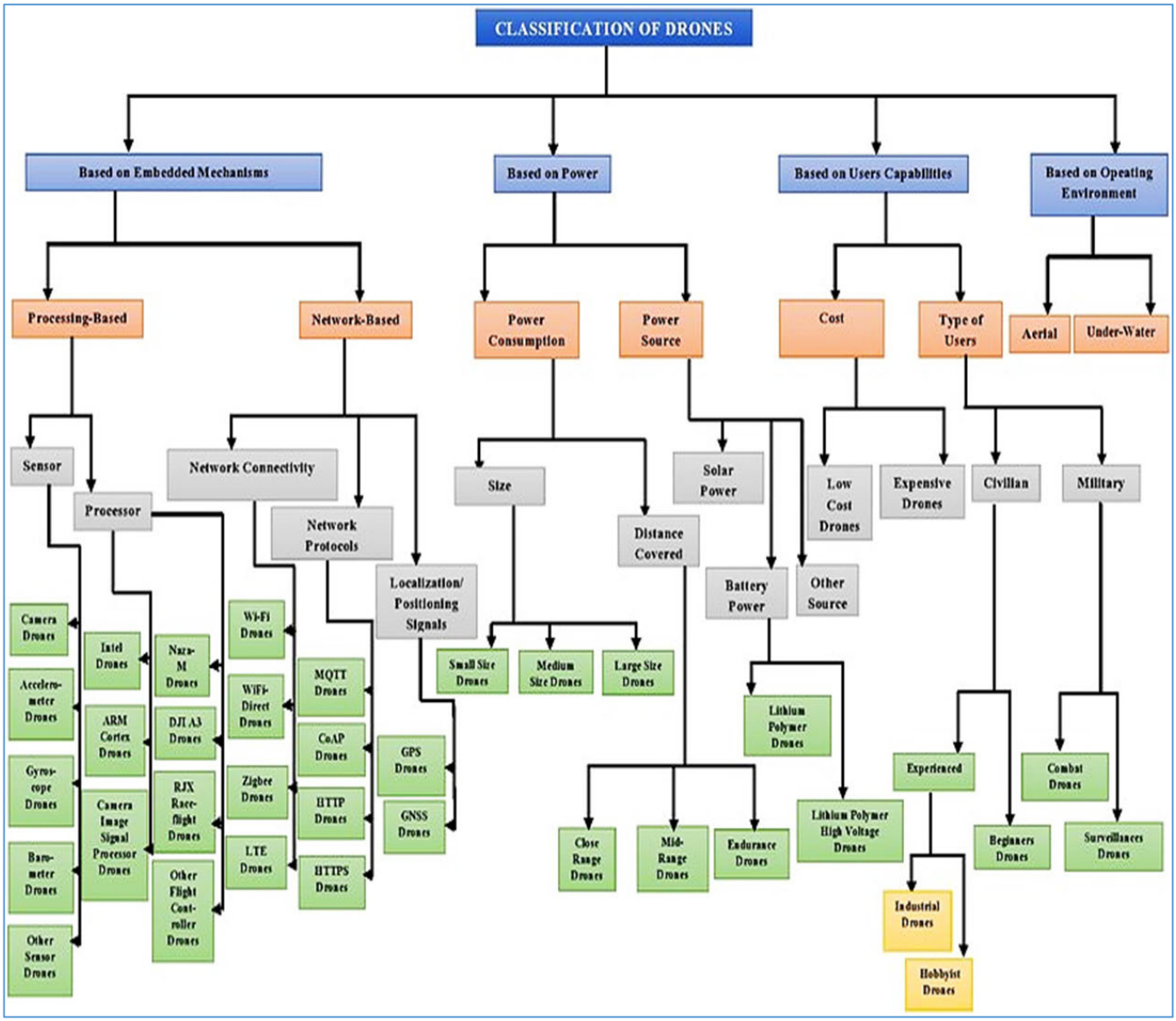

FIGURE 6. The proposed taxonomy of drones.

can accommodate better security and privacy mechanisms, and thus, become better security. Also, the drones used by the military and other experienced users are more secured than the drones used by civilian and beginner users. Moreover, the nature of the embedded mechanisms on drones affects their security and privacy as seen in Table 3. The more secure the embedded mechanism, the more secure the respective drone and vice versa.

III. THE SAFETY ISSUES AND ATTACKS ON THE INTERNET OF DRONES NETWORK

This section discusses the physical threats that affect the drones' safety, which are the most important entities of the internet of drones (IoD) network. These safety issues significantly affect the accomplishment of the targeted mission. Besides, threat models, security and privacy models, and attacks on the IoD network are also presented.

A. SAFETY ISSUES ON THE INTERNET OF DRONES

Apart from the IoD network's security and privacy issues, the drones, which are the IoD network's key components, are vulnerable to physical threats that affect their safety, which hinders the mission accomplishment. The most severe physical threat is theft and vandalism. Because drones are operated in open air/water, they are vulnerable to theft, physical hijack, and destruction using guns and anti-drone ripples [56]. Maldrone, a software virus, is used by hackers to sabotage and disrupt the data link communication and force civilian drones to land instantly [57]. Another scenario is employing hostile drones to act as predators to the drone. These

malicious drones are built with a fishing net that physically catches a target drone. The second most dangerous physical threats of drones are weather conditions and civil challenges. Harsh weather conditions, including low or high temperatures, turbulence, thunderstorm, and freezing rain, may cause a drone accident. Small size drones are more prone to this threat as compared to larger size drones. The civil elements that affect drone navigation include tall buildings, big trees, and electric cables. The third physical threat to drones is a collision between friendly drones in motion. This happens when different drones belonging to the same IoD network unintentionally strike with one another due to the inbuilt sense-and-avoid mechanism's fault.

As discussed in this section, drones' sizes have serious effects on their safety. Smaller drones are more vulnerable to safety threats compared to bigger drones. This is because the smaller drones cannot accommodate efficient safety mechanism due to their resource constraint features. Therefore, future researches are required on the development of lightweight safety mechanisms suitable for smaller drones.

B. THREAT MODELS ON THE INTERNET OF DRONES NETWORK

Threat models are procedures by which potential vulnerabilities or attacks are identified and their mitigation could be specified. The models describe the nature of the attackers, the attack vectors, the network areas to be easily attacked, and the control measures to be taken. In a nutshell, threat modelling is the procedure of specifying all potential threats that may harm a network or system [71]. Several threat modelling methods have been developed over years. However, not all of them are comprehensive enough for a complex cyber-physical network like the internet of drones (IoD). Therefore, threat models for the IoD network should be more robust with a clear picture of the potential threats. There are many threat models employed on the IoD network by various researchers. The major and the most acceptable threat models for the IoD network are given in this section.

1) DOLEV YAO THREAT MODEL

The Dolev Yao threat model is proposed by Dolev and Yao [72]. It is widely accepted for cryptographic protocols. The threat model is characterized by the following:

a) Information is exchanged through an insecure channel
b) An adversary (attacker) can obtain any information exchanged in the network.
c) The attacker can be any networ's genuine entity.
d) The attacker can send information to any of the network genuine entity by impersonating other entities.

Generally, the adversary is considered to have total control of the communication channel including all the exchanged messages. However, the adversary is restricted from having the following features:

a) The adversary cannot deduce a random number (nonce) chosen from a large space.
b) The adversary cannot decrypt an encrypted message without a corresponding private key.
c) The adversary cannot deduce the private keys of the genuine network entities from the corresponding public keys.

2) CANETTI KRAWCZYK (CK) THREAT MODEL

The CK threat model is proposed by Canetti, R, and Krawczyk, H [73]. The threat model has all the characteristics of the Dolev Yao model. Besides, apart from all the privileges given to the adversary in the Dolev Yao model, the adversary of the CK model can compromise the secret parameters including private keys stored in the memory of the genuine network entities by employing a power analysis attack.

3) ATTACK TREE THREAT MODEL

The attack tree threat model employs attack trees methodology on cyber-physical systems and networks [74]. The attack trees threat model was first proposed by Bruce Schneider [75] in 1999. The attack tree is a diagrammatic illustration of attacks in a tree form [76]. The tree's root signifies the goal of the attack, and the leaves symbolize the ways to achieve the goal. Different goals are represented with separate trees which results in a threat analysis model involving a set of trees [76]. Attack trees threat modelling is quite easy to employ. However, it requires a broad knowledge of the corresponding network or system and its security concern.

C. SECURITY AND PRIVACY MODELS ON THE INTERNET OF DRONES NETWORK

Security and privacy models are the architectural design and procedures that represent network entities and their relationship in establishing security and privacy. The models aimed at establishing security and privacy requirement of the network or system under consideration. Many security and privacy models have been considered on the IoD network by researchers. The most accepted models are classified into the following:

1) AUTHENTICATED KEY AGREEMENT IOD SECURITY AND PRIVACY MODEL

This model comprises three main entities: A trusted authority centre (TAC), flying drones, and a ground control station (GCS) [42], [77], [78]. The TAC is fully trusted by all the internet of drones (IoD) network's entities. It registers all the other IoD entities and generates their key pairs. The flying drones are the key components of the IoD network located at their various flying zones. The overall control of the drones is carried out by the GCS. After successful registration of the network entities and key generation by the TAC, registered entities that want to communicate will generate and agree upon a shared session key. The Shared session key will be used for ensuring secure and authentic communication.

TABLE 3. The class of drones based on embedded mechanisms.

Main Class	Sub-Class	Types	Descriptions	Security Threats
Processing-Based	Sensors	Camera Drones	These drones are embedded with cameras to access the typical view of the flight or take aerial photography and videos. They are usually used for surveillance, search and rescue, environmental, and military operations. Examples include TOYEN GordVE-FPV, DJI Spark, and Holy Stone HS100 FPV drones.	These drones are highly vulnerable to image forgery attacks. Moreover, third-party can easily access the information on sensors.
		Accelerometer and Gyroscope Drones	These drones use the embedded accelerometer with a gyroscope to detect any changes in its location. Both linear and rotational changes are recorded. The flight orientation of the drone is also control [58]. All Quad-copter drones are embedded with both accelerometer and gyroscope.	
		Barometer Drones	A barometer is embedded on these drones to measure air pressure values for determining the altitude attained by the drones. Examples are DJI Mavic Pro and new DJI Mavic Air drones	
		Other Sensor Drones	The other sensors embedded on drones include a magnetometer used to measure the magnetic field strength and direction for determining and adjusting of drone route. A rangefinder sensor is used to detect how far a drone is away from the ground. Also, obstacle avoidance sensors are embedded in some drones.	
	Processor (including both onboard processor and flight controller/ground controller)	Intel Drones	They have high efficiency, reduced risk, the capability of gathering more accurate data, and lower cost. An example includes Tello Quad-copter Drone.	Modern processors (Intel, IBM, and some ARM-based) are highly vulnerable to meltdown and spectre attacks which allow programs to steal the processed data of the mobile devices.
		ARM Cortex Drones	They have the capability of reading data from all the embedded sensors. It processes the data and controls the drone's speed. An example includes a Parrot AR drone.	
		Camera Image Signal Processor Drones	Drones equipped with camera image signal processors are characterized by advanced computer vision functionality capable of producing very high-quality images in action scenes. An example includes Parrot AR. drone	
		Naza-M Drones	They can do self-stabilization and keep up their altitude while flying. Naza-M controller-based drones are expensive because the flight controller is not open-source [59]. Examples include Quad-rotor drones.	The drones are used by professionals Hence, they are equipped with advanced security mechanisms and, therefore, are secured
		DJI A3 Drones	DJI A3 flight controller-based drones have dynamic differential technology for improved accuracy and centimetre-level 3-D positioning (exact centimetre vertical and horizontal positioning). This enables precise and repeatable flight routes fractionation. Example include DJI Matrice 600 Pro[60].	
		RJX Race-flight F4 Drones	They use the RJX Race-flight F4 flight controller. The controller enables the drones to recover from accidental rotations, flips, fast rolls and allow full tunable ability. The controller always tries to avoid crashes. The drones are low-cost due to the meagre price of the associated controller. Example include RISE Vusion 250 FPV Drone Racer and Blade Mach 25 FPV Racer.	These drones are resource-constraints with small size and low cost. Hence are not incorporated with the security mechanisms. Therefore, they are highly vulnerable to attacks
		Other Flight Controller Drones	Other flight controllers embedded into drones include Crazepony F3 Flight Controller which is also embedded in racing drones, Naze32 Rev 6 Flight Controller which is designed for small indoor or medium size outdoor multi-rotor drones, and KISS FC–32bit Flight Controller V1.03 designed for mini Quad-core drones.	

