IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 1 June 2024, accepted 27 June 2024, date of publication 10 July 2024, date of current version 20 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3426028

SURVEY

Forensic Examination of Drones: A Comprehensive Study of Frameworks, Challenges, and Machine Learning Applications

ELHAAM ABDULRAHMAN DEBAS[1], ABDULLAH ALBUALI[2], (Member, IEEE), AND M. M. HAFIZUR RAHMAN[2]

[1]College of Computer Science and Information Technology, King Faisal University (KFU), Al Hassa 31982, Saudi Arabia
[2]Department of Computer Networks Communications, King Faisal University (KFU), Al Hassa 31982, Saudi Arabia

Corresponding author: Elhaam Abdulrahman Debas (223002140@student.kfu.edu.sa)

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia, under Grant KFU241345.

ABSTRACT Unmanned Aerial Vehicles (UAVs) have evolved into necessary assets across various sectors, motivating a need for strong controllability technologies in applications like flight path enhancement and avoiding obstacles. This survey offers a comprehensive exploration of drone forensics, providing an extensive literature review on models and methodologies for examining malfunctions and attacks. Including key challenges, from machine learning applications to autopilot systems, the survey spans evidence collection techniques, incorporating neural network architectures like Transformers in forensic investigations. Real-world scenarios and forensic examination tools employed by law enforcement are discussed, illuminating the complex process of drone analysis, particularly in conflict areas. The paper delves into the role of machine learning in intrusion detection and attack classification, highlighting both challenges and recent advancements in drone detection. Outlining future research opportunities for the field of study, it highlights the importance of standardized methodologies in drone forensics. These research directions aim to overcome current obstacles and contribute to more effective solutions for detecting evasive malware. This investigation contributes valuable insights into the multifaceted landscape of drone forensics, offering a roadmap for ongoing research at the intersection of technology and law.

INDEX TERMS UAV, drone forensics, machine learning, intrusion detection.

ABBREVIATIONS

The following abbreviations are used in this review:

SLR	Systematic Literature Review
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
UAVs	Unmanned Aerial Vehicles
GCS	Ground Control Stations
IoT	Internet of Things
M2M	Machine-to-Machine
IoFT	Internet of Flying Things
GUI	Graphical User Interface
CCAFM	Comprehensive Collection and Analysis Forensic Model
Ue-IoE	UAV-enabled IoE
ICT	Information and Communication Technology
NLP	Natural Language Processing
ALFA	AirLab Failure and Anomaly
DRF	Drone Forensics
RF	Radio Frequency
MLP	Machine Learning Process
OC-SVMs	One-Class Support Vector Machines
LOF	Local Outlier Factor
ML	Machine Learning
NIST	National Institute of Standards and Technology
NN	Neural Network

The associate editor coordinating the review of this manuscript and approving it for publication was Mohammad J. Abdel-Rahman.

MLP	Multi-Layer Perceptrons
SVMs	Support Vector Machines
eVTOLs	electric Vertical Take-Off and Landing aircraft
OEM	Original Equipment Manufacturer
SAE	Society of Automotive Engineers
CAVs	Connected and Autonomous Vehicles
UASs	Unmanned Aircraft Systems

I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs), commonly known as drones, signify a noteworthy leap in aircraft technology. These autonomous flying machines, devoid of human pilots, can either be operated remotely by skilled individuals or programmed to follow predetermined flight paths [1]. With a dual classification distinguishing them into civilian and military sectors, UAVs play diverse roles in contemporary society. In the civilian domain, these remarkable aerial devices have proven their utility across various fields. In agriculture, UAVs contribute to precision farming, optimizing crop management. During disaster relief efforts, their capabilities aid in swift response and assessment. Additionally, UAVs significantly enhance the monitoring and observation of extensive construction sites, revolutionizing project management and safety protocols.

Conversely, military-grade UAVs, designed for precision and strategic applications, play a pivotal role in bolstering national security. They are employed for crucial tasks like border surveillance, safeguarding territorial integrity, and transmitting incursion data to specialised Ground Control Stations (GCS) or dedicated servers specifically designed for this purpose [2]. This unique set of skills underscores the indispensable role of UAVs in ensuring the security and defence of nations.

UAV technology has recently garnered considerable interest and enthusiasm from academic and business spheres alike. Their inherent flexibility and adaptability have spurred groundbreaking research and development, showcasing their potential to challenge established paradigms and provide innovative solutions to various problems [3]. The versatility of UAVs is vividly illustrated in Figure. 1, emphasising their impact across different domains. The evolving landscape of UAVs promises continued advancements, making them a focal point for exploration and innovation.

The survey questions that the paper covers are:

- What are the open issues in the drone forensics field?
- What are the challenges in the forensics examination of drones?
- What are the future directions in the drone forensics field?

In this paper, the survey methodology is systematically outlined in Section II, employing the PRISMA flow diagram to depict the meticulous process of literature selection for the analysis. Section III conducts a thorough literature survey, exploring the current landscape of drone forensics and categorizing diverse research contributions. Subsequently, Section IV discusses the identified challenges, advancements, and open issues in the field, critically assessing existing methodologies. Section V narrows the focus to the specific challenges encountered in the forensic examination of drones. In Section VI, a comparative analysis with other review papers is undertaken to validate findings and identify research gaps. Section VII propels the discourse forward, delineating future research directions and offering insights into potential areas for innovation. The paper concludes in Section VIII, summarising major findings and emphasising the significance of sustained research and development efforts in the dynamic realm of drone forensics. Figure 2 presented the paper outline.

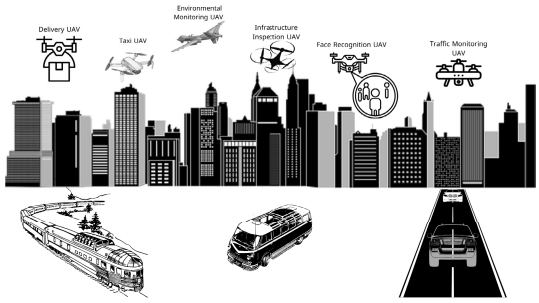


FIGURE 1. UAV types.

II. SURVEY METHODOLOGY

A three-stage systematic literature search was carried out in compliance with the PRISMA guidelines, a helpful tool for managing the data flow [4]. The search terms "(Drone OR UAV) AND (Simulation OR Real) AND (Machine learning OR Attack) OR (Drone dataset OR Drone Forensics)" during the identification stage were used to search Google Scholar and the Saudi Digital Library which have papers from different publishers such as IEEE, MDPI, and Springer. The search covered only peer-reviewed publications published between 2016 and 2023. Studies discussing the forensics investigation of drone malfunctions and attacks met the inclusion criteria. Thirty articles in all were chosen for this review of the literature. The PRISMA methodology is shown in Figure 3. During the identification stage, items are chosen for inspection. Because of several factors, including duplicate entries and an automation tool called Zotero designating them as ineligible, 71,148 records were removed through this stage before screening. In this phase, the papers undergo screening and selection for review articles that were examined for their title and abstract during the screening stage were disqualified because they did not nearly meet the criteria. For inclusion at the eligibility stage, the papers meet the requirements. At the included stage, a list of the studies that will be part of the systematic review will be created. 30 of the articles that were chosen for inclusion in the included stage were later rejected for various reasons, including being out of range, written in

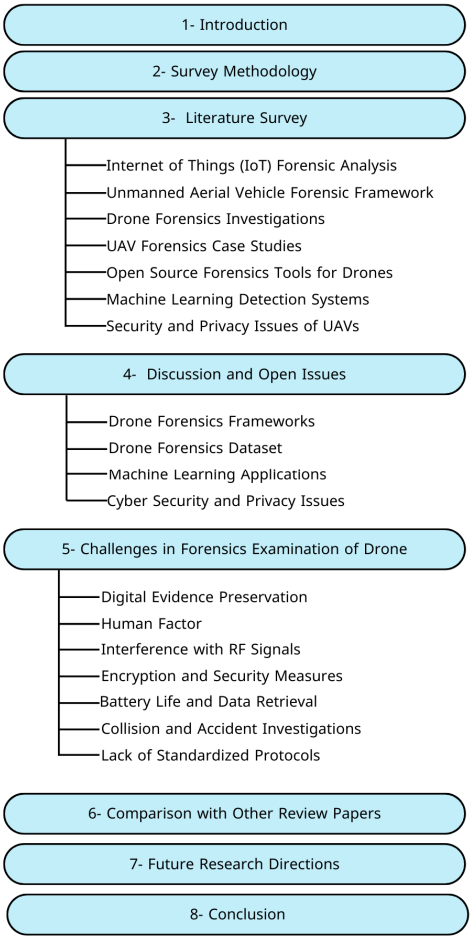


FIGURE 2. Paper outline.

a foreign language, or lacking access to the records. This left 30 articles selected for review.

III. LITERATURE SURVEY

In this section, research papers are presented and reviewed, illustrating certain models that may be utilized for forensic analysis of drone malfunctions and attacks. Additionally, concerns and obstacles connected to drone forensics, machine learning, datasets, and autopilot are highlighted. This section presents the important conclusions from each chosen paper. (see tab 10).

A. INTERNET OF THINGS (IOT) FORENSIC ANALYSIS

Mazhar et al. [5] put forth a Machine-to-Machine (M2M) framework-based intelligent forensic analysis mechanism that can automatically identify attacks on IoT devices. The M2M framework was developed by leveraging a diverse set of forensic analytic tools and machine learning to identify various types of attacks. Furthermore, the introduction of a third-party logging server addressed the challenge of gathering evidence during attacks on IoT devices. IoT device forensics in a directly connected environment were more

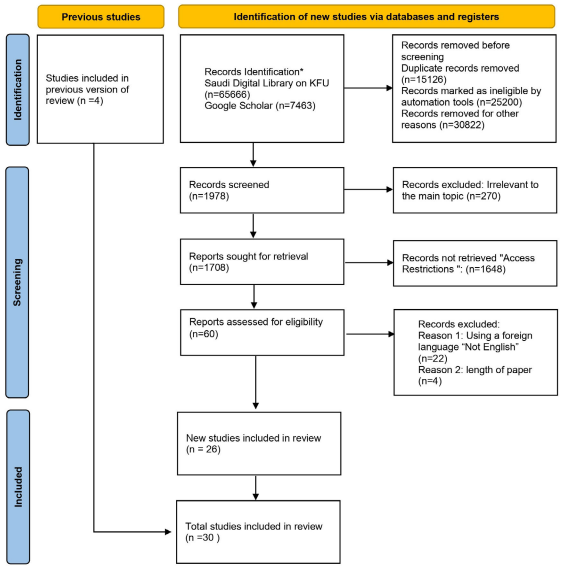


FIGURE 3. Literature review using PRISMA.

reliable and efficient with the proposed forensic system. Network traffic was diverted to the logging server without interfering with device connectivity, where it was then evaluated by comparing it with rules. To detect attacks, several machine-learning models have been created and tested. The decision tree algorithm's maximum accuracy was 97.29%. When a Pi camera was installed on the network, their proposed solution was tested in a real-time setting. With the decision tree having the maximum accuracy of 96.01%, the performance of machine learning models was marginally decreased. The characteristics of the attack type, the number of times an attack was conducted, and the suggested course of action were then described in several reports.

