



## OPEN ACCESS

## EDITED BY

Áine MacDermott,  
Liverpool John Moores University,  
United Kingdom

## REVIEWED BY

Vaibhavi Tiwari,  
Montclair State University, United States  
Mircea Constantin Scheau,  
University of Craiova, Romania

## \*CORRESPONDENCE

Abiodun Esther Omolara,  
✉ esther.oludare@uniabuja.edu.ng  
Oludare Isaac Abiodun,  
✉ aioludare@gmail.com

RECEIVED 08 July 2025

ACCEPTED 06 August 2025

PUBLISHED 24 September 2025


## CITATION

Mohammed UM, Omolara AE, Abiodun OI,  
Rasheed J, Osman O, Lar PM, Adeyinka PO and  
Olugbenga AG (2025) Cyber threat in drone  
systems: bridging real-time security, legal  
admissibility, and digital forensic  
solution readiness.  
*Front. Commun. Netw.* 6:1661928.  
doi: 10.3389/frcmn.2025.1661928

## COPYRIGHT

© 2025 Mohammed, Omolara, Abiodun,  
Rasheed, Osman, Lar, Adeyinka and Olugbenga.  
This is an open-access article distributed under  
the terms of the [Creative Commons Attribution  
License \(CC BY\)](#). The use, distribution or  
reproduction in other forums is permitted,  
provided the original author(s) and the  
copyright owner(s) are credited and that the  
original publication in this journal is cited, in  
accordance with accepted academic practice.  
No use, distribution or reproduction is  
permitted which does not comply with these  
terms.

# Cyber threat in drone systems: bridging real-time security, legal admissibility, and digital forensic solution readiness

Usman Mistura Mohammed<sup>1</sup>, Abiodun Esther Omolara<sup>1\*</sup>,  
Oludare Isaac Abiodun<sup>1\*</sup>, Jawad Rasheed <sup>2,3,4,5</sup>, Onur Osman<sup>6</sup>,  
Patricia Manko Lar<sup>7</sup>, Philip Oyadiran Adeyinka<sup>8</sup> and  
Adeola Grace Olugbenga<sup>9</sup>

<sup>1</sup>Department of Computer Science, University of Abuja, Gwagwalada, Nigeria, <sup>2</sup>Department of Computer Engineering, Istanbul Sabahattin Zaim University, Istanbul, Türkiye, <sup>3</sup>Department of Software Engineering, Istanbul Nisantasi University, Istanbul, Türkiye, <sup>4</sup>Research Institute, Istanbul Medipol University, Istanbul, Türkiye, <sup>5</sup>Applied Science Research Center, Applied Science Private University, Amman, Jordan, <sup>6</sup>Department of Electrical and Electronics Engineering, Istanbul Topkapi University, Istanbul, Turkey, <sup>7</sup>Department of Microbiology, University of Jos, Jos, Nigeria, <sup>8</sup>Department of Public Administration, University of Abuja, Gwagwalada, Nigeria, <sup>9</sup>Department of Chemical Engineering, Faculty of Engineering, University of Abuja, Gwagwalada, Nigeria

The rapid expansion of drones otherwise known as Unmanned Aerial Vehicles (UAVs), in critical sectors has increased their exposure to cyber threats such as GPS spoofing, command hijacking, and firmware tampering. Existing forensic tools often fail to address UAV-specific challenges like volatile memory and limited storage, hindering effective investigations. Hence, to address this gap, this study proposes the Enhanced UAV Forensic Framework (EUAVFF) a modular, forensic-by-design model integrating blockchain audit trails, secure logging, telemetry offloading, and UAV-friendly encryption. Validated through a literature review and a stakeholder survey (n = 100), results showed that over 70% of respondents lacked awareness of UAV cyber risks, and current drones were rated poorly in key forensic areas, including tamper-proof logging and legal evidence handling. Only 28% were familiar with drone-specific threats, reflecting critical gaps in preparedness. These findings emphasize the urgent need for proactive forensic integration. EUAVFF offers a structured path to secure, accountable, and resilient UAV operations in increasingly hostile cyber environments.

## KEYWORDS

UAV security threats, UAV digital forensics solution, forensic readiness, cybercrime investigation, forensic framework, real-time evidence collection

## 1 Introduction

Unmanned Aerial Vehicles (UAVs), commonly referred to as drones, have become an integral part of modern technological systems, revolutionizing operations in defense, agriculture, logistics, surveillance, disaster response, and urban planning (Mohsan et al., 2023; Khan et al., 2022). Their ability to operate remotely and autonomously has introduced significant efficiencies across various industries (Fisher and Schnittger, 2012). However, the increasing deployment of UAVs has raised serious concerns about their vulnerability to cyber-crimes (Ezeji, 2024; Yaacoub et al., 2022). UAV systems, which rely heavily on

TABLE 1 Some cyber-attacks against UAVs and their estimated economic impacts.