TABLE 3. *(Continued)* **The class of drones based on embedded mechanisms.**

Network-Based	Network Connectivity	WiFi Drones	With this type of drone, a smartphone can be connected to access the flight view from the sky through the embedded WiFi (Wireless Fidelity) [61]. Also, the drone can be automatically controlled through the connected smartphone. Example of these drones includes TOYEN GordVE-FPV and UDI U818A drones.	WiFi is categorized under wireless local area network (WLAN). Therefore, it is vulnerable to all the attacks that affect WLAN. These attacks include man-in-the-middle, denial of service, and distributed denial of service, physical tampering, etc. [62].
		WiFi-Direct Drones	The WiFi-Direct paradigm allows two drones located within 200m proximity to communicate without the internet connection [63]. WiFi has a higher bandwidth than LTE-Direct and Bluetooth [64].	Drones connected through WiFi-Direct also connect to a standard WiFi network for other reasons. Therefore, the WiFi-Direct based drones are vulnerable to all the security threats suffered by the WiFi drones.
		Zigbee Drones	They are characterized by accurate positioning control and more stable flight formation in indoor and outdoor environments [65]. The localization error of drones can be easily corrected using Zigbee network connections.	Zigbee is classified under a wireless personal area network (WPAN). WPAN is vulnerable to attacks that include spoofing, snooping, man-in-the-middle, denial of services, etc. [66]. Therefore all the drones under this class are vulnerable to these attacks.
		LTE Drones	The short distance limitation of drones is eliminated with long-term evolution (LTE) network connection. Thus, LTE drones are characterized by long-range communication ability. They are also free from a high signal-to-noise ratio compared to other drones [67].	LTE is under the wireless wide area network (WWAN) category. The security and privacy threats in WWAN are grouped into two. The first is a threat to availability that includes signalling, amplification, insider, and denial of service attacks. The second group is a threat to privacy that includes a smart jamming attack. Hence, drones under this class are also vulnerable to these threats [68].
	Network Protocols	MQTT Drones	The drones use the MQ Telemetry Transport (MQTT) protocol which has the advantage of maintaining reliable messaging through unreliable connectivity (the keep-alive property). Also, the new messages transferred by the drones are cached regularly by the MQTT broker.	They are highly secured because the broker of MQTT support TLS that ensures transport security.
		CoAP Drones	The drones that use Constrained Application Protocol (CoAP) are suitably applied to the environmental monitoring areas where live streaming of sensor data is required, for example, agricultural applications. In this application, energy efficiency and faster communication are essential.	CoAP is vulnerable to IP spoofing, leading to the distributed denial of service (DDOS) attack; hence the CoAP-based drones are not secured
		HTTP Drones	The drones that communicate over the Hypertext Transfer Protocol (HTTP) are very similar to the CoAP based drones. The only difference is that HTTP works on Transmission Control Protocol (TCP) packets, while CoAP works on User Datagram Protocol (UDP) that has a lighter data transfer format. Hence CoAP is more efficient for lightweight devices like drones than HTTP.	Attackers can access all request and responses over HTTP; hence the drones that use HTTP are not secured.
		HTTPS Drones	The 'S' in HTTPS protocols stands for secure. Hence the only difference between drones that uses HTTP and HTTPS is security issues.	HTTPS uses TLS or SSL to encrypt the request and response data over the network; hence all drones that use HTTPS protocols are highly secured.
	Localization/Positioning Signals	GPS Drones	GPS (Global Positioning System) is used by these drones to connect to the spaced satellite. This allows the drones to navigate flight direction and automatically hold their flight position at a fixed location or altitude, or even return to their home base station if any problem is encountered or when the mission is terminated. Examples include DJI Mavic Pro, Hubsan H501S X4, and Contixo F20 drones.	GPS and GNSS signals are vulnerable to spoofing and jamming attacks; therefore, the drones under these classes are highly vulnerable to these attacks
		GNSS Drones	The global navigation satellite system (GNSS) based drones are characterized by having higher navigational capabilities and are more reliable and having better localization accuracy than GPS based drones. Examples include Autel X-Star and DJI Phantom 4 Pro drones.	

2) BLOCKCHAIN-BASED IOD SECURITY AND PRIVACY MODEL

The typical blockchain-based security and privacy model for the IoD network consist of three layers: A user layer, an infrastructure layer, and an IoD layer [28], [30], [79]. In the user layer, the interaction between two users and the interaction between user and drone is specified. The number of users and drones are combined to make clusters of the

TABLE 4. The class of drones based on power.

Main Class	Sub-Class	Types	Descriptions	Security Threats
Power Consumption	Size	Small Size Drones	These types of drones are very small that can fit the top of human fingers. Their size can be up to 20 inches. Example include Altair Falcon AHP Pocket and Potensic A20 Tiny drones	Small and medium-sized drones lack integrated protection mechanisms due to their small sizes. Hence, are highly vulnerable to attacks
		Medium Size Drones	These drones' length is up to two meters and weighed up to 440 pounds (199.581 kg). Two strong people can carry them. Examples include SYMA X5C-1 and Parrot Airborne Cargo Mini drones	
		Large Size Drones	The size of these drones is similar but not up to the size of a small aeroplane. The military mostly uses them for surveillance during the war. Examples include General Atomics MQ 1B Predator and MQM 107E Streaker subscale aerial target drones	These drones are used by the military. All military drones are highly secured
	Distance Covered	Close Range Drones	These drones can cover up to 50Km and can stay up to 45 minutes to 12 hours in the air. Examples include Holy Stone Quad-copter and DJI Mavic Pro drones	Close and mid-range drones are not fully secured because of the associated resource-constraint features. Not every security mechanism can fit them
		Mid-Range Drones	The speed of these drones is higher than that of small drones. They cover up to 150Km and can stay for more than 12 hours in the flying mode. An example includes Raven UAV flying drone	
		Endurance Drones	This type of drones cover more than 450km and can stay on the air for hours or even days. The military mostly uses them. Examples include Heron TP static and Holy Stone HS170 Predator Mini drones	These drones are used by the military. All military drones are highly secured
Power Source	Solar Power	NA	Solar-powered drones are characterized by the longest continuous flight with the greatest altitude and long endurance compared to other powered drones. Solar-powered drones can fly for multiple numbers of days [69]. An example includes the PHASA-35 drone	These drones are used by the military or other special applications. Hence, they are highly secured
	Battery Power	Lithium Polymer Drones (LiPo)	The lithium-polymer battery is having a lower cost, high adaptability because they are available in different packaging shapes. However, they are having limited power compared to other power sources. The hobbyists' drones mostly use them. LiPo cell has a full charge of 4.2V	The battery-powered drones are vulnerable to battery draining attacks. Moreover, both battery-powered and hydro fuel cell-powered drones are usually small. Therefore are highly vulnerable to attacks due to a lack of an integrated protection mechanism
		Lithium Polymer High Voltage (LiHV) Drones	The only difference between LiPo and LiHV is the charging features. The LiHV cell has 4.35V at full charge. LiHV provides more power compared to LiPo, however, its voltage drastically drops when discharging, thus making it difficult to decide the flight time [70]. While LiPo is characterized by linear discharge. They are also mostly used by hobbyists drones	
	Other Sources	Hydro Fuel Cell	Drone powered by hydro fuel cells can last for about two hours compared to the Lithium polymer drones that last for a few minutes. Most importantly, the refuelling process is quick and easy. Examples include HyDrone 1800 and Narwhal 2 drones	
		Combustion Engine	These drones can last for almost one hour flying. The combustion engine upper more power than the LiPo battery; however, the powered drones produce noise and are dangerous as they carry along with flammable gas. Examples include Goliath Quadcopter and Yeair Hybrid Quad drones.	The sizes of these drones are relatively larger than the battery and hydro fuel cell drones. Therefore, they are secured because they can be incorporated with security mechanisms.
		Tethered	A tethered powered drone can stay in the air for years. Continuous electrical power is provided to the drone directly from a power supply unit. However, the drones run only for a minimal flying area. They also fly up to a few hundred meters of altitude due to the flexible connecting cable attached. An example includes Orion UAS.	The tethered and laser transmitter drones are better than the battery, hydro fuel cell, and combustion engine drones in terms of sizes and computational power. Hence, these drones are highly secured because they can be incorporated with various security mechanisms.
		Laser Transmitter	They have no limit on flying time. They can fly forever because they are powered directly by a light beam from the ground station. The light is then converted to electrical energy.	

blockchain with a drone as a master controller. Each cluster is used to control and coordinate the behaviour of drones. The blockchain provides security and privacy to the network. The infrastructure layer specifies connectivity and control of users and drones through the ground control station (or base station). Lastly, the IoD layer specifies the communication between user and drone for efficient and secure data exchange using blockchain technology. They communicate

TABLE 5. The class of drones based on user capabilities.

Main Class	Sub-Class	Types	-	Descriptions	Security Threats
Cost	Low-Cost Drones	NA	NA	The sizes of drones under this category range between very small to medium size. Most of the drones are very easy to use, even without any skill. The price range $50 to $5,000. Example include Syma X5C 4 Channel and Parrot Bebop 2 drones.	These drones are resource constraint in nature and cannot be incorporated with security mechanisms. Therefore, they are highly vulnerable to attacks.
	Expensive Drones	NA	NA	As compared to the category of the cheaper drones, these drones are larger, and their operation requires a highly skilled expert. The military mostly uses them. Their prices range from $25,000 to $131million. Examples include DJI Phantom and Boeing Scan Eagle Unmanned Aerial drone.	The computational ability of these drones is very high, as such advanced security mechanisms can be incorporated. Therefore, they are highly secured.
Type of Users	Civilian	Experienced	Industrial Drones	Industrial drones communicate directly to the industrial control system compared to the military, hobbyist, and beginner drones with end-to-end communication networks between the user and ground control centre. They are used to monitor industrial processes that humans may not monitor due to human uncertainty features or inaccessible to humans due to size or environmental hazards conditions. They have better performance than the hobbyist and beginner drones. They also use advanced sensors and innovative technologies. Examples include Asctec Falcon 8 and Intel Falcon 8+ drones.	Industrial and hobbyist drones are incorporated with collision avoidance features and integrated with a security mechanism. Therefore, these drones are secured.
			Hobbyist Drones	Hobbyist drones are used for enjoyment or educational purposes only. They are not meant for commercial purposes. They are mostly meant for taking photographs for personal use only. Examples include SYMA X5C explorer and HUBSAN X4 drones.	
		Beginners Drones	NA	This class of drones is specially designed for people without any knowledge of how to use a drone. No setting or customization is required. They are easy and quick to navigate. The drones take off, fly, and lands easily. They cover a minimum range of flight. Example include Holy Stone HS170 Mini and Parrot Airborne Cargo Mini drones.	These drones are tiny. As such, they are not incorporated with security mechanisms. Hence, they are highly vulnerable to attacks.
	Military	Combat Drones	NA	These drones are designed mainly for military strikes operations. Examples include MQ-1C Gray Eagle and General Atomics MQ 1B Predator drones	Typically, due to the nature of the military drones' application and sizes, they are more secured compared to civilian drones because they use advanced security mechanisms
		Surveillances Drones	NA	These drones are used to provide the military with an exact picture of the target area, even at night-time. Additionally, they are used for reconnaissance and decoys applications. Examples include IAI Heron TP and Raven drones	

through the internet and their updated information is stored in the blockchain.

3) USER AUTHENTICATION IOD SECURITY AND PRIVACY MODEL

A typical user authentication security and privacy model for the IoD network comprises flying drones, server (control room), and users [26]. The flying drones send data continuously to the server. A remote authentication between the flying drones and users is established through the server. The user and the flying drones share a common session key and start communication after the mutual authentication. Therefore, each of the users on the IoD network can obtain information securely from the flying drones.

TABLE 6. The class of drones based on the operating environment.

Classes of Drones	Descriptions	Security Threats
Aerial	These drones are meant to be operated on air. All drones are aerial except the under-water class of drones.	The aerial drones used by the military, those classified as expensive, and those classified under experienced users are typically secured, while the remaining are either not fully or not secured.
Under-Water	These drones are designed purposely to be operated on or under the water' surface. Their electronic components are tightly sealed to prevent being damaged by water.	Typically, all underwater drones are used for special purposes by experienced users or the military; they are highly secured.

4) GROUP AUTHENTICATION IOD SECURITY AND PRIVACY MODEL

In this type of security and privacy model, several IoD network entities with the same or even different features merge to form a group in performing authentication [80]. This significantly reduces the computational overheads as compared to individual authentication. A group manager, with better resources as compared with all the group members generates all the parameters needed for the group authentication process. A group member can be a ground control station (base station), a mobile edge computing device (MEC), or a trusted authority.

D. ATTACKS ON THE INTERNET OF DRONES NETWORK

On the one hand, the primary purpose of attacks on the internet of drones (IoD) network just like other typical attacks is to gain access and alter the attacked messages for fulfilling the needs of the attacker [77], [81]–[83]. On the other hand, attacks on the drone compared to the typical cyber-attacks usually occur due to the severe design loopholes and lack of wireless security protection mechanisms. There are many attacks on IoD; therefore, there is a need for classifying them for exploring their effects in detail. Also, exploring the existing countermeasures for each class is essential.

