frontiers | Frontiers in Energy Research

TYPE Original Research
PUBLISHED 10 December 2024
DOI 10.3389/fenrg.2024.1491332

Enhancing unmanned aerial vehicle and smart grid communication security using a ConvLSTM model for intrusion detection

Raed Alharthi*

Department of Computer Science and Engineering, University of Hafr Al-Batin, Hafar Al Batin, Saudi Arabia

OPEN ACCESS

EDITED BY
Stavros Shiaeles,
University of Portsmouth, United Kingdom

REVIEWED BY
Ahsan Farid,
University of Science and Technology Beijing, China
Paramjyot Kumar Jha,
Chandigarh University, India
Abdul Ghaffar,
Raffz Ltd., United Kingdom

*CORRESPONDENCE
Raed Alharthi,
✉ ralharthi@uhb.edu.sa

RECEIVED 04 September 2024
ACCEPTED 15 November 2024
PUBLISHED 10 December 2024

CITATION
Alharthi R (2024) Enhancing unmanned aerial vehicle and smart grid communication security using a ConvLSTM model for intrusion detection.
Front. Energy Res. 12:1491332.
doi: 10.3389/fenrg.2024.1491332

The emergence of small-drone technology has revolutionized the way we use drones. Small drones leverage the Internet of Things (IoT) to deliver location-based navigation services, making them versatile tools for various applications. Unmanned aerial vehicle (UAV) communication networks and smart grid communication protocols share several similarities, particularly in terms of their architecture, the nature of the data they handle, and the security challenges they face. To ensure the safe, secure, and reliable operation of both, it is imperative to establish a secure and dependable network infrastructure and to develop and implement robust security and privacy mechanisms tailored to the specific needs of this domain. The research evaluates the performance of deep learning models, including convolutional neural networks (CNN), long short-term memory (LSTM), CNN-LSTM, and convolutional long short-term memory (ConvLSTM), in detecting intrusions within UAV communication networks. The study utilizes five diverse and realistic datasets, namely, KDD Cup-99, NSL-KDD, WSN-DS, CICIDS 2017, and Drone, to simulate real-world intrusion scenarios. Notably, the ConvLSTM model consistently achieves an accuracy of 99.99%, showcasing its potential in securing UAVs from cyber threats. By demonstrating its superior performance, this work highlights the importance of tailored security mechanisms in safeguarding UAV technology against evolving cyber threats. Ultimately, this research contributes to the growing body of knowledge on UAV security, emphasizing the necessity of high-quality datasets and advanced models in ensuring the safe, secure, and reliable operation of UAV systems across various industries.

KEYWORDS

smart grid, unmanned aerial vehicles, communication security, intrusion detection, cyber resilience

Abbreviations: CNN, convolutional neural network; CPU, central processing unit; DL, drone layer; DNN, deep neural network; DoS, denial of services; FTP, file transfer protocol; HTTP, hypertext transfer protocol; IoD, Internet of drones; IoT, Internet of Things; LSTM, long short-term memory; OS, operating system; PL, privacy layer; RAM, random access memory; SL, security layer; SSH, secure shell; SSL, secure sockets layer.; TL, transfer learning; UAV, unmanned aerial vehicle.

1 Introduction

Flying *ad hoc* wireless devices (FAWD), or UAVs, are increasingly being deployed and gaining much awareness. This rising interest is attributed to their LoS connection to the ground users, their mobility, and the modularity that makes them affordable to deploy. Indeed, in places where the fixed network has been affected by natural disasters and the physical wiring infrastructure has been brought down, the UAVs can usefully establish cellular network coverage. UAVs can act as flying base stations in mobile wireless networks and offer telecommunication utilities to locations where it is realistically impossible to erect fixed cellular sites due to client limitations or cost (Majeed et al., 2022). Furthermore, UAVs play an important role in emergency response operations, weather monitoring, industrial infrastructure surveillance, logistical assistance, fast disaster management in impacted regions, and surveillance at homes (Khan et al., 2022). The Federal Aviation Administration (FAA) of the United States predicts that demand for commercial UAV installation will quadruple by 2023 (Administration, 2019). Due to the enormous potential of UAVs, several countries are devoting significant financial resources to their broad commercial deployment. UAV-assisted networks continue to face several difficulties despite the growing potential and many uses of UAVs. These difficulties include concerns with the planning of routes, privacy concerns, hurdle handling, energy efficiency, and optimizing for minimal delays (Ateya et al., 2019). These problems must be dealt with adequately if we are to harness the potential offered by UAVs.

UAVs or drones have impacted several sectors and have become almost indispensable in daily operations in the commercial world. They are employed in capturing images from the sky and acquiring information that will be relayed to base stations to aid in decision making, especially in areas of surveillance and monitoring (Rogers, 2018). The overall advancement in the use and application of drones, especially in day-to-day activities, has, however, come with several impacts. This has raised concerns over the safety and security of the public, hence calling for definite legislation over the matter establishing accountability for the privacy of individuals and the public at large (Robakowska et al., 2019). Despite the present challenges, small-sized drones are increasingly being adopted in various industries, such as agriculture, shipping, and manufacturing industries, among others. However, problems associated with privacy and security have arisen because of the high level of application of drones coupled with the need for quick response (Nassi et al., 2021). Scientists state the problems of mounting small sensors on drones that would expand their performance and opportunities. Drones can be made to perform better in other concrete applications that require much more challenging tasks through the installation of transmitters, sensors, and cameras. Drone technology has many applications in the civil and defense industries. However, drone design and architecture aggravate their exposure to privacy or safety threats, as mentioned below in more detail. The IoT and the Internet of Drones (IoD) have new possibilities but are also connected with security and privacy threats. Thus, modification and innovation must occur at the most basic levels of structuring and designing of drones.

Security of smart grid communication has become a critical aspect of the successful functioning of the contemporary power system. The integration of information and communication technology (ICT) in the grid focuses on several threats of cyberattack, including data interception, denial of service, and man-in-the-middle attacks, as noted by Yan et al. (2012). Security measures refer to the methods used to safeguard the information exchanged in the grid and ensure that the data are as they were when they were transmitted. The use of cryptographic techniques to secure the system data, together with strong authentication measures and intrusion detection systems, are some of the measures that should be taken to fight these threats (Metke and Ekl, 2010). In addition, the use of decentralized and highly resilient structures enhances the possibility of countering cyber threats to maintain grid operation despite unfavorable circumstances (Hu et al., 2014). In the ever-changing grid system made up of renewables such as solar and IoT devices, security options must adapt and be scalable (Danev et al., 2012). Recent advancements in deep learning (DL) have demonstrated exceptional capabilities in extracting meaningful patterns from complex datasets, making them a compelling choice for intrusion detection systems (IDSs) (Alsubai et al., 2024; Umer et al., 2022).

Cyberphysical systems (CPSs) represent a class of systems that integrate computational and physical functionalities, enabling interactions with individuals through a range of managed processes. UAVs are an appropriate CPS component due to three basic parts of CPS: a strong compute unit, *ad hoc* wireless networks, and adaptive control capabilities. The primary advantages of integrating UAVs into applications of CPS originate from their distinct characteristics, which include mobility, frictionless deployment, changeable height, customized control, and the ability to give exact real-world evaluations at any place and at any time (Shakeri et al., 2019). UAV-based CPS, despite having great potential as an ideal CPS component, is vulnerable because of its unpredictably changing environment, wireless channels, 3D positioning, and absence of established standards for security. In any CPS, the security of a network is important, mandating a high-priority strategy to address security concerns while also ensuring the system's stability and safety for commercial implementation (Rani et al., 2022). At this point, researchers are actively looking toward practical and effective security measures to safeguard these systems, emphasizing the security issues related to UAV-assisted CPS (Consul et al., 2022). In this study, we discuss the potential security risks and vulnerabilities of UAV-based systems. Furthermore, the investigation also highlights the emerging security vulnerabilities present at multiple UAV layers. Additionally, we propose a novel approach that integrates layer-specific adaptive security measures with AI assistance to significantly enhance UAV security.

1.1 Major contributions

The proposed approach promotes the merging of drone and Internet of Things (IoT) technology to produce intelligent drones with decision-making skills. Drones are prone to security flaws and unauthorized access, much like other IoT devices. Threat actors could breach data security and privacy by exploiting drone system flaws. Additionally, drones' extensive data transmission and collection pose questions regarding data security and possible exploitation. The evolution of the Internet of Drone Things (IoDT) can only be maximized with the help of a security architecture to be implemented.

- This paper focuses on the new trends in drone safety, security, and privacy aspects, as well as the field of the Internet of Drones (IoD). It underlines the need to develop protective measures to create reliable and robust drone networks that would not be vulnerable to hackers and corresponding breaches.
- The paper describes and compares the assessment of different deep learning models such as CNN, LSTM, CNN-LSTM, and convolutional long short-term memory (ConvLSTM) in applying IDS for UAVs.
- The proposed model is evaluated with five real-life and different datasets: KDD Cup-99, NSL-KDD, WSN-DS, CICIDS 2017, and Drone. Such inclusive dataset selection enables this model to be evaluated under different intrusion paradigms, thus increasing the applicability and realism of the results.
- The authors emphasize the ConvLSTM's performance to be better, with an accuracy of 99. 99%, whether on the chosen dataset or other datasets. Consequently, this research implies that ConvLSTM is an efficient approach for UAV intrusion detection, making it possible to develop a solid ground for other cybersecurity developments in the future.
- In this case, this research paper provides an approach that can be used to enhance the security and reliability of different systems, such as surveillance and package deliveries, as well as the IoT-assisted UAVs.

1.2 Paper organization

Section 2 of this paper examines the body of knowledge about detecting flaws and vulnerabilities in drones and IoT devices. A few studies have suggested that adding authentication techniques can improve the security of these drone systems. A thorough description of the drone architecture and a layered framework for preserving the integrity of drone systems are given in Section 3. In Section 5, the concepts of access control and authentication in relation to drones are presented. Section 6 summarizes the results and discussion. Section 7 summarizes the findings from the study and makes suggestions for further research.

2 Related work

UAV networks are increasingly employed to transmit sensitive information in critical missions and applications. However, due to their limited computing and communication resources, anomalies and attacks pose a risk to the infrastructure of UAVs. Intrusion detection systems in UAVs are developed to detect a wide range of abnormalities and threats, such as viruses and malware, message and route forging or manipulation, routing attacks, and UAV hijacking or spoofing (Abro et al., 2022). In the recent past, machine learning-based methods have been used to develop cybersecurity measures meant to protect communication inside the IoT and CPS from various cyberattacks and intrusions. However, the research on the utilization of deep learning approaches for intrusion detection is limited (Gao et al., 2019; Shone et al., 2018; Ahmad et al., 2021. Ahmad et al. (2021) published a comprehensive evaluation focused on machine learning and deep learning models meant to address a variety of UAV difficulties, including but not limited to channel modeling, resource management, navigation, and security. Bithas et al. (2019) investigated numerous attacks and defense tactics across many network levels, beginning with the physical and application layers.