Ahmed et al. [6] explored the growing use of UAVs in STEM (science, technology, engineering, and mathematics) project-based learning and emphasized the risks that staff, students, and educators may encounter when using inexpensive consumer drones that are vulnerable to cutting-edge cyberattacks. The ECU-IoFT dataset was created in response to the dearth of publicly accessible labeled datasets illustrating cyberattacks on the Internet of Flying Things (IoFT). The ECU-IoFT dataset structure consisted of several key features, including the ID, which is an integer that identifies a collected sample; the timestamp of the collected sample; the source and destination addresses of the collected sample; the protocol used; the length of the frame in bytes; captured details about the sample; binary classification; identifying the type of attack; and the attack scenario in which the sample was collected.

Liu et al. [7] provided a detailed analysis of the potential and challenges of using UAVs to increase the capabilities of the Internet of Everything (IoE). They talked about the IoE and its three key expectations, which are diversity, intelligence, and scalability. They also covered the IoE's enabling technologies, which include big data analytics,

cloud computing, and the Internet of Things (IoT). They presented a UAV-enabled IoE (Ue-IoE) solution that integrates UAVs with contemporary Information and Communication Technology (ICT) technologies to enhance the scalability, intelligence, and diversity of IoE. They also discussed the main issues and problems (coverage, battery, computing, and security constraints) that hindered the realization of IoE. They emphasized how the IoE powered by UAVs has the potential to transform several sectors, including disaster relief, transportation, and agriculture.

B. UNMANNED AERIAL VEHICLE FORENSIC FRAMEWORK

Renduchintala et al. [8] described a drone forensic paradigm that includes both hardware/physical and digital forensics and was determined to be appropriate for the analysis of drone activity following takeoff. The authors developed a model that can examine the drone parts at the crime scene in the context of physical forensics. Also, they provided a robust digital drone forensic program that used JavaFX 8.0 to create a Graphical User Interface (GUI) and was largely focused on the examination of crucial drone log metrics. They have developed a tool that can handle several representations of sensor recordings without any hiccups or lags. The tool included several tabs that could display different flight data at once and used Google Maps to correctly plot the flight path.

Jain et al. [9] proposed a framework to aid in the systematic analysis of a drone through a series of 12 stages and to analyze the basic architecture of a drone. Privacy infringement is one of the most important problems with drone operations. Also, they proposed a generic drone forensic model that would improve the digital investigation process. They recommended how to perform forensics on various drone components, such as the camera and Wi-Fi. To verify the different phases in the suggested structure, they looked at five commercial drones: the DJI Phantom 2.0, Parrot AR, Drone 2.0, the Syma X5C-4CH, the Align M690L Multicopter, and the IRIS+3BR. The proposed drone forensic framework was divided into 12 phases that aid in understanding the fundamental drone architecture.

C. DRONE FORENSICS INVESTIGATIONS

Alotaibi et al. [10] discussed the importance of gathering and preserving evidence from drones for forensic analysis. They highlighted the need for a standardized and unbiased approach in drone forensics, addressing gaps in existing models biased towards specific drone systems. The authors introduced the Comprehensive Collection and Analysis Forensic Model (CCAFM), combining existing processes into a unified model. CCAFM facilitates the collection, safeguarding, reconstruction, and analysis of both volatile and nonvolatile data from suspect drones. This model could enhance drone forensic procedures and security protocols, serving as a guide for future studies in the field.

Mozaffari et al. [11] provided key guidelines on how to analyze, optimize, and design UAV-based wireless communication systems and presented a thorough tutorial on the possible advantages and uses of UAVs in wireless communications. Furthermore, a thorough investigation was conducted into the significant difficulties and fundamental tradeoffs in UAV-enabled wireless networks. Then, unresolved issues and prospective future areas for study in UAV communications were presented. Finally, a variety of analytical frameworks and mathematical methods are discussed, including game theory, stochastic geometry, optimization theory, machine learning, and transport theory. The application of such tools for solving certain UAV issues was also demonstrated.

Alotaibi et al. [12] offered a proactive forensic viewpoint that has been absent from the DRF literature, as well as a research article on a novel forensic readiness framework applicable to the drone forensics field. They contend that a proactive rather than reactive strategy can aid in the identification, capture, preservation, reconstruction, analysis, and documentation of drone incidents. They examined the body of research on DRF and noted any gaps in the field. Proactive forensics and reactive forensics are the two stages of their new forensic readiness framework. Proactive forensics is the first step, where potential drone incidents are anticipated and prepared for before they happen. Reactive forensics, the second step, deals with handling real-world drone incidents.

Editya et al. [13] presented the idea of using the Transformer to aid in the forensic examination of a drone engine malfunction. The Transformer's three key processes are multi-head attention, scaled dot-product attention, and position-wise feed-forward network. For this reason, the authors used Transformer and its variants, particularly Informer and FEDformer. The Transformer obtained the highest F1 score value of 93.04%. In this work, the authors used the AirLab Failure and Anomaly (ALFA) dataset, which used an open-source autopilot platform for autonomous navigation and control applications and supported a variety of UAVs, including fixed-wing aircraft, multi-rotors, and rovers [40]. They prove that the transformer can not only be used in Natural Language Processing (NLP) but can also be used to analyze drone malfunctions.

Renduchintala et al. [14] investigated the fundamental primary log parameters of the autonomous drone and suggested a thorough software architecture for drone forensics, along with some early findings. Users will be able to extract and study the onboard flight data using their in-progress software's user-friendly Graphical User Interface (GUI). When examining criminal cases involving drones, the forensic science community would then have a useful tool. The 3DR Solo, Yuneec Typhoon H, and DJI Phantom 4 are three common commercial drones that were compared in terms of their technical specs. These specs included logging capacity, file type, flight time, range, autopilot software, maximum payload, battery, rotors, operating frequency, obstacle avoidance, and cost.

Zhao et al. [15] discussed the Dalian University of Technology Anti-UAV dataset, which consists of 20 videos

for tracking and 10,000 images for detection. The dataset captures UAVs in various scenarios, evaluating detection algorithms' performance. The paper proposed a straightforward tracking algorithm, enhancing UAV tracking by integrating detection. The algorithm involves three stages: initialization, tracking, and detection. A deep learning-based detector identifies UAVs in each frame, and a Kalman filter predicts their position and velocity during tracking. The algorithm updates tracks based on each frame's detection using a data association method. This approach significantly improves method-level UAV tracking performance.

Al-Dhaqm et al. [16] explored drone-related investigations and proposed the Drone Forensics (DRF) model. This comprehensive framework covers all procedures, ideas, tasks, and activities essential for digital investigations on drone devices. The DRF model introduces two new processes, pre-incident and post-incident, not found in current models. The presentation of evidence is emphasized for clarity and understanding. A comparison with existing models, focusing on digital forensic processes, highlights the DRF model's unique features, including tasks like identifying compromise indicators and ensuring digital forensic readiness. Notably, the DRF model covers tasks like data integrity verification, which is not addressed in current models.

D. UAV FORENSICS CASE STUDIES

Stanković et al. [17] created a criminal-like scenario, on the first test day, they conducted four distinct flight scenarios with the drone, and on a subsequent day, they conducted further flights to evaluate its capacity to carry weight. In the four flights, both the iPhone 7 and the Samsung Galaxy S7 utilized the DJI Fly application for drone control, flying, and navigating to the location using native map apps on each phone. The data was collected and examined using a variety of digital forensic software tools such as Autopsy, Magnet AXIOM, and Cellebrite UFED, as shown in Table 1. These tools can be used by law-enforcement agencies and professionals.

Allahham et al. [18] introduced the DroneRF dataset, a valuable resource for understanding and analyzing drone activity. This dataset includes recordings of Radio Frequency (RF) signals from different drones like Bepop, AR, and Phantom, as well as background RF activity in the absence of drones. RF receivers intercepted the communication between the drones and their flight control modules, collecting the data for later analysis. The experiment used various equipment, including flight controllers and mobile phones, to transmit and receive RF commands. The dataset comprises 227 recorded segments from drones and background radioactivity. The collected data is stored in a database and can be utilized for analyzing anti-drone and UAV detection systems, particularly for deep learning-based RF-based drone identification and detection.

Yang et al. [19] explored the field of drone forensics, emphasizing the importance of recovering vital flight data for establishing ownership and understanding drone-related incidents. Focusing on DJI Spark and Mavic Air, popular drone models, the study aimed to equip investigators with tools to analyze digital data from flight artifacts and associated mobile devices. They proposed a mathematical method to correlate information from flight files, SD cards, and mobile phones. This integrated approach helps forensic analysts identify evidence, connect drones with SD cards and mobile phones, and reconstruct events. This method proves valuable for resolving cases involving drone misuse or criminal activities.

TABLE 1. Tools and applications.

Software Name	Usage	Availability
DJI Fly on Android	Flight Operation	Freeware
DJI Fly on iPhone	Flight Operation	Freeware
Autopsy	Examination and Analysis	Open-source
Magnet AXIOM Process	Acquisition	Proprietary
Magnet AXIOM Process	Acquisition	Proprietary
Magnet ACQUIRE	Acquisition	Freeware
Magnet AXIOM Examine	Examination and Analysis	Proprietary
Cellebrite UFED	Acquisition	Proprietary
Cellebrite Physical Analyzer	Examination and Analysis	Proprietary
Cellebrite Reader	Examination and Analysis	Freeware
Binwalk	Entropy measurement	Open-source
ExifTool	Reading meta information	Open-source
DatCon	Decryption of the .DAT files	Freeware

Ojo et al. [20] investigated the use of a Machine Learning Process (MLP) for real-time evidence detection and collection using a drone. The drone's task was to identify vehicles in specific areas at certain times, avoiding densely vegetated locations for a clearer view. The focus was on object detection to provide evidence. The team synchronized the drone with software for scenario planning based on GPS coordinates. The chosen method achieved 100% accuracy in recognizing object types or specific vehicle models. However, license plate reading accuracy was around 80%, influenced by the camera type and viewing angle. Optimal drone configuration involved flying at 6 meters, 7 kph speed, and a 33% window overlap. The study highlighted the potential manipulation of drone positions stored in the eMotion app, which could impact the validity of evidence obtained from such drones.