CLASSIFICATION OF ATTACKS ON THE INTERNET OF DRONES

The classification of the attacks on the internet of drones (IoD) is given in this section. Localization or position estimation is the essential need of any cyber-physical system like the IoD [84]. Therefore, the attacks that lead to a localization error of IoD entities are devastating. Hence, in this review work, all the IoD network attacks are classified into only two major categories. All attacks that hinder the secure position estimation of drones are categorized under localization error attacks, and the remaining attacks are categorized under the attacks on security and privacy requirements. The attacks on security and privacy requirements are subcategorized into attacks on integrity, availability, authenticity, confidentiality, and privacy. Figure 7 shows the proposed taxonomy of IoD attacks. The categories and sub-categories of the attacks with their corresponding countermeasures are as follows.

1) LOCALIZATION ERROR ATTACKS ON THE INTERNET OF DRONES AND THE CORRESPONDING COUNTERMEASURES

The sub-categories of the localization error attacks and the corresponding mitigation methods are given in this section. The description of the major attacks is shown in Table 7.

a: ATTACKS ON NAVIGATIONAL SIGNALS

The navigational signals used for estimating a location in the IoD network include Global Positioning Systems (GPS) signals, Global Navigation Satellite Systems (GNSS) signals, and Ground Control Signals (GCSs). The attacks on these navigational signals and the countermeasures used in mitigating some of the attacks are provided next.

i) GPS SPOOFING ATTACK

Here, the attacker sends fake Global Positioning System (GPS) signals to the drone's control system and forces it to a direction specified by the attacker. In an attempt to mitigate the attack, authors in [85] employed a deep learning-based intrusion detection system that is intelligent enough to differentiate between spoofed and original GPS signals. Authors in [86] used the monocular camera visual sensor and information fusion based inertial measurement unit (IMU) of the drone to detect GPS spoofing attack. Additionally, the authors provided a method of assisting the drone to return in the event of a GPS spoofing attack. Similarly, in [87] the authors suggested using spoofing-detecting sensors attached to the drone for encasement of mitigating GPS spoofing attack. Although authentication of GPS signal can help in mitigating GPS spoofing, authors in [88] argued that the use of the conventional cryptographic algorithms involves complex computations that may need changes to the structure of the satellite system. Similarly, authors in [89] claimed that encrypting the GPS signal with a digital signature is an old method of mitigating GPS spoofing attack. However, alternative methods that did not use encryption are still unproven. Authors in [90] employed a rule-based intrusion detection system to mitigate the effect of a GPS spoofing attack. The nodes' normal behaviour is modelled using GPS spoofing's characteristics detection rules.

ii) GPS JAMMING ATTACK

In this type of attack, the malicious entity barricades all the global positioning system (GPS) navigation signals from

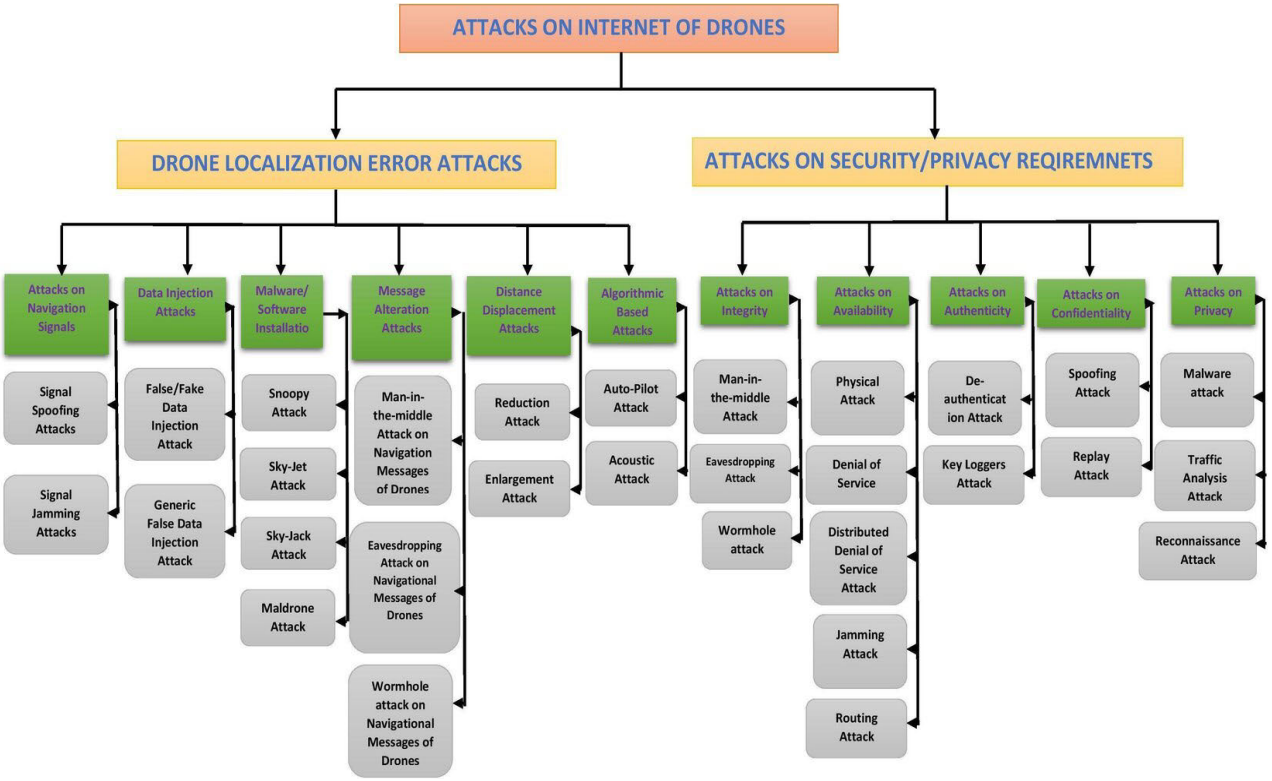

FIGURE 7. The proposed taxonomy of attacks on the internet of drones.

TABLE 7. The description of the major localization error attacks on the internet of drones.

S/N	ATTACKS	DESCRIPTION
1	Attacks on Navigation Signals	Here, the adversary alters the signals used to determine drones' location. This leads to a false estimation of the drones' current location by its onboard guidance systems.
2	Data Injection Attacks	The adversary feeds malicious data to the drone control system to control its direction-finding system.
3	Malware/Software Installation Attacks	The attacker installed software or malware on a drone. Once installed, the software/malware automatically creates a secret connection for sending a command to the infected drone.
4	Message Alteration Attacks	Here, the attacker manipulates and send to the affected drone the navigation and other confidential and vital messages communicated between the targeted drone and its corresponding navigation control system.
5	Distance Displacement Attacks	The adversary fabricates the distance measurement data computed by the corresponding navigation control system to be different from the real measurement and then send it in advance to the targeted drone.
6	Algorithmic-Based Attacks	The attacker manipulates the location state control algorithms to compromise the drones' flight path leading them away from the predetermined direction.

reaching the drone. This consequently leads to hijacking or even the crash of the drone. To mitigate the attack, authors in [91] proposed a software-based mechanism that takes the full record of the drone flight controlling commands from take-up. This record is then used to return the drone to the take-off location after an attack is detected. Authors in [88] recommended that the best way of mitigating GPS jamming attacks is to use alternative navigation methods. In line with this, authors in [92] used a vision inertial navigation system when the drone fails to receive GPS signals. Besides, authors in [90] employed a rule-based GPS jamming attack detection method by modelling the GPS jamming attack's characters.

iii) GNSS SPOOFING ATTACK

Here, the adversary sends a forged global navigational satellite system (GNSS) signals to the drone, and so force it in the wrong direction. To mitigate the GNSS spoofing attack, Zangvil et al. [93] proposed a patent system for detecting the attack. A radio frequency absorber attached to the GNSS antenna is used to show the direction of incoming signals. A processing circuitry coupled to memory enables the system to identify the received GNSS signals' characteristics and analyses it to know either it is spoofed or original.

iv) GNSS JAMMING ATTACK

In this type of attack, the adversary stops all the GNSS signals from reaching the targeted drone. This results in having total control over the attacked drone.

v) GCSS SPOOFING ATTACK

In this attack, the third party sends false ground control signals (GCSs) to the drone to direct it to a specified place.

In trying to mitigate this attack, authors in [88] suggested that confidentiality, authenticity, and integrity mechanisms can be employed in dealing with GCSs spoofing attack. Because GCSs are stationary, the authors also agreed that drones could use location-based authentication mechanisms to find the source of the GCSs to find out whether they are spoofed or genuine.

vi) GCSS JAMMING ATTACK

The adversary obstructs all the ground control signals (GCSs) from the ground control system from reaching the drone. This results in taking control of the drone by the adversary.

b: ATTACKS DUE TO DATA INJECTION

In this section, the localization error attacks that resulted from injecting falsified data to the original control communicated messages will be discussed.

i) FALSE/FAKE DATA INJECTION ATTACK

The malicious entity manipulates the drone's direction state estimation by modifying the corresponding direction measurement data so that a bad measurement detector may not detect it. Authors in [94] proposed a novel detector capable of detecting FDI attack. The detector's computational overhead is relatively low compared to the conventional Kalman-Filter (KF) based employed by most of the researchers in curbing the effect of FDI attack.

ii) GENERIC FALSE DATA INJECTION ATTACK

In this type of attack, the invader alters the drones' position estimation data to a specific value within a given range [94].

c: ATTACKS DUE TO SOFTWARE/MALWARE INSTALLATION

The localization error attacks that originated as a result of software or malware effect on the targeted IoD entities will be elaborated in this section

i) SNOOPY ATTACK

The third party installed a snoopy malicious software on a drone to gather its personal information and used a WiFi-enabled smartphone to track and manipulate the infected drones' navigation control.

ii) SKYJET ATTACK

In this attack, the adversary installed ready-made hijacking software to deactivate the infected drone's navigation controller and connect it to itself [95].

iii) SKYJACK ATTACK

The attacker installed Skyjack malicious software on a targeted drone to detect all the wireless networks within the vicinity of the drone [11]. The attacker can deactivate any client connected to the infected drone in the wireless network, such as the navigation controller.

iv) MALDRONE ATTACK

The adversary installed Maldrone malware on a targeted drone. The malware automatically serves as a proxy between the infected drone's flight controller and sensor communication. Thus, the infected drone can be easily hijacked and directed by the attacker to any desired place [96].

d: MESSAGE ALTERATION ATTACKS

These are localization error attacks initiated by altering the control and other vital communicated messages. They include:

i) MAN-IN-THE-MIDDLE ATTACK ON NAVIGATIONAL DATA OF DRONES

The attacker secretly manipulates the navigation messages communicated between the drone and its corresponding navigational control system and sends them to the drone without its knowledge [97]. This enables the attacker to hijack the drone to the desired place. To prevent drones' hijacking due to this attack, authors in [98] employed a machine learning-based authentication scheme. They evaluate the time-series telemetry traces of the drone during the flight. The authors then used three different machine learning methods: K-Nearest Neighbor, Support Vector Machine and Logistic Regression Machine. Results showed that a K-Nearest Neighbor was the best method.

ii) EAVESDROPPING ATTACK ON NAVIGATIONAL DATA OF DRONES

The malicious party takes advantage of the unsecured communication channel to intercepts the communicated navigational messages between the targeted drone and its navigation controller. Later, the attacker manipulates and resend it to the drone without its knowledge [99].

iii) WORMHOLE ATTACK ON NAVIGATIONAL DATA OF DRONES

The attacker listens to and records the navigational and other control messages sent to the targeted drone by the navigational control system after establishing itself as the network's shortage path. It then manipulates and channels it to the drone as if it is coming from the legitimate navigation control system [100].

e: ATTACKS DUE TO POSITION ALTERATION

These are localization error attacks that alter the position estimation information of the IoD entities.

i) REDUCTION ATTACK

The adversary falsifies the drone distance measurement data computed by the corresponding navigation control system to be shorter than the real. It is then sent in advance to the targeted drone [100].

ii) ENLARGEMENT ATTACK

The adversary falsifies the drone distance measurement data computed by the corresponding navigation control system to be larger than the real signal, and then sends it in advance to the targeted drone [100].

f: ALGORITHMIC-BASED ATTACK

Here, we present localization attacks based on algorithms.

i) AUTOPILOT ATTACK

The attacker exploits the autopilot state estimation algorithms' weaknesses for an autopilot drone to make it follow a misleading flight path. The attacker injects a fake state into the navigational control of the targeted IoD devices [101].

ii) ACOUSTIC ATTACK

The attacker employs a malicious drone equipped with a speaker capable of generating a sound different from the targeted drone's gyroscope resonant frequency to steer at the targeted drone. This automatically distorts the acoustic position control algorithm of the targeted drone [102].

Position estimation is very essential in the IoD network. Therefore, attacks causing localization error are quite devastating. As observed in this section, a few mitigation techniques for various localization error attacks are found in the literature. Therefore, more localization error attacks mitigation techniques are required.