Year	Incident description	Estimated damage in US (USD)	Region affected
Jan–May 2025	GPS spoofing of a commercial delivery UAV	\$9 million	United States
2024	Hijacking of a police surveillance drone	\$5.4 million	United Kingdom
2023	Data breach from UAV surveying sensitive infrastructure	\$4.2 million	Germany
2022	Drone crash due to malware attack	\$3.8 million	South Korea
2021	Jamming attack on agricultural UAV swarm	\$2.5 million	Brazil
2020	UAV hijack during military training operation	\$7 million	Israel
2019	Unauthorized UAV access to secure airspace	\$1.6 million	Canada
2018	Distributed denial-of-service (DDoS) attack on UAV fleet	\$2.3 million	Japan
2017	UAV firmware corruption causing data loss	\$1.1 million	Australia
2016	Drone network infiltration disrupting delivery operations	\$3.4 million	China
2024	Spoofing attack on reconnaissance UAV during border conflict	\$6.5 million	Ukraine
2023	UAV command channel hijack over military zone	\$7.2 million	Russia
2022	UAV-based smuggling and surveillance disruption	\$2.1 million	Nigeria
2021	Jamming and UAV loss in anti-poaching operation	\$1.3 million	Kenya
2020	Surveillance drone taken offline during protest monitoring	\$2.8 million	South Africa
2019	Cyberattack on UAV fleet used for crop monitoring	\$1.9 million	Argentina
2018	GPS signal interference during rainforest mapping mission	\$1.5 million	Peru

(Author's own processing).

wireless communication, GPS navigation, and embedded software, are often exposed to cyber-attacks that can disrupt missions, compromise sensitive data (Kumar and Thampi, 2025), or even weaponize drones for malicious purposes. The growing reliance on UAVs has revealed a critical cybersecurity issue such as jamming, UAV eavesdroppers (Tang et al., 2019) and gaps (Shafik et al., 2023; Rugo et al., 2022; Krishna and Murphy, 2017).

While numerous studies have addressed general UAV security through encryption techniques, intrusion detection systems, and secure routing protocols (Hadi et al., 2023; Shafique, et al., 2021), there remains an evident lack of comprehensive digital forensic solutions specifically tailored for UAVs (Studiawan et al., 2023). This absence is particularly concerning in scenarios where UAVs are involved in incidents or cyber-attacks (Giannaros et al., 2023), and post-event investigation is essential for determining the cause, impact, and responsible parties (Kouros, 2025). Existing digital forensic tools are predominantly designed for traditional computing systems, and their application in UAV contexts is often limited (Salamh et al., 2021a), inefficient (Alsulami, 2022), or fails to meet real-time operational demands (Baig et al., 2017). Although the literature has proposed several mechanisms for enhancing UAV security such as anomaly-based intrusion detection and secure UAV communication architectures (Ntizikira et al., 2023; Whelan et al., 2020). However, these approaches largely focus on prevention and detection rather than forensic readiness and post-incident investigation (Ab Rahman and Choo, 2015; Rowlingson, 2004).

Consequently, when cyber-attacks do occur, there is often insufficient forensic evidence to reconstruct events, identify attack

vectors, or prosecute offenders (Brown, 2015; Chaikin, 2006). The persistence of this problem is due to challenges such as limited onboard memory, power constraints, the complexity of real-time data logging during flight (Verma, 2024; Marinoni et al., 2006). Then, the lack of standardized forensic models for UAV ecosystems (Salamh et al., 2021b). A documented cyber-attacks or incidents involving UAVs and their associated damage (Cosar, 2022), over the last 10 years is significant that call for urgent attention. Therefore, some figure of documented cyber-attacks against UAVs and their description with related economic damages across some countries over the past 10 years is presented in Table 1.

These estimated damages in Table 1 highlight the increasing cost and frequency of UAV-related cyber incidents, emphasizing the urgent need for solutions that go beyond preventive security and encompass comprehensive forensic capabilities. Hence, this research proposes the design and implementation of a UAV-specific digital forensic framework that could integrates real-time anomaly detection, secure forensic data logging, and autonomous evidence preservation mechanisms.