Atkinson et al. [21] explored the data extraction capabilities of drones and the value of that data. They utilized main and secondary datasets, including interviews with a Digital Forensic Analyst and a UAV fly test. The study revealed that drones can store valuable information for forensic investigations, such as flight paths, flight date and time, altitude, home point, and alerts for restricted airspace. Despite

manufacturers incorporating Anti-Forensics software, end users were found unable to utilize these techniques.

E. OPEN SOURCE FORENSICS TOOLS FOR DRONES

Mahdi and Ibrahim [22] explored digital forensics, emphasizing artificial intelligence techniques like machine learning. They provided an overview of its significance and types. Also, they discussed top digital forensic tools: EnCase, FTK, X-Ways Forensics, and Autopsy. The choice of tools depends on investigation needs, budget, and team expertise. Autopsy, being free and open-source, suits smaller investigations, while EnCase, FTK, or X-Ways Forensics are suitable for larger, complex cases. The selection process should consider usability and a trial period in a controlled environment. The paper also discussed parameters for evaluating digital forensic tools in computer, network, and live forensics, emphasizing the importance of selecting tools based on specific investigation needs.

Barton and Azhar [23] examined the DJI Phantom 3 Professional drone and its associated mobile platforms, Motorola Moto G 3rd Generation, and Samsung Galaxy S4 Mini. They utilized scripting tools like Bash, Perl, and Python, and they compiled languages for Linux-based forensics tool development on a Kali Linux workstation. The research focused on analyzing flight logs, media, and crucial files for identifying artefacts. They demonstrated constructing adaptable forensic tools using simple scripts. The study emphasized the challenges of drone forensic analysis, such as interpreting flight data and dealing with the multi-platform nature of drone systems. The DJI Phantom 3 Professional's features, including vision, GPS, autonomous flight, and obstacle avoidance, make it versatile but also raise concerns about its potential use in criminal activities. The research showcased the effective use of open-source tools to retrieve data from the UAV and control devices, highlighting the importance of correlating artefacts for comprehensive drone forensic analysis. The study revealed the potential of open-source tools in drone forensic analysis, providing insights into challenges and solutions for examining captured drones in conflict zones.

Azhar et al. [24] examined DJI Phantom 3 Professional and Parrot AR drones, focusing on extracting artifacts from recorded flight data and associated mobile devices. They utilized simple scripts and open-source software, aligning with the Association of Chief Police Officers' guidelines for forensically sound techniques. Despite variations in drone tasks, the study demonstrated the applicability of these methods. The DJI Phantom drone, being professional-grade, yielded more artifacts with its advanced sensors and higher-resolution data capture compared to the A.R drone. The study highlighted the DJI Phantom's automatic GPS recording, aiding in the interpretation of three-dimensional movement data. Successful identification and extraction of potential artifacts facilitated suspect identification, flight recreation, and media retrieval. The research also acknowledged the effectiveness of certain anti-forensics methods.

F. MACHINE LEARNING DETECTION SYSTEMS

Moustafa and Jolfa [25] proposed an autonomous intrusion detection method for identifying cyberattacks in drone networks. They set up a testbed to conduct malicious attacks, collecting honest and dishonest drone network observations. Various machine learning models, including decision trees, k-nearest neighbours, naive Bayes, support vector machines, and deep learning multi-layer perceptrons, were trained and evaluated. The decision tree emerged as the best model, achieving 99.99% accuracy and the highest F1 score in categorizing normal and attack traffic. The multi-layer perceptron and k-nearest neighbours were the second-best classifiers, with 99.98% accuracy and similar F1 scores. Support vector machine ranked third with close to 99% accuracy but had a larger fall-out. Naive Bayes showed the lowest performance with 39.9% accuracy and suboptimal recall and F1 score.

Whelan et al. [26] introduced a novelty-based intrusion detection method for UAVs using one-class classifiers. They simulated UAV attacks, including a common GPS spoofing attack, using PX4 autopilot and a Gazebo robotics simulator. The dataset included various UAV types, such as Quadcopter, Hexacopter, VTOL, Tailsitter, and Plane. Hardware-in-loop and software-in-loop simulations were conducted for accuracy.

Three one-class classifiers were discussed:

- One-Class Support Vector Machines (OC-SVMs): Supervised algorithms trained only on normal data to detect any abnormal data as an intrusion.
- Autoencoder Neural Network: Comprising input data, encoding and decoding functions, and a loss function to evaluate performance.
- Local Outlier Factor (LOF): An unsupervised algorithm for anomaly detection.

The goal was to enhance the detection rate while reducing false positives, measured using precision, recall, and the F1 score. Results showed the autoencoder achieved an average F1 score of 94.81%, OC-SVMs had an average F1 score of 81.17%, and LOF achieved 58.93%.

Taha and Shoufan [27] conducted a detailed analysis of machine learning-based drone detection and classification. The study covered single-modality and multi-modal approaches, emphasizing performance indicators, datasets, and benchmarks used for testing. They explored the benefits of machine learning in object recognition, especially in challenging scenarios. Various detection modalities like radar, vision, acoustics, and radio-frequency were discussed, highlighting existing challenges such as recognizing small or distant drones and the need for real-time processing. The study emphasized the importance of multi-modal approaches to address diverse scenarios. The conclusion outlined areas for future research, including the development of more precise algorithms and reference datasets, as well as the exploration of novel sensor technologies. While machine learning-based drone classification shows promise, further research is needed for reliable and effective solutions.

Chen and Chen [28] discussed a Machine Learning (ML) attack on UAV-based wireless networks. The attacker, having both plaintext and ciphertext, collects pairs of different sizes to train an ML classifier for decrypting UAV messages. Simulations revealed that a basic Neural Network (NN) can successfully decrypt UAV location data. The authors introduced a network coding-based encryption technique but highlighted the need to keep UAV operation times reasonable to prevent cyberattacks. As artificial intelligence advances, there's a growing risk of more potent ML-based attacks, emphasizing the importance of developing robust encryption strategies for multi-UAV scenarios. The focus should be on ensuring secure wireless data transmission in untrusted aerial environments, considering network coding techniques.

Syed et al. [29] proposed a novel machine-learning method using Multi-Layer Perceptrons (MLP), Support Vector Machines (SVMs), Gradient Boosting, and RF to detect engine faults. They applied this technique to the ALFA dataset, which includes various faults in aerial vehicles. Google Colaboratory facilitated dataset organization, testing, and result analysis. Employing K-folds cross-validation for training, their approach achieved a remarkable 21% accuracy improvement over recent studies, showcasing superior detection capabilities. Training with and without engine failures yielded an average accuracy of 97% for RF and Gradient Boosting algorithms. The suggested method offers efficient engine defect detection for Vertical Take-Off and Landing aircraft (eVTOLs), eliminating the need for costly and time-consuming Original Equipment Manufacturer (OEM) support. This approach reduces maintenance downtime, enhances engine utilization, and prevents in-flight issues, all thanks to RF and Gradient Boosting.

G. SECURITY AND PRIVACY ISSUES OF UAVS

Mekdad et al. [30] provided a thorough analysis of the security and privacy concerns surrounding UAVs in this work by classifying them systematically at four levels: hardware, software, communication, and sensor. Specifically, they looked closely at common vulnerabilities affecting UAVs for potential malicious actor attacks, threats presently posing a risk to UAVs used for civilian purposes, active and passive attacks by adversaries aimed at breaching UAV security and privacy, and possible defenses and mitigation strategies to shield UAVs from such malicious activity for each level. Additionally, they outlined the key findings that emphasize the privacy and security risks of UAVs. They wrapped up their poll by outlining important risks and interesting future research directions for UAV security and privacy.

Peleshko et al. [31] sought to improve city management efficacy by developing mechanisms that allowed for decision-making based on the results of monitoring and analysis of urban environment features. Concepts for visualizing and techniques for analyzing parameter dynamics using drone sensors have been developed. The research project utilized rented equipment, including a copter-type drone with specific features, various environmental sensors, a noise meter, and microcontrollers. The project aims to produce results accessible to educational, scientific, and socio-environmental institutions, as well as for security purposes and the general public.

Javed et al. [32] conducted a thorough survey of computer forensics, delving into current research, tools, techniques, challenges, and future directions in digital forensics. The paper identified state-of-the-art concepts and provided an extensive overview of computer forensic domains and toolkits. The examined domains included operating systems, file systems, live memory, web, email, network, and multimedia forensics. The authors offered a comparative analysis of toolkits, featuring a scoring model for both paid and unpaid options to aid investigators in toolkit selection. Notable computer forensic toolkits like Autopsy, Redline, Belkasoft, OS, Prodiscover, XWays, Encase, and FTK were discussed.

Sihag et al. [33] focused on protocols, related threats, targeted security features, and solutions suggested in the literature. They discussed the pertinent artifacts, tools, and benchmark datasets, looked at the security and privacy issues associated with drones, and presented a thorough drone forensics methodology for the analysis of drone systems. To ensure the security and data integrity of UAVs, they developed a thorough drone forensics methodology that includes the analysis of drone systems, pertinent artifacts, tools, and benchmark datasets. Also, they examined recent drone system assaults, protocols, related threats, and targeted security features. In addition, they outlined upcoming challenges in the field and emphasized security and privacy issues related to drone systems.

Zhang [34] explored the use of drones in various fields and proposed the application of passive radio frequency sensing for affordable and reliable RF-based drone detection. The author evaluated six machine learning models on an open drone dataset, with XGBoost achieving state-of-the-art results. Three classification problems were considered: detecting the presence of a drone, identifying its type, and determining its flight mode. The paper presented a straightforward yet effective workflow for RF-based drone detection using machine learning, demonstrating the framework's efficacy.

IV. DISCUSSION AND OPEN ISSUES

One of the challenges with UAVs is the concern regarding power, safety, privacy, and security in unmanned systems. For example, privacy concerns arise from UAVs collecting personal data, and there may be dangers associated with the lack of GPS alerts about the surrounding areas. The susceptibility of UAV signals to hacking and jamming attempts is another security concern [37].

A. DRONE FORENSICS FRAMEWORKS

CCAFM was introduced in [10], encompassing three key processes: Acquisition and Presentation, Reconstruction and Analysis, and Post-investigation. This model provides a comprehensive approach to drone forensics, covering crucial

TABLE 2. Summary of framework forensic models for drone investigation.