2) TECHNIQUES AND OTHER COUNTERMEASURES FOR CURBING THE ATTACKS ON SECURITY AND PRIVACY REQUIREMENTS ON THE INTERNET OF DRONES

The class of attacks on security and privacy requirements on the IoD network will be explored in this section. Security and privacy requirements are the capabilities and functions employed in eliminating threats and vulnerabilities [19]. Such requirements on the Internet of Drones (IoD) include integrity, availability, authenticity, confidentiality, and privacy. Moreover, the existing mitigating techniques to the identified attacks are also explored. Table 8 illustrates the security and privacy requirements of IoD and their description. Also, Table 9 illustrates the various attacks on IoD security and privacy requirements and their description.

a: TECHNIQUES AND OTHER COUNTERMEASURES FOR CURBING THE ATTACKS ON SECURITY AND PRIVACY REQUIREMENTS ON THE INTERNET OF DRONES

Drones are resource constraint devices characterized by low computational power, low memory capacity, and low energy consumption. As such, the traditional mitigating techniques for curbing attacks applicable to other similar aircraft architectures may not be applied on the internet of drone (IoD). Attacks mitigating techniques applicable to IoD and other countermeasures will be discussed in this section.

TABLE 8. Description of the IoD Security and privacy requirements.

Security/Privacy and Safety requirements	Description
Integrity	This ensures that the transferred messages are delivered to authorized IoD entities without manipulation from an adversary.
Availability	It ensures that all the IoD genuine entities can access all the provided services at any time.
Authenticity	This ensures thorough monitoring, verification of IoD genuine entities, and establishing trust among them.
Confidentiality	It ensures that only genuine IoD entities have the right to get access to the communicated messages in the IoD environment.
Privacy Preservation	It ensures that all the IoD entities' information is kept unrevealed under monitoring.

i) MITIGATION TECHNIQUES FOR ATTACKS ON INTEGRITY

To mitigate man-in-the-middle, eavesdropping, and wormhole attacks on the internet of drones (IoD), authors in [88] have suggested the use of cryptographic encryption protocols. Furthermore, the authors recommended the use of strong intrusion detection techniques, strong and reliable antivirus applications, strict policies, and firewalls. According to the authors, a side-channel analysis should be used to detect deadly Trojans. Additionally, logging procedures used for tracking the sequence of events in the IoD network should be devised as said by the authors. However, the authors fail to specify the security mechanisms suitable to the resource-constraints IoD network. Furthermore, authors in [103] utilized a blockchain-enabled order processing on drone delivery services for ensuring the integrity of the information exchanged in the drone services platform.

ii) MITIGATION TECHNIQUES FOR ATTACKS ON AVAILABILITY

Authors in [104] proposed a lightweight and low power defence mechanism applicable to the resource constraint drones for mitigating the physical attack in the IoD network. A microphone-based acoustic sensing mechanism called Droppler Dodge is developed. It is used to identify the approaching flying objects that are about to hit the drones. An acoustic signal is transmitted a couple with droppler frequency shifts in the reflected signals for predicting the flying objects' intention. To offer solutions to drones' physical attack in the IoD network, authors in [105] developed a smart parachute that provides safe-crash solutions to drones. Cyber-physical action language (CPAL), a lightweight design model for embedded systems is used in the design, simulation, and verification phases. Authors in [106] argue that commercial drones are only equipped with proximity sensors that detect only large static objects and may not detect speedy and dynamic objects directed towards them. Therefore, to solve this problem, the authors proposed an onboard sensor and actuator modules couples with small footping inferencing algorithms.

To mitigate the effects of the denial of service (DOS), and the distributed denial of service (DDOS) attacks that affects

TABLE 9. Description of attacks on the IoD security and privacy requirements.

Attacks	Description
	Attacks on Integrity
Man-in-the-middle Attack	Here, the malicious party, connects to the communication channel of the IoD network, intercept, and in some cases manipulates the communicated messages, and send it to genuine IoD entities without their knowledge.
Eavesdropping Attack	Here, the attacker connects itself with the IoD communication channel, steals and manipulates the communicated messages.
Wormhole Attack	The mischievous party connects to the IoD communication channel, it listens and records the communicated message, and then manipulates and sends it to the legitimate IoD entity as if it is coming from a genuine source.
	Attacks on Availability
Physical Attacks	The intruder attacks the drone physically. These include theft and vandalism using guns, anti-drone ripples, Maldrone, hostile drones (drones' predators). Moreover, harsh weather, civic challenges, and a collision between drones of the same IoD network contributed to the threats affecting the IoD network.
Denial of Service (DOS) Attack	The attacker floods the IoD communication channel with an unnecessary request to overload the network to make resources unavailable to genuine entities.
Distributed Denial of Service (DDOS) Attack	A DDOS attack is similar to a DOS attack except that the DDOS involves more than one adversary attacking from different locations. The adversaries engulf the IoD network with unnecessary messages to make it unworkable [113].
Jamming Attack	The adversary blocks all the communicated messages from reaching the target IoD entity.
Routing Attack	The intruder intentionally tries to take off the targeted IoD entities' resources.
	Attacks on Authenticity
De-authentication Attack	The attacker disconnects the target genuine entity from the IoD network. Thus taking over the infected entity.
Key Loggers Attack	The malicious party use specific key struck recording software to intercept and monitors the targeted IoD entities.
	Attacks on Confidentiality
Spoofing Attack	The attacker sends false messages to the targeted IoD genuine entity with the intention of impersonation and stealing data.
Replay Attack	The third-party intercepts and manipulates the communicated messages from the genuine IoD entities and later sends it to the target entity as if it is from the first sender. Unlike the man-in-the-middle attack in which the attacker might or might not manipulate the intercepted messages, in the replay attack, the attacker always alters the intercepted message before forwarding it.
	Attacks on Privacy
Malware Attacks	The intruder inserts spying software into the targeted IoD entities for monitoring purposes.
Traffic Analysis Attack	The attacker intercepts and examines the IoD network traffic intending to deduce information from the communicating entities.
Reconnaissance Attack	The malicious party gathers as much vital information about the target IoD network by using social engineering and other automated tools available. The information may include the genuine entities' IP addresses and uniform resource locator.

the availability requirements in the IoD network, authors in [107] evaluates the effects of both DOS and DDOS attacks on drones. A falsifying mechanism for alerting users when drones are exceeding the flight limit range is presented. This significantly evades the attacks. In [88], the authors suggested anonymous-based intrusion detection in IoD to differentiate between genuine and corrupted communications resulting from the DOS and DDOS attacks. Additionally, the authors suggested advanced sensors capable of cross-checking the drones' flight status. This may significantly allow the flight control system to tolerate specific components malfunctions or even alteration that may significantly affects availability requirements.

iii) MITIGATION TECHNIQUES FOR ATTACKS ON CONFIDENTIALITY

To ensure trust among the entities of a drone delivery platform, authors in [103] proposed a blockchain-based scheme that enables smart contract between the sellers and buyers on the platform. Also, to set up authentication of IoD communication entities, authors in [108] proposed a novel temporal credential-based lightweight authentication scheme called TCALAS. The scheme is proved to be resistant to the known authentication attack. However, authors in [109] found that the TCALAS scheme is not scalable because it can only work on one IoD flying zone. Also, it is vulnerable to traceability and stolen verifier attacks. In the stolen verifier attack, the attacker intercepts a genuine network entity's verifier during the authentication session. It uses it to generate a communication message and conveys it to the targeted network entity. Hence, the authors proposed an enhanced TCALAS scheme called iTCALAS, and it is proved to solve the highlighted problems and can work when there are multiple flying zones in the IoD network. In [110], the authors proposed a lightweight energy-efficient cryptographic scheme for ensuring authentic communication in the IoD network. They employed the elliptic curve cryptography and used self-certified keys for eliminating the maintenance overhear associated with the Public Key Infrastructure (PKI) model. For better computation overhead, a FourQ elliptic curve is used. The BPV-FourQ-Schnorr's signature optimization technique is employed to speed up the elliptic curve scalar multiplication. The experimental analysis shows that the proposed scheme has less energy consumption than other benchmarking schemes. Similarly, authors in [26] proposed a novel authentication and key agreement technique between the IoD's communicating entities with the use of a server. The scheme can work on IoD with many flying zones. The authors employed only XOR operations and hash functions in the scheme's design, hence it has less computation and communication costs.

To mitigate a de-authentication attack on the IoD network, Pigatto *et al.* [111] proposed a novel scheme called Sphere. The scheme allows every drone in the IoD network to share information securely. At the drone start-up process, the central security unit checks the database credentials for all the drones' modules. Once found, permission is guaranteed, and the drone is authenticated, else permission is denied. Authors in [88] suggested that only legitimate drones should be granted access to the

IoD network resources. Additionally, access control policies and authentication mechanisms should be implemented to prevent the adversary from getting access to the network. During communication, mutual authentication should be established between the communicating entities. Additionally, operation-specific distance bounding protocols should be incorporated into the authentication scheme. This will expressively mitigate the key loggers attack when the adversary is not near to the targeted drone.

iv) MITIGATION TECHNIQUES FOR ATTACKS ON CONFIDENTIALITY

Dey *et al.* [112] proposed mitigating spoofing attacks on the confidentiality requirement on the internet of drones (IoD) network. According to them, anti-spoofing and anti-jamming receivers help much in curbing the associated attack. Furthermore, the authors suggested the use of an encryption technique in protecting the library files, and the use of obfuscators in preventing reverse engineering and decompiling of firmware, and using encryption on the entire firmware libraries and storing the encryption keys on the hardware components of drones for mitigating the replay attack. Similarly, a lightweight identity-based encryption scheme called IBE-LITE is proposed in [24]. Elgamal and Advance encryption standard (AES) cryptographic protocols are used to encrypt the navigational information of the requesters. The scheme is enough for ensuring the secure transfer of information in the IoD network, which mitigates both the spoofing and replay attacks. The uniqueness of the technique is the ability to use an arbitrary string for generating a public key, and the capability of generating a public key from the corresponding secret key. Authors in [88] suggested the use of cryptographic protocols such as the advanced encryption standard (AES) in the IoD network in trying to mitigate the replay attack. This may significantly mitigate the unauthorized disclosure of sensitive information during the communication process.

To ensure a confidential exchange of information between drones and the ground control server in the IoD network, authors in [30] proposed a blockchain-based access control scheme. A ripple protocol consensus algorithm (RPCA) is used to place the transactions resulted from the information being communicated by the IoD entities into blocks which are later added to the blockchain. Similarly, the research by authors in [114] ensures a secure transfer of confidential information among drones using a deep learning-based blockchain scheme. A deep Boltzmann machine is used to select a miner node using features such as computational resources, battery power, or flight time of the drone.

v) MITIGATION TECHNIQUES FOR ATTACKS ON PRIVACY PRESERVATION

In the scheme proposed by authors in [111], a health check module is centralized which assures a safer operation of the drones in the IoD in trying to mitigate the traffic analysis attack. In another technique, authors in [115], proposed a blockchain-enabled drone delivery framework. Hash functions and small signatures are employed by the scheme to achieve privacy preservation requirement.

It can be observed from this section that there are more authenticity and availability attacks mitigation techniques as compared to the remaining security and privacy requirements. Moreover, most of the techniques for curbing authenticity attacks are either not suitable due to the high computation and communication costs or provide an inadequate level of security. Thus, there is a need for more efficient techniques.

b: PERFORMANCE EVALUATION METHODS AND THE PERFORMANCE METRICS EMPLOYED BY THE ATTACKS MITIGATION TECHNIQUES

In this section, performance evaluation analysis methods and the metrics employed by the attacks mitigating techniques described in the earlier sections will be explored. Performance evaluation analysis is conducted to check the level of the proposed attack mitigating techniques' soundness. Evaluation metrics are used as a measure of performance. Table 10 illustrates the performance evaluation methods and the corresponding metrics employed by the attack mitigating techniques proposed for the IoD deployment.

Table 10 shows that researchers have made many efforts to curb the attacks affecting the IoD network. However, the suggested techniques to mitigate localization error attacks are not much compared to the attack curbing techniques for security and privacy requirements. Therefore, it remains challenging to develop techniques for mitigating localization error attacks for IoD deployment. On the other hand, regarding the remaining attacks on the security and privacy requirements, several techniques have been proposed to mitigate the attacks on authenticity requirements compared to the other requirements. However, most schemes lack experimental methods for efficiency evaluation.

Moreover, the security analysis employed by the techniques is broadly classified into two: Formal security analysis, and informal security analysis. The formal security analysis is further classified into analysis with tools and analysis with methods. The tools used in the first category include the cryptographic protocol verification tool called ProVerif [116], and the automated verification tool for internet security protocols and application called AVISPA [117]. Other security verification tools that exist in the literature and not used by the explored technique are Syther [118], Athena [119], NRL [120], and Hermes [121]. The Athena, NRL, and Hermes tools are not commonly used because they are not freely available for download as only their current version has a web interface [122]. Likewise, the methods under the second category of the formal security analysis include the Burrows, Abadi and Needham logic (BAN Logic) [123], [124], and the Random-Oracle-Model [125], [126]. Figure 8 illustrates the classification of security analysis. Moreover, a brief overview of the formal security tools are given as follows:

TABLE 10. The performance evaluation methods and the corresponding evaluation metrics employed by the IoD attacks mitigation schemes.

