Scientific Research Publishing

Journal of Computer and Communications, 2025, 13(2), 250-281
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Weighted Voting Ensemble Model Integrated with IoT for Detecting Security Threats in Satellite Systems and Aerial Vehicles

Raed Alharthi

Department of Computer Science and Engineering, University of Hafr Al-Batin, Hafar Al-Batin, Saudi Arabia
Email: ralharthi@uhb.edu.sa

How to cite this paper: Alharthi, R. (2025) Weighted Voting Ensemble Model Integrated with IoT for Detecting Security Threats in Satellite Systems and Aerial Vehicles. *Journal of Computer and Communications*, **13**, 250-281.
https://doi.org/10.4236/jcc.2025.132016

Received: January 16, 2025
Accepted: February 25, 2025
Published: February 28, 2025

Abstract

Small-drone technology has opened a range of new applications for aerial transportation. These drones leverage the Internet of Things (IoT) to offer cross-location services for navigation. However, they are susceptible to security and privacy threats due to hardware and architectural issues. Although small drones hold promise for expansion in both civil and defense sectors, they have safety, security, and privacy threats. Addressing these challenges is crucial to maintaining the security and uninterrupted operations of these drones. In this regard, this study investigates security, and preservation concerning both the drones and Internet of Drones (IoD), emphasizing the significance of creating drone networks that are secure and can robustly withstand interceptions and intrusions. The proposed framework incorporates a weighted voting ensemble model comprising three convolutional neural network (CNN) models to enhance intrusion detection within the network. The employed CNNs are customized 1D models optimized to obtain better performance. The output from these CNNs is voted using a weighted criterion using a 0.4, 0.3, and 0.3 ratio for three CNNs, respectively. Experiments involve using multiple benchmark datasets, achieving an impressive accuracy of up to 99.89% on drone data. The proposed model shows promising results concerning precision, recall, and F1 as indicated by their obtained values of 99.92%, 99.98%, and 99.97%, respectively. Furthermore, cross-validation and performance comparison with existing works is also carried out. Findings indicate that the proposed approach offers a prospective solution for detecting security threats for aerial systems and satellite systems with high accuracy.

Keywords

Intrusion Detection, Cyber-Physical Systems, Drone Security, Weighted

Ensemble Voting, Unmanned Vehicles, Security Strategies

1. Introduction

The integration of the Internet of Things (IoT) with satellite systems and unmanned aerial vehicles (UAVs) has brought significant advancements in both civil and military applications. However, with this integration comes an increased risk of security and privacy threats [1]. As drones and IoT systems continue to evolve, they are becoming more susceptible to cyber-attacks, such as interception and unauthorized access, which pose challenges to the safety and privacy of these technologies [2]. Addressing these vulnerabilities is crucial for ensuring the resilience and security of IoT-embedded airborne systems and satellite networks. In response to these concerns, this study proposes a smart framework that utilizes a weighted ensemble of convolutional neural networks (CNNs) to enhance the detection and prevention of cyber threats [3]. By focusing on intrusion detection within IoT-based aerial systems, this framework achieves a high level of accuracy, up to 99.89%, making it a robust solution for mitigating cybersecurity risks in drone and satellite systems [4]. Recent years have shown significant progress in drone technology, leading to the emergence of compact drone models, such as quad-copters and mini-drones [5] [6]. These drones come with numerous benefits, notably their capacity to access and stay suspended within indoor spaces for monitoring and surveillance objectives. This capability finds practical applications across various sectors, *i.e.*, site surveillance for industries, reconnaissance, and various other civil and military purposes [7] including disaster management, emergency responses [8], marine logistics [9], and tech-oriented agriculture [10] [11]. The variants specific to commercial intents have promising prospects in domains including forecasts, area surveillance, and photography. In the last two decades, pervasive settings have witnessed a notable surge. This surge can be attributed to the increasing importance of pervasiveness and the intelligence embedded in objects within diverse environments, ranging from structures and urban areas to recreational spaces and commercial complexes. The integration of pervasiveness in these environments enhances the control, performance, and efficiency of various tasks by connecting numerous devices and sensors. Furthermore, it facilitates improved responsiveness to events and the provision of services.

UAVs or drones are autonomous air-borne devices, often utilized for various purposes like monitoring, data collection in hard-to-go areas, etc. [12]. Moreover, drones have made a substantial impact on various sectors, significantly influencing daily life, especially due to their widespread use in commercial applications. Drones capture and relay aerial images and pertinent data to central stations, facilitating well-informed decision-making in areas such as monitoring and surveillance [13]. Nevertheless, the extensive integration of drones into everyday life has brought about a multitude of consequences. It has raised concerns about the safety

and security of the general population, necessitating the development of regulations effectively dealing with liability and individual privacy concerns and that of the public [14]. Compact drones are on the rise in sectors, such as agriculture, logistics, and manufacturing, owing to their numerous benefits. However, the widespread adoption of drones brings with it significant concerns regarding privacy and security, necessitating careful attention [15]. To augment the intelligence of drones, scientists have been investigating the integration of miniature sensors that these devices can accommodate. The inclusion of transmitters, sensors, and cameras has the potential to augment the functionalities of drones, rendering them more versatile and efficient across a diverse spectrum of intricate applications.

The primary beneficiaries of drone utilization are the defense and civil sectors, where their applications have yielded significant advantages. However, the susceptibility of drones to both security and discretion threats arises from inadequacies within the design and architecture. While both the IoT and the Internet of Drones (IoD) introduce fresh possibilities, they also bring forth challenges in relevance to data security. To mitigate these concerns, fundamental alterations are essential in the architecture and design of drone devices. In previous works like [16], a layered architectural approach has been employed, composing drones with a distinct structure, equipped with a drone tier, a processing tier for the edge, a connectivity tier, a data processing tier, a repository tier, and finally a visualization tier. With the increasing adoption of drones across various industries, efficient scheduling of these UAVs has become critical for maximizing their potential in commercial and public sector applications. The comprehensive review by [17] focuses on addressing the intricacies of drone scheduling, particularly in contexts such as logistics, surveillance, and emergency response operations. The review systematically categorizes and evaluates existing methodologies used for solving drone scheduling problems (DSP), highlighting the distinct challenges posed by the dynamic and constrained nature of drone operations. One of the major contributions of this study is the identification of key factors influencing DSP, such as battery life limitations, airspace regulations, and the need for real-time adaptability. Additionally, the study emphasizes the importance of incorporating multi-objective optimization techniques and real-time data to improve scheduling accuracy and operational efficiency [17]. By providing a comprehensive assessment of current methods and suggesting future research directions, the review significantly advances the understanding of drone scheduling and proposes avenues for enhancing the scalability and performance of drone networks in intelligent transportation systems.

The rapid proliferation of IoT-enabled small drones and satellite systems has introduced significant security and privacy concerns. Despite their transformative potential in both civil and defense sectors, these systems remain vulnerable to various cyber-attacks due to their open architecture and design flaws. As drones become increasingly integrated into critical applications, such as surveillance, transport, and communication, ensuring the robustness of their networks against

malicious intrusions becomes paramount. Existing security mechanisms have shown limitations in mitigating these threats effectively, which underscores the need for novel, advanced cybersecurity frameworks [1] [3]. Like various IoT devices, drones are inclined towards unauthorized intrusion and unauthorized breaches. Hostile entities can exploit weaknesses in drone systems to breach data security and privacy. Moreover, the extensive data transmission and collection activities conducted by drones raise concerns about data security and potential misuse. To harness the capabilities of the IoDT, a resilient security framework is imperative. The primary focus of the proposed method revolves around a unified framework for both IoT and drone security. To ascertain the confidentiality and anonymity of intelligent drones, the respective study suggests incorporating blockchain technology. The proposed framework spans into seven layers unique in their functionality, comprising the edge processing as the first, strictly followed by a drone and a data retention layer, similarly, down the hierarchy we have a connection layer, an authorization layer, and two more layers for data processing and visualization. Beyond conventional drone functions, this layered methodology incorporates data protection and analytical methodologies. Enhanced security for drones is achieved through the utilization of deep Learning-based ensemble models.

The integration of IoT with drones and satellite systems has introduced significant advancements but also presents major cybersecurity challenges. Current security mechanisms are insufficient to counter evolving threats like interception and unauthorized access, leaving IoT-enabled airborne systems vulnerable. Moreover, the architectural design of existing drone and IoT systems suffers from open architecture and inadequate data protection, which heightens their susceptibility to cyber-attacks. Another gap in the literature is the lack of real-time, precise intrusion detection for UAV and satellite systems, especially in IoT-based networks. Current frameworks are not scalable or adaptable enough to handle the complexity and evolving nature of these systems, making them ineffective for dynamic cybersecurity needs.

The central objectives of the architecture proposed in this paper are:

- It explores the most recent advancements in terms of the inviolability, protection, and confidentiality of drones. It underscores the necessity for networks of drones that are well-shielded and unassailable from hacking or other unauthorized access.
- The proposed framework integrates a deep learning-based weighted ensemble within IoT drone structure to effectively mitigate cyber-security for risk alleviation, ultimately enhancing both the adaptability and security of the technology.
- The strategy put forth in this study outperforms earlier algorithms by attaining an accuracy of 99.89% on the drone dataset and up to 99.98% on alternative benchmark datasets. This showcases the efficiency of the proposed framework in bolstering the strength of satellite networks and IoT-embedded airborne

systems.

- A smart framework is introduced that serves as a pathway to enhance the security and durability of a diversity of systems, inclusive of cyber-physical, satellites, and IoT-propped airborne systems.

The rest of the paper is structured as follows. In Section 2, an examination of the prior research is conducted, specifically focusing on the identification of loopholes and weaknesses in systems and drones with IoT features. The review highlights the fact that only a scant number of studies explored drone confidentiality augmentation through the implementation of authentication methods. Section 3 elucidates the architecture and the framework designed as an ensuring measure of the reliability of drone systems. Access control and Authentication for drones are explored in Section 4. The proposed approach's evaluation metrics are discussed in Section 5, whereas Section 6 encompasses the results drawn from the study and gives directions for future research.