Abu Al-Haija and Zein-Sabatto (2020) investigated an unsupervised learning-driven approach to detect active eavesdropping within UAV networks. This system uses the uplink phase to authenticate users. The authors used one-class support vector machines (OC-SVMs) and K-means clustering to detect possible attacks during authentication. The authors also introduced two new methods: one for creating test data from wireless signals and one for generating artificial training data based on channel state information. Their analysis showed that the one-class SVM outperformed K-means clustering when the eavesdropper's transmitted power was moderate or low, but K-means clustering performed better when the eavesdropper's transmitted power was high.

Several issues must be addressed in order to achieve reliable wireless connectivity for UAVs and ensure security. The difficulties include signal interference, limited bandwidth, signal attenuation, and security problems. The authors discussed several issues related to achieving cellular-connected UAV transport systems by using ANN (Challita et al., 2019). Guerber et al. (2021) discussed a novel machine learning-based strategy built on the flow generation events for the equal fight against insider attacks utilizing the random forest classifier algorithm. They introduce two new components that are specific to the nature of network activity and help in budding common network attacks that include brute force, denial of services, and port scanning. These functionalities are, however, easily accessible by the controller. The researchers improved the secrecy rates of the networks by using physical layer security and creating secure communication (Aboueleneen et al., 2023). They also cut the net energy consumption of the IoD network by improving drone transmission and jamming features, as well as through the utilization of energy scavenging mechanisms for wireless charging of drones. As an optimization problem, it was cast into the form of a Markov decision process and solved using a deep reinforcement learning technique.

The researchers applied a supervised learning approach through the deep neural networks (DNNs) to detect GPS spoofing. Using feature engineering, the authors decided that only the signal-to-noise ratio and the Doppler shift are appropriate for the investigation because they can greatly influence the prediction results. They explored network topologies, using one or two-layer hidden neural networks along with large numbers of neurons utilized in creating the model. The authors employed five available features to generate several model runs with some variations in the features offered. The best overall results achieved by them depicted an accuracy percentage near about 98% with the help of one hidden layer containing only ten neurons. Wang and Ghaleb (2023) developed an attention-based CNN model for intrusion detection, improving feature usage and computational efficiency. Donkol et al. (2023) proposed a hybrid IDS combining LPPSO and LSTM-RNN, yielding high detection accuracy and reducing the false alarm rate. Wang et al. (2022) introduced an unsupervised IDS using autoencoders and isolation forest but faced challenges in detecting certain attacks. Mbow et al. (2021) addressed the class imbalance in intrusion detection using a hybrid sampling technique and deep learning, achieving better detection but with room to reduce the false alarm rate.

Some reinforcement learning techniques have been considered to address this problem. The paper by Xiao et al. (2018) presents the development of an anti-jamming system for UAVs employing a game-theoretic method together with reinforcement learning that is different from other existing approaches, namely, policy hill climbing (PHC). In their devised system, UAVs are intermediary because they relay information from the roadside units (RSUs) to VANET on-board units (OBUs). The main objective is to find those RSUs that are very much interfered with by jammers and shift the OBU signal to RSUs that experience little or no jamming at all. Their simulation findings demonstrated that their technique could indeed reduce the BER of OBU messages compared to the QL-based system.

The KDD Cup 99 dataset or some of its modifications was used to recommend and evaluate different IDS options. Hybrid techniques, namely, necessary snapshot ensemble learning and group convolution networks, have been employed by Wang et al. (2021) to improve IDS generality. The authors attained 85.82% accuracy using six predicting attributes and several compared machine learning frameworks: naive Bayes, decision tree, support vector machine, random forest, and XGBoost. Devan and Khare (2020) integrated an XGBoost model with the deep learning model. For XGBoost, feature engineering and reduction of dimensions are the main tasks accomplished, whereas the deep learning model constructs the classifier. Their research strategy was tested and compared with NB, SVM, and LR using the NSL-KDD dataset.

Machine learning, when incorporated into UAV systems, provides a plethora of opportunities and introduces state-of-the-art approaches in various domains. Kurunathan et al. (2023) explained the application of machine learning techniques in UAV services and operations. They elaborated that machine learning plays a very crucial role in the regeneration of features, feature extraction, planning, operation, and control. CNNs based on deep learning frameworks have enabled a far better detection rate than previously used machine learning approaches; the abovementioned approaches are challenging, where the development of new abnormalities is especially challenging. The article also describes how the CNN technique can successfully separate UAV drones from various other objects in the air, including birds and airplanes, which is one of the major benefits of using CNN for UAV detection (Ivanov et al., 2020). Wang et al. (2019) applied long short-term memory (LSTM) in an intrusion detection system (IDS) on UAV network construction. In this study, the goal of anomaly identification was defined as a time-series analysis problem with a focus on point anomaly. The authors measured the system's performance using real UAV transmission data and also conducted simulations using assault scenarios. The current study uses an architecture that is influenced by both CNN and LSTM. A preliminary study indicates that integrating CNN with LSTM has a greater potential in identifying two-fold difficult patterns and sequences in network traffic data, which will further improve the efficiency and reliability of detecting security threats and abnormalities.

Prior studies discussed in this paper highlight the need for an integrated solution to reduce cybersecurity risks and protect drone data. Although several works have documented the troubles and concerns associated with the drone security threat, many have a lack of recommendations on how to counter these threats (Bera et al., 2020). Previous studies have shown that machine learning models are capable of mitigating attacks in different network contexts; however, little has been done in the context of drones. In addition, some of the authentication mechanisms stated earlier in this paper may not be applicable to IoT-based drone networks. Therefore, it is pivotal to close the research gap to ensure that drones meet the standards of the industry and are suitable for commercial purposes while at the same time being safe and non-intrusive in terms of privacy. Tables 1, 2 lists the related studies that have adopted deep learning techniques.

2.1 Comparative analysis with relevant literature

Some gaps identified in the literature are that current models used to solve cybersecurity threats facing UAV networks employ a limited number of deep learning methods and have difficulty detecting intrusions due to the many types of attacks. Although current studies have focused on machine learning-based methods, their practical use in UAV cybersecurity is still limited (Gao et al., 2019; Shone et al., 2018; Ahmad et al., 2021). Some have dealt with some particular issues like the detection of active eavesdropping (Abu Al-Haija and Zein-Sabatto, 2020), and others have dealt with issues such as network security and energy efficiency (Challita et al., 2019; Guerber et al., 2021; Aboueleneen et al., 2023). The techniques to identify threats, such as GPS spoofing, include reinforcement learning and supervised learning with deep neural networks (Manesh et al., 2019; Xiao et al., 2018). Furthermore, the use of hybrid machine-learning frameworks has been proven to enhance the effectiveness of intrusion detection (Wang et al., 2021; Devan and Khare, 2020). The implementation of machine learning in UAV systems has potential in nearly every field because it makes real-time monitoring and prediction possible and improves the functioning of systems (Kurunathan et al., 2023; Bader et al., 2023). Nonetheless, there are calls for more flexible and large-scale solution approaches to tackle more cybersecurity threats in the UAV networks, which ConvLSTM models may help to overcome because these models can process sequence data and capture temporal and spatial dependencies. ConvLSTM models are one of the most suitable solutions for the cybersecurity issues of drones and their intrusion identification. They satisfactorily process sequential data streams from drones, providing timely identification and prevention of cyber threats. Further comparisons of the models are presented in the "Related Work" section of the manuscript.

3 UAVs and smart grid communication framework

This study is primarily concerned with improving the cybersecurity of IoT-enabled UAV devices and the Smart Grid, with a particular emphasis on tiny drones, by improving their underlying

TABLE 1 Deep learning-based intrusion detection system for networked UAVs.

Ref.	Attack	Method	Dataset	Findings
Gao et al. (2019)	DoS, Probe, R2L, and U2R	Adaptive voting classifier	NSL-KDD	Accuracy score 85.2%
Sapre et al. (2019)	DoS, Probe, R2L, and U2R	ANN	KDDCup99 and the NSL-KDD	92.39% on KDDCup99, 78.51% on NSL-KDD
Abu Al-Haija and Zein-Sabatto (2020)	DoS, R2L, U2R, and Probe	CNN	NSL-KDD	Accuracy score 99.3%
Manesh et al. (2019)	GPS spoofing signals	ANN	Real UAV data	Accuracy score 98.3%
Wang et al. (2021)	DoS, R2L, U2R, Worms, Backdoors, and Fuzzers	Group convolution ensemble	NSL-KDD, UNSW-NB15	Accuracy score 85.82% on NSL-KDD and 80.38% on UNSW-NB15
Rajadurai and Gandhi (2020)	DoS, R2L, U2R, and Probe	Stacked ensemble model	NSL-KDD	Accuracy score 91.06%
Tao et al. (2021)	Jamming attacks	Deep reinforcement learning	NSL-KDD	Real UAV data detection in terms of time slots
Wang et al. (2019)	Simulated anomalies	LSTM	Real UAV data	Accuracy score 99.7%
Devan and Khare (2020)	DoS, R2L, U2R, and Probe	NSL-KDD	XGBoost-DNN	Accuracy score 97.6%
Jiang et al. (2020a)	DoS, R2L, U2R, and Probe	NSL-KDD and UNSW-NB15	CNN-BiLSTM	Accuracy scores of 83.58% on NSL-KDD and 77.16% on UNSW-NB15

TABLE 2 Layer-wise cybersecurity threats to smart drones.

Layer	Cybersecurity threat	Detection using machine learning
Perception layer	Spoofing attacks	SVM (Panice et al., 2017), dynamic selection (Talaei Khoei et al., 2022), and K-learning model (Shafique et al., 2021)
	Jamming attacks	Q-learning (Gupta et al., 2022; Sajid et al., 2022), and DQN (Thanh et al., 2022)
Communication layer	Eavesdropping attacks	SVM-KNN (Hoang et al., 2019) and Ensemble learning (Das et al., 2023)
	Denial of service attack	Neural networks (Butt et al., 2020) and Q-learning (Yaseen and Al-Saadi, 2023)
Control layer	Command injection attack	Decision tree (Vuong et al., 2015)
	Traffic blockage	Q-learning (Shingate et al., 2020)
System layer	Malware attacks	Q/Dyna-Q/PDS (Xiao et al., 2017)
	Intrusion	(Alsheikh et al., 2014), SVM (Alsheikh et al., 2014), Neural network (Almiani et al., 2020), and kNN (Liu et al., 2022)

architecture. The study's goals include reducing privacy dangers, addressing cybersecurity difficulties, minimizing interception pandemonium, and establishing strong security measures. A tiered strategy is used to accomplish these objectives by methodically reviewing the analysis methodologies and security problems inside each layer, therefore strengthening data security in traditional drone activities/operations. The layered structure also makes future improvements easier to integrate. Machine intelligence, as applied through machine learning classifiers, is critical in enhancing drone data security. Figure 1 depicts the suggested framework.