Ref.	Attack Mitigation Category	Performance Evaluation Method	Purpose of the Evaluation	Evaluation Metrics
[85]	GPS Spoofing Attack	Simulation (Using the ONE simulator)	To analyze the vulnerability of the drone autopilot system and the sensitivity of the intrusion detection system. Also, to measure the robustness against known and unknown attacks.	Attack Detection Accuracy
[86]	GPS Spoofing Attack	Testbed Experiment (Using DJI Phantom 4 drone)	To analyze the GPS spoofed signals based on the inertial measurement unit of the drone.	Measuring Errors
[90]	GPS Spoofing and Jamming Attacks	Simulation (using NS3)	To analyze the proposed attack detection technique on a realistic IoD network.	Detection Rate, False Positive Rate, Efficiency, and Communication Overhead
[94]	False/fake Data Injection Attack	Simulation (using MATLAB and Ardupilot)	To analyze the proposed attack on Kalman Filter based position estimation and autopilot controller.	Computational Overhead, and Altitude Estimation
[98]	Man-in-the-middle Attack on Navigation Data of Drones	Simulation (using Ardupilot)	To analyze the drone flight path for detecting if it is fake or real. Also, to simulate the real-time behaviours of drones.	Precision, Recall Rate, and Overhead Time
[103]	Attacks on Integrity	Simulation (using Ethereum-based Test Network)	To evaluate the scheme's performance and dependencies in real-time.	Gas Price, Transaction Time, and Mining Time
[105]	Attacks on Availability (Physical attack)	Simulation (Algorithm modelled in CPAL)	To analyze the resilience to errors and faults that occur on the real runtime of the proposed algorithm.	Network Quality Ratio, Average Execution Time, and Latency
[106]	Attacks on Availability (Physical attack)	Experiment (Prototype)	To access the performance of the projectile intrusion detection module.	Detection Accuracy, and Computational Latency
[107]	Attacks on Availability	Testbed Experiment (using drones)	To perform attacks on a real drone for analyzing the effect of the denial of service and distributed denial of service attacks on the availability	Latency
[103]	Attacks on Authenticity	Simulation (using Ethereum-based Test Network)	To evaluate the scheme's performance and dependencies in real-time.	Gas Price, Transaction Time, and Mining Time
[108]	Attacks on Authenticity	Security Simulation (using AVISPA tool),	To measure the secrecy and mutual authenticity of the proposed authentication algorithm	Private Key Secrecy
[109]	Attacks on Authenticity	Security Simulation (using ProVerif tool)	To measure the secrecy of the proposed authentication algorithm	Ephemeral and private key secrecy
[110]	Attacks on Authenticity	Hardware Implementation (on two drone Processors)	To measure the performance and energy efficiency	Bandwidth, Memory Overhead, CPU Time, and CPU Cycle
[26]	Attacks on Authenticity	Security Simulation (using AVISPA tool), Simulation (using NS2)	To analyse the proposed authentication technique on a realistic IoD network	Throughput, and Packet Loss
[24]	Attacks on Confidentiality	Testbed Experiment (using Tmote Sky Sensor)	To evaluate the lightweight feature of the proposed technique	Computational and Communication costs
[30]	Attacks on Confidentiality	Security Simulation (using AVISPA tool),	To analyse the security strength of the proposed technique	The confidentiality of the exchanged messages
[114]	Attacks on Confidentiality	Real-time performance analysis through programmed modules	To validate the scalability and suitability of the proposed scheme under various conditions	Computational Time, Block Generation Time
[115]	Attacks on Privacy Preservation	Simulation	To evaluate the efficiency of the proposed scheme	Accuracy, Training Time, Test Time, Communication Overhead, and Latency of the Blockchain Consensus

i) PROVERIF TOOL

This is an automatic symbolic-based cryptographic protocol verification tool. The main advantage of the ProVerif tool is that it allows an unbounded number of parallel processing. Protocols are represented by Horn clauses in two types of input files that include Horn clauses and Pi-calculus [116].

ProVerif is used to verify secrecy, observational equivalence properties, and authentication for cryptographic security protocols.

ii) AVISPA TOOL

This tool allows the implementation and specification of internet security protocols using a high-level protocol specification language (HLPSL) [117]. Later, the HSPSL is translated into a form that can be used by the numerous tools embedded in the AVISPA for the security analysis process [122]. The advantage of the AVISPA tool is its capability to use numerous verification techniques on a single protocol specification.

iii) SYTHER TOOL

Syther tool works based on a pattern refinement algorithm that has the capability of generating concise representations of an infinite set of traces [118]. The advantages of a Syther tool is multifarious. Firstly, it provides a graphical user interface for easy protocol verification by the users. Secondly, it allows termination while at the same time provide the correctness of a protocol. Thirdly, it allows verification of both bounded and unbounded number of runs [122]. Fourthly, it allows multi-protocol analysis [118].

iv) ATHENA TOOL

This tool allows specification of security properties in a very simple and powerful logic which pave ways to efficient proof search algorithms [119]. The Athena tool is developed to solve the state space explosion problems suffered by most of the similar existing security protocol verification tools, such as the NRL tool. The state-space explosion problems hinder the analysis of complex security protocols [119]. The main advantage of the Athena tool is its capability of providing security proofs under arbitrary configurations that eliminate the state pace explosion problems.

v) NRL TOOL

The NRL tool uses a theorem proven approach for the analysis of security protocols. The tool is based on the Dolev-Yao threat model, and protocols are specified as a set of transitions of a state machine [127]. The tool initially starts from an insecure state and proceed to perform a backward search until it proves the unreachability of the insecure state [119]. The main advantage of the NRL tool is its ability to proving a protocol for quite several participants. Also, it uses symbolic variables that reduce symmetric redundancy [119]. However, the NRL tool requires human interaction and support that increases the running time as compared to other similar tools like the Athena tool.

vi) HERMES TOOL

This tool allows cryptographic protocols to be modelled as a set of transitions with terms constructed by applying pairing and encryption parameters [121]. In the Hermes tool, an attacker is modelled according to the Dolev-Yao threat model [121]. The tool is mainly used to verify the secrecy attributes of the cryptographic protocols. The advantages of using the Hermes tool is that there are no restrictions on the messages size, number of entities, or number of sessions. Besides, a proof tree is generated at the end of every proof of correctness of a protocol for certification purposes [121].

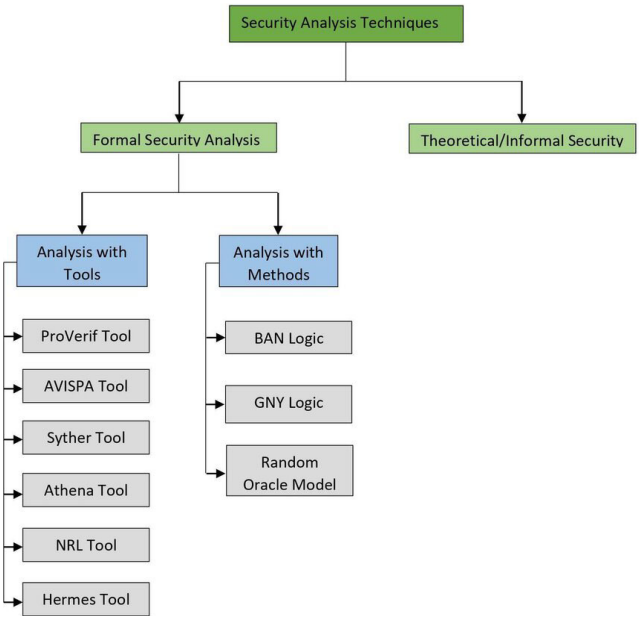

FIGURE 8. The classification of the security analysis techniques.

Moreover, a brief description of the formal methods is given below:

1) BAN LOGIC

A Burrows-Abadi-Needham (BAN) logic is a formal procedure for proving the security strength of protocols based on belief logics. BAN logic is used to prove the beliefs of trustworthy parties involved in authentication protocols [124]. It allows for prove of mutual authenticity and integrity of communication parties. To use BAN logic, basic notations, assumption, logical postulates, and goals need to be defined. Afterwards, rules are applied to the assumptions to achieve the stated goals. A proof of security protocol with BAN logic is a perfect proof of correctness. However, the logic does not exclude possible attacks in its semantics [123].

2) GNY LOGIC

Gong, Needham, and Yaholom (GNY) proposed an extended version of the BAN logic called the GNY logic [128]. The GNY logic uppers more advantages as compared to the BAN logic as it distinguishes between possession and beliefs, thus enabling reasoning at a lower level [128]. The GNY logic incorporates additional rules and concepts that allow more protocols to be verified. However, Mathuria A et al. [129] pointed out several loopholes of the GNY logic that include the presence of unsound rules, the possibility of generating

unsound conclusion by combining rules, the incompleteness of the set of rules, and the presence of rules with redundant properties.

3) RANDOM ORACLE MODEL

The random oracle model is proposed by Bellare and Rogaway [130]. The formal security analysis method gives thorough proof of the security of certain cryptographic protocols. The basic function of the model is modelling a Hash function by a random oracle. In a nutshell, the modelled Hash function serves as a black box for responding to a query for a bit string hash value by given a random value [125]. The random oracle model proves to be powerful in practice. However, it is not clear what happens when a random oracle is implemented even though a clear statement regarding the security of a protocol is made strong with the model [126].

IV. DISCUSSION AND FUTURE RESEARCH DIRECTIONS

Over the years, there have been significant efforts towards enhancing the Internet of Drones (IoD) network. However, as highlighted in the paper, the most significant development efforts have been limited to the IoD architecture. Thus, most researchers barely touched the architecture's security and privacy. Hence, in this paper, we propose a secured IoD architecture. This will ensure proper security and privacy of the IoD entities and the communicated data.

Additionally, as pointed out in this paper, various drones exist in the market. Thus, selecting one out of them for a particular application is quite difficult. To tackle this problem, many efforts toward the classification of drones have been made by many researchers. However, the level of security and privacy threats associated with the various categories of drones have been mostly missed. As such, we provided a comprehensive taxonomy of drones with the relative level of security and privacy corresponding to each category. It can be observed that the sizes of drones significantly affects the level of security and privacy. Smaller drones are not fully secured because it is often difficult to add security and privacy mechanisms to them compared to the bigger drones with more computing power. Moreover, we thoroughly investigate and classify attacks that can be launched on the IoD networks. It can be observed that the most devastating category of the attack on the IoD network is the localization error attack since position estimation is essential in IoD networks. Apart from the IoD network attacks, the physical threats that affect the IoD network entities' safety are also highlighted in this paper. Proper mitigation of these physical threats will ensure the accomplishment of a robust IoD paradigm.

Various techniques and mechanisms developed by various researchers for mitigating the attacks on the IoD network have been investigated in this paper. The performance evaluation methods and the metrics employed by the techniques are also stated. It has been noted that the existing techniques proposed for mitigating attacks on authenticity requirements are either not suitable due to the high computation and communication costs or provide an inadequate level of security. Thus, there is a need for a proper balance between these two often conflicting requirements.

Before achieving the IoD paradigm's successful functionality, several open issues need to be addressed. This will pave the ways for future researchers to investigate more on the IoD network. The significant open challenges are as follows:

A. CONSIDERING SECURITY AND PRIVACY SINCE FROM THE DESIGN STAGE

Security and privacy should be taken as key components when developing any hardware or application to be deployed to the internet of drones (IoD) network. Moreover, when designing IoD architecture, incorporating security and privacy mechanisms is the best practice for eliminating attacks. Besides, forensic requirements should be incorporated into the design of the IoD systems. The idea of forensic-by-design [131] should be added in the IoD network design as recommended to other cyber-physical networks and systems. Forensic mechanisms are capable of tracing and reconstructing an attack event.

B. EFFICIENT INTRUSION AND ATTACK DETECTION TECHNIQUES

Strong and intelligent intrusion and attack detection schemes are needed for deployment to the IoD network. With the advancement in technology, a newer version of instruction and attacks strategies are been applied on the IoD network. Therefore, researchers can utilize this opportunity to design more intelligent and sophisticated intrusion/attack detection and prevention solutions to mitigate this crucial challenge.

C. SECURE DATA AGGREGATION

Drones gather a lot of data in the IoD network. These data need to be secured and amassed into a single unit before transmission with the use of efficient data aggregation schemes. The aggregation of data before the transmission will also reduce energy and communication cost which is highly required for the resource containing the IoD network. Encryption techniques can be used to aggregate several ciphertexts into a single unit. It is recommended that an aggregation scheme for the IoD network deployment should simultaneously provide confidentiality and access control of data in addition to the aggregation capability.

D. ARTIFICIAL INTELLIGENCE BASED SECURITY AND PRIVACY MITIGATION TECHNIQUES

Several new sophisticated attacks are now deployed to the IoD network. Therefore, there is a need for Artificial Intelligence (AI) based on mitigating mechanisms. Employing an artificial neural network, deep learning, and machine learning algorithms to optimize security and privacy on the IoD network will show prominent advantages. However, there are great challenges in implementing artificial intelligence-based techniques. Moreover, the selection of an appropriate AI algorithm for particular security and privacy requirements on the IoD network still need further research exploration.