2. Related Works

The widespread applications of drones are found in military and defense contexts, with a diverse size range, spanning from a 200-foot military giant to a diminutive micro-drone with an inch-wide proportion. The drone size plays a pivotal role in determining its suitable utilization. Furthermore, the drone's flying range is subject to substantial variation based on its type, exemplified by some advanced military drones having the capacity to cover large distances worth 17,000 miles autonomously. The maximum flight duration is subject to fluctuation and relies on factors like altitude, terrain, or surface conditions. The machines are capable of operating at various altitudes, from marginal elevations to a soaring approx. 19.8km above ground [16]. The growing interest in securing IoT-based aerial and satellite systems has led to the development of numerous approaches to mitigate threats in these domains. Several recent studies have explored frameworks and methodologies aimed at detecting and addressing security vulnerabilities within such networks. [18] [19] proposed a multi-layer security framework for detecting cyber threats in IoT-enabled satellite systems. Their framework integrates machine learning (ML) models with intrusion detection systems (IDS) to detect anomalies and provide real-time alerts for potential threats. This work lays the groundwork for securing critical satellite infrastructure but lacks a comprehensive evaluation in terms of the adaptability of its models to aerial vehicle systems. [20] [21] introduced a blockchain-based security solution for UAV and satellite IoT systems, addressing data integrity, privacy, and secure communication between nodes. The study demonstrated enhanced protection against man-in-the-middle and data tampering attacks, focusing on distributed architectures. This solution significantly improves trustworthiness in UAV networks, although its integration with deep learning techniques for intrusion detection remains unexplored. [22] [23] developed a deep reinforcement learning-based approach to safeguard IoT-connected drones and satellites from cyberattacks. The model autonomously

adapts to dynamic security threats and optimizes security measures to ensure mission-critical data is not compromised. This approach is highly relevant to our study, as it emphasizes adaptability and real-time security. However, the lack of ensemble learning methods in their implementation limits their performance in complex network environments. [24] [25] focused on an AI-driven IDS that uses CNNs to detect threats in IoT and satellite communication systems. Their study achieved remarkable results, with an accuracy of over 99.5% on multiple drone datasets. Their contribution is aligned with the need for robust defense mechanisms in IoT networks, yet the model's reliance on a single detection algorithm may limit its effectiveness in diverse attack scenarios, compared to our proposed ensemble-based approach.

2.1. Perils to UAV Safety

The safety protocols for drones encompass a variety of layers and categories, contingent on their intended application, dimensions, and control methods. Generally, drones make use of a communication protocol [26] based on IEEE 802.11, as outlined in [27]. By incorporating both the ground stations and WiFi networks, drones lack encryption technologies, rendering them susceptible to intrusions and potential hijacking [7]. The man-in-the-middle (MITM)-based incursions, with an effective area range of up to 2 km, represent a prevalent method for compromising drones [28]. In the realm of military applications, the IoD has gained increasing prominence, introducing challenges related to privacy and security considerations in the design phase [29]. Safeguarding data requires addressing privacy concerns including data accessibility, information disclosure, and ciphering and deciphering techniques [30]. Recent investigations have categorized security threats into four distinct groups encompassing sensor threats, malign interference with signals, and jeopardized modules. A thorough overview of these categories can be found in **Table 1**.

Table 1 provides a literature overview primarily focusing on vulnerability detection in drones and scarce remedial discussions. One research avenue explored the implementation of encryption algorithms for a bidirectional secure data transmission of drones and their stations [29]. The popularity of miniature drones has grown due to their compactness, simultaneously eliciting potential concerns of threats to privacy [39]. Additionally, challenges related to drone security have been thrown light upon by valuable research [26] [40]-[43]. As an example, an effective model assessment proposed by Tian et al. for the IoD is supported by edge computing to enhance data security in drone networks [44]. Similarly, a robust system to secure drone data in both commercial and industrial settings has been proposed by [5]. In 2019, [6] proposed a novel concept that involved gas leakage-sensing drones to ensure timely responses in critical scenarios. Drones are predominantly employed for monitoring purposes in fields such as agriculture and security. In the past decade, security threats concerning drones have become a prominent topic in research circles. The privacy concerns in pertinence to smart

Table 1. Pervasive data anonymity and security challenges to smart-drones.

Type of attack	Security risks	Relevant literature	Remedial measures
Protocol	Communication Security	[27] [30]-[32]	[30]
	Data Confidentiality	[12]	
	Attack Replay	[33] [34]	[35]
	Data disclosure	[12] [32]	
	Deprovisioning attacks	[7] [27]	
Sensor	Spoofing & jamming of GPS	[15]	[36]
	Spoofing of motion sensors	[37]	[38]
	Spoofing or jamming of UAV's	[15]	
Component Hijacking	IoT Vulnerability	[15]	
	Interceptions	[15] [31]	
Jamming	DoS	[7] [15] [27]	
	Halted packet delivery	[29]	[29]

city-based applications are thoroughly addressed in [32], while **Table 1** sheds light on other crucial concerns. Researchers in the realm of cyber-security have shown particular interest in exploring network incursions on drones, with their possible limitations [45]. Commercial sectors are faced with similar challenges and opportunities, as demonstrated in related studies [8] [46] [47], leveraging blockchain and cryptographic technologies, combined with 5G and IoT-based drones, to ensure secure data transmission [47]. The current manual identification of threat intensity and nature has its limitations, emphasizing the pressing need for a secure and intelligent drone system capable of both investigating attacks and implementing measures to safeguard the integrity of drone data. Some studies endeavored to resolve authentication issues by effectively employing both the agreement [48] and key-enabled data [9] yielding a reliable propagation of drone data. The drones in the commercial sector [48] face a common challenge, which is the potential jeopardizing of drones, UAVs, and drones used in agriculture, facilitated by IoT whose effective solutions are weighted in [10] [11]. Similarly, other relevant reservations to UAVs pertain to tracking via GPS [49], necessitating impenetrable and trustworthy solutions. The interception and unauthorized access also feature prominently in studies [50].

2.2. Machine Learning-Based Drone Security Implementation

Many researchers have extensively applied ML models in various domains, including cloud-based computing, networks, and systems with IoT integrations [51]-[54], to combat cyber attacks. To illustrate this, [55] synergized self-learning models and supervised learning, utilizing a combination of long short-term memory (LSTM), auto-encoder and random forest (RF) classifiers to pinpoint

distributed denial of services (DDoS) attacks. Their approach yielded notable results, achieving accuracy up to 94% for scenarios involving varying traffic levels. The most promising outcomes were the results of their proposed LSTM-RF hybrid model, which employed a window size of 100.

Existing research did not exploit the unparalleled potential of ML models in drone networks for the identification of cyber attacks. Nevertheless, an alternative study recommended the probabilistic viewpoint within a circumscribed cyber-physical system for effective management and detection of actuation attacks [56]. The respective research predominantly focused on the PA2 attack, characterized by the interruption of communication between actuators and the controller. A collection of parallel detectors was introduced in this study, oriented around a hypothesis-testing methodology. For coping with uncertainties, certain objective functions were formulated tailored around detection and control, via a probabilistic take. Additionally, a security access control system was put forth for drones and previously applied ML techniques to enhance network anonymity (wi-net).

Existing studies signify the pressing requirement for a comprehensive resolution to confront threats related to cyber-security whilst ensuring the protection of data relayed through drones. While challenges and reservations pertinent to confidentiality have been put to light, only a limited number have put forth viable strategies to reduce these risks [47]. Though ML has displayed potential in identifying intrusive attempts at various networks, the gaps within the research persist within the network-based applications. Moreover, authentication systems presented in studies might not line up sufficiently for drone networks. Hence, bridging the rift is imperative to render drones compliant with industry and commercial standards, all the while upholding their security and safeguarding their privacy.

Securing drones mandates the adoption of an ingenious surveillance infrastructure that autonomously scrutinizes compromised data and executes context-specific corrective measures, all while eliminating the necessity for manual intervention. Although ML models have shown their mettle in fortifying mobile and sensor-based networks against cyber threats, their potential in fortifying drone-based vehicles remains a largely untrodden path. This study takes on the intricate challenge of redefining access control and authentication techniques for drones through the introduction of an innovative ML-driven approach.

3. UAV Design and Structure

The core objective of this study centers on fortifying the cybersecurity of IoT drone devices, with a distinctive emphasis on small drones, by elevating their fundamental architecture. The study's pursuits encompass not only mitigating privacy concerns and cyber-security vulnerabilities but also curbing the potential chaos of data interception while instilling robust security measures. To accomplish these ambitious aims, an innovative layered approach is set in motion, systematically scrutinizing analysis techniques and security challenges within each stratum. This approach results in an augmenting data security foundation for

traditional drone operations, with the added perk of adaptability for future enhancements. Moreover, the infusion of machine intelligence via advanced ML models functions as an added layer of defense, further safeguarding the integrity of the device. The proposed ML-based secure framework is depicted in Figure 1.

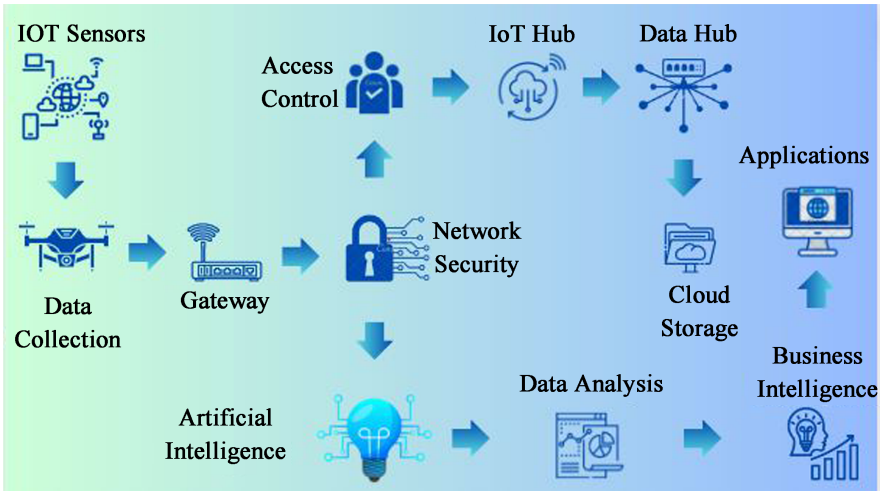

Figure 1. Layer-wise architecture of a smart security drone.

The emergence of small drones has ushered in new possibilities for both public and military applications. However, the lack of sophisticated design and structure makes these devices vulnerable to confidentiality risks. While developments in IoD and IoT offer promising opportunities, they also unveil additional challenges in terms of privacy. The current landscape falls short in ensuring credible security and relaying of data, rendering it less reliable.

3.1. Hierarchical Structure for Intelligently Secured Smart Drones

Existing blueprints for commonly employed smart [16], as delineated in Figure 1, adhere to a structural hierarchy. To bolster its confidentiality based attributes, an additional stage is incorporated, whereas certain modifications are introduced in the data-processing layer by replacing it with machine intelligence-embedded alternatives.

The data layer stands as a pioneering stage within the intricate framework of industrial drones, primarily because of housing a camera-toting miniature drone or nimble quadcopter. This stratum comes to life through an influx of IoT sensor data, where an ensemble of cutting-edge sensors, encompassing cameras, GPS, and radar, takes the helm. Their collective prowess empowers the drone to not only sense and seize data but also orchestrate their seamless transmission to the ensuing layer in the drone's data journey.

In the subsequent layer, a UAS drone takes on the pivotal roles of data acquisition and drone flight management. This UAS drone is equipped with a remote interaction module alongside a ground controller. A practical example of this design and architecture concept can be found in (DJIS Phantom-3 drones) originating

from (Shenzhen, China). Drones like these have a communication interface with a remote controller for controlled maneuvers. The architecture also accommodates the addition of auxiliary sensors as needed.