Framework	Paper	Strengths	Considerations	Framework Description
CCAFM	[10]	Comprehensive approach covering Acquisition, Reconstruction, Analysis, and Post-investigation.	Complexity may be a challenge in practical implementation.	Acquisition and Presentation, Reconstruction and Analysis, and Post-investigation process.
Drone Forensics Framework	[12]	Systematic framework defining components and techniques for drone forensics.	Scalability and adaptability to diverse drone technologies.	Forensic model and defines various components and techniques needed for drone forensics.
IoT Device Forensic Analysis Framework	[19]	Addresses evidence acquisition without disrupting IoT device performance.	Applicability in dynamic and unpredictable IoT-drone interaction scenarios.	Framework resolves the evidence acquisition without interrupting the performance of IoT devices.
Drone Forensic Framework	[27]	Ten-phase structure for a systematic breakdown of drone architecture.	Practical effectiveness in real-world forensic scenarios.	Framework with ten phases that help understand the basic drone architecture.
DRFRF	[31]	Emphasizes proactive forensic readiness in the drone domain.	Practical effectiveness in real-world forensic scenarios.	A novel forensic readiness framework using the design science method.

stages from data acquisition to post-investigation analysis. Renduchintala et al. contributed to the field with their Drone Forensics Framework [14], which outlines a forensic model and defines various components and techniques essential for effective drone forensics. The framework assists in systematically approaching drone forensic investigations. Mazhar et al. [5] developed a Framework for Forensic Analysis of IoT Devices, addressing challenges in evidence acquisition without disrupting the normal functioning of IoT devices. Jain et al.'s Drone Forensic Framework [9] stands out with its ten-phase structure, providing a systematic breakdown to comprehend the fundamental architecture of drones during forensic examinations. Alotaibi et al. [12] proposed the Drone Forensics Readiness Framework (DRFRF), a novel contribution achieved through the design science method. This framework emphasizes proactive forensic readiness in the drone domain. Each of these frameworks plays a crucial role in advancing the field of drone forensics, addressing specific challenges, and contributing to a more systematic and comprehensive approach to investigations.

Determining which drone forensics framework is better depends on the specific needs, objectives, and context of the forensic investigation. Each framework has its strengths and may be better suited for different scenarios. In Table 2, the frameworks mentioned are briefly evaluated:

The decision is based on several factors, including the investigation's purpose, the complexity of drone technology, the available resources, and the desired level of detail. Combining or customizing frameworks based on case-specific requirements and cutting-edge forensic practices may be advantageous. It's also important to update frameworks regularly to keep up with technological developments [38].

B. DRONE FORENSICS DATASET

Drone movement and operations can be uncovered by processing data collected during flight, which is recorded in log files. The processing exposed time stamps, flight duration, power speed, yaw, pitch and roll, altitude, and drone type, among other details [20]. Researchers have introduced several datasets for drone detection studies, each offering unique features and applications. Allahham et al. curated the DroneRF dataset [18], utilizing radio frequency signals for drone detection. This dataset includes signals from a Ryze Tello TLW004 drone, providing valuable insights into RF-based detection, classification, and identification of drones. Syed et al. contributed to the ALFA dataset [29], which focuses on drone detection through unsupervised machine learning and flight path analysis. The dataset involves simulations with a Carbon Z T-28 model plane, offering controlled environments for studying machine learning-based detection methods. Whelan et al. compiled the UAV Attack Dataset [26], known for its diversity with various drones like 3DR IRIS+, Holybro S500, Yuneec H480, DeltaQuad VTOL, Standard Tailsitter, and Standard Plane. This dataset includes both real-world and simulated scenarios, making it suitable for comprehensive studies on drone detection across different drone types and environments. Ahmed et al. presented the ECU-IoFT dataset [6], emphasizing cyber-attacks on the Internet of Flying Things. This dataset involves a Ryze Tello Drone and aims to facilitate the analysis of cyber threats targeting unmanned aerial vehicles, providing valuable data for research on security and forensics in the drone domain. Researchers can choose datasets based on their specific research goals, whether focusing on RF-based detection, machine learning applications, or cybersecurity aspects of drones. Table 3 provides a summary of datasets used in various drone detection studies, including information about the author, dataset name, drone type, and traffic type.

C. MACHINE LEARNING APPLICATIONS

In addition to using relevant tools like Autopsy, FTK imager, OSforensics, etc., investigating drone forensics also makes use of machine learning algorithms to verify the accuracy of the data and proof collected from the drones [39]. Various machine-learning applications have been employed across different studies for drone detection. Zhang [34] explored XGBoost, AdaBoost, decision tree, random forest, k nearest neighbor, and multilayer perceptron models on the same

TABLE 3. Datasets on drone detection studies.

Author	Dataset	Drone Type	Traffic Type	Pros	Cons
Allahham et al. [18]	DroneRF dataset	Ryze Tello TLW004	Real	Real-world dataset providing authentic drone signals.	Limited to the Ryze Tello TLW004 drone.
Syed et al. [29], [40]	ALFA dataset	Carbon Z T-28 model plane	Simulation	Includes a simulation dataset, allowing controlled experiments.	Limited to the Carbon Z T-28 model plane.
Whelan et al. [26]	UAV attack dataset	3DR IRIS+, Holybro S500, Yuneec H480, DeltaQuad VTOL, Standard Tailsitter, and Standard Plane	Real and Simulation	Diverse dataset with multiple drone types in real and simulated scenarios.	The variety might add complexity, and it includes both real and simulated traffic.
Ahmed et al. [6]	ECU-IoFT dataset	Ryze Tello Drone	Real	Real-world dataset with the Ryze Tello Drone.	Limited to a specific drone model

dataset. Syed et al. [29] and Editya et al. [13] utilized the ALFA dataset, employing Multi-Layer Perceptrons (MLP), Support Vector Machines (SVMs), Gradient Boosting, Random Foresting (RF), Transformer, Informer, and FEDformer for machine learning-based drone detection. In contrast, Whelan et al. [26], [40] used OC-SVMs, Autoencoder Neural Networks, and Local Outlier Factor (LOF) on the UAV Attack Dataset, which includes logs from both simulated and real-world combat scenarios. These diverse machine-learning approaches reflect the versatility of techniques applied to address the complexities of drone detection across different datasets and scenarios. As shown in Table 8 presents the summary of the drone detection in the related work.

D. CYBER SECURITY AND PRIVACY ISSUES

The integration of drones into various domains has raised significant concerns regarding cyber security and privacy issues. Researchers such as Renduchintala et al. [14], Al-Dhaqm et al. [16], and Sihag et al. [33] have highlighted the vulnerability of drones to cyber attacks, emphasizing the need for robust security measures. The potential risks include unauthorized access to sensitive data, exploitation of communication channels, and the use of drones as tools for malicious activities. Additionally, the increasing use of drones in urban environments, as discussed by Peleshko et al. [31], poses challenges in managing privacy concerns related to surveillance and data collection. The comprehensive survey by Mekdad et al. [30] sheds light on security and privacy issues associated with UAVs, emphasizing the importance of addressing these concerns to ensure the safe and responsible deployment of drones across various applications. These studies collectively underscore the critical importance of developing effective security frameworks and regulatory guidelines to mitigate cyber security and privacy risks in the realm of drone technology.

E. IMPORTANCE OF STANDARDIZED PERFORMANCE METRICS AND NUMERICAL COMPARISONS IN FORENSIC EXAMINATION OF DRONES

Drawing insights from the NIST event on standards and performance metrics for autonomous vehicles [50], it is evident that standardized, quantifiable metrics are essential for objective assessments. This ensures consistency and reliability across different systems. Table 4 outlines the key performance metrics relevant to both autonomous vehicles and the forensic examination of drones, emphasizing the importance of proper numerical comparisons.

TABLE 4. Key Performance metrics for autonomous vehicles and forensic examination of drones.

Metric	Description
Safety	Measures the ability to avoid collisions and handle complex scenarios. For drones, this includes avoiding obstacles, safe operation in various environments, and the ability to respond to emergency situations effectively.
Reliability	Assesses the consistency of performance under diverse conditions. For drones, this means stable operation across different weather conditions, altitudes, and environments. It includes evaluating the drone's operational uptime, fault tolerance, and maintenance requirements.
Efficiency	Evaluates energy usage, flight time, and resource management. This includes optimizing battery life, efficient flight paths, and overall operational time. Efficiency metrics also encompass the drone's ability to perform tasks with minimal resource expenditure.
Accuracy	Considers the precision of data collection and processing. This involves the accuracy of sensors, cameras, and other data-gathering tools used in forensic examination. Accuracy metrics include the resolution of images, the precision of GPS and other location-based data, and the reliability of data transmission.
Adaptability	Measures the capability to learn from new situations and improve over time. For drones, this includes the ability to update software and algorithms based on new data and experiences. Adaptability metrics assess the drone's capacity for machine learning, its ability to incorporate new findings into its operational framework, and its responsiveness to environmental changes.
Interoperability	Evaluates the ability to integrate and operate with other systems. This includes compatibility with various data formats, communication protocols, and coordination with other drones or devices during forensic operations.
Security	Assesses the robustness of the drone against cyber threats and unauthorized access. Security metrics include encryption of data, resistance to hacking attempts, and measures to ensure data integrity and confidentiality during forensic investigations.

Incorporating proper numerical comparisons for these metrics ensures a robust and objective framework for evaluating the forensic capabilities of drones. This approach not only standardizes assessments but also fosters innovation

and improvement in drone technology and forensic methodologies. Proper numerical comparisons involve developing quantifiable and reproducible tests for each metric, ensuring transparency and comparability across different drone systems. This includes establishing benchmarks and standard protocols for testing, as well as utilizing data-driven approaches to continually refine and improve performance evaluations.

F. COMPLEXITY OF DRONE FORENSICS

Addressing the complexity of drone forensics compared to other digital gadget forensics is essential for understanding the unique challenges in this field. One major aspect contributing to this complexity is the integration of multiple data types generated by drones. Unlike traditional digital gadgets like smartphones or computers, drones produce a diverse range of data, including flight logs, GPS coordinates, video and audio recordings, sensor readings, and telemetry data [28]. This variety demands forensic analysts to possess proficiency in handling and synchronizing diverse datasets to reconstruct events accurately. Furthermore, drone forensics often requires real-time data processing capabilities due to the dynamic operating environments of drones. Analyzing a drone's flight path alongside environmental factors and real-time video footage necessitates sophisticated tools and methodologies [46]. This level of real-time data processing is less prevalent in other digital forensics scenarios, such as examining a static hard drive or a mobile phone.