As has been observed, UAV communication networks and smart grid communication protocols have several similarities in terms of architecture, types of data exchanged, and the security concerns they encounter. Below is a detailed discussion of these parallels:

1. Decentralized and distributed architecture: It is noteworthy, therefore, that no such principle is for sale and that the civil service, the putative repository of these principles, has been moving in the opposite direction.

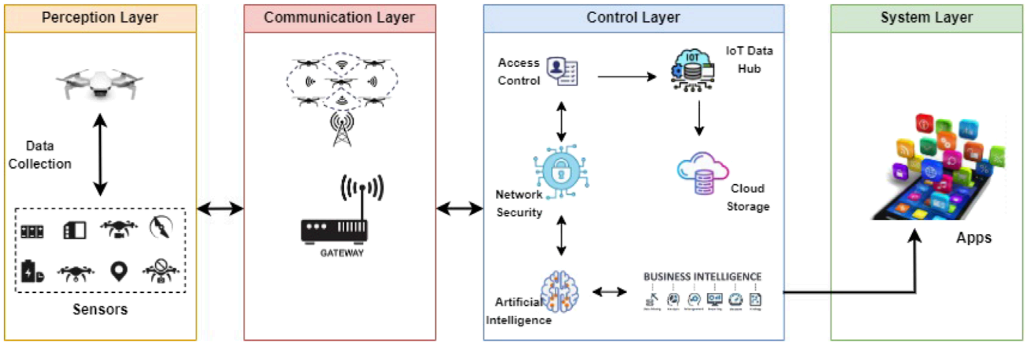

FIGURE 1
Layer-wise architecture for drone security.

- *UAV communication networks:* UAVs may act as an independent system even though they can be a part of a swarm or closely cooperating fleet of drones that communicate with one another and with a base station. The dynamism in the network requires the network to accommodate distributed nodes such as the drones that may often come and go.
- Smart grid communication protocols: Smart grids are focused by nature and consist of numerous servers like smart meters, sensors, substations, and control centers. The distributed nature must have reliable communication protocols to ensure proper data exchange between different components.

2. Real-time data transmission:
    - UAV communication networks: UAVs include many features with continuous, high-speed data transceiving processes in areas such as navigation, environment sensing, and task performing. It is perhaps obvious that a breakdown or even delay in this communication can have catastrophic consequences and that no solution should be considered if it may interfere with the continuing flow of the communication.
    - Smart grid communication protocols: Similarly, a smart grid requires a real-time information display for controlling electrical distribution. The data acquired in real-time are essential in terms of absorbing the loads, identifying the faults, and the overall stability of the grids. Failure in communication might result in the establishment of power breakdown or failure of demand response systems.
3. High-reliability requirements:
    - Security and privacy challenges: Of significant importance to the UAV networks is the reliability of the traffic. This is more so when the drones are either fully autonomous or remotely controlled. The communication system provided for this system must be very resilient to loss of signal, interference, and other issues that may arise without affecting the mission.
    - UAV communication networks: In smart grids, communication reliability is equally important because of the changes in the supply and demand of energy. High reliability is expected to ensure stability, especially during peak load incidences.
4. Security and privacy challenges:
    - UAV communication networks: UAVs are subject to various cyber threats, such as jamming, spoofing, and unauthorized access. Security of the communication network must be ensured, as adversaries can tap the network or modify the data being transferred.
    - Smart grid communication protocols: A smart grid has many security concerns and risks, including hacking of the communication network with a view of cutting off the power supply or hacking to access consciousness. The two systems must have protection as they engage in their communications; this includes encryption, authentication, and intrusion detection (Shiaeles et al., 2012).
5. Scalability:
    - UAV communication networks: The network should be expandable; that is, it should be capable of incorporating a few UAVs at a certain time and a few more or less at other times, depending on the mission. The proposed communication protocol should also effectively address resource constraints in the system, such as bandwidth and power in several UAVs.
    - Smart grid communication protocols: Smart grids must be flexible by allowing the incorporation of other energy sources, devices, and technologies. The communication protocols must be designed in a way that they are capable of simultaneously embracing this flood of data and the ever-growing number of connected devices without compromising performance (Ramsdale et al., 2020).
6. Integration with IoT:
    - UAV communication networks: Drones can work in parallel with IoT systems in collecting, analyzing, and transmitting data and information. This implies that the communication network must be compatible with the IoT devices and hence may present other layers of security and compatibility issues.
    - Smart grid communication protocols: The smart grid forms an important part of the IoT, controlling millions of devices and connecting them to enhance the grid's functioning and consumption. The communication protocols should

guarantee the compatibility of IoT devices to the general network and keep the security of the interconnected systems in check (Shiaeles and Papadaki, 2015).

The advent of compact UAVs has unlocked fresh opportunities in multiple civilian applications. Nevertheless, due to the absence of sophisticated infrastructure and planning, these state-of-the-art devices face vulnerabilities related to security and privacy. Although progress in the realm of the IoDs and the IoT offers promising opportunities, it simultaneously gives rise to fresh security and privacy concerns. The current circumstances do not sufficiently guarantee data privacy and security, diminishing the IoDT's reliability.

3.1 Structured framework for ensuring the security of intelligent drones

A layered architecture for drone security within cyberphysical systems (CPS) is systematically divided into several essential layers:

- Perception layer: Operating at the lowest level is the perception layer, which is responsible for data acquisition from the drone's various sensors, such as cameras, GPS, and gyroscopes, among others. The result is that these data are further subjected to extensive processing and analysis, thus creating a complex model of the environment surrounding the drone. In addition, it is engaged in identifying potential threats at an early stage to promptly guard the drone's security and integrity. The architectural design of a drone includes carrying a mini drone or quadcopter capable of housing a camera. This layer is then enriched with IoT sensor data updates comprising complex sensors such as cameras, GPS, and radars, among others. It also enables the drone to feel its surroundings to collect important data and relay such information to the next level in real-time (Siracusano et al., 2018).
- Communication layer: The communication layer adapts the crucial task of enabling the flow of data between the drone and its ground control station (GCS). Here, the data transmission is done securely using secure protocols to pass information from one point to the other to avoid cases of intrusion and modification. The secure communication layer plays an important role in ensuring that communications are secure and the data are not tampered with in the process. Thus, to address the security of data transmitted through the communication layer, encryption and cryptographic techniques are embraced to minimize vulnerability to eavesdropping and data tampering. This layer aims at data credibility and proper transfer and sharing with the cloud layer. It connects to different wired, mobile, and wireless gateway devices, with Wi-Fi as a high-speed transmission. Connecting devices to the cloud, data security, caching, and data flooding are well managed in this layer by a well-designed system. The Azure IoT gateway is the connection path in the cloud with design principles that are informed by research on IoT gateway architecture.
- Control layer: Operating at an abstract level to the layers discussed above is the control layer: this layer is responsible for the planning and coordination of a drone's movement and is situated at a strategic location within the architecture. It also employs information from the concern or perception layer to prevent potential risks in its operations and movements. In addition, it also acts as the drone's guardian; it is responsible for identifying and isolating hostile action through the help of advanced anomaly detection and intrusion prevention systems. The fourth layer of the control layer is known for its capability for identifying and discouraging malicious attempts. In terms of function, the control layer involves device authentication and access security, which are best enhanced by utilizing prototypes. It also complies with data safety standards and security that are critical to the IoT structure. Furthermore, privacy concerns are also stated and addressed because they give rise to risks that could compromise the system. To minimize the security risks, the control layer strictly executes the authentication systems and protocols. It is also aware of potential intruders' efforts to violate the security loopholes by penetrating, faking, interposing, and or launching denial of service (DoS) attacks (Alsubai et al., 2024).
- System layer: The system layer is responsible for the coherence of the drone's subordination, including such essential sections as power, navigation, and communication subsystems. In this layer, a well-interlinked security structure begins to develop to prevent any unauthorized access and control of the drone. These protective measures include firmware signing and a trusted execution environment to strengthen the operational system of the drone and prevent unauthorized control and alteration of its components. The system layer implements firmware signing and a trusted execution environment to protect the drone's important parts from code tampering and invasive procedures. IoT gateways are important components in IoT systems that help intermediaries connect IoT devices with a hub situated in the cloud. They add another layer of security through, for example, the identification of devices and connection management. The hub is the main access point of the IoT and IoT applications, and therefore, it is responsible for communication between IoT devices, applications, cloud systems, and other connected devices. Strict security measures are in place to restrict access to authorized devices. Data collected from sensors within tagged networks and drones are transmitted to a cryptographic blockchain client, ensuring secure storage within a database hosted in the cloud server.

4 Potential cybersecurity risks in smart grid cyberphysical systems

In this section, specific key challenges in terms of cybersecurity and focus on the concerns and risks with regard to smart grid structures are identified. In general, there are two main risks associated with a smart grid: the dependency of the grid's complex systems on AI-automated communications and the propensity for intelligent cyber warfare activities (Haider et al., 2022).

4.1 Unauthorized access to control systems

Probably one of the gravest threats of smart grid systems is when the attackers gain access to the control stations of the grid because this lets them control the flow of energy, alter the supply distribution system, or even cause blackouts. This threat is particularly pervasive in smart grids because of the cascading relationship that exists between their cyber and the physical layers. As is the case with many UAV control systems, smart grid infrastructures need strict access control to protect critical processes.

4.2 GPS spoofing and data injection attacks

In smart grids, GPS signals are crucial for synchronizing energy distribution across large areas. Like UAVs, smart grids are susceptible to GPS spoofing, where false signals can mislead the system into incorrect actions, leading to power instability. Attackers can inject false data into the grid's sensor networks, potentially manipulating energy flow or causing misalignment in grid synchronization.

4.3 DoS (denial of service) attacks

DoS attacks in smart grid systems target communication channels, overwhelming them with excessive data and disrupting normal grid functions. Like UAV systems, these attacks can prevent real-time monitoring and control of energy distribution, leading to power blackouts or failures in critical infrastructure. Implementing real-time monitoring and anomaly detection powered by AI can mitigate the risk of DoS attacks.

4.4 Malware and command injection attacks

Smart grid control systems are at risk of malware infiltration, which may affect control centers, sensors, or automated units. Like UAVs, introducing malicious software into these systems can result in unauthorized commands, data breaches, or even damage to vital infrastructure. To defend against such threats, secure communication protocols, prompt system updates, and effective intrusion detection mechanisms are necessary.