E. REAL-TIME ISOLATION MECHANISMS

To reduce the localization error, there is a need for a mechanism that will instantly isolate an IoD entity infected by security and privacy threats. This would serve as a fault isolation scheme and prevent an entire network collapse. Moreover, there is a need for a mechanism that will return a drone to its initial base station once the line-of-sight connection is lost.

F. LIGHTWEIGHT PROVEN SECURITY TECHNIQUES

Most of the existing schemes for curbing security and privacy attacks on the IoD networks either have security flaws or are not lightweight enough for deployment. Maintaining a trade-off between these two features is necessary and most important. Therefore, the design of lightweight, proven security techniques for IoD deployment is still a hot research area. To ensure this, Mobile edge computing (MEC) devices are added to the architecture. The MEC devices are mobile, supporting the flying drone's mobility features. Compared to drones, MEC devices have more computing power and memory capacity, thereby providing faster and efficient communication. Consequently, to reduce the computational and communication costs, the communicated messages are offloaded to the nearest authenticated MEC device for processing.

G. DETECT-AND-AVOID OBSTACLE SENSORS AND COLLISION AVOIDANCE TECHNOLOGY

IoD model's most catastrophic effect is the crashing of its drones entities on people and their properties, or even worst colliding with the flying aircraft. The challenge facing the existing IoD paradigm is the technology for reliable detection of the presence of obstacles in real-time that can be small enough for its deployment. When considering collision avoidance mechanisms, it is very important to understand the various types of IoD communication services [132].

H. ADVANCED COMPUTER VISION SOFTWARE

Instead of using an onboard surrounding analytical tool that increases weight and energy consumption to drones, advanced computer vision software for streaming the surrounding images and feeding them back to an object recognition server for feature analysis may be incorporated into the flying drones.

I. LIGHTWEIGHT LONG-LASTING BATTERIES OR SUFFICIENT POWER SOURCES FOR THE CIVILIAN DRONES

The embedded electronic components in civilian drones are becoming smaller and lighter due to technological advancement. However, power is still lagging. The latest civilian drone batteries last for only 30 minutes. For the proper operation of these drones, lightweight and longer-lasting batteries need to be developed. Moreover, other power sources such as fuel cells, lightweight gasoline-power generators for charging the onboard batteries, and solar power need to be developed.

V. CONCLUSION

Advancement in IoT has brought improvement in the functionality and applicability of the Internet of Drones (IoD). The IoD networks are equipped with advanced technological mechanisms. These mechanisms can collaborate with drones to make them more robust. A thorough study of secured IoD architecture, safety issues, and attacks are presented in this paper. Moreover, a new classification of drones and their different vulnerabilities were discussed. Finally, the research challenges of the IoD networks were provided.

NOMENCLATURE

AES:	Advanced Encryption Standard
AVISPA:	Automated Validation of Internet Security Protocols
CoAP:	Constrained application protocol
CR:	Control Room
CASA:	Australian Civil Aviation Safety Authorities
CPAL:	Cyber-Physical Action Language
DR:	Drone
DOS:	Denial of Service
DDOS:	Distributed Denial of Service
FANETs:	Flying Ad Hoc Networks
FAA:	Federal Aviation Administration
FDI:	False/fake Data Injection
GPS:	Global Positioning System
GNSS:	Global Navigational Satellite System
GCSs:	Ground Control Signals
GSS:	Ground Station Server
GCS:	Ground Control Station
HTTP:	hypertext transfer protocol
HTTPS:	hypertext transfer protocol Secure
HALE:	High Altitude Long Endurance
HTOL:	Horizontal Take-Off and Landing
IoD:	Internet of Drones
IoT:	Internet of Things
ISTAR:	Intelligence, Surveillance, Target, Acquisition, and Reconnaissance
IMU:	Inertial Measurement Unit
KF:	Kalman-Filter
LTE:	Long Term Evolution
LIDAR:	Light Detection and Ranging
LiPo:	Lithium Polymer
LiHV:	Lithium Polymer High Voltage
LALE:	Low Altitude Long Endurance
MQTT:	MQ Telemetry Transport
MANETs:	Mobile Ad Hoc Networks
MEC:	Mobile Edge Computing
MIT:	Massachusetts Institute of Technology
MAVs:	Micro Air Vehicles
MALE:	Medium Altitude Long Endurance
MUAV:	Mini UAV
MAV:	Micro UAV
MATLAB:	Matrix Laboratory
NAVs:	Nano-Air Vehicles

NS2:	Network Simulator 2
ONE:	Opportunistic Network Environment
PKI:	Public Key Infrastructure
ProVerif:	Protocol Verifier
RIS:	Robotics and Imaging Sensing
SARs:	Synthetic Aperture Radars
TCP:	Transmission Control Protocol
TUAV:	Tactical UAV
UAV:	Unmanned Aerial Vehicle
UAS:	Unmanned Aircraft System
UUV:	Unmanned Under-Water Vehicle
UDP:	User Datagram Protocol
VANETs:	Vehicular Ad Hoc Networks
VTOL:	Vertical Take-Off and Landing
WiFi:	Wireless Fidelity

ACKNOWLEDGMENT

The authors would like to thank the reviewers for their positive observations, comments, and suggestions to enhance the article contents. They also thank Mohammed G. Ragab and MM Proofreading and Editing Services LTD for the English editing of the manuscript.

REFERENCES

[1] J.-H. Kang, K.-J. Park, and H. Kim, "Analysis of localization for drone-fleet," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2015, pp. 533–538.

[2] E. Mitka and S. G. Mouroutsos, "Classification of drones," *Amer. J. Eng. Res.*, vol. 6, pp. 36–41, Jul. 2017.

[3] H. González-Jorge, J. Martínez-Sánchez, M. Bueno, and A. P. Arias, "Unmanned aerial systems for civil applications: A review," *Drones*, vol. 1, no. 1, p. 2, Jul. 2017.

[4] M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of drones," *IEEE Access*, vol. 4, pp. 1148–1162, 2016, doi: 10.1109/ACCESS.2016.2537208.

[5] G. Choudhary, V. Sharma, T. Gupta, J. Kim, and I. You, "Internet of drones (IoD): Threats, vulnerability, and security perspectives," 2018, *arXiv:1808.00203*. [Online]. Available: http://arxiv.org/abs/1808.00203

[6] S. Times. *Food Delivery Via Drones in Cyberjaya by End of the Month*. Accessed: Apr. 4, 2020. [Online]. Available: https://www.nst.com.my/lifestyle/bots/2019/06/497157/food-delivery-drones-cyberjaya-end-month

[7] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling drones in the Internet of Things with decentralized blockchain-based security," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6406–6415, Apr. 2021, doi: 10.1109/JIOT.2020.3015382.

[8] A. D. Boursianis, M. S. Papadopoulou, P. Diamantoulakis, A. Liopa-Tsakalidi, P. Barouchas, G. Salahas, G. Karagiannidis, S. Wan, and S. K. Goudos, "Internet of Things (IoT) and agricultural unmanned aerial vehicles (UAVs) in smart farming: A comprehensive review," *Internet Things*, Mar. 2020, Art. no. 100187, doi: 10.1016/j.iot.2020.100187.

[9] S. Magistretti and C. Dell'Era, "Unveiling opportunities afforded by emerging technologies: Evidences from the drone industry," *Technol. Anal. Strategic Manage.*, vol. 31, no. 5, pp. 606–623, May 2019, doi: 10.1080/09537325.2018.1538497.

[10] D. Paddeu, T. Calvert, B. Clark, and G. Parkhurst, "New technology and automation in freight transport and handling systems," Univ. West England, Bristol, U.K., Survey, 2019.

[11] E. Vattapparamban, I. Guvenc, A. I. Yurekli, K. Akkaya, and S. Uluagac, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Sep. 2016, pp. 216–221.

[12] M. Półka, S. Ptak, and Ł. Kuziora, "The use of UAV's for search and rescue operations," *Procedia Eng.*, vol. 192, pp. 748–752, 2017, doi: 10.1016/j.proeng.2017.06.129.

[13] V. Kharchenko and V. Torianyk, "Cybersecurity of the Internet of drones: Vulnerabilities analysis and IMECA based assessment," in *Proc. IEEE 9th Int. Conf. Dependable Syst., Services Technol. (DESSERT)*, May 2018, pp. 364–369.

[14] D. Kovar, "Cybersecurity and non-military UAVs (AKA drones)," *Integriography: J. Broken Locks, Ethics, Comput. Forensics*, to be published.

[15] F. Thiobane, "Cybersecurity and drones," Utica College, Utica, NY, USA, Tech. Rep., 2015.

[16] M. Rodrigues, J. Amaro, F. S. Osorio, and R. L. J. C. B. Kalinka, "Authentication methods for UAV communication," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2019, pp. 1210–1215.

[17] M. F. B. A. Rahman, "Smart CCTVS for secure cities: Potentials and challenges," Nanyang Technol. Univ., Singapore, Policy Rep., 2017.

[18] M. Mohan, "Cybersecurity in drones," Ph.D. dissertation, Fac. Utica College, Utica College, Utica, NY, USA, 2016.

[19] M. Yahuza, M. Y. I. B. Idris, A. W. B. A. Wahab, A. T. S. Ho, S. Khan, S. N. B. Musa, and A. Z. B. Taha, "Systematic review on security and privacy requirements in edge computing: State of the art and future research opportunities," *IEEE Access*, vol. 8, pp. 76541–76567, 2020, doi: 10.1109/ACCESS.2020.2989456.

[20] V. Chang, P. Chundury, and M. Chetty, "Spiders in the sky: User perceptions of drones, privacy, and security," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, May 2017, pp. 6765–6776, doi: 10.1145/3025453.3025632.

[21] M. Wazid, A. K. Das, and J.-H. Lee, "Authentication protocols for the Internet of drones: Taxonomy, analysis and future directions," *J. Ambient Intell. Humanized Comput.*, pp. 1–10, Aug. 2018.

[22] G. S. Ilgi and Y. K. Ever, "Critical analysis of security and privacy challenges for the Internet of drones: A survey," in *Drones Smart-Cities*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 207–214.

[23] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100218, doi: 10.1016/j.iot.2020.100218.

[24] C. Lin, D. He, N. Kumar, K.-K.-R. Choo, A. Vinel, and X. Huang, "Security and privacy for the Internet of drones: Challenges and solutions," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 64–69, Jan. 2018.

[25] M. Leccadito, T. Bakker, R. Klenke, and C. Elks, "A survey on securing UAS cyber physical systems," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 33, no. 10, pp. 22–32, Oct. 2018, doi: 10.1109/MAES.2018.160145.

[26] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of drones deployment," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3572–3584, Apr. 2019, doi: 10.1109/JIOT.2018.2888821.

[27] J. Yao and N. Ansari, "QoS-aware power control in Internet of drones for data collection service," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6649–6656, Jul. 2019, doi: 10.1109/TVT.2019.2915270.

[28] S. Aggarwal, M. Shojafar, N. Kumar, and M. Conti, "A new secure data dissemination model in Internet of drones," in *Proc. ICC - IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[29] B. Qureshi, A. Koubâa, M.-F. Sriti, Y. Javed, and M. Alajlan, "Dronemap-a cloud-based architecture for the Internet-of-Drones," in *Proc. Int. Conf. Embedded Wireless Syst. Netw.*, 2016, pp. 1–2.

[30] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of drones deployment," *Comput. Commun.*, vol. 153, pp. 229–249, Mar. 2020, doi: 10.1016/j.comcom.2020.02.011.

[31] P. Zhang, C. Wang, Z. Qin, and H. Cao, "A multidomain virtual network embedding algorithm based on multiobjective optimization for Internet of Drones architecture in industry 4.0," *Software: Pract. Exper.*, pp. 1–19, Mar. 2020, doi: 10.1002/spe.2815.

[32] J. Wang, C. Jiang, Z. Han, Y. Ren, R. G. Maunder, and L. Hanzo, "Taking drones to the next level: Cooperative distributed unmanned-aerial-vehicular networks for small and mini drones," *IEEE Veh. Technol. Mag.*, vol. 12, no. 3, pp. 73–82, Sep. 2017, doi: 10.1109/MVT.2016.2645481.

[33] Y.-J. Chen and L.-C. Wang, "Privacy protection for Internet of drones: A network coding approach," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1719–1730, Apr. 2019, doi: 10.1109/JIOT.2018.2875065.

[34] V. Chamola, P. Kotesh, A. Agarwal, Naren, N. Gupta, and M. Guizani, "A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques," *Ad Hoc Netw.*, vol. 111, Feb. 2021, Art. no. 102324, doi: 10.1016/j.adhoc.2020.102324.

[35] N. Hossein Motlagh, T. Taleb, and O. Arouk, "Low-altitude unmanned aerial vehicles-based Internet of Things services: Comprehensive survey and future perspectives," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 899–922, Dec. 2016, doi: 10.1109/JIOT.2016.2612119.