Unprocessed raw data is sourced from the IoT devices, via the intermediate edge processing drone layer (EPL) and relayed to the privacy layer (PL). PL plays a pivotal role in data authentication and monitoring transmission to the cloud layer (CL). For cloud communication, the Azure IoT gateway is utilized in conjunction with the IoT gateway.

The drone's confidentiality layer focuses on authenticating devices and controlling access using ML models. This layer is responsible for enforcing data safety and security, both integral components of the framework. Herein, the detection and mitigation of potential privacy threats take place, as they present a substantial risk to the system. Some examples of privacy threats that can manifest at this level include:

1) A physical incursion hazard signifying unsanctioned access or meddling with physical gadgets sensors or drone apparatus.

2) A user-centric behavioral privacy challenge is intricately entwined with the acquisition of personal data, achieved by meticulously observing and documenting user interactions.

3) An unsanctioned geospatial privacy encroachment, centering on the tracking or revelation of an individual's whereabouts against their wishes.

Addressing security vulnerabilities necessitates the utilization of a versatile array of authentication techniques and protocols malign actors if left unchecked can leverage an assortment of breaches to launch threats encompassing a diverse range of incursions that can yield havoc on transmissions, control, and functionality. Within the proposed framework deep learning-based algorithms come to the fore for device authentication with early detection of potentially unauthorized penetration. This equips users with the capability to receive timely alerts and adopt preemptive measures to intervene in the wake of these looming threats.

Within the connection layer, the IoT gateways play a pivotal role in establishing connections between the base stations and a cloud IoT hub. Enhanced security, orchestration, and automation are guaranteed by introducing an additional module, permitting connectivity exclusively for authenticated devices. This hub serves as a transmission channel, by effectively facilitating communication at both ends *i.e.*, cloud and network. Here, measures are implemented to grant network access solely to authenticated devices. Data from sensing devices originating off of networks and drones is securely transmitted to the client utilizing both robust cryptographic and blockchain technology, ensuring data integrity and safe-keeping.

For analysis, the data is routed to the processing layer, where novel modules are introduced inclusive of machine intelligence and hub services. Instead of relying on individual ML algorithms, it employs a weighted ensemble of CNN models, offering unparalleled adaptability across diverse scenarios and data prerequisites. The crux of this research lies in the application of an intelligent ML approach for

device authentication. It is the IoT hub layer's responsibility to authenticate devices by meticulously time-stamping data emanating from drones at predetermined intervals. These datasets, derived from drone flights, form the bedrock for model training and testing. The model undergoes rigorous training, followed by meticulous testing to assess its efficacy in detecting any ill-activity. If detected, the alerts are generated and the services are suspended with the cloud, for abrupt interventions.

A myriad of security threats loom over flight operations, and among these, interception attacks, where an external entity wrests power over the device, are frequent. Similar perils reside in the realm of unauthorized access, wherein malicious actors manipulate drones to disseminate misleading information, underscoring the multifaceted landscape of security risks in drone operations. Herein, a voting of CNN models is employed in fashion a model which is subsequently utilized for validating fresh aircraft trajectories. For effective evaluation against the metrics, the KDD-CUP 99 dataset was used.

In the drone data storage layer, analyzed data is methodically archived within data centers. This repository encompasses a range of results generated by drones, including drone-specific data extracted via sensors and network data in a cloud-based NoSQL database, which resides within the drone layer. Storage of this valuable data takes place.

NoSQL, signified for multi-faceted data storages, allows for quick and easy retrieval of data. Their proficiency in managing substantial volumes cast them as a preferred choice over conventional databases. Given their inherent automatic indexing, common data structures found in non-relational repositories encapsulate the graph-oriented key-value document-based and columnar formats.

The layer responsible for analyzing drone data brings forth an array of resources and utilities for proficient data observation. This platform harnesses MS Azure Services—the outcomes derived from the Data Visualization Language (DVL) are presented through a mobile application showcasing the forecasts generated by the intelligent model. Concerning a drone's security level (SL), the Naive Bayes model is skillfully utilized for the detection of drone attacks. The business intelligence structure by stream analytics (SA) disseminates results through the MS Power-BI application and is securely contained in dedicated centers.

3.2. Physical Components

The experiments utilized accessible, cost-effective peripherals. For sensing, an Arduino Mega 2560 microcontroller sourced from Somerville, USA, connected with a WiFi module ESP8266 was procured for processing.

Drone selection offers a plethora of size and shape choices, and their deployment depends largely on the use cases. In this particular experiment, the Phantom 3 Standard by DJI, took center stage. It was operated with a custom wireless controller, enabling remote functionalities such as tracking, locating, and identifying objects. These tasks were accomplished using radar sensors that use electromagnetic

energy transmission with the demonstration of the superior accuracy of radar sensors over optical ones. HC-SR04 proximity sensors are used in this paper as part of the experimentation. Because of the proficient pattern identification, this sensor offers a multifaceted approach to the task.

The GY-GPS6MV2, crafted by UBLOX, headquartered in Zurcherstrasse, Switzerland, is a GPS signal receiver featuring an onboard NEO-6M chip. It activates an LED indicator, powered by a battery when transmitting or receiving GPS data. Notably, this module showcases a remarkable sensitivity down to −161 dBm.

The sensor, BMP180 stands out in terms of energy efficiency delivering pinpoint accuracy in elevation measurements tailored to specific locations. Its exceptional precision defies its compact size and in terms of altitude and pressure sensors, this OEM module outshines its counterparts. The distinctive communication traits offered by ZigBee, notably the specific ability to transmit varying signal types contributed to its broad usage.

4. Drone Security

Establishing a solid system that can simultaneously protect drone integrity while analyzing attack data is necessary for UAV security measures. Because of the complexities of IoD, creating a reliable and safe system requires constant attention to important details like anonymity and reliability. Although ML has been used repeatedly in cybersecurity, its potential for drone-based security of this data has so far remained untapped. Thus, to strengthen access control and authentication procedures and improve the security of drones, a novel ML-driven solution is presented in this study.

The evaluation of the cybersecurity framework involves the use of various metrics that conveniently respond to a wide range of evaluation criteria. Hence, the following parameters are used to evaluate the performance of the systems [57]:

- Exposure of cyber-security threats.
- DDoS service denial attacks.
- Attacks of malicious nature.
- Jamming Attacks.
- Spoofing Attacks.

This study substantially improves reliable access control for devices by addressing the previously untapped areas within unmanned device security. By integrating with ML-based solutions, the intention is to transform them into effective tools for commercial and industrial monitoring. As previously discussed, the proposed system consists of seven layers dedicated to secure autonomy. Security protocols are implemented within (the security/privacy layer (SPL)) before being handed over to the device connection layer (DCL), guaranteeing safeguarding of information transference and control. In threat cases, a mobile alert is promptly dispatched.

The aim is to close the research gap, improve the safety and reliability of drones in the face of serious cyber-security threats and make them usable for commercial and industrial purposes.

4.1. Communication Security Threats

As technology develops, airborne systems such as UAVs continue to provide a wide range of advantages. But as other studies have noted, they also have several drawbacks and raise issues with safety, security, and privacy. To reduce these worries and control unauthorized aerial photography, laws and licensing procedures must be put in place. Globally, authorities have enforced strict regulations to tackle the problem of unapproved aerial photography.

When assessing network security and conducting risk analysis, it is important to recognize that UAVs have distinctive characteristics. Distinctions primarily arise from resource constraints and the broader coverage area inherent to UAVs, which necessitates a different approach to security and risk assessment, as highlighted in earlier research [58].

The set of regulations that govern drone operations within a specific area is commonly known as the authentication, authorization, and accounting (AAA) framework. This framework provides various benefits to drone operators on their administrative rights and enforces rigorous methods of authentication to avoid unauthorized access by unidentified entities. Tracking and identification of drones alongside the operators can also be carried out in situations of uncertainty and illegal activities, thereby reducing the likelihood of being stalked, breached, or intruded. In addressing these security concerns, several mechatronic engineering solutions have been put forward, as documented in prior research [59].

The market's immediate access to reasonably priced drones has raised apprehensions concerning their possible exploitation in illicit activities. Their capability to transport external payloads adds to the concern, as it allows them to transport hazardous chemicals or explosives without attracting undue attention [60]. Moreover, their capacity for accessing remote and difficult-to-reach places is a critical risk. Drone operations over heavily populated areas raise safety concerns because of the possibility of collisions or accidents that could result in tragic events. Several suggestions are made to improve public safety in response to these occurrences and worries:

- Implementing a fail-safe mechanism that permits drones to enter a hover mode in the event of hacking or unintended deviations from their prescribed flight path, allowing for the recovery of control.
- Creating drone filters with the capability to identify signal jammers, which might otherwise take control of the drones for malicious cyber-attacks.
- Resolving privacy issues linked to the use of UAV cameras by prohibiting unauthorized private-property recording. Before being hovered over private areas, consent must be obtained by both parties. This is something that Canadian Public Safety (CPS) has supported [61].

4.2. Implemented Methodology

A pragmatic methodology is proposed for improving drone's robustness to

attempted infiltration of their infrastructure, covering both the hardware and software components. Modern technologies are incorporated into the design of the suggested framework in an effort to reduce exclusivity concerns related to drone operations. To guarantee clarity and the capacity to repeat the findings, the attempted procedures and the dataset used for deep learning tasks are meticulously explained and documented.

A seven-layer-based architecture is presented for drone security. Transference of data takes place from edge processing (EP) to SPL, where the incursions are detected using the proposed ensemble scheme. After EP-based authentication of data, it is propagated to a cloud repo where MS Azure-based authentication procedures are practiced. A pre-trained model is implemented in MS Azure cloud storage, utilizing drone data combined with NSL-KDD, KDD CUP, and Edge-IoT datasets. This model is in charge of forecasting possible attacks, and it is this model that initiates a mobile alert upon detection of an attack.

4.2.1. Drone Parts

The following parts are used to build the smart secure drone: A wireless module, namely XBee Pro S1, has been used along with a GY-GPS6MV2 GPS module, HC-SR04 ultrasonic sensor, BMP180 barometric pressure sensor, and Mega 2560 microcontroller. These parts were purchased from Amazon. For central processing, the Mega-2560 micro-controller is used first for the initial jump start laced with adequate processing capacity and controlling prowess. It performs flight control algorithms, gathers sensor data, and establishes communication with other components [62]. In order to monitor flight duration and data, the Mega 2560 microcontroller additionally logs the current time. Obstacle avoidance and detection are handled by the HC-SR04 ultrasonic sensor. The drone can modify its flight path to prevent collisions by using the ultrasonic waves it emits, measuring its reflection time, and using this information to identify objects in the vicinity. Based on this data, it makes decisions about moving and changing its position.