Moreover, the unique vulnerabilities associated with UAVs add another layer of complexity to drone forensics. Drones can be susceptible to GPS spoofing, signal interference, and hacking attempts, requiring forensic analysts to possess a thorough understanding of cybersecurity principles in the forensic analysis [53]. While traditional digital gadgets are also vulnerable to cyber attacks, drones face additional challenges due to their mobility and operational characteristics. The physical mobility of drones introduces forensic challenges such as the retrieval of physical evidence and jurisdictional issues, as drones can traverse vast areas and cross multiple jurisdictions [28]. Developing specialized methodologies and tools tailored to address these unique challenges is crucial for advancing the field of drone forensics and ensuring a comprehensive and accurate analysis of UAV-related evidence.

Table 5 provides a comparison of the complexity in drone forensics versus traditional digital gadget forensics, highlighting the unique aspects of each field.

Table 6 provides an overview of the sub-components in drones that require different data acquisition and analysis techniques.

V. CHALLENGES IN FORENSICS EXAMINATION OF DRONE

The forensic examination of drones presents a myriad of challenges stemming from the evolving complexity of drone technology and the intricate interplay of human factors in investigations. Drones, with their diverse functionalities and technological sophistication, create hurdles for forensic investigators in the collection, preservation, and analysis of digital evidence. The rapid advancements in drone capabilities, such as autonomous flight and encrypted communication, contribute to the intricacy of forensic examinations. Moreover, the specialized expertise required for effective drone forensics, including knowledge of aeronautics, electronics, and data science, poses a significant challenge for forensic professionals. Human factors, encompassing legal and ethical considerations as well as collaboration with drone operators and manufacturers, add layers of complexity to the investigative process. From technological complexities to the interdisciplinary nature of the field, this section provides an outline for an extensive examination of the difficulties associated with drone forensic examinations [41].

A. DIGITAL EVIDENCE PRESERVATION

Digital forensic investigations require the preservation of digital evidence on drones. The researchers in [36] used a methodical approach in their case study, which included testing, creating scenarios, mending equipment, gathering data, and analyzing it. The collected data was divided into four sections since pertinent data is kept on four different devices: smartphones, laptops/desktops, controllers, and drones, where logical backups are kept and synchronized. Following analysis of the collected data, files of interest containing flight records, credential information, and other pertinent data were found. Multiple tests were carried out, including tests about the internal SD card in the drone and a logical smartphone backup, to guarantee the established approach and conclusions were accurate [39].

In the context of digital forensic investigations, [42] addressed the significance of preserving digital data related to drones. It highlighted the necessity for digital investigators to possess the expertise and comprehend the essential functions, features, and processes of drones to retrieve vital forensic evidence regarding actions recorded by the drone during an incident involving it. The authors looked into six popular drone manufacturers and gathered pertinent forensic data, including location data, photos and videos taken during the drones' flights, information about who owned the confiscated drone, and drone flight trajectories [41].

B. HUMAN FACTOR

In the context of drone forensics investigations, there are several challenges and human factor considerations. Specialized training and expertise in drone forensics stand out as another significant challenge, requiring forensic investigators to acquire new skills and knowledge and demanding essential time and resources. The human factor introduces complexities, emphasizing the need for effective communication and collaboration skills as investigators engage closely with drone operators, manufacturers, and stakeholders. This interaction requires an understanding of the legal and ethical dimensions

TABLE 5. Comparison of complexity in drone forensics vs. traditional digital gadget forensics.

Aspect	Drone Forensics	Traditional Digital Gadget Forensics
Data Types	Integration of diverse data types, including flight logs, GPS coordinates, video and audio recordings, sensor readings, and telemetry data.	Limited range of data types, primarily consisting of files, logs, and metadata stored on the device's storage.
Real-time Processing	Often requires real-time data processing capabilities for analyzing dynamic operating environments and events captured in real-time.	Real-time processing is less common, typically performed for immediate analysis of live system activity or network traffic.
Vulnerabilities	Susceptible to GPS spoofing, signal interference, hacking attempts, and physical interception, requiring expertise in cybersecurity principles.	Vulnerable to various cyber attacks such as malware infections, data breaches, and unauthorized access, necessitating cybersecurity measures.
Mobility and Jurisdiction	Mobility introduces challenges in evidence retrieval and jurisdictional issues, as drones can traverse vast areas and cross multiple jurisdictions.	Stationary nature simplifies evidence retrieval and jurisdictional issues, as devices are typically recovered from fixed locations within a defined jurisdiction.

TABLE 6. Sub-components in drones requiring different data acquisition and analysis techniques.

Sub-component	Data Acquisition and Analysis Techniques
Flight Logs	Extraction and analysis of flight log data to reconstruct flight paths, identify anomalies, and determine flight behavior.
GPS Coordinates	Collection and interpretation of GPS coordinates to track drone movements, determine geographic locations, and establish timelines.
Video and Audio Recordings	Forensic examination of video and audio recordings to analyze visual and auditory evidence, identify objects or individuals, and reconstruct events.
Sensor Readings	Acquisition and interpretation of sensor data (e.g., altitude, temperature, humidity) to assess environmental conditions, identify potential malfunctions, and correlate with other data sources.
Telemetry Data	Collection and analysis of telemetry data to monitor drone performance, assess system health, and detect anomalies or deviations from expected behavior.
Wireless Communication Logs	Extraction and analysis of communication logs to identify communication patterns, assess network activity, and detect unauthorized access or interference.
Data Transmission Protocols	Examination of data transmission protocols to ensure data integrity, assess encryption methods, and identify vulnerabilities in communication channels.

inherent in drone investigations. In [43] and [44], it is highlighted that there is a need for a multi-skilled approach that involves experts in drone technology, forensics, and law enforcement working together and emphasized how important it is to continue providing training and education to investigators so they have the necessary knowledge and abilities to analyze drone data effectively.

C. INTERFERENCE WITH RF SIGNALS

Interference with RF signals poses a substantial challenge in the realm of drone technology, and scholarly works delve into various aspects of this concern. RF interference can occur due to various factors, such as weather conditions, physical obstructions, and other wireless devices operating in the same frequency range. This interference can cause data loss or corruption, which can impact the accuracy and completeness of the evidence collected. To mitigate this challenge, investigators can use specialized equipment to capture and analyze RF signals, and they can also conduct tests to determine the impact of interference on the data collected [45]. In [44], it is mentioned that drones controlled by WiFi use IEEE 802.11 standards, and all communication between the drone and ground station controller typically uses the WiFi network, which is vulnerable to security breaches. An unencrypted Wi-Fi used with a drone allows any individual to connect and hack the drone, and professional drones can be hijacked because of the lack of encryption on their onboard chips and can perform man-in-the-middle attacks up to two kilometers away. To keep ahead of new threats and guarantee the safe and secure use of drones in smart cities.

D. ENCRYPTION AND SECURITY MEASURES

In a related context, [47] discusses the implementation of privacy-enhancing technologies, including encryption, to safeguard personal information in RFID applications. The paper highlights the importance of regulatory mechanisms to mitigate the impacts of various surveillance technologies on civil liberties. When addressing Unmanned Aircraft Systems (UASs), the paper acknowledges that existing regulations aim to address some privacy concerns related to UAS surveillance but fall short in addressing all ethical implications, such as social sorting and discrimination. The authors argue for a combination of top-down, legislated requirements and bottom-up impact assessments to effectively protect privacy and civil liberties in UAS deployments.

The authors in [47] addressed the use of privacy-enhancing technologies, such as encryption, to protect private data in RFID applications. They also emphasized the necessity of regulatory frameworks to lessen the negative effects of different types of surveillance technologies on civil liberties. The authors acknowledged that while current regulations

aim to address some privacy concerns related to UAS surveillance, they do not adequately address all ethical implications, including social sorting and discrimination. Therefore, they argued that the best way to effectively protect privacy and civil liberties in UAS deployments is to combine top-down, legally mandated requirements with bottom-up impact assessments.

E. BATTERY LIFE AND DATA RETRIEVAL

Drones rely heavily on volatile memory, and the flight data stored therein will vanish if the battery drains out, which suggests that the battery life of a drone can impact the ability to retrieve flight data during a forensic investigation and that not all commercial drones have flight controllers that are equipped with data logging capabilities. Therefore, the ability to retrieve flight data may depend on the specific drone model and its features [46]. For information on battery life, it reports that research is being undertaken on a solar-powered UAV that could stay airborne for up to five years. The endurance of other drones varies depending on their specific capabilities and attachments. For example, the institute can carry out surveillance for up to 15 hours with both low-light and infrared cameras attached [47]. For drone forensics and incident response, battery life and data retrieval are critical considerations.

F. COLLISION AND ACCIDENT INVESTIGATIONS

The use of drones in smart cities and other urban environments introduces additional complexities and safety considerations, making collision and accident investigations particularly important. As drone technology continues to evolve and the integration of drones into urban airspace increases, the need for effective collision and accident investigation procedures becomes even more significant [48].

G. LACK OF STANDARDIZED PROTOCOLS

The lack of standardized protocols in the context of Connected and Autonomous Vehicles (CAVs) is a significant challenge for cybersecurity and forensics. Without standardized protocols, it is difficult to ensure that all CAVs are designed and built with the same level of security and that all incidents are investigated and resolved consistently and effectively. One of the main reasons for the lack of standardized protocols is the rapid pace of technological development in the field of CAVs. As new technologies are developed and implemented, it can be challenging to keep up with the latest security threats and vulnerabilities. Additionally, there are many different stakeholders involved in the development and deployment of CAVs, including manufacturers, regulators, and law enforcement agencies, which can make it difficult to establish a unified approach to cybersecurity and forensics.

To address the lack of standardized protocols, there have been initiatives to develop guidelines and best practices for cybersecurity and forensics in CAVs. For example, the Society of Automotive Engineers (SAE) has developed a set of guidelines for automotive cybersecurity, known as SAE J3061, which provides a framework for identifying and mitigating cybersecurity risks in CAVs. Additionally, the National Institute of Standards and Technology (NIST) has initiated workshops to develop standards and performance metrics for CAVs [49].

H. IMPLEMENTING STANDARDIZED METRICS

1) VARIABILITY IN DRONE HARDWARE AND SOFTWARE

A significant challenge in implementing standardized metrics is the variability in drone hardware and software configurations, which can affect the consistency of performance measurements. Different drones may have varying sensor qualities, processing capabilities, and flight dynamics, leading to inconsistent data that complicates direct comparisons. Additionally, software updates and custom configurations can further diverge the operational characteristics of drones, impacting their performance in forensic tasks.