4.5 Traffic blockage and eavesdropping

Disruptions in smart grid communication channels, like traffic blockages, can prevent critical information from reaching its destination, leading to system failures or poor energy distribution. Eavesdropping threatens the privacy of grid operations. Employing strong encryption, frequency-hopping, and secure communication protocols is essential to mitigate these vulnerabilities, as they are crucial in UAV systems.

4.6 AI and malware defense

As AI's role in smart grids grows, the threat of malware on AI controls increases. Malicious actors can manipulate AI algorithms to produce false outputs, causing poor energy management decisions. Securing AI systems with strong cybersecurity measures like secure boots, digital signatures, and advanced threat detection is vital to protect smart grid functions.

5 Securing drones

A proper system for drone security is needed to prevent attacks and examine attack data to execute protective measures that maintain drone safety. In analyzing the requirements of constructing a dependable and lawful system in the domain of IoD, the following pivotal characteristics have been identified: security, dependability, and consistency. Although some studies have developed deep learning models to improve the cybersecurity of sensors for wireless networks and mobile nets, the case of drones' security domain has not been examined. Therefore, to enhance the security of drones, this study examines a deep learning-based approach for optimizing authentication and gaining access control mechanisms. This research work has primarily addressed cyberphysical systems and UAV threats rather than smart grid cyberattacks for multiple reasons, including the unavailability of benchmark datasets and technical and infrastructure constraints (setting up experiments for smart grid systems often requires specialized infrastructure, such as access to real energy grids, smart meters, and control systems), which may not be feasible in a typical research setting.

This research has utilized the KDD dataset, which shares characteristics of both cyberphysical and smart grids. Originally intended for detecting network intrusions in traditional computing environments, the KDD Cup 99 dataset exhibits several features applicable to smart grid cybersecurity. Both smart grids and traditional computer networks depend significantly on communication protocols and the exchange of data between interconnected systems. The WSN-DS dataset is tailored to detect intrusions in wireless sensor networks, which are crucial in both UAV communications and smart grid networks. These systems extensively use sensors: UAVs for monitoring their surroundings and smart grids for overseeing energy distribution. The CICIDS2017 dataset is a contemporary intrusion detection dataset designed to capture intricate attack patterns like distributed denial of service (DDoS), botnets, and advanced persistent threats (APT). These cyberthreats increasingly challenge both UAVs and smart grids. In the context of smart grids, a DDoS attack can saturate communication links, obstructing energy distribution, like the potential for disruption in UAV networks through interference in communications. The dataset's emphasis on complex, multi-layered attacks aligns with the intricate vulnerabilities of smart grids, where attacks can target both digital and physical systems to cause service interruptions.

5.1 Datasets for intrusion detection

An IDS is crucial for improving the state of cybersecurity because it identifies and prevents unauthorized access and cyberattacks on the networks. The fundamental data sources for an IDS are a variety of datasets that help it detect an intrusion successfully and efficiently. Such datasets equip the system with the required and relevant knowledge as well as background knowledge to evaluate a scenario and make a decision.[1,2,3,4]

The experiments used data collected on a real-time basis through the drones and included essential GPS information such as longitude, latitude, and altitude. The dataset by Alturki et al. (2023), which comprises drone on-board diagnostics (OBD) data, was also integrated. Such a large set of records allows for assessing the model's performance and its ability to address diverse, realistic, and constantly changing conditions.

The KDD Cup 99 dataset is constituted of data used in the KDD Cup, an annual competition for data mining and machine learning organized by the KDD conference. The data for this set have been compiled from different sources with the intention of examining the real environment. It includes all the details of the network traffic, including connections, size of packets, and types of protocol, thus mirroring real-life network conditions. Additionally, it encompasses data regarding security breaches, DoS attacks, and various forms of network intrusions. The dataset is bifurcated into two segments: a training set for model development and training purposes and a test set for assessing model performance. Widely adopted in research, the KDD Cup 99 dataset has been featured in many academic articles.

It is important that two connection records, or 136,489 and 136,497, were excluded from use in the testing procedure. This curation of data by NSL-KDD ensures that the machine learning algorithm does not bend the results by inclining toward a particular conclusion. The abuse identification is especially suitable for the KDD Cup 99 dataset because it has some shortcomings manifested in the ability to capture real-time characteristics of the network throughput. The statistics relevant to the KDD Cup 99, Drone dataset, and NSL-KDD are discussed in detail in the Table 3. Realized for IDSs in wireless sensor networks, the WSN-DS dataset was developed by Singh et al. (2020) and Khan et al. (2024). It includes four different kinds of DoS attacks: blackhole, grayhole, flooding, and scheduling. Specific protocols employed in the experiment include hierarchical low-energy adaptive clustering (LEACH) protocol data gathered by using the network simulator-2 (NS-2). After that, data preprocessing was conducted, which led to the identification of 23 characteristics. For this purpose, a real-world WSN-DS dataset is used.

One of the real-world network traffic datasets is the CICIDS2017 dataset (Stiawan et al., 2020), which focuses on the current network activities, both normal and anomalous. More emphasis was placed on the practical recording of the background traffic data using the B-profile technology during the development. This non-malicious traffic collection is for 25 users, and the protocols include HTTP, HTTPS, FTP, SSH, and email. Original network traffic data were captured systematically for five consecutive days, with 1 day for normal traffic and the following 4 days with incorporated attack. The injection attacks in the dataset are brute force FTP, brute force SSH, DoS, heartbleed, web assaults, infiltration, botnet activities, and DDoS. It is worth mentioning that the dataset's producers believe that their collection meets 11 key criteria specified in previous research. Please see Table 4 for more information on the CICIDS2017 dataset, which includes extensive statistics and details.

TABLE 3 Details of KDD Cup 99, Drone, and NSL-KDD datasets.

Attack type	Description
Normal	Normal, legitimate network traffic and activities that do not exhibit any malicious or intrusive behavior
DoS	Denial of service attack aims to disrupt services and make them inaccessible
Probe	Probe is an initial reconnaissance step to identify potential entry points
R2L	Remote-to-local attacks occur when an attacker attempts to gain unauthorized access to a target system from a remote location
U2R	User-to-root attacks involve gaining unauthorized access to a user account and then attempting to gain administrative or root-level access to the system

TABLE 4 Details of the CICIDS2017 dataset.

Attack type	Description
Normal	This category represents normal, benign network traffic and activities
SSH Patator	SSH Patator is a type of attack where an attacker attempts to gain unauthorized access to a system by using an automated tool that systematically tries various username and password combinations for secure shell (SSH) authentication
FTP Patator	Attackers use automated tools to try multiple username and password combinations to gain unauthorized access to FTP servers
DoS	Denial of service attacks disrupt normal network operations with a flood of traffic or requests
Web	Web attacks include various types of malicious activities targeting web applications and services
Bot	Bot attacks involve the deployment of a network of compromised computers (botnets) to perform coordinated malicious activities
DDoS	Distributed denial of service attacks involve a network of compromised devices working together to flood a target system with traffic, causing a denial of service
PortScan	Port scanning is a reconnaissance technique used by attackers to discover open ports and services on a target system

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

[2] https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds

[3] https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset

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

TABLE 5 Experimental setup for the proposed system.

Element	Details
Language	Python 3.8
OS	64-bit Windows 10
RAM	32 GB
GPU	Nvidia, 1060, 8 GB
CPU	Intel Xeon eight-core CPUs with 2.8 GHz processor

TABLE 6 Results of deep learning models on KDD Cup 99.

Model	Accuracy	Precision	Recall	F1-score
CNN	89.10%	87.23%	85.43%	86.31%
LSTM	92.25%	93.82%	94.86%	92.84%
CNN-LSTM	95.11%	95.31%	98.21%	96.16%
ConvLSTM	**99.99%**	**99.99%**	**99.99%**	**99.99%**

The bold values indicating that the proposed model accuracy is better than all other models compared with it.

5.2 Deep learning models

Convolutional neural networks (CNNs) have exceptional feature extraction capabilities, making them useful for a broad range of applications such as image classification, recognition, and a variety of other fields (Bhatt et al., 2021). Although CNNs are most typically linked with computer vision tasks (Terkawi et al., 2018), their applications extend to areas such as forgery analysis (Diallo et al., 2020) and intrusion detection (Chen et al., 2020). Through convolution and pooling layers, CNNs excel at effectively extracting critical characteristics from raw data. CNNs, as opposed to traditional multi-layered neural networks, are a feed-forward deep learning model with distinct characteristics such as parameter sharing and sparse interaction. These characteristics distinguish them from the completely connected networks where each of the input neurons is connected with all the output neurons.

LSTM is a type of RNN model with a feedback connection (Yu et al., 2019; Abu-zanona et al., 2022). The important feature of LSTM is that it considers the whole data sequence, not data points, as RNN does, and, therefore, is ideal for jobs that require time-series data processing and classification. Usually, long data sequences pose difficulties to the computation of gradients for RNNs, which gives rise to LSTM. One of the key aspects of LSTM network design is the cell memory unit, which has the capability of both forgetting the old knowledge and storing new inputs. The LSTM model is made up of four major components: the input gate, the forget gate, the output gate, and the cell state, which are depicted as four LSTM gates.

The network layer parameters of CNN-LSTM architecture can be adjusted to suit one's preference (Lu et al., 2020). A pooling layer and a dense layer are frequently used in a sequence convolutional LSTM layer. In each layer, filter size, kernel size, and stride can be adjusted to alter the model's performance and learning rate. This allows the number of parameters to be changed, directly influencing the model's performance. Dependent inputs are first accepted by the convolutional layer, and the result from this layer is then passed into the pooling layer to reach the LSTM layer. The CNN-LSTM architecture has been used in many tasks, such as human activity recognition (Mutegeki and Han, 2020; Albalas et al., 2019) and forecasting gold prices (Livieris et al., 2020).

5.3 Proposed approach

The proposed neural network model combines the features of both CNN and LSTM layers. CNNs have excellent feature extraction capabilities, making them useful in a variety of applications. Through convolution and pooling layers, CNN efficiently extracts meaningful features from raw data. CNN is a kind of feed-forward deep learning model that offers parameter sharing and sparse interaction characteristics while differing from a multi-layered deep neural network that is fully connected (each input neuron being interconnected with each output neuron). In other words, under CNN, feature extraction is enhanced while the connection's complexity is reduced. An LSTM is an extension of a recurrent neural network that has feedback connections. Although other types of RNNs, like RNN, work point by point in the datasets, LSTM works end to end and hence can easily handle and solve time-series data algorithms and classification.