An essential component of providing accurate positioning and navigation data is the GY-GPS6MV2 GPS module. It obtains the position ID of the UAV with its real-time coordinates by receiving signals from GPS satellites. Waypoint navigation, flight planning, and tracking all depend on this data. By measuring atmospheric pressure with the BMP180 barometric pressure sensor, the drone can estimate its altitude with a high degree of accuracy. To maintain stable flight and carry out tasks involving altitude changes, these altitude data are crucial. These parts and sensors improve the secure drone system's ability to avoid obstacles, navigate precisely, and control altitude. They are essential to its operation. The pressure applied to the drone is also detected by this sensor.

For reliable communication of an UAV with its parent station, an information exchange module for wireless transference of real-time data XBee Pro S1 is essential. Aiding remote control, real-time data monitoring, and transmission of ongoing operation status. These are the requisites for a smart, secure, and reliably operational drone, ensuring the system operates safely and effectively by combining

secure communication channels, dependable navigational capabilities, and advanced sensor functionalities.

4.2.2. Dataset

Real-time drone data, including KDD intrusion detection features[1,2], drone OBD data[3], and GPS-based attributes like longitude, latitude, and altitude, were used in this experiment for analysis[4]. Drone datasets are included within the provided link along with a few benchmarks related to intrusion detection and cyber-attack prediction[5].

For a detailed overview of the dataset classes, please refer to Table 2.

Table 2. Specifics of the dataset's classes.

Category	Type explanation
DDoS Attack	Authorized users are only permitted to use resources or services
Normal	Connections are created by mimicking user behavior.
UtR attacks	Unauthorized entities are able to access administrator account types.
Prob attack	Unauthorized parties have access to system information.
RtL attacks	Illegal entities are able to access hosts.

4.2.3. Weighted Ensemble Model

The weighted ensemble CNN voting model plays a pivotal role in elevating prediction accuracy and bolstering robustness. Figure 2 shows the architecture of the weighted voting ensemble [63].

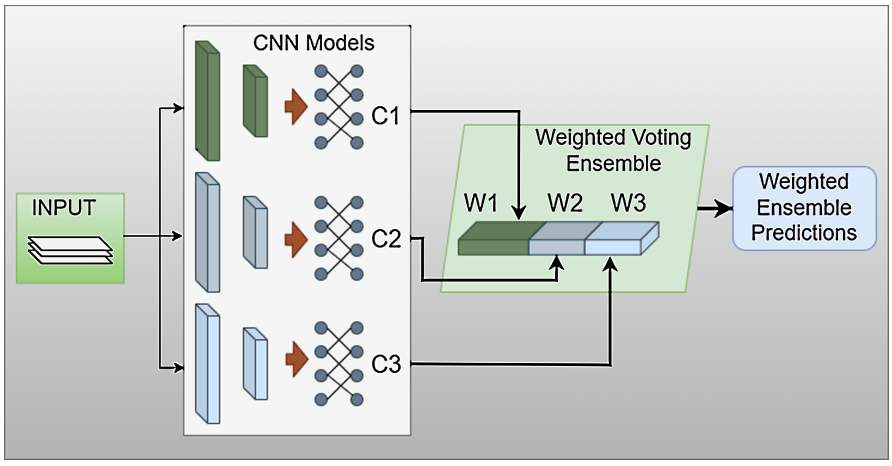

Figure 2. Weighted voting ensemble of CNNs.

[1]https://www.kaggle.com/datasets/hassan06/nslkdd

[2]https://www.cse.wustl.edu/jain/iiot2/index.html

[3]https://github.com/MUmerSabir/MDPIElectronics

[4]https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot

[5]https://ieee-dataport.org/documents/x-iiotid-connectivity-and-device-agnostic-intrusion-dataset-industrial-internet-things

Algorithm 1: Weighted Ensemble CNN for Network Attack Prediction

Input: Preprocessed dataset D (KDD, NSL-KDD, X-IoT, OBD Drone, Real-time Drone, WUSTL, EDge IIoT)
Output: Prediction results for network attack in aerial/satellite systems
Step 1: Data Preprocessing
- Normalize data, remove noise, handle missing values
- Split datasets into training and testing sets (70% training, 30% testing)
Step 2: Model Initialization
- Initialize three CNN models: CNN_1, CNN_2, CNN_3 with different architectures
- Define each CNN architecture with:
  – Convolution layers
  – Activation functions (ReLU)
  – Pooling layers
  – Dense layers and softmax output layer
Step 3: Model Training
for each CNN model CNN_i **do**
- Train CNN_i on the training dataset
- Use backpropagation with Adam optimizer to minimize cross-entropy loss
- Repeat until convergence (no improvement in validation loss or predefined epochs reached)
end for
Step 4: Weighted Voting Ensemble
- Combine predictions from CNN_1, CNN_2 and CNN_3 using weighted voting
- Assign weights w_1, w_2, w_3 to models based on validation accuracy:
  – $P_{\text{final}} = w_1 \cdot P(\text{CNN}_1) + w_2 \cdot P(\text{CNN}_2) + w_3 \cdot P(\text{CNN}_3)$
- The final prediction P_{final} is computed for each test instance
Step 5: Performance Evaluation
- Evaluate performance on the test dataset using the following metrics:
  – Accuracy, Precision, Recall, and F1
- Compare model results on all datasets (KDD, NSL-KDD, X-IoT, OBD Drone, Real-time Drone, WUSTL, EDge IIoT)
Step 7: Model Validation and Stability Check
- Validate the model on all datasets to verify stability and generalization
- Check the model's robustness against noise, unseen attack patterns, and dataset shifts
- Adjust the framework based on real-time performance and feedback

In drone security, where precision and dependability are of utmost importance, the adoption of ensemble learning techniques proves highly advantageous as they harness the strengths of multiple CNN models, each offering distinct advantages in capturing different facets of the data. This diversity not only enhances accuracy but also fortifies predictions against noise and outliers, as models sensitive to such factors can be assigned lower weights. Furthermore, these ensembles help balance biases within individual models, promote better generalization, mitigate over-fitting, and reduce prediction variance. Both the features of model selection and fine-tuning allow them to be powerful tools for modeling complex decision forming and changes in data patterns. In other words, weighted voting ensemble CNN models are a precious safeguard to strive for more accurate and reliable predictions in various fields. In this paper, we introduced the ensembling model known as the WV-CNN which comprises three 1D CNN models to ensure the highest

accuracy which boosts the strong decision-making by different models for the safety of the drones [64]. The algorithm of the proposed framework is given in Algorithm 1. The structure of each of the three CNN models that formed the contribution is shown below in Table 3.

Table 3. Architecture for the proposed weighted ensemble CNN models.

Layers	Filter	Neuron	Kernels	Dropouts	Activations
ECN-1					
Conv-1D	5	-	4	-	ReLU
Flattened	-	-	-	-	-
Dense		5	-	-	ReLU
Dense	-	Length (Classes)	-	-	Softmax
ECN-2					
Conv-1D	4		4	-	ReLU
Flattened	-		-	-	-
Dense Neurons	6		-	0.2	ReLU
Dense Neurons	-	Length (Classes)	-	-	Softmax
ECN-3					
Conv-1D	6		4	-	ReLU
Flattened	-		-	-	-
Dense Neurons	-	Length (Classes)	-	-	Softmax

Table 4. Parametric configuration for proposed ensemble models.

Optimizer	L.Rate	Beta1	Beta2	Epsilon	Decay	AMS-Grad	Ensemble Weight
ECN-1							
Adam	0.001	0.9	0.999	1.00E−07	0	FALSE	0.4
ECN-2							
Adam	0.001	0.9	0.999	1.00E−07	0	FALSE	0.3
ECN-3							
Adam	0.001	0.9	0.999	1.00E−07	0	FALSE	0.3

ECN-1 (Ensemble Convolutional Network 1): A 1D feature vector v of the dataset D is used to train a sequential convolution model known as ensemble convolution network 1 (ECN-1). The ECN-1 model used the 1-d convolution layer with 4 as the F_n filter number and 3 as the K_s kernel size that is shown in Table 4. For the layer activations, rectified linear unit (ReLU) activation was used for this convolutional layer and max pooling layer. The feature extraction layer is a dense layer with 6 neurons, followed by the last layer with neurons corresponding

to the length of the classes to be trained and the softmax nonlinearity function to obtain the probability distribution of the input label.

ECN-2 (Ensemble Convolutional Network 2): The feature vector v' is used to feed the second sequential convolution model, ECN-2, to get class probability values. The type of model architecture that is used, as indicated in Table 4, is a 1D Conv Layer where F_n is defined as 3 and K_s also equals 3. Next, there is the dense layer with eight neurons, the flatten layer to reshape feature vectors, drop-out layer with the value 0.3 to reduce the over-fitting of the model. The last layer is the dense layer with the same number of neurons as the classification classes.

ECN-3 (Ensemble Convolutional Network 3): In the same way as in the first two models, the input feature vector v' is transferred to the proposed sequential network to get the classification scores. As elaborated in Table 4, regarding the layered architecture of the model, a 1D Convolutional Layer has been applied which includes $F_n = 5$ and $K_s = 3$ with ReLU activation function. The next layers are flatten layers and the last dense layer corresponds to the number of predicted classes using a softmax classifier.

In the case of each of the models in the bag, their parametric setup is described next. For all models, Adam is used as optimizer because it is faster to compute and has fewer parameters as compared to other algorithms. Hence, the learning rate α is set as 0.001, β_1 (meaning momentum) and β_2 (scaling term for the gradients) are set to 0.9 and 0.999, respectively. Likewise, it is necessary to fix the epsilon value which is used to avoid division by zero, see Table 4.

Weighted Voting Convolutional Neural Network: The output probabilities of the three proposed models, that is ECN-1, ECN-2, and ECN-3 are used to get better prediction values in the framework of an ensemble voting system. These agreed-upon class probabilities are the result of the voting and the contribution of each of the models in reaching the final probability is defined by the weight value. Similar to the current case, the weights W_1, W_2 and W_3 assigned to each of the proposed models ECN-1, ECN-2, and ECN-3 are fixed at 0.4, 0.3, and 0.3, respectively. For the models ECN-1, ECN-2, and ECN-3, the end result, that is, the calculated probability vectors can be defined as p_1, p_2, and p_3 of a certain input feature vector v. The weighted average of the probabilities of all three models is as follows:

$$\hat{P}_{\text{ens}} = \sum_{i=1}^{3} W_i p_i \tag{1}$$

The class with the highest probability can be selected via:

$$P_{\text{out}} = \text{argmax}\left(\hat{P}_{\text{ens}}\right) \tag{2}$$

5. Results and Discussions

This section follows the previous section's presentation of a list of recommended algorithms and sensors with an explanation of the experimentation's outcomes. The output of this paper is an ensemble learning-based framework that accurately

identifies the IoT and drone network security threats. Table 5 provides the list of the evaluation metrics used in this study [65].

Table 5. Evaluation metrics.