The protocol would establish a controlled and consistent framework for evaluating drone performance, ensuring that all drones are assessed under comparable conditions. Key components of this benchmarking protocol include defining standardized test scenarios that reflect typical forensic applications, conducting tests in controlled environments to minimize variable influences, and implementing uniform data collection methods to ensure comparability. Additionally, establishing core benchmarking metrics covering safety, reliability, efficiency, and accuracy, along with using baseline drone models as reference points, will provide a robust framework for fair and objective performance evaluation. Implementing this universal benchmarking protocol can significantly enhance the consistency and reliability of performance measurements across different drone systems [46].

2) RAPID EVOLUTION OF DRONE TECHNOLOGY

The rapid evolution of drone technology presents another challenge for maintaining up-to-date performance metrics. As new drone models and capabilities are introduced, existing metrics may become obsolete or inadequate, complicating the process of performance evaluation. This issue is exacerbated by the frequent updates in drone software, the introduction of novel sensor technologies, and advancements in autonomous functionalities, which all contribute to a dynamic landscape requiring constant adaptation of evaluation criteria.

To overcome this challenge, the use of adaptive machine learning models is proposed. These models can evolve alongside technological advancements by continuously learning from new data and experiences. Adaptive machine learning models can analyze vast amounts of flight data, sensor outputs, and operational logs to identify patterns and trends that signify performance improvements or degradations. By integrating feedback loops, these models can update performance metrics in real-time, ensuring that evaluations remain relevant and accurate. This approach not only

TABLE 7. Comparison of selected papers in drone forensics.

Feature	Our Paper	Alotaibi et al. [10]	Al-Dhaqm et al. [16]	Mekdad et al. [30]	Sihag et al. [33]
Model or Framework	✓	✓	✓	✗	✓
Artifacts	✓	✗	✓	✗	✓
Tools	✓	✓	✓	✗	✓
Security and Privacy	✓	✓	✓	✓	✓
Datasets	✓	✗	✗	✗	✓
Challenges	✓	✓	✓	✓	✓
Case Studies	✓	✗	✓	✗	✗
Machine Learning	✓	✓	✗	✗	✗
Internet of Things	✓	✗	✗	✗	✗

✓when the paper discusses this feature, and ✗when the paper does not discuss this feature.

TABLE 8. Summary of related work to drone detection.

Author	Publ.	Dataset	Publicly Available	Dataset Description	Model
Allahham et al. [18]	2019	DroneRF dataset	Yes	A dataset of drones operating in various modes based on RF.	
Zhang [34]	2021	DroneRF dataset	Yes	A dataset of drones operating in various modes based on RF	XGBoost, AdaBoost, decision tree, random forest, k nearest neighbour, and multilayer perceptron.
Syed et al. [29], [40]	2022	ALFA dataset	Yes	Data from a fixed-wing UAV's autonomous flight that shows various control surface failures that may occur during the flight.	MLPs, SVMs, Gradient Boosting, and RF
Editya et al. [13], [40]	2023	ALFA dataset	Yes	Data from a fixed-wing UAV's autonomous flight that shows various control surface failures during the flight.	Transformer, Informer, and FEDformer.
Whelan et al. [26]	2020	UAV attack dataset	No	Logs from both simulated and real-world combat contain information from both a safe flight and one in which the UAV is attacked (GPS Spoofing and Ping DoS).	OC-SVMs, Autoencoder Neural Network, and LOF.

accommodates the rapid pace of technological change but also provides a robust framework for predicting future performance trends and identifying areas for further innovation. Such adaptability ensures that performance metrics can effectively guide the development and deployment of next-generation drone technologies, maintaining high standards of safety, reliability, and efficiency over time [51].

3) DATA PRIVACY AND SECURITY CONCERNS

Implementing standardized metrics in drone forensics raises significant concerns about data privacy and security, particularly when dealing with sensitive forensic data. Ensuring the confidentiality and integrity of this data during forensic examinations is crucial to prevent unauthorized access, data breaches, and cyber threats. Sensitive data collected from drones can include flight logs, GPS coordinates, and potentially personally identifiable information (PII), which, if compromised, could lead to severe legal and security implications.

To address these concerns, robust encryption techniques should be incorporated to secure data at rest and in transit. This includes using advanced encryption standards (AES) for data storage and secure socket layer (SSL) or transport layer security (TLS) protocols for data transmission. Additionally, secure data handling protocols must be established, involving access controls, authentication mechanisms, and audit trails to monitor data access and modifications. Implementing multi-factor authentication (MFA) and role-based access control (RBAC) can further enhance security by ensuring that only authorized personnel can access sensitive data. Regular security audits and compliance checks should also be conducted to identify and mitigate potential vulnerabilities. Adopting these measures will help safeguard forensic data from unauthorized access and cyber threats, thereby maintaining the integrity and reliability of the forensic examination process [46].

I. UAV FORENSICS

The field of UAV forensics, while a part of the broader forensic analysis landscape, presents several unique challenges that distinguish it from traditional forensic disciplines. One significant challenge is the integration of diverse data sources. UAVs generate various types of data, including flight logs, GPS coordinates, video footage, and sensor readings [21]. Forensic analysts must possess the technical expertise to collect, process, and analyze this multifaceted data accurately.

Another unique challenge is the rapid pace of technological advancement in UAVs. New models and capabilities are frequently introduced, requiring forensic methodologies to adapt continuously. Traditional forensic fields, such as fingerprint or DNA analysis, do not face the same rate of technological change, making the need for adaptive machine

TABLE 9. The literature survey overview on drone forensics.

Authors	Publ.	Issues being presented	Major Findings
Mazhar et al. [5]	2020	Enhancing the security and forensic analysis of IoT devices due to their vulnerability to continuous attacks.	Proposed an intelligent forensic analysis mechanism that automatically detects the attack performed on IoT devices using a machine-to-machine (M2M)
Ahmed et al. [6].	2022	Most publicly accessible datasets of network traffic are simulated and do not accurately represent the attacks and scenarios found in an actual test environment.	Labeled datasets that are accessible to the public and show cyberattacks on the Internet of Flying Things (IoFT).
Liu et al. [7]	2020	The critical challenges including the restricted network coverage and the limited resource of existing network technologies	A comprehensive survey on opportunities and challenges of UAV-enabled IoE
Renduchintala et al. [8]	2019	Problems of analyzing both physical and digital aspects of drone forensics, providing a comprehensive forensic program with a user-friendly interface for examining drone log metrics.	The development of an efficient tool for handling sensor recordings, including large log files, and the integration of Google Maps API for accurate flight path plotting in the digital forensic program.
Jain et al. [9]	2017	The public and the government are at risk due to the vulnerabilities in drone technology.	Proposed framework would aid investigators in systematically examining drones.
Alotaibi et al. [10]	2022	The lack of a standardized and comprehensive drone-based data collection and analysis paradigm in the field of drone forensics.	A novel CCAFM.
Mozaffari et al. [11]	2019	The growing utilization of UAVs, or drones, in wireless communication systems	Provide guidelines on how to analyze, optimize, and design wireless communication systems based on UAV technology.
Alotaibi et al. [12].	2022	The lack of a standardized forensic model or framework to deal with different drone crimes.	Provided a novel forensic readiness framework that can be applied to the drone forensics field.
Editya et al. [13]	2023	Using Transformer-based neural network architectures for analyzing drone engine failures, expanding the applicability of Transformers beyond NLP to address complex technical problems.	The Transformer achieved the highest F1 score of 93.04% in analyzing drone engine failure data, showcasing its suitability for technical analysis beyond NLP applications.
Renduchintala et al. [14]	2017	A comprehensive software architecture for drone forensics, enabling users to extract and analyze on-board flight data through a user-friendly graphical interface, addressing the need for forensic tools in drone-related criminal cases.	Conducted a comparative analysis of technical specifications among three common commercial drones (3DR Solo, Yuneec Typhoon H, and DJI Phantom 4), including factors such as logging capacity, flight time, range, autopilot software, payload capacity, and cost.
Zhao et al. [15].	2022	A further effort to enhance the method-level UAV tracking performance	Described the Dalian University of Technology Anti-UAV dataset.
Al-Dhaqm et al. [16]	2021	The lack of a standardized drone forensics methodology, proposing a comprehensive Drone Forensics (DRF) model for guiding investigators in the collection, preservation, analysis, and presentation of digital evidence from drone devices.	Provides a detailed understanding of research challenges and opportunities in investigating drone-related events, emphasizing the need for a uniform forensic paradigm for UAVs, and introducing a more comprehensive DRF model compared to existing models.
Stanković et al. [17]	2021	Evaluated the drone's performance, including its ability to carry weight, and conducted digital forensics analysis using various tools on data collected during the flights.	An error, "Not Enough Force/ESCError," was observed during a flight when the drone was carrying a load, highlighting a potential operational limitation.
Allahham et al. [18]	2019	Valuable insights into the potential uses of the dataset and its significance in the domain of RF-based drone detection and classification.	Development and description of the DroneRF dataset, a radio frequency (RF) based dataset of drones functioning in different modes.
Yang et al. [19]	2021	The need for drone forensics to recover flight data and aid investigators in establishing ownership and digital data identification from drone artefacts.	Provides insights into drone forensics, focusing on the identification and individualization of digital data from flight artefacts and mobile devices for two popular drone systems, DJI Spark and Mavic Air.
Ojo et al. [20]	2022	By generating the attack route using predictions, the attackers concentrated on employing this machine-learning technique to obstruct the UAV's operations.	They studied the usage of a Multilayer Perceptron (MLP) machine learning algorithm for the detection technique and demonstrated that it can achieve high detection rates of about 100% for natural picture capture.
Atkinson et al. [21]	2021	Drone forensic programs often fail due to technology misunderstanding and resource limitations.	Drones have the capacity to store a plethora of material that may be highly helpful to forensics investigations.
Mahdi et al. [22].	2023	The need for effective digital forensic tools and techniques to investigate digital crimes and attacks.	Provides a comprehensive overview of the different types of digital forensics tools
Barton & Azhar [23]	2017	The development and application of forensics tools on Linux-based platforms, focusing on interpreting flight data, identifying artefacts, and testing anti-forensics methods in UAV investigations.	Focused on the DJI Phantom 3 Professional Edition and associated mobile platforms, emphasizing the use of scripting tools for forensics.

TABLE 10. The literature survey overview on drone forensics.