ConvLSTM is an advanced version of LSTM that includes convolutional operations inside the LSTM cell. It represents a particular kind of RNN that proves to be efficacious for modeling long-term dependencies in a specific manner. Unlike the standard LSTM structures, in ConvLSTM, matrix operations in each of the gates of the cell are replaced with convolution operations. This modification is useful for extracting spatial features in multi-dimensional data, making the ConvLSTM model superior to the basic CNN-LSTM model. Because of its flexibility and applicability in various fields, ConvLSTM has been used in travel demand prediction, slip direction identification, and agriculture forecasting. ConvLSTM is a powerful tool in the field of deep learning domains; the best part of the ConvLSTM architecture is that it smoothly incorporates both spatial and temporal features, which in turn helps to provide better and more accurate predictions from multi-dimensional data. The proposed model's complete working algorithm is shared in Algorithm 1.

6 Results and discussion

This section presents the outcomes of the experiments following the discussion of suggested models in the preceding section. The results demonstrate the effectiveness of drones in enhancing security, as discerned through a deep learning-based approach. Four assessment criteria were employed to evaluate and contrast the prototype performances, with the confusion matrix being a pivotal tool in these evaluations. The confusion matrix comprises key elements, including true positive (TP), false positive (FP), true negative (TN), and false negative (FN).

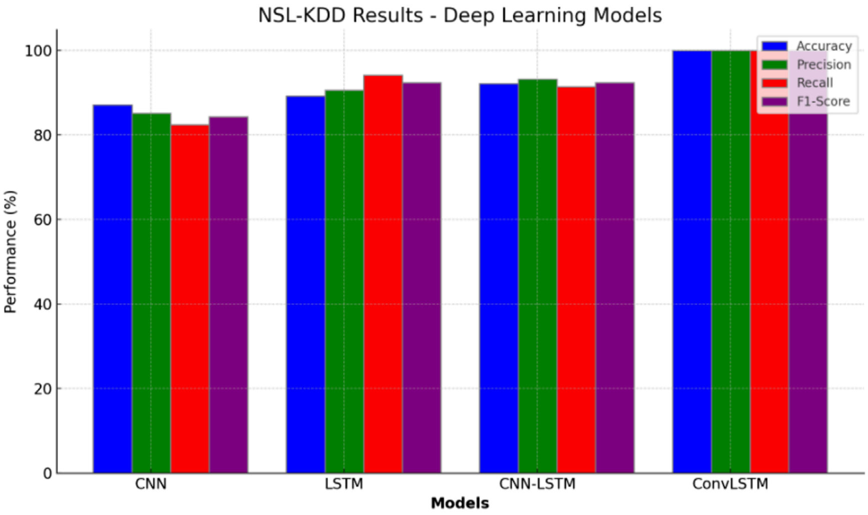

FIGURE 2
Results of deep learning models on NSL-KDD.

TABLE 7 Results of deep learning models on NSL-KDD.

Model	Accuracy	Precision	Recall	F1-score
CNN	87.10%	85.13%	82.42%	84.35%
LSTM	89.25%	90.62%	94.16%	92.34%
CNN-LSTM	92.21%	93.21%	91.41%	92.37%
ConvLSTM	**99.99%**	**99.99%**	**99.99%**	**99.99%**

The bold values indicating that the proposed model accuracy is better than all other models compared with it.

6.1 Experimental results

The results of the experiments are provided in this section. The proposed model's performance is evaluated on five datasets. The results are also compared to other cutting-edge approaches from the existing literature. The datasets were divided into 70:30 training and testing sets. The tests are carried out on a Dell PowerEdge T430 GPU with an 8 GB graphics card, as well as twin Intel Xeon eight-core CPUs running at 2.8 GHz and 32 GB of DDR4 RAM. The studies were done in the Jupyter Notebook environment, with Python and Anaconda as programming languages. Additional information is provided in Table 5.

In this research, the CNN, LSTM, CNN-LSTM, and ConvLSTM deep learning models were employed. These models underwent a comprehensive comparative analysis using five publicly available datasets: KDD Cup 99, NSL-KDD, Drone, WSN-DS, and CICIDS 2017. The primary objective of this analysis was to evaluate the effectiveness of these deep learning models in the context of intrusion detection within UAVs or drones. The results of deep learning models on KDD Cup-99 presented in Table 6 and Figure 2 provide a comprehensive overview of their performance. CNN achieved an accuracy of 89.10%, indicating the percentage of correctly classified instances. Its precision, recall, and F1-score are 87.23%, 85.43%, and 86.31%, respectively. The LSTM model demonstrated higher accuracy, reaching 92.25%. The hybrid model (CNN-LSTM) performed exceptionally well, with an accuracy of 95.11%. It also exhibited a high precision of 95.31% and a recall of 98.21%, leading to an F1-score of 96.16%. However, the ConvLSTM model outperformed all others, achieving an astonishing accuracy of 99.99%. It also achieved exceptional precision, recall, and F1-score, all 99.99%.

Table 7 and Figure 3 summarize the performance of various deep learning models on the NSL-KDD dataset for intrusion detection. CNN achieved an accuracy of 87.10%, with corresponding precision, recall, and F1-score values of 85.13%, 82.42%, and 84.35%, respectively. LSTM showed an accuracy of 89.25% and performed well with 90.62% precision, 94.16% recall, and 92.34% F1-score. CNN-LSTM achieved an accuracy of 92.21%, and ConvLSTM demonstrated exceptional results, with accuracy, precision, recall, and an F1-score of 99.99%.

Table 8 and Figure 4 display the performance results of various deep learning models for intrusion detection on the WSN-DS dataset. The CNN achieved 90.10% accuracy, 87.23% precision, 89.83% recall, and 88.71% F1-score. LSTM demonstrated an accuracy of 94.25%, and CNN-LSTM exhibited an accuracy of 97.31%. ConvLSTM outperformed the other models with remarkable results, showing an accuracy of 99.99%.

Table 9 presents the performance results of various deep learning models on the CICIDS2017 dataset, which is used for intrusion detection. CNN achieved an accuracy of 91.10% and demonstrated good performance in precision, recall, and F1-score. LSTM showed an accuracy of 95.25% and performed well in precision, although it had a slightly lower recall and F1-score. CNN-LSTM exhibited high accuracy, scoring 98.11%, and also delivered excellent results in precision, recall, and F1-score. ConvLSTM outperformed the other models with outstanding results, achieving an accuracy, precision, recall, and F1-score of 99.99%.

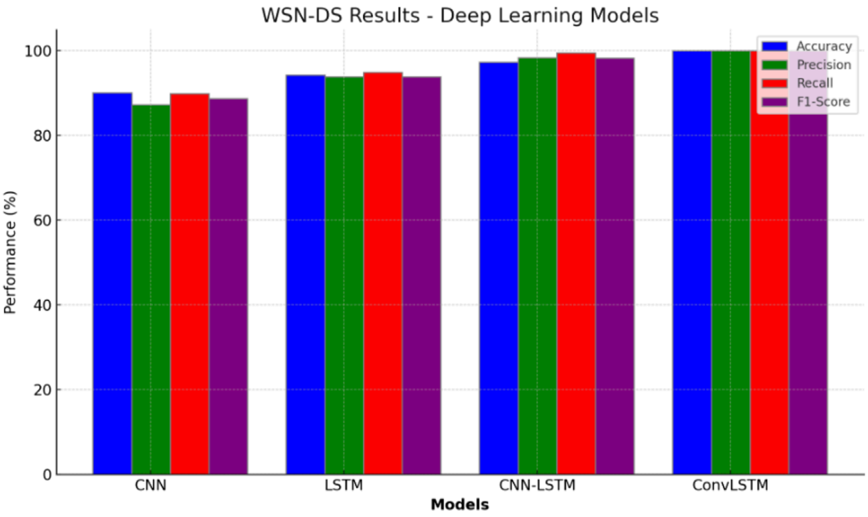

FIGURE 3
Results of deep learning models on WSN-DS.

TABLE 8 Results of deep learning models on WSN-DS.

Model	Accuracy	Precision	Recall	F1-score
CNN	90.10%	87.23%	89.83%	88.71%
LSTM	94.25%	93.82%	94.86%	93.84%
CNN-LSTM	97.31%	98.31%	99.51%	98.26%
ConvLSTM	**99.99%**	**99.99%**	**99.99%**	**99.99%**

The bold values indicating that the proposed model accuracy is better than all other models compared with it.

Table 10 presents the results of deep learning models on the Drone dataset. CNN achieved an accuracy of 87.10% and showed good performance in precision (88.23%), recall (87.43%), and F1-Score (86.31%). LSTM demonstrated an accuracy of 90.25%, and CNN-LSTM exhibited an accuracy of 94.11%. ConvLSTM outperformed the other models with outstanding results, achieving accuracy, precision, recall, and F1-score of 99.99%. This suggests that ConvLSTM is highly effective in making accurate predictions on the Drone dataset.

The ConvLSTM model is highly effective in identifying intrusions in UAV and smart grid communication systems, thanks to its capability to concurrently capture spatial and temporal characteristics. The convolutional layers within the model efficiently learn local patterns from spatial information, while the LSTM units manage temporal relationships, making the model ideally designed for complex time-series data such as intrusion detection (Wu et al., 2020). Furthermore, the hybrid structure of ConvLSTM overcame the limitations seen in standalone CNN and LSTM models, resulting in improved generalization and heightened accuracy for processing sequential network data (Altunay and Albayrak, 2023). Research indicates that ConvLSTM models surpass traditional machine learning techniques in detecting advanced cyberattacks, especially in UAV networks where the data involve temporal dependencies and spatial correlations (Dubey et al., 2024). The model's exceptional performance is further supported by leveraging large, varied datasets, which boost its robustness and adaptability to various network conditions (Sharafaldin et al., 2018). This flexibility is vital in environments like smart grids and UAVs, where threats are dynamic and constantly evolving.

6.2 Statistical analysis

This subsection presents the results of a statistical *t*-test analysis between the two best-performing models on all datasets. The *t*-test results for comparing CNN-LSTM and ConvLSTM models across different datasets are as follows:

- KDD Cup-99:
  - t-statistic = −5.35
  - *p*-value = 0.0127
- NSL-KDD:
  - t-statistic = −20.84
  - *p*-value = 0.0002
- WSN-DS:
  - t-statistic = −3.64
  - *p*-value = 0.0356
- CICIDS 2017:
  - t-statistic = −41.98
  - *p*-value = 0.00003
- Drone dataset:
  - t-statistic = −3.51
  - *p*-value = 0.0391

In all cases, the *p*-values are below the significance level (0.05), indicating that the performance differences between CNN-LSTM and ConvLSTM are statistically significant, with ConvLSTM outperforming CNN-LSTM.