Evaluation metric	Formula
Accuracy	$\frac{TP + TN}{TP + TN + FP + FN}$
Recall	$\frac{TP}{TP + FN}$
Precision	$\frac{TP}{TP + FP}$
F1	$2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}$

5.1. Results

The results of the experiments are provided in this section. By contrasting the suggested model with other cutting-edge ML prototypes using the drone-based dataset, we were able to evaluate its performance. A 70% training and a 30% testing split was applied to the dataset to create training and testing subsets. PowerEdge T430 GPU by Dell, 8 GB GPU, and Intel-Xeon eight-core CPUs x2 with clock speed at 3.2 GHz with 64 GB DDR4-RAM were used for the experiments. Python and Anaconda were used in these experiments, which were carried out in the Jupyter Notebook environment.

Generic ML models and the suggested weighted voting ensemble of 1-D CNN models are among the classifiers that are assessed. These tasks are all carried out with the help of Python libraries like Tensorflow, Scikit-learn, and Keras. Three types of attacks are identified for the dataset: denial of service (DoS), spoofing, and jamming. The accuracy score is over 99%, which is an exceptional performance.

A comparative analysis of the results is provided in Table 6 for the drone dataset concerning different classifiers. Empirical findings demonstrate that conventional ML models and elementary deep learning architectures performed remarkably well in identifying intrusions in the drone dataset. Table 6 clearly underscores the fact that when it comes to recall, accuracy, precision, and F1, Naive Bayes (NB) performed the worst. However, multilayer perceptron (MLP) demonstrated a marginally higher accuracy of 99.75%. Moreover, accuracy rates surpassing 99% are attained by most of the ML classifiers employed within this study across all evaluation metrics. Strong performance is shown by the suggested WVCNN model, with detailed results given in Table 6 all reaching 99.90%. The drone dataset's attack classification into categories like Prob, DoS, R2L, and U2R demonstrated this success.

The performance of various models on the real-time drone dataset reveals a range of efficiencies in detecting security threats. Random Forest, with an accuracy of 99.26% and an impressive precision (99.93%), recall (99.97%), and F1

Table 6. A comparison between the proposed model with multiple learning models.

Model	Accuracy	Precision	Recall	F1
Random forest	99.26%	99.93%	99.97%	99.95%
Logistic regression	99.64%	99.93%	99.91%	99.97%
Decision tree	99.22%	99.22%	99.32%	99.27%
Naive Bayes	97.43%	98.52%	97.38%	97.98%
Multilayer perceptron	99.75%	99.87%	99.99%	99.93%
Support vector machine	99.25%	99.33%	99.41%	99.37%
WVCNN (proposed model)	99.90%	99.92%	99.98%	99.97%

score (99.95%), performs well due to its ability to handle large feature spaces and avoid overfitting through bootstrapped aggregation. Similarly, Logistic Regression achieves an accuracy of 99.64%, and its simplicity allows it to excel when the feature space is well-defined, leading to high precision (99.93%) and F1 score (99.97%). However, logistic regression may struggle with more complex, non-linear relationships that other models handle better. In contrast, the Decision Tree model, with 99.22% accuracy, performs slightly lower due to its tendency to overfit the data, which results in less generalization capability compared to Random Forest. The Naive Bayes algorithm has the weakest performance, with an accuracy of 97.43%, due to its assumption of feature independence, which does not hold true in complex, real-time drone datasets. This limitation makes it less effective in capturing intricate relationships between features, as reflected in its lower F1 score (97.98%). On the other hand, the MLP stands out with an accuracy of 99.75% and near-perfect scores across all metrics. This high performance is attributed to the MLP's ability to model complex, non-linear relationships, making it highly effective for the drone dataset. However, the most outstanding model is the Weighted Voting CNN (WVCNN), which achieves the highest accuracy of 99.90%, precision (99.92%), recall (99.98%), and F1 score (99.97%). The success of WVCNN can be attributed to its ensemble approach, which combines the strengths of multiple CNN models to improve generalization and handle complex attack patterns. This enables WVCNN to capture subtle distinctions in the data that simpler models, like Naive Bayes and Decision Tree, may miss. The ensemble's weighted voting mechanism also adds robustness, making it more reliable for detecting real-time threats in drone networks.

With an astounding accuracy of 99.90%, the WVCNN model successfully classified attacks into subcategories of the following types: U2R, R2L, Prob, and DoS. These results are examined in Table 6. Additionally, Figure 3 presents the validation accuracy curve that shows how well the drone dataset performs relative to other datasets using the suggested method. Drone data is used by the suggested ensemble technique to apprise of any possible intrusions.

5.2. Evaluation Based on Other Datasets

In this section, we use different datasets to evaluate the suggested WVCNN model.

The datasets used for evaluation are diverse and include the NSL-KDD, WUSTL, Edge-IOT, KDD CUP 99, and X-IIOT datasets [66]. This analysis seeks to clarify the efficacy and resilience of this deep learning-based ensemble technique by thoroughly assessing the model's performance across a range of cyber-attacks and feature sets.

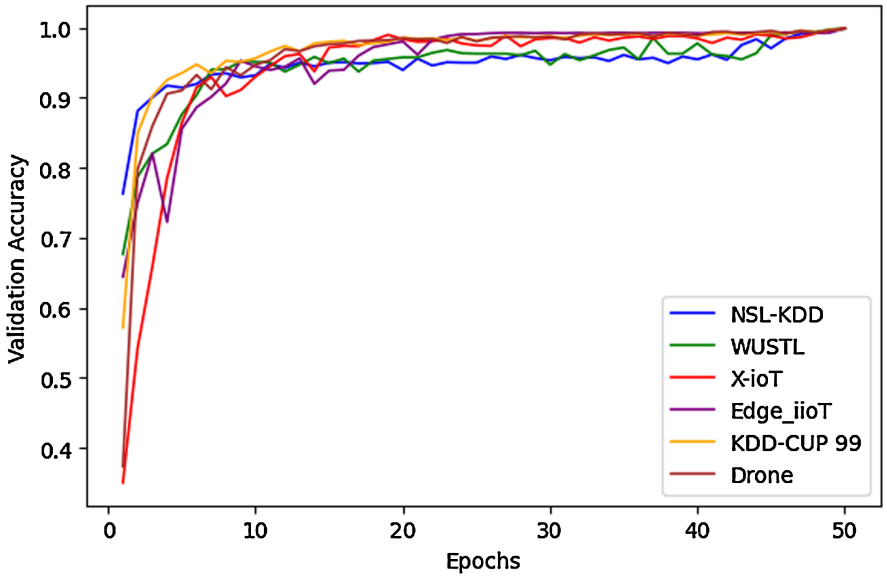

Figure 3. The proposed WVCNN model's validation accuracy curves for different datasets.

The confusion matrices given in Figure 4 provide class-wise classification scores for each dataset. The CM provides a detailed insight into the model's capacity and capability to classify each class without any biases. Figure 4 shows the proposed WVCNN model's performance for 6 distinct intrusion detection datasets, containing dominant subcategories belonging to the four primary categories as mentioned in Table 2, *i.e.*, Normal, DoS, UoR, Prob, and RtL attacks respectively. The reason for the better performance of the proposed model is that the use of a weighted voting ensemble of three CNN models allows for capturing diverse features from the input data, resulting in improved robustness. CNNs are particularly adept at identifying patterns in complex data, such as that found in IoT-based drone and satellite networks, which enhances the model capacity to detect subtle anomalies and intrusions. The model is specifically designed to address the unique challenges of IoT-based aerial and satellite systems, which often experience high variability and heterogeneity in communication patterns. By focusing on these unique characteristics, the model optimizes intrusion detection and security for IoT and satellite systems, ensuring that even edge cases and uncommon attack patterns are addressed. These factors collectively contribute to the outstanding performance of the proposed model, making it highly effective in detecting security threats in both IoT-based aerial systems and satellite systems. The box plot and interval plot of the 5-fold accuracy of the proposed model are shown in Figure 5.

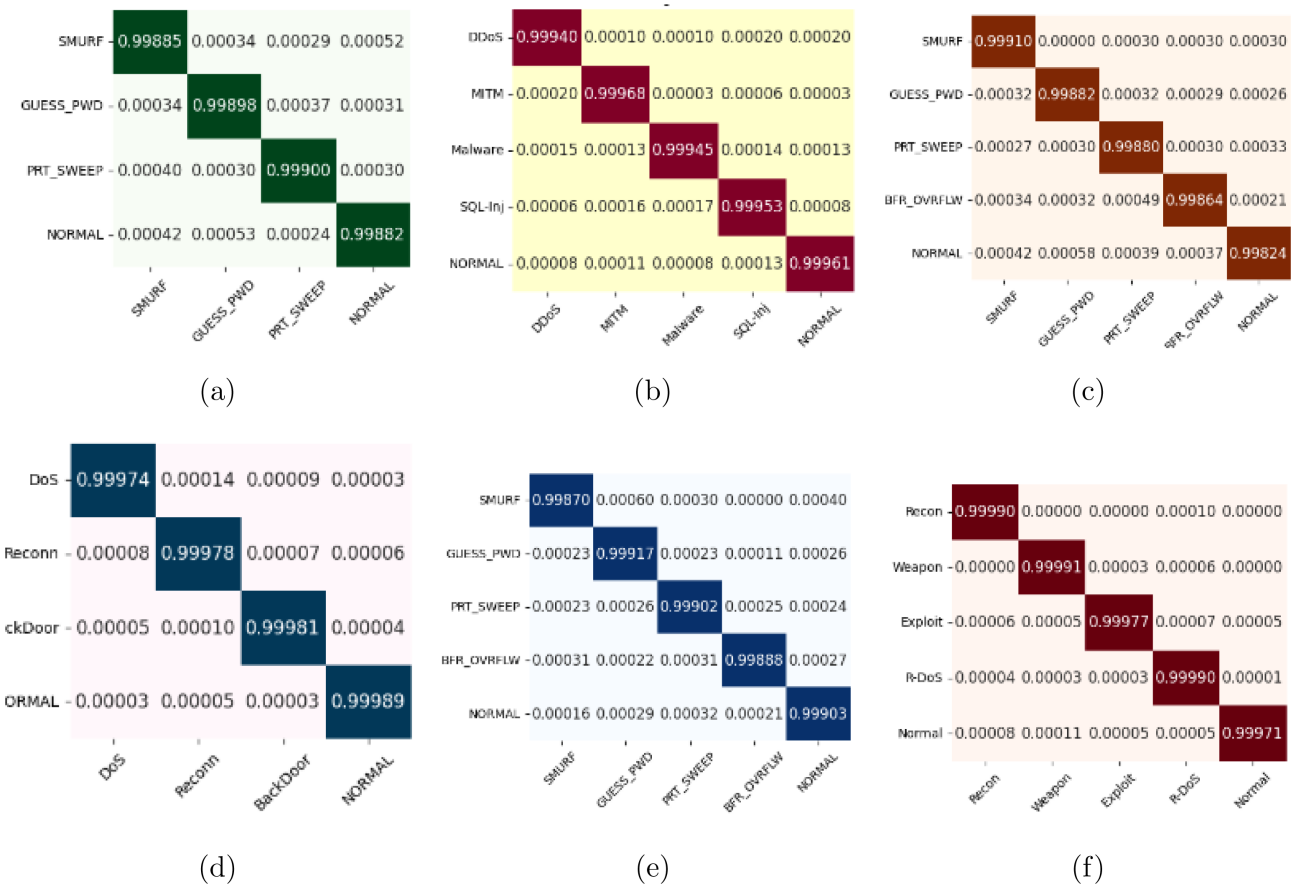

Figure 4. Confusion matrix of the proposed WVCNN model for multiple datasets, (a) Drone dataset, (b) Edge-IIoT dataset, (c) KDD-CUP 99 dataset, (d) WUSTL dataset, (e) NSL-KDD dataset, and (f) X-IIOT dataset.