Azhar et al. [24]	2018	Resolved the need for forensic analysis of drones captured from crime scenes	The DJI Phantom drone presented a greater number of artefacts and facilitated more straightforward flight data interpretation compared to the A.R drone.
Moustafa & Jolfaei [25]	2020	An autonomous intrusion detection method for identifying advanced cyberattacks in drone networks, utilizing machine learning models, with the decision tree achieving the highest accuracy.	The decision tree model outperformed other machine learning models in categorizing between normal and attack traffic, achieving an accuracy of 99.99% and the highest F1 score.
Whelan et al. [26]	2020	The problem of intrusion detection in UAVs by proposing a novelty-based approach using one-class classifiers to detect abnormal behaviour or attacks in UAV systems.	Among the three classifiers tested, the autoencoder neural network achieved the highest average F1 score of 94.81%, indicating superior performance in UAV intrusion detection.
Taha & Shoufan [27]	2019	Machine learning-based drone detection and classification, covering various modalities, datasets, and challenges in the field.	Machine learning-based drone classification holds promise, but further research is needed to develop more accurate and reliable solutions.
Chen & Chen [28]	2019	The issue of machine learning-based attacks on UAV-based wireless networks and the need for encryption strategies.	Neural network (NN) can successfully decrypt UAV location data.
Syed et al. [29]	2022	A novel machine learning technique for detecting engine faults in aerial vehicles, achieving superior accuracy compared to previous studies.	The machine learning technique, specifically Random Forest (RF) and Gradient Boosting, demonstrated high accuracy in detecting engine faults.
Mekdad et al. [30]	2023	The security and privacy challenges associated with the rapid proliferation of UAVs, offering a comprehensive analysis of vulnerabilities and threats across hardware, software, communication, and sensor levels.	The paper provides insights into common vulnerabilities, threats, attack techniques, and countermeasures related to UAV security and privacy, highlighting the need for enhanced security measures in the UAV industry.
Peleshko et al. [31]	2020	l Improve the quality of life of the population and ensure the sustainable development of cities.	developed technologies and methods for collecting, accumulating and presenting urban environment parameters.
Javed et al. [32].	2022	The need for effective and efficient digital forensic tools and techniques to investigate cybercrimes.	A careful and in-depth study of each tool's features can help investigators pick the most appropriate tool for investigation, thus saving investigation time and effort.
Sihag et al. [33].	2023	The unique challenges and solutions for ensuring the security and data integrity of UAVs.	Developed a comprehensive drone forensics methodology for the analysis of drone systems and relevant artefacts, tools, and benchmark datasets.
Zhang [34].	2021	The need for reliable and cost-effective methods for drone detection and identification.	XGBoost outperforms other machine learning models and presents an open benchmark dataset for RF-based drone detection.

learning models and updated evaluation metrics particularly critical in UAV forensics [52].

Additionally, UAV forensics demands specialized expertise in understanding UAV systems and their operation. Forensic analysts must be familiar with various UAV platforms, communication protocols, and potential vulnerabilities to conduct thorough investigations [16]. This requirement for specialized knowledge distinguishes UAV forensics from other forensic fields, where established procedures and techniques are more standardized and widely understood.

VI. COMPARISON WITH OTHER REVIEW PAPERS

In this section, four research papers—**Alotaibi et al. [10]**, **Al-Dhaqm et al. [16]**, **Mekdad et al. [30]**, and **Sihag et al. [33]**—are examined alongside the paper on UAV forensics. Each of these works contributes to the understanding and development of UAV forensics but exhibits distinct focuses and methodologies, as summarized in Table 7.

The study delves into the intricate relationship between drone forensics, machine learning, and cybersecurity. The primary objective is to scrutinize the current landscape of drone forensics, emphasizing the utilization of machine learning models for enhanced forensic examination of drones. The investigation delves into the specialized expertise required for effective drone forensics, spanning aeronautics, electronics, and data science. The human factor is a central theme, highlighting the legal and ethical dimensions of investigations, necessitating collaboration with drone operators and manufacturers. The need for multidisciplinary approaches is underscored, emphasizing collaboration with experts in drone technology, forensics, and law enforcement. Specific challenges, including interference with RF signals, encryption, security measures, battery life, data retrieval, collision investigations, and the absence of standardized protocols, are comprehensively explored. This study provides an exhaustive examination of the complexities associated with drone forensic examinations, offering a unique perspective compared to existing literature. Unlike other studies, the investigation is distinctive in its empirical validation, providing insights into the limitations of existing models and paving the way for future advancements in drone forensics. The comparison with other studies highlights the comprehensive nature of the investigation, contributing

significantly to the evolving landscape of drone forensics and machine learning applications in this domain.

In addition to discussing the current forensics models, the authors of [5] provided a CCAFM. To assess its efficacy and completeness, the suggested model was contrasted with other models put forth on this subject in the past. The literature's studies on machine learning in the context of processing drone data to find illegal activity were also covered. In [15], the authors examined the difficulties and prospects in drone forensics and contrasted the shortcomings of the current DRF models with their own. They also displayed artifacts related to drone forensics. The four aspects of sensors, hardware, software, and communication were introduced by the authors [23]. These factors were compared in four categories: common vulnerabilities, existing threats, active and passive attacks, and potential computer defenses. The authors [32] discussed drone architecture and communications, security and privacy in levels of networks and communication. drone forensics framework, artifacts, tools, and datasets.

VII. FUTURE RESEARCH DIRECTIONS

Future research directions in drone forensics cover a wide range of topics, including:

- Enhancing the CCAFM involves adjusting it to accommodate new drone technologies, investigating its practicality in real-world situations, and addressing any identified shortcomings [10].
- Further investigation into the application of Transformer-based neural network architectures in drone forensics is suggested, with a focus on enhancing model interpretability, scalability across different drone models, and performance under diverse malfunction scenarios [13].
- Enhancing and extending the autonomous intrusion detection method is suggested, exploring its robustness against evolving cyber threats, expanding its applicability to different drone network architectures, and enhancing its adaptability to changing attack landscapes [25].
- Expanding the comprehensive micro UAV forensic framework, incorporating advanced visualization tools, optimizing the processing of large log files, and addressing challenges associated with real-time forensic analysis in the context of micro UAVs [8], [14].
- Exploring the capacity of drones to store valuable material for forensic investigations is suggested, including identifying and categorizing the types of information stored on drones. Additionally, there is a need to develop standardized protocols for extracting and preserving digital evidence, as well as exploring the legal and ethical implications of utilizing drone-collected data in forensic investigations [21]. Through the identification of these critical areas for future research, scientists can make a substantial contribution toward surmounting current obstacles in the detection of evasive malware and toward the advancement of more potent and versatile solutions.

VIII. CONCLUSION

In conclusion, the exploration of drone forensics reveals a multifaceted landscape, demanding a nuanced interplay between technical proficiency and forensic acumen. From probing current forensic practices utilizing advanced neural network architectures like Transformers to scrutinizing evidence collection methods in drone systems, the study underscores the challenges in analyzing drone attacks and malfunctions. This underscores the urgent need for robust, standardized models capable of keeping pace with the rapid technological evolution of UAVs. The intricacies of analyzing captured drones, particularly in conflict zones, emphasize the necessity for a comprehensive approach that considers operational complexities and technical diversity. Machine learning's pivotal role in enhancing intrusion detection and classification systems introduces new challenges related to data management, model interpretation, and ethical implications. The examination also underscores the critical requirement for meticulous frameworks in drone forensics to guide practitioners through intricate evidence gathering, analysis, and presentation procedures, ensuring integrity and admissibility in legal contexts. As drone technology advances and its applications diversify, future developments in drone forensics will necessitate more sophisticated forensic methodologies, the integration of innovative analytical tools, and the refinement of machine learning models. In essence, drone forensics remains a dynamic and challenging field, demanding continuous innovation and adaptation at the crossroads of technology and law. To sustain its effectiveness as a crucial tool for security and justice, ongoing advancements must not only align with technical excellence but also uphold moral and legal principles.

DATA AVAILABILITY STATEMENT

No new data was created or analyzed in this study. Data sharing is not applicable to this article.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their insightful scholastic comments and suggestions, which improved the quality and clarity of the article.

REFERENCES

[1] A. A. Laghari, A. K. Jumani, R. A. Laghari, and H. Nawaz, "Unmanned aerial vehicles: A review," *Cognit. Robot.*, vol. 3, pp. 8–22, Jan. 2023.
[2] K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber attacks—An approach to the risk assessment," in *Proc. 5th Int. Conf. Cyber Conflict (CYCON)*, Jun. 2013, pp. 1–23.
[3] K. Telli, O. Kraa, Y. Himeur, A. Ouamane, M. Boumehraz, S. Atalla, and W. Mansoor, "A comprehensive review of recent research trends on unmanned aerial vehicles (UAVs)," *Systems*, vol. 11, no. 8, p. 400, Aug. 2023.
[4] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, and R. Chou, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, p. 9, Mar. 2021.
[5] M. S. Mazhar, Y. Saleem, A. Almogren, J. Arshad, M. H. Jaffery, A. U. Rehman, M. Shafiq, and H. Hamam, "Forensic analysis on Internet of Things (IoT) device using machine-to-machine (M2M) framework," *Electronics*, vol. 11, no. 7, p. 1126, Apr. 2022.

[6] M. Ahmed, D. Cox, B. Simpson, and A. Aloufi, "ECU-IoFT: A dataset for analysing cyber-attacks on Internet of Flying Things," *Appl. Sci.*, vol. 12, no. 4, p. 1990, Feb. 2022.

[7] Y. Liu, H.-N. Dai, Q. Wang, M. K. Shukla, and M. Imran, "Unmanned aerial vehicle for Internet of Everything: Opportunities and challenges," *Comput. Commun.*, vol. 155, pp. 66–83, Apr. 2020.

[8] A. Renduchintala, F. Jahan, R. Khanna, and A. Y. Javaid, "A comprehensive micro unmanned aerial vehicle (UAV/drone) forensic framework," *Digit. Invest.*, vol. 30, pp. 52–72, Sep. 2019.

[9] U. Jain, M. Rogers, and E. T. Matson, "Drone forensic framework: Sensor and data identification and verification," in *Proc. IEEE Sensors Appl. Symp. (SAS)*, Mar. 2017, pp. 1–6.

[10] F. M. Alotaibi, A. Al-Dhaqm, Y. D. Al-Otaibi, and A. A. Alsewari, "A comprehensive collection and analysis model for the drone forensics field," *Sensors*, vol. 22, no. 17, p. 6486, Aug. 2022.

[11] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah, "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2334–2360, 3rd Quart., 2019.

[12] F. M. Alotaibi, A. Al-Dhaqm, and Y. D. Al-Otaibi, "A novel forensic readiness framework applicable to the drone forensics field," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–13, Feb. 2022.