[36] L. Yang, H. Yao, J. Wang, C. Jiang, A. Benslimane, and Y. Liu, "Multi-UAV-enabled load-balance mobile-edge computing for IoT networks," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6898–6908, Aug. 2020, doi: 10.1109/JIOT.2020.2971645.

[37] J. Wang, C. Jiang, Z. Wei, C. Pan, H. Zhang, and Y. Ren, "Joint UAV hovering altitude and power control for Space-Air-Ground IoT networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1741–1753, Apr. 2019, doi: 10.1109/JIOT.2018.2875493.

[38] M. Saleh, N. Jhanjhi, A. Abdullah, and Fatima-tuz-Zahra, "Proposing a privacy protection model in case of civilian drone," in *Proc. 22nd Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2020, pp. 596–602.

[39] A. Kumar and B. Muhammad, "On how Internet of drones is going to revolutionise the technology application and business paradigms," in *Proc. 21st Int. Symp. Wireless Pers. Multimedia Commun. (WPMC)*, Nov. 2018, pp. 405–410.

[40] A. D. Craze. *The Future of Drone Technology*. Accessed: Aug. 7, 2020. [Online]. Available: https://airdronecraze.com/drone-tech/

[41] D. Floreano and R. J. Wood, "Science, technology and the future of small autonomous drones," *Nature*, vol. 521, no. 7553, pp. 460–466, May 2015, doi: 10.1038/nature14542.

[42] Y. Tian, J. Yuan, and H. Song, "Efficient privacy-preserving authentication framework for edge-assisted Internet of drones," *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102354, doi: 10.1016/j.jisa.2019.06.010.

[43] B. Song, G. Qi, and L. Xu, "A survey of three-dimensional flight path planning for unmanned aerial vehicle," in *Proc. Chin. Control Decis. Conf. (CCDC)*, Jun. 2019, pp. 5010–5015.

[44] A. C. Watts, V. G. Ambrosia, and E. A. Hinkley, "Unmanned aircraft systems in remote sensing and scientific research: Classification and considerations of use," *Remote Sens.*, vol. 4, no. 6, pp. 1671–1692, Jun. 2012, doi: 10.3390/rs4061671.

[45] L. Brooke-Holland, "Unmanned aerial vehicles (drones): An introduction," U.K. House Commons Library Rep., Standard Note SN06493, Apr. 2013.

[46] S. G. Gupta, D. Ghonge, and P. M. Jawandhiya, "Review of unmanned aircraft system (UAS)," *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 2, no. 4, pp. 1646–1658, 2013.

[47] A. Cavoukian, "Privacy and drones: Unmanned aerial vehicles," Inf. Privacy Commissioner Ontario, Toronto, ON, Canada, pp. 1–30.

[48] R. Weibel and R. J. Hansman, "Safety considerations for operation of different classes of UAVs in the NAS," in *Proc. AIAA 3rd 'Unmanned Unlimited' Tech. Conf., Workshop Exhibit*, Sep. 2004, p. 6244.

[49] M. Hassanalian and A. Abdelkefi, "Classifications, applications, and design challenges of drones: A review," *Prog. Aerosp. Sci.*, vol. 91, pp. 99–131, May 2017, doi: 10.1016/j.paerosci.2017.04.003.

[50] A. Tahir, J. Böling, M.-H. Haghbayan, H. T. Toivonen, and J. Plosila, "Swarms of unmanned aerial vehicles—A survey," *J. Ind. Inf. Integr.*, vol. 16, Dec. 2019, Art. no. 100106, doi: 10.1016/j.jii.2019.100106.

[51] N. Homainejad and C. Rizos, "Application of multiple categories of unmanned aircraft systems (UAS) in different airspaces for bushfire monitoring and response," *ISPRS-Int. Arch. Photogramm., Remote Sens. Spatial Inf. Sci.*, vol. 40, pp. 55–60, Aug. 2015, doi: 10.5194/isprsarchives-XL-1-W4-55-2015.

[52] *Unmanned Aircraft System Operations in UK Airspace-Guidance*, Civil Aviation Authority (CAA), London, U.K., 2010, vol. 6.

[53] A. Arjomandi, S. Agostino, M. Mammone, M. Nelson, and T. Zhou, "Classification of unmanned aerial vehicle," Rep. Mech. Eng. Class, Univ. Adelaide, Adelaide, SA, Australia, 2006, pp. 1–48.

[54] D. Rassler, "Remotely piloted innovation: Terrorism, drones and supportive technology," Combating Terrorism Center, United States Mil. Acad., West Point, NY, USA, Oct. 2016, p. 77.

[55] E. Mitka and S. G. Mouroutsos, "Classification of Drones," *Amer. J. Eng. Res*, vol. 6, pp. 36–41, Jul. 2017.

[56] J. Euchi, "Do drones have a realistic place in a pandemic fight for delivering medical supplies in healthcare systems problems," *Chin. J. Aeronaut*, pp. 1–9, Jun. 2020, doi: 10.1016/j.cja.2020.06.006.

[57] E. Dahlman and K. Lagrelius, "A game of drones: Cyber security in UAVs," Dept. Elect. Eng. Comput. Sci., KTH Roy. Inst. Technol., Sweden, 2019.

[58] H. Bergkvist and A. Bjälemark, "Quadcopter control using android-based sensing," M.S. thesis, Dept. Autom. Control, Lund Univ., Lund, Sweden 2013.

[59] J. Zhu, J. Zhu, and C. Xu, "A testbed for aerial robots formation flight," in *Proc. IEEE Int. Conf. Inf. Autom. (ICIA)*, Aug. 2016, pp. 1183–1188.

[60] S. Swierczynski and A. Felski, "Determination of the position using receivers installed in UAV," in *Proc. Eur. Navigat. Conf. (ENC)*, Apr. 2019, pp. 1–4.

[61] A. Guillen-Perez, R. Sanchez-Iborra, M.-D. Cano, J. C. Sanchez-Aarnoutse, and J. Garcia-Haro, "WiFi networks on Drones," in *Proc. ITU Kaleidoscope: ICTs Sustain. World (ITU WT)*, Nov. 2016, pp. 1–8.

[62] N. A. Idris and M. N. Kassim, "Wireless local area network (LAN) security guideline," Cyber Secur. Malaysia, Kuala Lumpur, Malaysia, 2010. [Online]. Available: https://html.scirp.org/file/1-4000110x9.png

[63] Z. Belghazi, N. Benamar, A. Addaim, and C. A. Kerrache, "Secure WiFi-direct using key exchange for IoT device-to-device communications in a smart environment," *Future Internet*, vol. 11, no. 12, p. 251, Dec. 2019, doi: 10.3390/fi11120251.

[64] J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," in *Proc. 33rd Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Nov. 2007, pp. 46–51.

[65] S. Min and H. Nam, "A formation flight control of UAVs using ZigBee," in *Proc. 13th Int. Conf. Ubiquitous Robots Ambient Intell. (URAI)*, Aug. 2016, pp. 163–165.

[66] T. Kennedy and R. Hunt, "A review of WPAN security: Attacks and prevention," in *Proc. Int. Conf. Mobile Technol., Appl., Syst. (Mobility)*, 2008, pp. 1–8, doi: 10.1145/1506270.1506342.

[67] S. Hayat, C. Bettstetter, A. Fakhreddine, R. Muzaffar, and D. Emini, "An experimental evaluation of LTE–A throughput for drones," in *Proc. 5th Workshop Micro Aerial Vehicle Netw., Syst., Appl. (DroNet)*, 2019, pp. 3–8, doi: 10.1145/3325421.3329765.

[68] K. Vachhani, "Security threats against LTE networks: A survey," in *Proc. Int. Symp. Secur. Comput. Commun.* Singapore: Springer, 2018, pp. 242–256, doi: 10.1007/978-981-13-5826-5_18.

[69] S. Morton, R. D'Sa, and N. Papanikolopoulos, "Solar powered UAV: Design and experiments," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst. (IROS)*, Sep. 2015, pp. 2460–2466, doi: 10.1109/IROS.2015.7353711.

[70] H. Ghassan, M. Omar, K. Soliman, I. Alhouti, M. Al-Shabi, and M. E. H. Assad, "Hybrid Drone powered by combined gasoline and electric motors," *Proc. SPIE*, vol. 11425, Apr. 2020, Art. no. 114250W, doi: 10.1117/12.2566117.

[71] A. Almulhem, "Threat modeling of a multi-UAV system," *Transp. Res. A: Policy Pract.*, vol. 142, pp. 290–295, Dec. 2020, doi: 10.1016/j.tra.2020.11.004.

[72] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[73] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2002, pp. 337–351.

[74] B. Potteiger, G. Martins, and X. Koutsoukos, "Software and attack centric integrated threat modeling for quantitative risk assessment," in *Proc. Symp. Bootcamp Sci. Secur.*, Apr. 2016, pp. 99–108, doi: 10.1145/2898375.2898390.

[75] B. Schneier, "Attack trees," *Dr. Dobb's J.*, vol. 24, no. 12, pp. 21–29, 1999.

[76] N. Shevchenko, T. A. Chick, P. O'Riordan, T. P. Scanlon, and C. Woody, "Threat modeling: A summary of available methods," Softw. Eng. Inst., Carnegie Mellon Univ., Pittsburgh, PA, USA, 2018.

[77] M. Yahuza, M. Y. I. Idris, A. W. A. Wahab, T. Nandy, I. B. Ahmedy, and R. Ramli, "An edge assisted secure lightweight authentication technique for safe communication on the Internet of drones network," *IEEE Access*, vol. 9, pp. 31420–31440, 2021, doi: 10.1109/ACCESS.2021.3060420.

[78] C.-L. Chen, Y.-Y. Deng, W. Weng, C.-H. Chen, Y.-J. Chiu, and C.-M. Wu, "A traceable and privacy-preserving authentication for UAV communication control system," *Electronics*, vol. 9, no. 1, p. 62, 2020, doi: 10.3390/electronics9010062.

[79] B. Bera, A. K. Das, and A. K. Sutrala, "Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of drones environment," *Comput. Commun.*, vol. 166, pp. 91–109, Jan. 2021, doi: 10.1016/j.comcom.2020.12.005.

[80] Y. Aydin, G. Karabulut Kurt, E. Ozdemir, and H. Yanikomeroglu, "Group handover for drone-mounted base stations," 2020, *arXiv:2012.09221*. [Online]. Available: http://arxiv.org/abs/2012.09221

[81] T. Nandy, M. Y. I. B. Idris, R. Md Noor, L. Mat Kiah, L. S. Lun, N. B. Annuar Juma'at, I. Ahmedy, N. Abdul Ghani, and S. Bhattacharyya, "Review on security of Internet of Things authentication mechanism," *IEEE Access*, vol. 7, pp. 151054–151089, 2019, doi: 10.1109/ACCESS.2019.2947723.

[82] T. Nandy, M. Y. I. B. Idris, R. M. Noor, I. Ahmedy, and S. Bhattacharyya, "An enhanced two-factor authentication protocol for V2 V communication in VANETs," in *Proc. 3rd Int. Conf. Inf. Sci. Syst.*, Mar. 2020, pp. 171–176, doi: 10.1145/3388176.3388185.

[83] T. Nandy, R. M. Noor, M. Yamani Idna Bin Idris, and S. Bhattacharyya, "T-BCIDS: Trust-based collaborative intrusion detection system for VANET," in *Proc. Nat. Conf. Emerg. Trends Sustain. Technol. Eng. Appl. (NCETSTEA)*, Feb. 2020, pp. 1–5, doi: 10.1109/NCETSTEA48365.2020.9119934.

[84] A. A. M. A. Abdelhafez, "Localization of cyber-physical systems: Privacy, security and efficiency," Ph.D. dissertation, Technische Univ. München, Munich, Germany.

[85] M. P. Arthur, "Detecting signal spoofing and jamming attacks in UAV networks using a lightweight IDS," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Aug. 2019, pp. 1–5.

[86] D. He, Y. Qiao, S. Chan, and N. Guizani, "Flight security and safety of drones in airborne fog computing systems," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 66–71, May 2018, doi: 10.1109/MCOM.2018.1700916.

[87] F. Al-Turjman, M. Abujubbeh, A. Malekloo, and L. Mostarda, "UAVs assessment in software-defined IoT networks: An overview," *Comput. Commun.*, vol. 150, pp. 519–536, Jan. 2020, doi: 10.1016/j.comcom.2019.12.004.

[88] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Trans. Cyber-Phys. Syst.*, vol. 1, no. 2, pp. 1–25, Feb. 2017, doi: 10.1145/3001836.

[89] K. Wesson and T. Humphreys, "Hacking drones," *Sci. Amer.*, vol. 309, no. 5, pp. 54–59, Oct. 2013.

[90] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 9, pp. 1594–1606, Sep. 2018, doi: 10.1109/TSMC.2017.2681698.