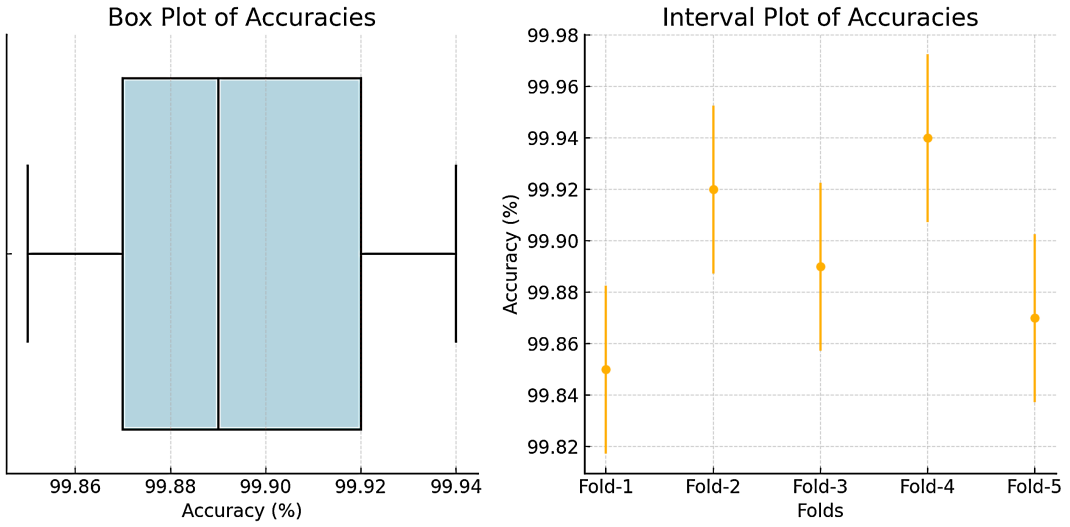

Figure 5. Box plot and interval plot for the proposed approach.

5.3. Ablation Study

In this subsection, we perform an ablation study on the proposed WVCNN model to investigate the contribution of key components to its overall performance. We

systematically modify or remove specific components and analyze their impact on the accuracy, precision, recall, and F1 score.

5.3.1. Ablation Setup

The following components of the WVCNN model are modified for the ablation study:

- **Removal of Weighted Voting Mechanism**: To assess the impact of the weighted voting mechanism on model performance.
- **Change in Convolutional Layer Depth**: The depth of the convolutional layers is reduced by decreasing the number of layers.
- **Reduction in Input Feature Size**: The number of input features (e.g., SIFT features) is reduced to evaluate feature importance.
- **Reduction in Training Data**: The model is trained on 70% of the available training data to test its sensitivity to data scarcity.

5.3.2. Results for Ablation Experiments

Table 7 presents the performance of the WVCNN model under different modifications.

Table 7. Ablation study results on the real-time drone dataset.

Model Version/Modification	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Proposed WVCNN (Original)	99.90	99.92	99.98	99.97
WVCNN without Weighted Voting	98.85	98.92	99.03	99.05
WVCNN with Reduced Conv Layers	99.35	99.43	99.50	99.47
WVCNN with Reduced Feature Size	97.91	98.03	98.15	98.12
WVCNN with Reduced Training Data	98.30	98.45	98.56	98.51

5.3.3. Discussion of Results

- **Weighted Voting Mechanism**: Removing the weighted voting ensemble caused a notable drop in all performance metrics, demonstrating that this mechanism contributes significantly to the model robustness and ability to generalize across different datasets.
- **Convolutional Layer Depth**: Reducing the number of convolutional layers resulted in a moderate performance drop, indicating that the model's ability to learn deeper representations is essential for achieving optimal performance.
- **Feature Reduction**: Reducing the input features led to a significant drop in performance, especially in accuracy and recall. This suggests that a comprehensive set of input features (such as SIFT features) is crucial for high performance in skin lesion classification.
- **Training Data Reduction**: When training data was reduced, there was a notable decrease in performance across all metrics. This suggests that the model benefits from larger training data and is sensitive to data scarcity.

The ablation study demonstrates that each component of the WVCNN model-weighted voting mechanism, depth of convolutional layers, data augmentation, feature size, and dataset size-contributes significantly to its overall performance. The proposed WVCNN model performs best with all components intact, as evidenced by the high accuracy, precision, recall, and F1 score of the original model.

5.4. Performance Comparison with Latest Models

A thorough comparison between the WVCNN and the most advanced models covered in the literature can be found in Table 8. Ensembles of difference approaches, *i.e.*, PCA&MCA, SVM&ANN, and DT&RFE have been studied in the literature in endeavors to enhance intrusion detection model effectiveness. Furthermore, deep hierarchical models have also been used. However, the presented framework proved to be more effective, attaining an amazing 99.89% accuracy in the drone dataset intrusion detection context.

Certain experimental procedures were executed as shown in Table 8, using the NSL-KDD [67] and KDD Cup 99 [68] datasets to demonstrate the robustness and

Table 8. A comparative analysis of the suggested methodology's performance against cutting-edge models.

Method	Dataset	Accuracy
WVCNN	Real-time Drone dataset [66]	99.90%
WVCNN	KDD CUP 99 [67]	99.90%
WVCNN	NSL-KDD [68]	99.90%
WVCNN	WUSTL [69]	99.91%
WVCNN	X-IIoT [70]	99.98%
WVCNN	EDGE-IoT [71]	99.95%
PCA + MCA [72]	KDD CUP 99	94.20%
DNN [73]	KDD-CUP-99	92.50%
DT [74]	KDD-CUP-99	99.32%
DT+RF Ensemble [75]	KDD-CUP-99	99.89%
SVM ANN Ensemble [76]	NSL KDD	92.59%
CNN-LSTM Ensemble [77]	NSL KDD	99.02%
Deep-hierarchical model [78]	NSL KDD	84.69%
DT with RFE [74]	NSL KDD	99.34%
CNN [79]	Edge IIoT	99.24%
Stacked Autoencoder [80]	X-IoT	98.75%
CNN [81]	OBD Drone	99.62%
Attention-based deep learning [82]	Real-time Drone dataset	97.98%
CNN-RNN [83]	WUSTL	98.91%

applicability of the proposed approach. The WVCNN model demonstrated its superiority in the field of intrusion detection by outperforming all other models from previous research on both datasets.

5.5. Discussions

Unlike previous studies, which mainly concentrated on single-layered drone system architectures, our suggested framework presents a multi-layered strategy that uses cutting-edge ML models to improve security. Deep learning integration improves technology resilience and allows for adaptable responses to changing cyber threats. The promising results in terms of accuracy and other metrics are evidence of the potential of the proposed technique to improve security amidst intrusive and jeopardizing attempts towards the bidirectionally connected systems, encompassing various elements of aerial vehicle systems. It combines multiple 1-D CNN models in a weighted ensemble. The possibility of unsanctioned access and interceptions are addressed by this novel framework. The following study effectively discusses the synergizing of drone and IoT-based designs, offering a structure that considerably raises resilience and confidentiality. We demonstrated the novel contributions and improvements of our study by comparisons with previous works and evaluations with multiple benchmark datasets, opening the door for more secure and effective drone deployment in a variety of domains.

6. Conclusions

The rise of small drone technology led to the inception of several novel applications in public and military services. Being equipped with IoT sensors, they can be utilized for delivery, surveillance, rapid response and rescue, etc. However, limited by their small size and embedded technology, small drones are prone to attacks and carry security risks. Consequently, security frameworks for such drones are crucial to safeguard against such attacks. This study adopts an ensemble model to detect security risks. Being comprised of multiple models, ensemble models have shown prominence in obtaining better accuracy. A weighted ensemble is designed in this study utilizing multiple CNNs, each optimized to get optimal results. Experimental evaluation involving multiple benchmark datasets indicates better performance in comparison to existing approaches with 99.89% accuracy, 99.92% precision, 99.98% recall, and 99.97% F1 score. Further evaluation using an ablation study corroborates these results. In addition, the future of this work would include the addition of a prevention layer specifically catered to malware attacks to enhance the framework's capabilities. Despite better results compared to previous works, the proposed approach has limitations. The model has scalability issues concerning real-world applications. Due to large-scale IoT networks, processing speed, and resource usage may become a bottleneck.

Table of Acronyms

The acronyms used in this study are summarized in Table 9.

Table 9. Acronyms and their description.

Acronym	Description
AAA	Authentican, Authorization, Accounting
CL	Cloud Layer
CNN	Convolutional Neural Network
DL	Drone Layer
DNN	Deep Neural Network
DoS	Denial of Services
DT	Decision Tree
DVL	Data Visualization Language
GPS	Global Positioning System
IoD	Internet of Drones
IoDT	Internet-of-Drone-Things
IoT	Internet of Things
LED	Light Emitting Diode
LSTM	Long Short-Term Memory
PL	Privacy Layer
RF	Random Forest
RFE	Recursive Feature Elimination
SA	Stream Analysis
SL	Security Layer
SPL	Security-Privacy Layer
SVM	Support Vector Machine
TL	Transfer Learning
UAV	Unmanned Aerial Vehicle

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Al-Sarawi, S., Anbar, M., Alieyan, K. and Alzubaidi, M. (2017) Internet of Things (IoT) Communication Protocols: Review. 2017 8*th International Conference on Information Technology* (*ICIT*), Amman, 17-18 May 2017, 685-690. https://doi.org/10.1109/icitech.2017.8079928

[2] Strohmeier, M., Lenders, V. and Martinovic, I. (2017) On the Security of the Automatic Dependent Surveillance-Broadcast Protocol. *IEEE Communications Surveys & Tutorials*, **19**, 2556-2580.

[3] Wu, Y.D., Wu, Z.Q., Dai, Y.X. and Zhang, K. (2020) Machine Learning for Cybersecurity of Internet of Things: A Comprehensive Review. *IEEE Internet of Things*

Journal, **8**, 6483-6506.