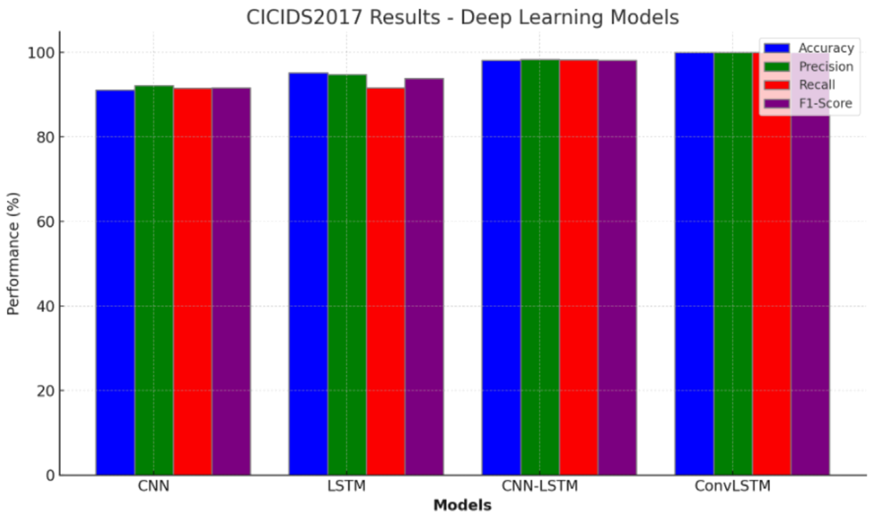

FIGURE 4
Results of deep learning models on CICIDS 2017.

TABLE 9 Results of deep learning models on CICIDS 2017.

Model	Accuracy	Precision	Recall	F1-score
CNN	91.10%	92.23%	91.53%	91.61%
LSTM	95.25%	94.82%	91.66%	93.84%
CNN-LSTM	98.11%	98.31%	98.21%	98.16%
ConvLSTM	**99.99%**	**99.99%**	**99.99%**	**99.99%**

The bold values indicating that the proposed model accuracy is better than all other models compared with it.

TABLE 10 Results of deep learning models on the Drone dataset.

Model	Accuracy	Precision	Recall	F1-score
CNN	87.10%	88.23%	87.43%	86.31%
LSTM	90.25%	91.82%	93.86%	92.74%
CNN-LSTM	94.11%	92.31%	98.21%	96.76%
ConvLSTM	**99.99%**	**99.99%**	**99.99%**	**99.99%**

The bold values indicating that the proposed model accuracy is better than all other models compared with it.

6.3 Sensitivity analysis

The sensitivity analysis demonstrates that while the ConvLSTM model maintains high performance metrics across various hyperparameters, slight adjustments can affect specific performance measures such as accuracy, precision, recall, and F1 score. The results indicate a strong robustness in the model, reinforcing its suitability for intrusion detection in UAV communication networks. This analysis highlights the importance of hyperparameter tuning in optimizing model performance for various operational conditions. The results of the sensitivity analysis on the Drone dataset are shared in Table 11.

6.4 Comparing the performance of the proposed ConvLSTM method to existing approaches

Table 12 presents the performance comparison of the proposed approach alongside state-of-the-art models on different datasets. The comparison table includes the dataset name, the method used, and the corresponding accuracy achieved by each method. The proposed ConvLSTM method outperforms other models, achieving an accuracy of 99.99%. Comparatively, the deep neural model (Andresini et al., 2020) achieved an accuracy of 92.49%, and the DNN model (Vinayakumar et al., 2019) achieved 93% accuracy on the KDDCup-99 dataset. In contrast, the SVM-ANN model (Hussain et al., 2016) achieved an accuracy of 91.48%, the deep hierarchical model (Jiang et al., 2020b) achieved 83.58% accuracy, and the DNN model (Vinayakumar et al., 2019) attained 80% accuracy on NSL-KDD dataset. The DNN model (Vinayakumar et al., 2019) obtained an accuracy of 99.2% on the WSN-DS dataset and 96.3% on the CICIDS-2017 dataset. The RegressionNet model (Alturki et al., 2023) reached an accuracy of 99.89%. Overall, the proposed ConvLSTM method consistently demonstrates superior performance across all datasets compared to the referenced state-of-the-art models, highlighting its effectiveness in intrusion detection.

6.5 Discussion

Table 12 shows the performance of four deep learning models: CNN, LSTM, CNN-LSTM, and ConvLSTM. The performance of

TABLE 11 Sensitivity analysis results for the ConvLSTM model on the Drone dataset.

Learning rate	Batch size	Layers	Dropout rate	Sequence length	Accuracy (%)	Precision (%)	Recall (%)	F1 score (%)
0.00375	64	2	0.1082	30	98.01	99.94	99.96	98.03
0.00951	64	5	0.4880	42	98.05	98.46	98.93	99.87
0.00732	64	5	0.4330	85	99.04	98.18	99.71	99.12
0.00599	64	5	0.1849	67	98.80	99.23	99.35	98.77
0.00157	128	4	0.1727	31	98.09	98.76	98.90	98.03

TABLE 12 Comparative analysis of the proposed methodology and state-of-the-art model performance.

Dataset	Approach	Accuracy
KDDCup-99	Deep neural model (Andresini et al., 2020)	92.49%
	DNN (Vinayakumar et al., 2019)	93%
	Proposed ConvLSTM	**99.99%**
NSL-KDD	SVM-ANN (Hussain et al., 2016)	91.48%
	Deep hierarchical model (Jiang et al., 2020b)	83.58%
	DNN (Vinayakumar et al., 2019)	80%
	Proposed ConvLSTM	**99.99%**
WSN-DS	DNN Vinayakumar et al., 2019)	99.2%
	Proposed ConvLSTM	**99.99%**
CICIDS-2017	DNN (Vinayakumar et al., 2019)	96.3%
	Proposed ConvLSTM	**99.99%**
Drone	RegressionNet (Alturki et al., 2023)	99.89%
	Proposed ConvLSTM	**99.99%**

The bold values indicating that the proposed model accuracy is better than all other models compared with it.

each model is assessed, and the corresponding values are shown in the table. ConvLSTM performs better than the others, with the highest accuracy, precision, recall, and F1-score of 99.99%. The findings derived from the study involving experiments on those various datasets for intrusion detection in UAVs or drones help evaluate deeper models' efficiency. The figures clearly show that the proposed ConvLSTM model performs exceptionally well in all the datasets used in the experiments, with an accuracy of 99.99% PDR on all the datasets, implying the model's excellent performance on intrusion detection in UAV's communication network. Such accuracy is important for strongly securing UAV

```
Input: ConvLSTM model and Datasets {KDD Cup-99, NSL-KDD, WSN-DS, CICIDS 2017, Drone}
Output: Evaluation metrics (Accuracy, Precision, Recall, F1-score)
Step 1: Data Preprocessing
For each dataset:
  Load the dataset
  Normalize and standardize feature values
  Split the dataset into training and testing sets
Step 2: ConvLSTM Model Training
 Initialize the ConvLSTM model architecture
 For each dataset:
  Train the ConvLSTM model on the training set
  Use cross-validation for hyperparameter tuning
Step 3: Model Evaluation
 For each dataset:
  Test the trained ConvLSTM model on the testing set
  Calculate evaluation metrics:
   Accuracy = $\frac{TP+TN}{TP+TN+FP+FN}$
   Precision = $\frac{TP}{TP+FP}$
   Recall = $\frac{TP}{TP+FN}$
   F1-score = $2 \times \frac{Precision \times Recall}{Precision+Recall}$
Step 4: Comparison of Results
 Compare the evaluation metrics across all five datasets
 Highlight performance differences of the ConvLSTM model
Step 5: Conclusion
 Analyze the ConvLSTM model's strengths and weaknesses across datasets
 Provide recommendations for future work based on performance results
```

Algorithm 1. Evaluation of ConvLSTM Model Using KDD Cup-99, NSL-KDD, WSN-DS, CICIDS 2017, and Drone datasets.

operations, unauthorized access, or cyberthreats that could lead to critical consequences. This outcome supports the understanding that more complex neural network architectures are needed for fully modeling both spatial and temporal structures of traffic data obtained from drone networks.

The datasets used in those experiments were selected in a manner that matches realistic business environments. They include various types of network traffic and intrusions that may exist in a mission field using UAVs. The datasets give a range of intrusions such as DoS, unauthorized access, probing, etc. This diversity ensures that intrusion detection models are exposed to a wide range of challenges, increasing their immunity to new challenges. These datasets, therefore, act as the gold standard against which the performance of intrusion detection models can be measured.

Last but not least, findings from such experiments demonstrate that ConvLSTM outperforms other models and, at the same time, stresses the necessity to leverage high-quality datasets for training and testing IDS solutions in the UAV setting. Both datasets are fundamental as they contribute to the formulation of effective security measures for drones, thus bringing safety to countless uses.

7 Conclusion

This work has explored the fundamental domain of cybersecurity for unmanned aerial vehicles (UAVs), which are increasingly integrated into various sectors, including agriculture, surveillance, and logistics. As UAV technology continues to advance, the need for robust IDS to protect these communication networks from cyber threats has become critical.

7.1 Findings

In this study, we investigated four deep learning models—CNN, LSTM, CNN-LSTM, and ConvLSTM—within the context of intrusion detection in UAV communication networks. Among these models, the ConvLSTM model demonstrated superior performance, achieving an accuracy of 99.99% across multiple datasets. This high level of accuracy suggests that complex neural network structures like ConvLSTM can be effectively leveraged to enhance cybersecurity for UAVs, offering a promising solution to counter evolving cyber threats.

7.2 Limitations

Despite the high accuracy of the ConvLSTM model, some limitations exist in this research. First, the datasets used, while diverse, may not cover all potential cyberattack scenarios that UAVs could encounter in real-world applications. Additionally, the computational complexity of ConvLSTM could pose a challenge for real-time deployment on resource-constrained UAV systems, limiting its practicality in some cases. Lastly, this study focused on intrusion detection by ignoring other factors of UAV cybersecurity, such as real-time anomaly detection or attack mitigation techniques.

7.3 Recommendations

Future research should address these limitations by exploring lighter, more efficient models that can be deployed in real-time on UAV systems with limited computational power. Furthermore, it would be beneficial to incorporate more diverse and representative datasets that simulate a wider range of cyberattacks in realistic environments. Expanding the scope to include real-time anomaly detection and response mechanisms could further enhance the robustness of UAV cybersecurity frameworks. Additionally, collaboration between cybersecurity experts and UAV manufacturers is recommended to develop standardized security protocols that can be integrated directly into the design of UAV communication networks.