[91] B. Nassi, A. Shabtai, R. Masuoka, and Y. Elovici, "SoK–security and privacy in the age of drones: Threats, challenges, solution mechanisms, and scientific gaps," 2019, *arXiv:1903.05155*. [Online]. Available: http://arxiv.org/abs/1903.05155

[92] A. D. Wu, E. N. Johnson, M. Kaess, F. Dellaert, and G. Chowdhary, "Autonomous flight in GPS-denied environments using monocular vision and inertial sensors," *J. Aerosp. Inf. Syst.*, vol. 10, no. 4, pp. 172–186, Apr. 2013.

[93] Y. Zangvil, Y. Zur, and G. Cohen, "System and method for identifying global navigation satellite system spoofing attacks on a protected vehicle," U.S. Patent 10 830 897 B2, Nov. 10, 2018.

[94] W. Chen, Y. Dong, and Z. Duan, "Manipulating drone position control," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 1–9.

[95] D. He, S. Chan, and M. Guizani, "Drone-assisted public safety networks: The security aspect," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 218–223, Aug. 2017, doi: 10.1109/MCOM.2017.1600799CM.

[96] S. P. Arteaga, L. A. M. Hernandez, G. S. Perez, A. L. S. Orozco, and L. J. G. Villalba, "Analysis of the GPS spoofing vulnerability in the drone 3DR solo," *IEEE Access*, vol. 7, pp. 51782–51789, 2019, doi: 10.1109/ACCESS.2019.2911526.

[97] A. Koubâa, B. Qureshi, M.-F. Sriti, A. Allouch, Y. Javed, M. Alajlan, O. Cheikhrouhou, M. Khalgui, and E. Tovar, "Dronemap planner: A service-oriented cloud-based management system for the Internet-of-Drones," *Ad Hoc Netw.*, vol. 86, pp. 46–62, Apr. 2019, doi: 10.1016/j.adhoc.2018.09.013.

[98] M. Karimibiuki, M. Aibin, Y. Lai, R. Khan, R. Norfield, and A. Hunter, "Drones' face off: Authentication by machine learning in autonomous IoT systems," in *Proc. IEEE 10th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2019, pp. 0329–0333.

[99] S. Sciancalepore, O. A. Ibrahim, G. Oligeri, and R. Di Pietro, "PiNcH: An effective, efficient, and robust solution to drone detection via network traffic analysis," *Comput. Netw.*, vol. 168, Feb. 2020, Art. no. 107044, doi: 10.1016/j.comnet.2019.107044.

[100] P. Perazzo, K. Ariyapala, M. Conti, and G. Dini, "The verifier bee: A path planner for drone-based secure location verification," in *Proc. IEEE 16th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2015, pp. 1–9.

[101] W. Chen, Y. Dong, and Z. Duan, "Compromising flight paths of autopiloted drones," in *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, Jun. 2019, pp. 1316–1325.

[102] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, and K. Choi, "Rocking drones with intentional sound noise on gyroscopic sensors," in *Proc. 24th USENIX Secur. Symp. (USENIX Secur.)*, 2015, pp. 881–896.

[103] M. Singh, G. S. Aujla, R. S. Bali, S. Vashisht, A. Singh, and A. Jindal, "Blockchain-enabled secure communication for drone delivery: A case study in COVID-like scenarios," in *Proc. 2nd ACM MobiCom Workshop Drone Assist. Wireless Commun. 5G Beyond*, 2020, pp. 25–30, doi: 10.1145/3414045.3415937.

[104] N. Garg and N. Roy, "Acoustic sensing for detecting projectile attacks on small drones," in *Proc. 21st Int. Workshop Mobile Comput. Syst. Appl.*, New York, NY, USA, 2020, p. 1, doi: 10.1145/3376897.3379167.

[105] L. Ciarletta, L. Fejoz, A. Guenard, and N. Navet, "Development of a safe CPS component: The hybrid parachute, a remote termination add-on improving safety of UAS," in *Proc. 8th Eur. Congr. Embedded Real Time Softw. Syst.*, 2016, p. 10.

[106] N. Garg and N. Roy, "Enabling self-defense in small drones," in *Proc. 21st Int. Workshop Mobile Comput. Syst. Appl.*, Mar. 2020, pp. 15–20, doi: 10.1145/3376897.3377866.

[107] G. Vasconcelos, R. S. Miani, V. C. Guizilini, and J. R. Souza, "Evaluation of dos attacks on commercial Wi-Fi-based UAVs," *Int. J. Commun. Netw. Inf. Secur.*, vol. 11, no. 1, pp. 212–223, 2019.

[108] J. Srinivas, A. K. Das, N. Kumar, and J. J. Rodrigues, "Tcalas: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, Oct. 2019, doi: 10.1109/TVT.2019.2911672.

[109] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles," *IEEE Access*, vol. 8, pp. 43711–43724, 2020, doi: 10.1109/ACCESS.2020.2977817.

[110] M. Ozgur Ozmen, R. Behnia, and A. A. Yavuz, "IoD-crypt: A lightweight cryptographic framework for Internet of drones," 2019, *arXiv:1904.06829*. [Online]. Available: http://arxiv.org/abs/1904.06829

[111] D. F. Pigatto, J. Smith, K. R. Lucas, and J. C. Branco, "Sphere: A novel platform for increasing safety & security on unmanned systems," in *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, Jun. 2015, pp. 1059–1066.

[112] V. Dey, V. Pudi, A. Chattopadhyay, and Y. Elovici, "Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study," in *Proc. 31st Int. Conf. VLSI Design 17th Int. Conf. Embedded Syst. (VLSID)*, Jan. 2018, pp. 398–403, doi: 10.1109/VLSID.2018.97.

[113] R. Kolandaisamy, R. M. Noor, I. Kolandaisamy, I. Ahmedy, M. L. M. Kiah, M. E. M. Tamil, and T. Nandy, "A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET," *J. Ambient Intell. Humanized Comput.*, pp. 1–14, Jul. 2020, doi: 10.1007/s12652-020-02279-2.

[114] M. Singh, G. S. Aujla, and R. S. Bali, "A deep learning-based blockchain mechanism for secure Internet of drones environment," *IEEE Trans. Intell. Transp. Syst.*, early access, Jul. 7, 2020, doi: 10.1109/TITS.2020.2997469.

[115] M. A. Ferrag and L. Maglaras, "DeliveryCoin: An IDS and blockchain-based delivery framework for drone-delivered services," *Computers*, vol. 8, no. 3, p. 58, Aug. 2019, doi: 10.3390/computers8030058.

[116] B. Blanchet, "Automatic verification of security protocols in the symbolic model: The verifier proverif," in *Foundations of Security Analysis and Design VII*. Cham, Switzerland: Springer, 2013, pp. 54–87.

[117] Y. Glouche, T. Genet, O. Heen, and O. Courtay, "A security protocol animator tool for AVISPA," in *Proc. ARTIST2 Workshop Secur. Specification Verification Embedded Syst.*, 2006, pp. 1–7.

[118] C. J. Cremers, "The scyther tool: Verification, falsification, and analysis of security protocols," in *Proc. Int. Conf. Comput. Aided Verification*. Berlin, Germany: Springer, 2008, pp. 414–418.

[119] D. X. Song, S. Berezin, and A. Perrig, "Athena: A novel approach to efficient automatic security protocol analysis 1," *J. Comput. Secur.*, vol. 9, nos. 1–2, pp. 47–74, 2001.

[120] C. Meadows, "Language generation and verification in the NRL protocol analyzer," in *Proc. 9th IEEE Comput. Secur. Found. Workshop*, Mar. 1996, pp. 48–61.
[121] L. Bozga, Y. Lakhnech, and M. Périn, "HERMES: An automatic tool for verification of secrecy in security protocols," in *Proc. Int. Conf. Comput. Aided Verification*. Berlin, Germany: Springer, 2003, pp. 219–222.
[122] C. J. Cremers, P. Lafourcade, and P. Nadeau, "Comparing state spaces in automatic security protocol analysis," in *Formal to Practical Security*. Berlin, Germany: Springer, 2009, pp. 70–94.
[123] J. Wessels, "Application of BAN-logic," *CMG Finance BV*, vol. 19, pp. 1–23, Mar. 2001.
[124] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Roy. Soc. London. A. Math. Phys. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.
[125] N. Koblitz and A. J. Menezes, "The random oracle model: A twenty-year retrospective," *Des., Codes Cryptogr.*, vol. 77, no. 2, pp. 587–610, 2015.
[126] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited," *J. ACM*, vol. 51, no. 4, pp. 557–594, 2004.
[127] C. Meadows, "A model of computation for the NRL protocol analyzer," in *Proc. Comput. Secur. Found. Workshop VII*, Jun. 1994, pp. 84–89.
[128] L. Gong, R. M. Needham, and R. Yahalom, "Reasoning about belief in cryptographic protocols," in *Proc. IEEE Comput. Soc. Symp. Res. Secur. Privacy*, May 1990, pp. 234–248.
[129] A. Mathuria, R. Safani-Naini, and P. Nickolas, *Some Remarks on the Logic of Gong, Needham and Yahalom*. London, U.K.: Citeseer, 1994.
[130] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. 1st ACM Conf. Comput. Commun. Secur.*, 1993, pp. 62–73.
[131] N. H. Ab Rahman, W. B. Glisson, Y. Yang, and K.-K. R. Choo, "Forensic-by-design framework for cyber-physical cloud systems," *IEEE Cloud Comput.*, vol. 3, no. 1, pp. 50–59, Jan./Feb. 2016.
[132] A. H. Sawalmeh and N. S. Othman, "An overview of collision avoidance approaches and network architecture of unmanned aerial vehicles (UAVs)," *Int. J. Eng. Technol.*, vol. 7, nos. 4–35, pp. 924–934, 2018.

MUKTAR YAHUZA (Graduate Student Member, IEEE) received the B.Eng. degree in computer engineering from Bayero University Kano, Nigeria, in 2010, and the M.Sc. degree in computer information and engineering from International Islamic University Malaysia (IIUM), in 2015. He is currently pursuing the Ph.D. degree in computer science with the University of Malaya, Malaysia.

His research interests include information security, Internet of Drones security and privacy, lightweight authentication and privacy, and image processing.

MOHD YAMANI IDNA IDRIS (Member, IEEE) received the B.E., M.Sc., and Ph.D. degrees in electrical engineering from the University of Malaya, Kuala Lumpur Malaysia.

He is currently an Associate Professor and the Deputy Dean Research and Development, Faculty of Computer Science and Information Technology, University of Malaya. He is the author of a book and several articles in reputable journals. His research interests include information security, embedded systems (system on chip, FPGA), image processing and computer vision, digital forensics, surveillance systems, digital signal processing (speech processing, and bio-signals), and wireless sensor networks.

ISMAIL BIN AHMEDY (Member, IEEE) received the B.Sc. degree in computer science from the University of Technology Malaysia, the M.Sc. degree in computer science from the University of Queensland, Australia, and the Ph.D. degree from the University of Technology Malaysia.

He is currently a Senior Lecturer with the Department of Computer Systems, Faculty of Computer Science and Information Technology, University of Malaya, Malaysia. His current research interests include wireless sensor networks, Internet-of-Things, optimization algorithms, and mobile computing.

AINUDDIN WAHID ABDUL WAHAB received the B.Sc. and M.Sc. degrees in computer science from the University of Malaya, Kuala Lumpur Malaysia, and the Ph.D. degree in multimedia network from Surrey University, U.K.

He is currently an Associate Professor and the Deputy Dean (Undergraduate) with the Department of Computer Systems, Faculty of Computer Science and Information Technology, University of Malaya. He published several articles in reputable journals. His research interests include information security, network security, information hiding, digital forensics, steganography, and sensor networks. He is an Associate Editor of the *Journal of Information security and Applications* (JISA) (Elsevier).

TARAK NANDY (Member, IEEE) received the B.Tech. and M.Tech. degrees in computer science and engineering from the West Bengal University of Technology, India. He is currently pursuing the Ph.D. degree with the University of Malaya, Malaysia. He is also working as a Graduate Research Assistant in computer system and technology with the University of Malaya. His major interests include vehicular communication, the IoT, cyber-physical security, machine learning, authentication, and privacy.

NOORZAILY MOHAMED NOOR received the M.Sc. and Ph.D. degrees in computer science from the University of Malaya, Kuala Lumpur, Malaysia. He is currently an Associate Professor with the Department of Computer Systems, Faculty of Computer Science and Information Technology, University of Malaya. He is the author of many articles in reputable journals. His research interests include information security, arithmetic and logic structures, and detection and estimation.

ABUBAKAR BALA (Student Member, IEEE) received the bachelor's degree (Hons.) in computer engineering from Bayero University Kano, Nigeria, in 2011, and the master's degree in computer engineering from the King Fahd University of Petroleum and Minerals (KFUPM), Saudi Arabia, in 2015. He is currently pursuing the Ph.D. degree in electrical engineering with the Universiti Teknologi PETRONAS (UTP), Malaysia. He is also a Lecturer with Bayero University Kano (BUK). He is developing new algorithms to optimize the echo state network (ESN)—a recurrent neural network. His research interests include optimization, artificial neural networks, fault predictions, cloud computing, and renewable energy.