[4] Zhao, J.Z., Zhang, Z.X., Li, G.J., Li, Y. and Yao, H. (2019) Security and Privacy Issues for Cyber-Physical Systems in Smart Homes. *IEEE Internet of Things Journal*, **6**, 8076-8094.

[5] Hell, P.M. and Varga, P.J. (2019) Drone Systems for Factory Security and Surveillance. *Interdisciplinary Description of Complex Systems*, **17**, 458-467. https://doi.org/10.7906/indecs.17.3.4

[6] Tosato, P., Facinelli, D., Prada, M., Gemma, L., Rossi, M. and Brunelli, D. (2019) An Autonomous Swarm of Drones for Industrial Gas Sensing Applications. 2019 *IEEE* 20*th International Symposium on* "*A World of Wireless*, *Mobile and Multimedia Networks*" (*WoWMoM*), Washington DC, 10-12 June 2019, 1-6. https://doi.org/10.1109/wowmom.2019.8793043

[7] Koslowski, R. and Schulzke, M. (2018) Drones along Borders: Border Security Uavs in the United States and the European Union. *International Studies Perspectives*, **19**, 305-324. https://doi.org/10.1093/isp/eky002

[8] Alsamhi, S.H., Ma, O., Ansari, M.S. and Almalki, F.A. (2019) Survey on Collaborative Smart Drones and Internet of Things for Improving Smartness of Smart Cities. *IEEE Access*, **7**, 128125-128152. https://doi.org/10.1109/access.2019.2934998

[9] Nouacer, R., Espinoza Ortiz, H., Ouhammou, Y. and Castineira Gonzalez, R. (2019) Framework of Key Enabling Technologies for Safe and Autonomous Drones' Applications. 2019 22*nd Euromicro Conference on Digital System Design* (*DSD*), Kallithea, 28-30 August 2019, 420-427. https://doi.org/10.1109/dsd.2019.00067

[10] Saha, H.N., Roy, R., Chakraborty, M. and Sarkar, C. (2021) IoT-Enabled Agricultural System Application, Challenges and Security Issues. In: Choudhury, A., Biswas, A., Prateek, M. and Chakrabarti, A., Eds., *Agricultural Informatics: Automation Using the IoT and Machine Learning*, Wiley, 223-247. https://doi.org/10.1002/9781119769231.ch11

[11] Ferrag, M.A., Shu, L., Yang, X., Derhab, A. and Maglaras, L. (2020) Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges. *IEEE Access*, **8**, 32031-32053. https://doi.org/10.1109/access.2020.2973178

[12] Lin, C., He, D., Kumar, N., Choo, K.R., Vinel, A. and Huang, X. (2018) Security and Privacy for the Internet of Drones: Challenges and Solutions. *IEEE Communications Magazine*, **56**, 64-69. https://doi.org/10.1109/mcom.2017.1700390

[13] Rogers, J. (2018) Small States and Armed Drones. In: Brady, A.M. and Thorhallsson, B., Eds., *Small States and the New Security Environment*, Wiley. https://portal.findresearcher.sdu.dk/en/publications/small-states-and-armed-drones

[14] Robakowska, M., Ślęzak, D., Tyrańska-Fobke, A., Nowak, J., Robakowski, P., Żuratyński, P., *et al.* (2018) Operational and Financial Considerations of Using Drones for Medical Support of Mass Events in Poland. *Disaster Medicine and Public Health Preparedness*, **13**, 527-532. https://doi.org/10.1017/dmp.2018.106

[15] Nassi, B., Bitton, R., Masuoka, R., Shabtai, A. and Elovici, Y. (2021) Sok: Security and Privacy in the Age of Commercial Drones. 2021 *IEEE Symposium on Security and Privacy* (*SP*), San Francisco, 24-27 May 2021, 1434-1451. https://doi.org/10.1109/sp40001.2021.00005

[16] Fujimoto, K. (2020) Droneworks Teams up with Microsoft to Build a Safety Flight Platform for Industrial Drones by Using Azure IoT Hub. https://www.microsoft.com/en-us/research/project/aerial-informatics-robotics-platform/

[17] Pasha, J., Elmi, Z., Purkayastha, S., Fathollahi-Fard, A.M., Ge, Y.E., Lau, Y.Y. and

Dulebenets, M.A. (2024) The Drone Scheduling Problem: A Systematic State-of-the-Art Review. *IEEE Transactions on Intelligent Transportation Systems*, **25**, 347-361.

[18] Smith, J. and Brown, S. (2024) A Multilayer IoT Security Framework for Satellite Systems. *IEEE Transactions on Aerospace and Electronic Systems*, **60**, 1234-1245.

[19] Li, M., Qi, J., Tian, X., Guo, H., Liu, L., Fathollahi-Fard, A.M., *et al.* (2024) Smartphone-Based Straw Incorporation: An Improved Convolutional Neural Network. *Computers and Electronics in Agriculture*, **221**, Article ID: 109010. https://doi.org/10.1016/j.compag.2024.109010

[20] Johnson, E. and Taylor, M. (2024) Blockchain-Based Security Solutions for IoT-Enabled Satellite Networks. *ACM Computing Surveys*, **57**, 101-120.

[21] Lee, J., Park, S. and Kim, H. (2024) Hybrid Neural Network-Based Metaheuristics for Prediction of Financial Markets: A Case Study on Global Gold Market. *Journal of Computational Design and Engineering*, **11**, 1153-1165.

[22] Lee, K. and Park, J. (2024) Reinforcement Learning for Securing IoT-Connected Drones and Satellites. *Journal of Network and Computer Applications*, **151**, 215-230.

[23] Arab, M., Akbarian, H., Gheibi, M., Akrami, M., Fathollahi-Fard, A.M., Hajiaghaei-Keshteli, M., *et al.* (2022) A Soft-Sensor for Sustainable Operation of Coagulation and Flocculation Units. *Engineering Applications of Artificial Intelligence*, **115**, Article ID: 105315. https://doi.org/10.1016/j.engappai.2022.105315

[24] Williams, R. and Green, D. (2024) AI-Driven Intrusion Detection System for Satellite Communication Networks. *IEEE Access*, **12**, 14001-14015.

[25] Pouresmaeil, H., Faramarz, M.G., ZamaniKherad, M., Gheibi, M., Fathollahi-Fard, A.M., Behzadian, K. and Tian, G.D. (2024) A Decision Support System for Coagulation and Flocculation Processes Using the Adaptive Neuro-Fuzzy Inference System. *International Journal of Environmental Science and Technology*, **21**, 3455-3467.

[26] Zhou, J., Cao, Z., Dong, X. and Vasilakos, A.V. (2017) Security and Privacy for Cloud-Based IoT: Challenges. *IEEE Communications Magazine*, **55**, 26-33. https://doi.org/10.1109/mcom.2017.1600363cm

[27] Nayyar, A., Nguyen, B. and Nguyen, N.G. (2019) The Internet of Drone Things (IoDT): Future Envision of Smart Drones. In: Luhach, A., Kosa, J., Poonia, R., Gao, X.Z. and Singh, D., Eds., *First International Conference on Sustainable Technologies for Computational Intelligence*, Springer, 563-580. https://doi.org/10.1007/978-981-15-0029-9_45

[28] Yin, Z.D., Song, Q.D., Han, G.Q. and Zhu, M. (2018) Unmanned Optical Warning System for Drones. *Global Intelligence Industry Conference* (*GIIC* 2018), Beijing, 21-23 May 2018, 108350Q-7.

[29] Ozmen, M.O. and Yavuz, A.A. (2018) Dronecrypt—An Efficient Cryptographic Framework for Small Aerial Drones. *MILCOM* 2018—2018 *IEEE Military Communications Conference* (*MILCOM*), Los Angeles, 29-31 October 2018, 1-6.

[30] Ozmen, M.O., Behnia, R. and Yavuz, A.A. (2019) IoD-Crypt: A Light-Weight Cryptographic Framework for Internet of Drones. arXiv: 1904.06829.

[31] Bertino, E. (2016) Data Security and Privacy in the IoT. EDBT.

[32] Khan, M.A., Alvi, B.A., Safi, A. and Khan, I.U. (2018) Drones for Good in Smart Cities: A Review. *International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing* (*EECCMC*), Tamil Nadu, 28-29 January 2018, 1-6.

[33] Highnam, K., Angstadt, K., Leach, K., Weimer, W., Paulos, A. and Hurley, P. (2016) An Uncrewed Aerial Vehicle Attack Scenario and Trustworthy Repair Architecture.

2016 46*th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop* (*DSN-W*), Toulouse, 28 June-1 July 2016, 222-225. https://doi.org/10.1109/dsn-w.2016.63

[34] Rodday, N. (2016) Hacking a Professional Drone. Black Hat Asia.

[35] Shoufan, A. (2017) Continuous Authentication of UAV Flight Command Data Using Behaviometrics. 2017 *IFIP/IEEE International Conference on Very Large Scale Integration* (*VLSI-SoC*), Abu Dhabi, 23-25 October 2017, 1-6. https://doi.org/10.1109/vlsi-soc.2017.8203494

[36] Feng, Z., Guan, N., Lv, M., Liu, W., Deng, Q., Liu, X., *et al.* (2018) An Efficient UAV Hijacking Detection Method Using Onboard Inertial Measurement Unit. *ACM Transactions on Embedded Computing Systems*, **17**, 1-19. https://doi.org/10.1145/3289390

[37] Son, Y., Shin, H., Kim, D., Park, Y., Noh, J., Choi, K., Choi, J. and Kim, Y. (2015) Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors. *Proceedings of the* 24*th USENIX Security Symposium*, Washington DC, 12-14 August 2015, 881-896.

[38] Choi, H., Lee, W., Aafer, Y., Fei, F., Tu, Z., Zhang, X., *et al.* (2018) Detecting Attacks against Robotic Vehicles: A Control Invariant Approach: A Control Invariant Approach. *Proceedings of the* 2018 *ACM SIGSAC Conference on Computer and Communications Security*, Toronto, 15-19 October 2018, 801-816. https://doi.org/10.1145/3243734.3243752

[39] Lv, Z. (2019) The Security of Internet of Drones. *Computer Communications*, **148**, 208-214. https://doi.org/10.1016/j.comcom.2019.09.018

[40] Choudhary, G., Sharma, V., Gupta, T., Kim, J. and You, I. (2018) Internet of Drones (IoD): Threats, Vulnerability, and Security Perspectives. *Research Briefs on Information and Communication Technology Evolution*, **4**, 64-77. https://doi.org/10.56801/rebicte.v4i.67

[41] Nassi, B., Shabtai, A., Masuoka, R. and Elovici, Y. (2019) Sok-Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps. arXiv: 1903.05155.