7.4 Conclusion

The findings of this study highlight the potential of ConvLSTM models to improve the safety, security, and reliability of UAV operations across various industries. As UAVs become more prevalent in daily activities, enhancing intrusion detection techniques will be crucial in minimizing cyber threats and ensuring the safe deployment of these systems.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material; further inquiries can be directed to the corresponding author.

Author contributions

RA: conceptualization, data curation, formal analysis, funding acquisition, investigation, methodology, project administration, resources, software, supervision, validation, visualization, writing–original draft, and writing–review and editing.

Funding

The author(s) declare that financial support was received for the research, authorship, and/or publication of this article. The authors extend their appreciation to the Deanship of Scientific Research, University of Hafer Al Batin for funding this work through the research group project No. (0025-1443-S).

Conflict of interest

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Aboueleneen, N., Alwarafy, A., and Abdallah, M. (2023). "Secure and energy-efficient communication for internet of drones networks: a deep reinforcement learning approach," in *2023 international wireless communications and mobile computing (IWCMC)* (IEEE), 818–823.

Abro, G. E. M., Zulkifli, S. A. B., Masood, R. J., Asirvadam, V. S., and Laouti, A. (2022). Comprehensive review of uav detection, security, and communication advancements to prevent threats. *Drones* 6, 284. doi:10.3390/drones6100284

Abu Al-Haija, Q., and Zein-Sabatto, S. (2020). An efficient deep-learning-based detection and classification system for cyber-attacks in iot communication networks. *Electronics* 9, 2152. doi:10.3390/electronics9122152

Abu-zanona, M., Elaiwat, S., Younis, S., Innab, N., and Kamruzzaman, M. (2022). Classification of palm trees diseases using convolution neural network. *Int. J. Adv. Comput. Sci. Appl.* 13, 10–14569. doi:10.14569/ijacsa.2022.01306111

Administration, F. A. (2019). FAA national forecast FY 2019-2039 full forecast document and tables. *Tech. Rep*.

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., and Ahmad, F. (2021). Network intrusion detection system: a systematic study of machine learning and deep learning approaches. *Trans. Emerg. Telecommun. Technol.* 32, e4150. doi:10.1002/ett.4150

Albalas, S., A'aqoulah, A., Alraoush, A., Ibdah, S., and Innab, N. (2019). Factors affecting the stability of faculty members at jordanian public universities. *Int. J. Public Sect. Perform. Manag.* 5, 178–188. doi:10.1504/ijpspm.2019.10019394

Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S., and Razaque, A. (2020). Deep recurrent neural network for iot intrusion detection system. *Simul. Model. Pract. Theory* 101, 102031. doi:10.1016/j.simpat.2019.102031

Alsheikh, M. A., Lin, S., Niyato, D., and Tan, H.-P. (2014). Machine learning in wireless sensor networks: algorithms, strategies, and applications. *IEEE Commun. Surv. and Tutorials* 16, 1996–2018. doi:10.1109/comst.2014.2320099

Alsubai, S., Umer, M., Innab, N., Shiaeles, S., and Nappi, M. (2024). Multi-scale convolutional auto encoder for anomaly detection in 6g environment. *Comput. and Industrial Eng.* 194, 110396. doi:10.1016/j.cie.2024.110396

Altunay, H. C., and Albayrak, Z. (2023). A hybrid cnn+lstm-based intrusion detection system for industrial iot networks. *Eng. Sci. Technol. Int. J.* 38, 101322. doi:10.1016/j.jestch.2022.101322

Alturki, N., Aljrees, T., Umer, M., Ishaq, A., Alsubai, S., Saidani, O., et al. (2023). An intelligent framework for cyber–physical satellite system and iot-aided aerial vehicle security threat detection. *Sensors* 23, 7154. doi:10.3390/s23167154

Andresini, G., Appice, A., Di Mauro, N., Loglisci, C., and Malerba, D. (2020). Multi-channel deep feature learning for intrusion detection. *IEEE Access* 8, 53346–53359. doi:10.1109/access.2020.2980937

Ateya, A. A. A., Muthanna, A., Kirichek, R., Hammoudeh, M., and Koucheryavy, A. (2019). Energy-and latency-aware hybrid offloading algorithm for uavs. *IEEE Access* 7, 37587–37600. doi:10.1109/access.2019.2905249

Bader, D., Innab, N., Atoum, I., and Alathamneh, F. (2023). The influence of the internet of things on pharmaceutical inventory management. *Int. J. Data Netw. Sci.* 7, 381–390. doi:10.5267/j.ijdns.2022.9.009

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 Trans. Veh. Technol.* 69, 9097–9111. doi:10.1109/tvt.2020.3000576

Bhatt, D., Patel, C., Talsania, H., Patel, J., Vaghela, R., Pandya, S., et al. (2021). Cnn variants for computer vision: history, architecture, application, challenges and future scope. *Electronics* 10, 2470. doi:10.3390/electronics10202470

Bithas, P. S., Michailidis, E. T., Nomikos, N., Vouyioukas, D., and Kanatas, A. G. (2019). A survey on machine-learning techniques for uav-based communications. *Sensors* 19, 5170. doi:10.3390/s19235170

Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., et al. (2020). A review of machine learning algorithms for cloud computing security. *Electronics* 9, 1379. doi:10.3390/electronics9091379

Challita, U., Ferdowsi, A., Chen, M., and Saad, W. (2019). Machine learning for wireless connectivity and security of cellular-connected uavs. *IEEE Wirel. Commun.* 26, 28–35. doi:10.1109/mwc.2018.1800155

Chen, L., Kuang, X., Xu, A., Suo, S., and Yang, Y. (2020). "A novel network intrusion detection system based on cnn," in *2020 eighth international conference on advanced cloud and big data (CBD) (IEEE)*, 243–247.

Consul, P., Budhiraja, I., Chaudhary, R., and Kumar, N. (2022). "Security reassessing in uav-assisted cyber-physical systems based on federated learning," in *MILCOM 2022-2022 IEEE military communications conference (MILCOM)* (IEEE), 61–65.

Danev, B., Zanetti, D., and Capkun, S. (2012). *On physical-layer identification of wireless devices*. New York, NY: Association for Computing Machinery. 45 (1).

Das, K., Ghosh, C., and Karmakar, R. (2023). "Eavesdropping attack detection in uavs using ensemble learning," in *2023 second international conference on electrical, electronics, information and communication technologies (ICEEICT)* (IEEE), 01–07.

Devan, P., and Khare, N. (2020). An efficient xgboost–dnn-based classification model for network intrusion detection system. *Neural Comput. Appl.* 32, 12499–12514. doi:10.1007/s00521-020-04708-x

Diallo, B., Urruty, T., Bourdon, P., and Fernandez-Maloigne, C. (2020). Robust forgery detection for compressed images using cnn supervision. *Forensic Sci. Int. Rep.* 2, 100112. doi:10.1016/j.fsir.2020.100112

Donkol, A.-B., Hafez, A., Hussein, A., and Mabrook, M. (2023). Optimization of intrusion detection using likely point pso and enhanced lstm-rnn hybrid technique in communication networks. *IEEE Access* 11, 9469–9482. doi:10.1109/access.2023.3240109

Dubey, K., Dubey, R., Panedy, S., and Kumar, S. (2024). A review of iot security: machine learning and deep learning perspective. *Procedia Comput. Sci.* 235, 335–346. International Conference on Machine Learning and Data Engineering (ICMLDE 2023). doi:10.1016/j.procs.2024.04.034

Gao, X., Shan, C., Hu, C., Niu, Z., and Liu, Z. (2019). An adaptive ensemble machine learning model for intrusion detection. *Ieee Access* 7, 82512–82521. doi:10.1109/access.2019.2923640

Guerber, C., Royer, M., and Larrieu, N. (2021). Machine learning and software defined network to secure communications in a swarm of drones. *J. Inf. Secur. Appl.* 61, 102940. doi:10.1016/j.jisa.2021.102940

Gupta, C., Johri, I., Srinivasan, K., Hu, Y.-C., Qaisar, S. M., and Huang, K.-Y. (2022). A systematic review on machine learning and deep learning models for electronic information security in mobile networks. *Sensors* 22, 2017. doi:10.3390/s22052017

Haider, M., Ahmed, I., and Rawat, D. B. (2022). "Cyber threats and cybersecurity reassessed in uav-assisted cyber physical systems," in *2022 thirteenth international conference on ubiquitous and future networks (ICUFN)* (IEEE), 222–227.

Hoang, T. M., Nguyen, N. M., and Duong, T. Q. (2019). Detection of eavesdropping attack in uav-aided wireless systems: unsupervised learning with one-class svm and k-means clustering. *IEEE Wirel. Commun. Lett.* 9, 139–142. doi:10.1109/lwc.2019.2945022

Hu, J., Pota, H. R., and Guo, S. (2014). Taxonomy of attacks for agent-based smart grids. *IEEE Transactions on Parallel and Distributed Systems* 25 (7), 1886–1895. doi:10.1109/TPDS.2013.301

Hussain, J., Lalmuanawma, S., and Chhakchhuak, L. (2016). A two-stage hybrid classification technique for network intrusion detection system. *Int. J. Comput. Intell. Syst.* 9, 863–875. doi:10.1080/18756891.2016.1237186

Ivanov, L. I., Obukhova, N. A., and Baranov, P. S. (2020). "Review of modern uav detection algorithms using methods of computer vision," in *2020 IEEE conference of Russian young researchers in electrical and electronic engineering (EIConRus)* (IEEE), 322–325.

Jiang, K., Wang, W., Wang, A., and Wu, H. (2020a). Network intrusion detection combined hybrid sampling with deep hierarchical network. *IEEE access* 8, 32464–32476. doi:10.1109/access.2020.2973730

Jiang, K., Wang, W., Wang, A., and Wu, H. (2020b). Network intrusion detection combined hybrid sampling with deep hierarchical network. *IEEE Access* 8, 32464–32476. doi:10.1109/access.2020.2973730

Khan, A., Gupta, S., and Gupta, S. K. (2022). Emerging uav technology for disaster detection, mitigation, response, and preparedness. *J. Field Robotics* 39, 905–955. doi:10.1002/rob.22075

Khan, Z., Alfwzan, W. F., Ali, A., Innab, N., Zuhra, S., Islam, S., et al. (2024). Intelligent computing for electromagnetohydrodynamic bioconvection flow of micropolar nanofluid with thermal radiation and stratification: levenberg–marquardt backpropagation algorithm. *AIP Adv.* 14. doi:10.1063/5.0187124

Kurunathan, H., Huang, H., Li, K., Ni, W., and Hossain, E. (2023). Machine learning-aided operations and communications of unmanned aerial vehicles: a contemporary survey. *IEEE Commun. Surv. and Tutorials* 26, 496–533. doi:10.1109/comst.2023.3312221

Liu, G., Zhao, H., Fan, F., Liu, G., Xu, Q., and Nazir, S. (2022). An enhanced intrusion detection model based on improved knn in wsns. *Sensors* 22, 1407. doi:10.3390/s22041407

Livieris, I. E., Pintelas, E., and Pintelas, P. (2020). A cnn–lstm model for gold price time-series forecasting. *Neural Comput. Appl.* 32, 17351–17360. doi:10.1007/s00521-020-04867-x

Lu, W., Li, J., Li, Y., Sun, A., and Wang, J. (2020). A cnn-lstm-based model to forecast stock prices. *Complexity* 2020, 1–10. doi:10.1155/2020/6622927

Majeed, S., Sohail, A., Qureshi, K. N., Iqbal, S., Javed, I. T., Crespi, N., et al. (2022). Coverage area decision model by using unmanned aerial vehicles base stations for *ad hoc* networks. *Sensors* 22, 6130. doi:10.3390/s22166130

Manesh, M. R., Kenney, J., Hu, W. C., Devabhaktuni, V. K., and Kaabouch, N. (2019). "Detection of gps spoofing attacks on unmanned aerial systems," in *2019 16th IEEE annual consumer communications and networking conference (CCNC)* (IEEE), 1–6.