[13] A. S. Editya, T. Ahmad, and H. Studiawan, "Forensic investigation of drone malfunctions with transformer," in *Proc. Int. Conf. Smart Syst. Appl. Electr. Sci. (ICSSES)*, Jul. 2023, pp. 1–5.

[14] A. L. P. S. Renduchintala, A. Albehadili, and A. Y. Javaid, "Drone forensics: Digital flight log examination framework for micro drones," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2017, pp. 91–96.

[15] J. Zhao, J. Zhang, D. Li, and D. Wang, "Vision-based anti-UAV detection and tracking," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 12, pp. 25323–25334, Dec. 2022.

[16] A. Al-Dhaqm, R. A. Ikuesan, V. R. Kebande, S. Razak, and F. M. Ghabban, "Research challenges and opportunities in drone forensics models," *Electronics*, vol. 10, no. 13, p. 1519, Jun. 2021.

[17] M. Stankovic, M. M. Mirza, and U. Karabiyik, "UAV forensics: DJI mini 2 case study," *Drones*, vol. 5, no. 2, p. 49, Jun. 2021.

[18] M. S. Allahham, M. F. Al-Sa'd, A. Al-Ali, A. Mohamed, T. Khattab, and A. Erbad, "DroneRF dataset: A dataset of drones for RF-based detection, classification and identification," *Data Brief*, vol. 26, Oct. 2019, Art. no. 104313.

[19] C.-C. Yang, H. Chuang, and D.-Y. Kao, "Drone forensic analysis using relational flight data: A case study of DJI spark and mavic air," *Proc. Comput. Sci.*, vol. 192, pp. 1359–1368, Jan. 2021.

[20] T. Ojo, H. Chi, and S. K. Erskine, "Unmanned aerial vehicle forensics investigation performance under different attacks," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2022, pp. 958–964.

[21] S. Atkinson, G. Carr, C. Shaw, and S. Zargari, "Drone forensics: The impact and challenges," in *Digital Forensic Investigation of Internet of Things (IoT) Devices*. Cham, Switzerland: Springer, 2021, pp. 65–124.

[22] K. Salih and N. Dabagh, "Digital forensic tools: A literature review," *J. Educ. Sci.*, vol. 32, no. 1, pp. 109–124, Mar. 2023.

[23] T. E. A. Barton and M. A. H. B. Azhar, "Open source forensics for a multi-platform drone system," in *Digital Forensics and Cyber Crime*, Prague, Czech Republic. Cham, Switzerland: Springer, 2017, pp. 83–96.

[24] M. A. H. Azhar, T. Barton, and T. Islam, "Drone forensic analysis using open source tools," *J. Digit. Forensics, Secur. Law*, vol. 13, no. 1, p. 6, 2018.

[25] N. Moustafa and A. Jolfaei, "Autonomous detection of malicious events using machine learning models in drone networks," in *Proc. 2nd ACM MobiCom Workshop Drone Assist. Wireless Commun. 5G Beyond*, Sep. 2020, pp. 61–66.

[26] J. Whelan, T. Sangarapillai, O. Minawi, A. Almehmadi, and K. El-Khatib, "Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles," in *Proc. 16th ACM Symp. QoS Secur. Wireless Mobile Netw.*, Nov. 2020, pp. 23–28.

[27] B. Taha and A. Shoufan, "Machine learning-based drone detection and classification: State-of-the-Art in research," *IEEE Access*, vol. 7, pp. 138669–138682, 2019.

[28] X.-C. Chen and Y.-J. Chen, "A machine learning based attack in UAV communication networks," in *Proc. IEEE 90th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2019, pp. 1–2.

[29] N. Syed, M. A. Khan, N. Mohammad, G. B. Brahim, and Z. Baig, "Unsupervised machine learning for drone forensics through flight path analysis," in *Proc. 10th Int. Symp. Digit. Forensics Secur. (ISDFS)*, Jun. 2022, pp. 1–6.

[30] Y. Mekdad, A. Aris, L. Babun, A. E. Fergougui, M. Conti, R. Lazzeretti, and A. S. Uluagac, "A survey on security and privacy issues of UAVs," *Comput. Netw.*, vol. 224, Apr. 2023, Art. no. 109626.

[31] D. Peleshko, T. Rak, J. R. Noennig, V. Lytvyn, and V. Vysotska, "Drone monitoring system DROMOS of urban environmental dynamics," in *Proc. ITPM*, 2020, pp. 178–193.

[32] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. R. Gadekallu, "A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions," *IEEE Access*, vol. 10, pp. 11065–11089, 2022.

[33] V. Sihag, G. Choudhary, P. Choudhary, and N. Dragoni, "Cyber4Drone: A systematic review of cyber security and forensics in next-generation drones," *Drones*, vol. 7, no. 7, p. 430, Jun. 2023.

[34] Y. Zhang, "RF-based drone detection using machine learning," in *Proc. 2nd Int. Conf. Comput. Data Sci. (CDS)*, Jan. 2021, pp. 425–428.

[35] S. Baldi, D. Sun, X. Xia, G. Zhou, and D. Liu, "ArduPilot-based adaptive autopilot: Architecture and software-in-the-loop experiments," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 5, pp. 4473–4485, Oct. 2022.

[36] D. A. Hamdi, F. Iqbal, S. Alam, A. Kazim, and A. MacDermott, "Drone forensics: A case study on DJI phantom 4," in *Proc. IEEE/ACS 16th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2019, pp. 1–6.

[37] Z. Baig, M. A. Khan, N. Mohammad, and G. B. Brahim, "Drone forensics and machine learning: Sustaining the investigation process," *Sustainability*, vol. 14, no. 8, p. 4861, Apr. 2022.

[38] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, "Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends," *Intell. Service Robot.*, vol. 16, pp. 109–137, Mar. 2023.

[39] I. G. Ferrão, L. M. da Silva, S. A. da Silva, C. Dezan, D. Espes, and K. C. Branco, "Intelligent diagnosis of engine failure in air vehicles using the ALFA dataset," in *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, Jun. 2023, pp. 871–878.

[40] A. Keipour, M. Mousaei, and S. Scherer, "ALFA: A dataset for UAV fault and anomaly detection," *Int. J. Robot. Res.*, vol. 40, nos. 2–3, pp. 515–520, Feb. 2021.

[41] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Cambridge, MA, USA: Academic Press, 2011.

[42] K. Al-Room, F. Iqbal, T. Baker, B. Shah, B. Yankson, A. MacDermott, and P. C. K. Hung, "Drone forensics: A case study of digital forensic investigations conducted on common drone models," *Int. J. Digit. Crime Forensics*, vol. 13, no. 1, pp. 1–25, Jan. 2021.

[43] G. Horsman, "Unmanned aerial vehicles: A preliminary analysis of forensic challenges," *Digit. Invest.*, vol. 16, pp. 1–11, Mar. 2016.

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

[45] R. Majeed, N. A. Abdullah, M. F. Mushtaq, and R. Kazmi, "Drone security: Issues and challenges," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 5, 2021.

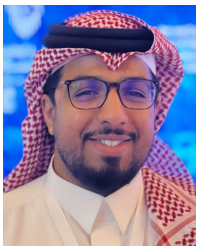
[46] H. Bouafif, F. Kamoun, F. Iqbal, and A. Marrington, "Drone forensics: Challenges and new insights," in *Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Feb. 2018, pp. 1–6.

[47] R. L. Finn and D. Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications," *Comput. Law Secur. Rev.*, vol. 28, no. 2, pp. 184–194, Apr. 2012.

[48] S. M. S. M. Daud, M. Y. P. M. Yusof, C. C. Heo, L. S. Khoo, M. K. C. Singh, M. S. Mahmood, and H. Nawawi, "Applications of drone in disaster management: A scoping review," *Sci. Justice*, vol. 62, no. 1, pp. 30–42, Jan. 2022.

[49] P. Sharma and J. Gillanders, "Cybersecurity and forensics in connected autonomous vehicles: A review of the state-of-the-art," *IEEE Access*, vol. 10, pp. 108979–108996, 2022.

[50] (2022). *National Institute of Standards and Technology. Standards and Performance Metrics for the Road To Autonomous Vehicles*. [Online]. Available: https://www.nist.gov/news-events/events/2022/03/standards-and-performance-metrics-road-autonomous-vehicles
[51] H. Studiawan, G. Grispos, and K.-K.-R. Choo, "Unmanned aerial vehicle (UAV) forensics: The good, the bad, and the unaddressed," *Comput. Secur.*, vol. 132, Sep. 2023, Art. no. 103340.
[52] A. E. Omolara, M. Alawida, and O. I. Abiodun, "Drone cybersecurity issues, solutions, trend insights and future perspectives: A survey," *Neural Comput. Appl.*, vol. 35, no. 31, pp. 23063–23101, Nov. 2023.
[53] W. Shafik, S. Mojtaba Matinkhah, and F. Shokoor, "Cybersecurity in unmanned aerial vehicles: A review," *Int. J. Smart Sens. Intell. Syst.*, vol. 16, no. 1, Jan. 2023.



ELHAAM ABDULRAHMAN DEBAS received the B.Sc. degree from the Department of Computer Networks and Communications, College of Sciences and Arts, King Khalid University, Asir, Saudi Arabia, in 2021. Her current research interest includes drone and cyber security.

ABDULLAH ALBUALI (Member, IEEE) received the B.S. degree in computer science from King Faisal University, in 2009, and the master's and Ph.D. degrees in computer science, with specialization in network security from Southern Illinois University, in 2014 and 2021, respectively. He is currently an Assistant Professor with the College of Computer Sciences and Information Technology, King Faisal University. His research interests include zero trust and identity management, cloud computing, edge computing, volunteer computing, the Internet of Things, underwater wireless sensor networks, cybersecurity, network security, blockchain, unmanned aerial vehicles (drones), and machine learning.

M. M. HAFIZUR RAHMAN received the B.Sc. degree in EEE from KUET, Khulna, Bangladesh, in 1996, and the M.Sc. and Ph.D. degrees in information science from JAIST, Japan, in 2003 and 2006, respectively. He is currently an Assistant Professor with the Department of CN, CCSIT, KFU, Saudi Arabia. Prior to joining KFU, he was an Assistant Professor with Xiamen University Malaysia, and IIUM, Malaysia; and an Associate Professor with the Department of CSE, KUET. He was also a Visiting Researcher with the School of Information Science, JAIST, in 2008; and a JSPS Postdoctoral Research Fellow with the Graduate School of Information Science (GSIS), Tohoku University, Japan, in 2009, and the Center for Information Science, JAIST, from 2010 to 2011. His current research interests include hierarchical interconnection networks, optical switching networks, and software-defined networks.