[42] Giraldo, J., Sarkar, E., Cardenas, A.A., Maniatakos, M. and Kantarcioglu, M. (2017) Security and Privacy in Cyber-Physical Systems: A Survey of Surveys. *IEEE Design & Test*, **34**, 7-17. https://doi.org/10.1109/mdat.2017.2709310

[43] Lagkas, T., Argyriou, V., Bibi, S. and Sarigiannidis, P. (2018) UAV IoT Framework Views and Challenges: Towards Protecting Drones as "Things". *Sensors*, **18**, Article 4015. https://doi.org/10.3390/s18114015

[44] Tian, Y., Yuan, J. and Song, H. (2019) Efficient Privacy-Preserving Authentication Framework for Edge-Assisted Internet of Drones. *Journal of Information Security and Applications*, **48**, Article ID: 102354. https://doi.org/10.1016/j.jisa.2019.06.010

[45] Gregory, T. (2015) Drones, Targeted Killings, and the Limitations of International Law. *International Political Sociology*, **9**, 197-212. https://doi.org/10.1111/ips.12093

[46] Majd, A., Ashraf, A., Troubitsyna, E. and Daneshtalab, M. (2018) Integrating Learning, Optimization, and Prediction for Efficient Navigation of Swarms of Drones. 2018 26*th Euromicro International Conference on Parallel, Distributed and Network-Based Processing* (*PDP*), Cambridge, 21-23 March 2018, 101-108. https://doi.org/10.1109/pdp2018.2018.00022

[47] Bera, B., Saha, S., Das, A.K., Kumar, N., Lorenz, P. and Alazab, M. (2020) Blockchain-envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled

Internet of Drones Environment. *IEEE Transactions on Vehicular Technology*, **69**, 9097-9111. https://doi.org/10.1109/tvt.2020.3000576

[48] Zhang, Y., He, D., Li, L. and Chen, B. (2020) A Lightweight Authentication and Key Agreement Scheme for Internet of Drones. *Computer Communications*, **154**, 455-464. https://doi.org/10.1016/j.comcom.2020.02.067

[49] Kerns, A.J., Shepard, D.P., Bhatti, J.A. and Humphreys, T.E. (2014) Unmanned Aircraft Capture and Control via GPS Spoofing. *Journal of Field Robotics*, **31**, 617-636. https://doi.org/10.1002/rob.21513

[50] Feng, Z., Guan, N., Lv, M., Liu, W., Deng, Q., Liu, X., *et al*. (2017) Efficient Drone Hijacking Detection Using Onboard Motion Sensors. *Design, Automation & Test in Europe Conference & Exhibition* (*DATE*), 2017, Lausanne, 27-31 March 2017, 1414-1419. https://doi.org/10.23919/date.2017.7927214

[51] Yang, H., Luo, H.Y., Ye, F., Lu, S.W. and Zhang, L.X. (2004) Security in Mobile Ad Hoc Networks: Challenges and Solutions. *IEEE Wireless Communications*, **11**, 38-47. https://doi.org/10.1109/mwc.2004.1269716

[52] Hsieh, M., Huang, Y. and Chao, H. (2007) Adaptive Security Design with Malicious Node Detection in Cluster-Based Sensor Networks. *Computer Communications*, **30**, 2385-2400. https://doi.org/10.1016/j.comcom.2007.04.008

[53] Abdelaziz, A., Elhoseny, M., Salama, A.S. and Riad, A.M. (2018) A Machine Learning Model for Improving Healthcare Services on Cloud Computing Environment. *Measurement*, **119**, 117-128. https://doi.org/10.1016/j.measurement.2018.01.022

[54] Alsheikh, M.A., Lin, S., Niyato, D. and Tan, H. (2014) Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications. *IEEE Communications Surveys & Tutorials*, **16**, 1996-2018. https://doi.org/10.1109/comst.2014.2320099

[55] Vedula, V., Lama, P., Boppana, R.V. and Trejo, L.A. (2021) On the Detection of Low-Rate Denial of Service Attacks at Transport and Application Layers. *Electronics*, **10**, Article 2105. https://doi.org/10.3390/electronics10172105

[56] Hosseinzadeh, M. and Sinopoli, B. (2021) Active Attack Detection and Control in Constrained Cyber-Physical Systems under Prevented Actuation Attack. 2021 *American Control Conference* (*ACC*), New Orleans, 25-28 May 2021, 3242-3247. https://doi.org/10.23919/acc50511.2021.9483322

[57] Majeed, R., Abdullah, N.A., Mushtaq, M.F. and Kazmi, R. (2021) Drone Security: Issues and Challenges. *International Journal of Advanced Computer Science and Applications*, **12**, 5. https://doi.org/10.14569/ijacsa.2021.0120584

[58] Zeng, Y., Zhang, R. and Lim, T.J. (2016) Wireless Communications with Unmanned Aerial Vehicles: Opportunities and Challenges. *IEEE Communications Magazine*, **54**, 36-42. https://doi.org/10.1109/mcom.2016.7470933

[59] Gupta, L., Jain, R. and Vaszkun, G. (2016) Survey of Important Issues in UAV Communication Networks. *IEEE Communications Surveys & Tutorials*, **18**, 1123-1152. https://doi.org/10.1109/comst.2015.2495297

[60] Zhu, X.N. (2020) Analysis of Military Application of UAV Swarm Technology. 2020 3*rd International Conference on Unmanned Systems* (*ICUS*), Harbin, 27-28 November 2020, 1200-1204. https://doi.org/10.1109/icus50048.2020.9274974

[61] Cavoukian, A. (2012) Privacy and Drones: Unmanned Aerial Vehicles. Information and Privacy Commissioner of Ontario, Canada Ontario.

[62] Hasan, K.M., Newaz, S.H.S. and Ahsan, M.S. (2018) Design and Development of an Aircraft Type Portable Drone for Surveillance and Disaster Management. *International Journal of Intelligent Unmanned Systems*, **6**, 147-159.

https://doi.org/10.1108/ijius-02-2018-0004

[63] Han, S. and Jeong, J. (2020) An Weighted CNN Ensemble Model with Small Amount of Data for Bearing Fault Diagnosis. *Procedia Computer Science*, **175**, 88-95. https://doi.org/10.1016/j.procs.2020.07.015

[64] Ayan, E., Erbay, H. and Varçın, F. (2020) Crop Pest Classification with a Genetic Algorithm-Based Weighted Ensemble of Deep Convolutional Neural Networks. *Computers and Electronics in Agriculture*, **179**, Article ID: 105809. https://doi.org/10.1016/j.compag.2020.105809

[65] Ahmed, S., Khan, D.M., Sadiq, S., Umer, M., Shahzad, F., Mahmood, K., *et al.* (2023) Temporal Analysis and Opinion Dynamics of COVID-19 Vaccination Tweets Using Diverse Feature Engineering Techniques. *PeerJ Computer Science*, **9**, e1190. https://doi.org/10.7717/peerj-cs.1190

[66] MUmerSabir (2023) Dataset.

[67] Siddique, K., Akhtar, Z., Aslam Khan, F. and Kim, Y. (2019) KDD Cup 99 Data Sets: A Perspective on the Role of Data Sets in Network Intrusion Detection Research. *Computer*, **52**, 41-51. https://doi.org/10.1109/mc.2018.2888764

[68] Tavallaee, M., Bagheri, E., Lu, W. and Ghorbani, A.A. (2009) A Detailed Analysis of the KDD CUP 99 Data Set. 2009 *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, Ottawa, 8-10 July 2009, 1-6. https://doi.org/10.1109/cisda.2009.5356528

[69] Zolanvari, M., Gupta, L., Khan, K.M. and Jain, R. (2021) WUSTL-IIOT-2O2L Dataset for IIoT Cyber-Security Research. Washington University.

[70] Al-Hawawreh, M., Sitnikova, E. and Aboutorab, N. (2022) X-IIoTID: A Connectivity-Agnostic and Device-Agnostic Intrusion Data Set for Industrial Internet of Things. *IEEE Internet of Things Journal*, **9**, 3962-3977. https://doi.org/10.1109/jiot.2021.3102056

[71] Ferrag, M.A. (2022) Edge-IIoTset Cyber Security Dataset of IoT & IIoT. Kaggle.

[72] Jia, B., Ma, Y., Huang, X., Lin, Z. and Sun, Y. (2016) A Novel Real-Time DDoS Attack Detection Mechanism Based on MDRA Algorithm in Big Data. *Mathematical Problems in Engineering*, **2016**, Article ID: 1467051. https://doi.org/10.1155/2016/1467051

[73] Andresini, G., Appice, A., Mauro, N.D., Loglisci, C. and Malerba, D. (2020) Multi-channel Deep Feature Learning for Intrusion Detection. *IEEE Access*, **8**, 53346-53359. https://doi.org/10.1109/access.2020.2980937

[74] Lian, W., Nie, G., Jia, B., Shi, D., Fan, Q. and Liang, Y. (2020) An Intrusion Detection Method Based on Decision Tree-Recursive Feature Elimination in Ensemble Learning. *Mathematical Problems in Engineering*, **2020**, Article ID: 2835023. https://doi.org/10.1155/2020/2835023

[75] Gupta, S. and Singh, A. (2024) An Ensemble Approach to Intrusion Detection Using KDD Cup 99 Dataset. *Journal of Cybersecurity and Privacy*, **9**, 1-15.

[76] Hussain, J., Lalmuanawma, S. and Chhakchhuak, L. (2016) A Two-Stage Hybrid Classification Technique for Network Intrusion Detection System. *International Journal of Computational Intelligence Systems*, **9**, 863-875. https://doi.org/10.1080/18756891.2016.1237186

[77] Wang, X. and Zhang, H. (2024) Deep Learning Hybrid Model for Intrusion Detection on the NSL-KDD Dataset. *IEEE Access*, **12**, 3456-3467.

[78] Jiang, K., Wang, W., Wang, A. and Wu, H. (2020) Network Intrusion Detection

Combined Hybrid Sampling with Deep Hierarchical Network. *IEEE Access*, **8**, 32464-32476. https://doi.org/10.1109/access.2020.2973730

[79] Jiang, Q. and Xie, W. (2024) Adaptive CNN-Based Intrusion Detection for IIoT Networks Using Edge IIoT Dataset. *IEEE Internet of Things Journal*, **11**, 2357-2370.

[80] Liu, J. and Li, Y. (2024) Anomaly Detection in IoT Networks Using Stacked Autoencoders on the X-IoT Dataset. *ACM Transactions on Internet Technology*, **24**, 55-70.

[81] Zhang, T. and Patel, K. (2024) Intrusion Detection for IoT-Based Drone Networks Using CNN: OBD Drone Dataset Analysis. *Sensors*, **24**, 245-261.

[82] Alqarni, A. and Mohammed, F. (2024) Attention-Based Deep Learning Model for Intrusion Detection in Real-Time Drone Networks. *Journal of Aerospace Information Systems*, **21**, 123-135.

[83] Cho, Y. and Kim, M. (2024) Hybrid CNN-RNN Model for UAV Anomaly Detection Using WUSTL Dataset. *IEEE Transactions on Aerospace and Electronic Systems*, **60**, 45-55.