Mbow, M., Koide, H., and Sakurai, K. (2021). "An intrusion detection system for imbalanced dataset based on deep learning," in *2021 ninth international symposium on computing and networking (CANDAR)*, 38–47.

Metke, A. R., and Ekl, R. L. (2010). Security technology for smart grid networks. *IEEE Trans. Smart Grid* 1, 99–107. doi:10.1109/tsg.2010.2046347

Mutegeki, R., and Han, D. S. (2020). "A cnn-lstm approach to human activity recognition," in *2020 international conference on artificial intelligence in information and communication (ICAIIC)* (IEEE), 362–366.

Nassi, B., Bitton, R., Masuoka, R., Shabtai, A., and Elovici, Y. (2021). "Sok: security and privacy in the age of commercial drones," in *2021 IEEE symposium on security and privacy (SP)* (IEEE), 1434–1451.

Panice, G., Luongo, S., Gigante, G., Pascarella, D., Di Benedetto, C., Vozella, A., et al. (2017). "A svm-based detection approach for gps spoofing attacks to uav," in *2017 23rd international conference on automation and computing (ICAC)* (IEEE), 1–11.

Rajadurai, H., and Gandhi, U. D. (2020). A stacked ensemble learning model for intrusion detection in wireless network. *Neural Comput. Appl.* 34, 15387–15395. doi:10.1007/s00521-020-04986-5

Ramsdale, A., Shiaeles, S., and Kolokotronis, N. (2020). A comparative analysis of cyber-threat intelligence sources, formats and languages. *Electronics* 9, 824. doi:10.3390/electronics9050824

Rani, S., Kataria, A., Chauhan, M., Rattan, P., Kumar, R., and Sivaraman, A. K. (2022). Security and privacy challenges in the deployment of cyber-physical systems in smart city applications: state-of-art work. *Mater. Today Proc.* 62, 4671–4676. doi:10.1016/j.matpr.2022.03.123

Robakowska, M., Skezak, D., Tyranska-Fobke, A., Nowak, J., Robakowski, P., Zuratynski, P., et al. (2019). Operational and financial considerations of using drones for medical support of mass events in Poland. *Disaster Med. Public Health Prep.* 13, 527–532. doi:10.1017/dmp.2018.106

Rogers, J. (2018). "Small states and armed drones," in *Small states and the new security environment* (Odense, Denmark: University of Iceland).

Sajid, M. B. E., Ullah, S., Javaid, N., Ullah, I., Qamar, A. M., and Zaman, F. (2022). Exploiting machine learning to detect malicious nodes in intelligent sensor-based systems using blockchain. *Wirel. Commun. Mob. Comput.* 2022, 1–16. doi:10.1155/2022/7386049

Sapre, S., Ahmadi, P., and Islam, K. (2019). A robust comparison of the kddcup99 and nsl-kdd iot network intrusion detection datasets through various machine learning algorithms. *arXiv Prepr. arXiv:1912.13204*. doi:10.48550/arXiv.1912.13204

Shafique, A., Mehmood, A., and Elhadef, M. (2021). Detecting signal spoofing attack in uavs using machine learning models. *IEEE access* 9, 93803–93815. doi:10.1109/access.2021.3089847

Shakeri, R., Al-Garadi, M. A., Badawy, A., Mohamed, A., Khattab, T., Al-Ali, A. K., et al. (2019). Design challenges of multi-uav systems in cyber-physical applications: a comprehensive survey and future directions. *IEEE Commun. Surv. and Tutorials* 21, 3340–3385. doi:10.1109/comst.2019.2924143

Sharafaldin, I., Lashkari, A. H., and Ghorbani, A. A. (2018). "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proceedings of the 4th international conference on information systems security and privacy - volume 1: ICISSP* (Setúbal, Portugal: INSTICC SciTePress), 108–116. doi:10.5220/0006639801080116

Shiaeles, S. N., Katos, V., Karakos, A. S., and Papadopoulos, B. K. (2012). Real time ddos detection using fuzzy estimators. *Comput. and Secur.* 31, 782–790. doi:10.1016/j.cose.2012.06.002

Shiaeles, S. N., and Papadaki, M. (2015). Fhsd: an improved ip spoof detection method for web ddos attacks. *Comput. J.* 58, 892–903. doi:10.1093/comjnl/bxu007

Shingate, K., Jagdale, K., and Dias, Y. (2020). Adaptive traffic control system using reinforcement learning. *Int. J. Eng. Res. Technol.* 9. doi:10.17577/IJERTV9IS020159

Shone, N., Ngoc, T. N., Phai, V. D., and Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Trans. Emerg. Top. Comput. Intell.* 2, 41–50. doi:10.1109/tetci.2017.2772792

Singh, N., Virmani, D., and Gao, X.-Z. (2020). A fuzzy logic-based method to avert intrusions in wireless sensor networks using wsn-ds dataset. *Int. J. Comput. Intell. Appl.* 19, 2050018. doi:10.1142/s1469026820500182

Siracusano, M., Shiaeles, S., and Ghita, B. (2018). "Detection of lddos attacks based on tcp connection parameters," in *2018 global information infrastructure and networking symposium (GIIS)* (IEEE), 1–6.

Stiawan, D., Idris, M. Y. B., Bamhdi, A. M., Budiarto, R., and Budiarto, R. (2020). Cicids-2017 dataset feature analysis with information gain for anomaly detection. *IEEE Access* 8, 132911–132921. doi:10.1109/access.2020.3009843

Talaei Khoei, T., Ismail, S., and Kaabouch, N. (2022). Dynamic selection techniques for detecting gps spoofing attacks on uavs. *Sensors* 22, 662. doi:10.3390/s22020662

Tao, J., Han, T., and Li, R. (2021). Deep-reinforcement-learning-based intrusion detection in aerial computing networks. *IEEE Netw.* 35, 66–72. doi:10.1109/mnet.011.2100068

Terkawi, A., Innab, N., al Amri, S., and Al-Amri, A. (2018). "Internet of things (iot) increasing the necessity to adopt specific type of access control technique," in *2018 21st Saudi computer society national computer conference (NCC)*, 1–5. doi:10.1109/NCG.2018.8593084

Thanh, P. D., Giang, H. T. H., and Hong, I.-P. (2022). Anti-jamming ris communications using dqn-based algorithm. *IEEE Access* 10, 28422–28433. doi:10.1109/access.2022.3158751

Umer, M., Sadiq, S., Karamti, H., Alhebshi, R. M., Alnowaiser, K., Eshmawi, A., et al. (2022). Deep learning-based intrusion detection methods in cyber-physical systems: challenges and future trends. *Electronics* 11, 3326. doi:10.3390/electronics11203326

Vinayakumar, R., Alazab, M., Soman, K., Poornachandran, P., Al-Nemrat, A., and Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *Ieee Access* 7, 41525–41550. doi:10.1109/access.2019.2895334

Vuong, T. P., Loukas, G., Gan, D., and Bezemskij, A. (2015). "Decision tree-based detection of denial of service and command injection attacks on robotic vehicles," in *2015 IEEE international workshop on information forensics and security (WIFS)* (IEEE), 1–6.

Wang, A., Wang, W., Zhou, H., and Zhang, J. (2021). Network intrusion detection algorithm combined with group convolution network and snapshot ensemble. *Symmetry* 13, 1814. doi:10.3390/sym13101814

Wang, B., Wang, Z., Liu, L., Liu, D., and Peng, X. (2019). "Data-driven anomaly detection for uav sensor data based on deep learning prediction model," in *2019 prognostics and system health management conference (PHM-Paris)* (IEEE), 286–290.

Wang, Y., Sun, G., Cao, X., and Yang, J. (2022). An intrusion detection system for the internet of things based on the ensemble of unsupervised techniques. *Wirel. Commun. Mob. Comput.* 2022, 1–11. doi:10.1155/2022/8614903

Wang, Z., and Ghaleb, F. (2023). An attention-based convolutional neural network for intrusion detection model. *IEEE Access* 11, 43116–43127. doi:10.1109/access.2023.3271408

Wu, Q., Zhou, Y., Wu, X., Liang, G., Ou, Y., and Sun, T. (2020). Real-time running detection system for UAV imagery based on optical flow and deep convolutional networks. *IET Intell. Transp. Syst.* 14, 278–287. doi:10.1049/iet-its.2019.0455

Xiao, L., Li, Y., Huang, X., and Du, X. (2017). Cloud-based malware detection game for mobile devices with offloading. *IEEE Trans. Mob. Comput.* 16, 2742–2750. doi:10.1109/tmc.2017.2687918

Xiao, L., Lu, X., Xu, D., Tang, Y., Wang, L., and Zhuang, W. (2018). Uav relay in vanets against smart jamming with reinforcement learning. *IEEE Trans. Veh. Technol.* 67, 4087–4097. doi:10.1109/tvt.2018.2789466

Yan, Y., Qian, Y., Sharif, H., and Tipper, D. (2012). A survey on smart grid communication infrastructures: motivations, requirements and challenges. *IEEE Commun. Surv. and Tutorials* 15, 5–20. doi:10.1109/surv.2012.021312.00034

Yaseen, H. S., and Al-Saadi, A. (2023). Q-learning based distributed denial of service detection. *Int. J. Electr. Comput. Eng.* 13, 972. doi:10.11591/ijece.v13i1.pp972-986

Yu, Y., Si, X., Hu, C., and Zhang, J. (2019). A review of recurrent neural networks: lstm cells and network architectures. *Neural Comput.* 31, 1235–1270. doi:10.1162/neco_a_01199