## 2 Paper organization

This paper is structured as follows: Section 1 introduces UAVs and their cybersecurity relevance and presents also the study motivation. Section 2 outlines the paper structure. Section 3 details the study's contributions. Section 4 research challenges. Section 5 highlights and discusses digital forensic solutions to the challenges of Cyber-Crimes against UAV systems. Section 6

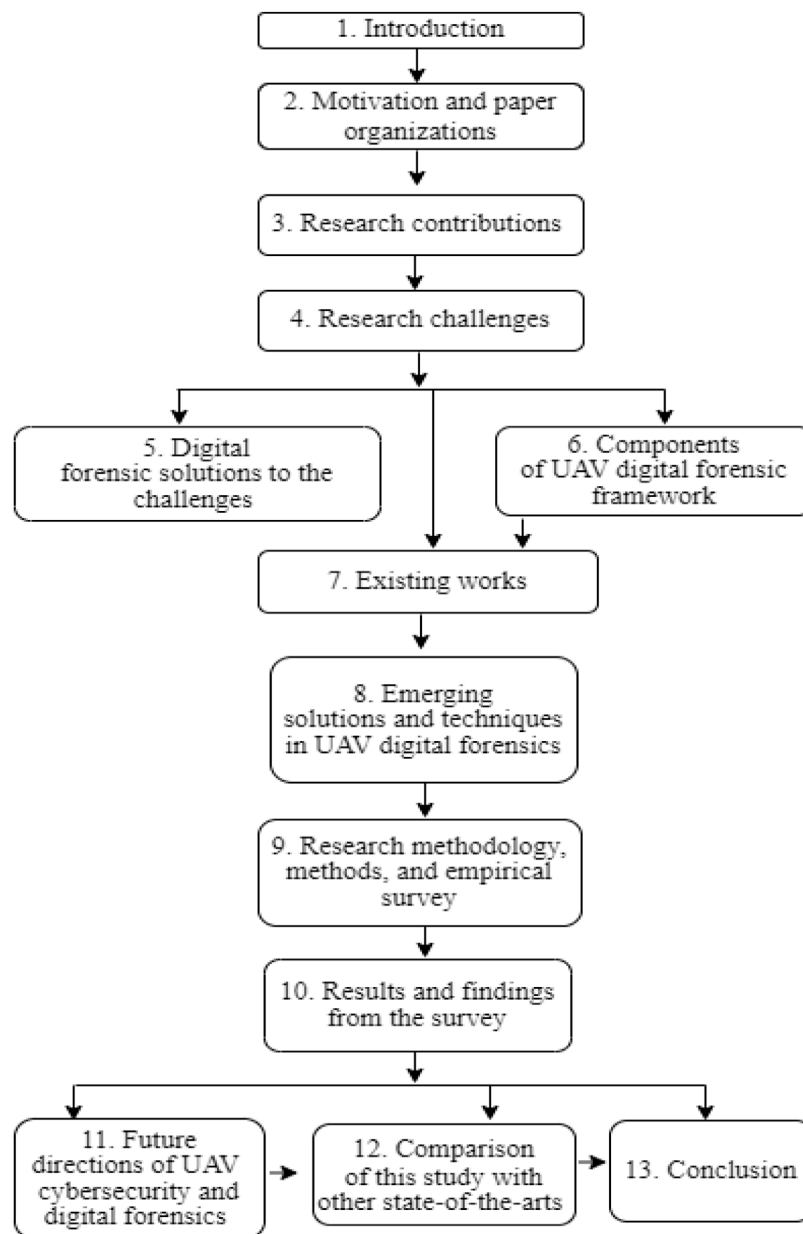


FIGURE 1  
Structure of the survey (Author's own processing).

discussed the components of UAV digital forensic framework. Section 7, discusses the literature review. Section 8 enumerates the emerging solutions and techniques in UAV digital forensics. Section 9 presents the research methodology then Section 10 outlines the result and findings from the comprehensive survey. Section 11 enumerated the future directions of UAV cybersecurity and digital forensics then Section 12 compared this study with other state-of-the-arts and finally Section 13 concludes the study based on its objective, the implications and the future. However, to aid in the reader's understanding and provide a clear visualization of how the paper is structured, an overview of the survey's organization is illustrated in Figure 1.

### 3 Paper contributions

This study contributes significantly to UAV cybersecurity and digital forensics by addressing key gaps in forensic readiness, threat detection, and post-incident investigation. It introduces the Enhanced UAV Forensic Framework (EUAVFF) a novel, UAV-specific model for secure, real-time, and legally admissible evidence collection. Adopting a forensic-by-design approach, the framework integrates tamper-proof logging, blockchain audit trails, modular compatibility, and secure data offloading to enable proactive forensic capabilities. The study identifies 21 core forensic challenges including volatile memory loss, encryption barriers,

TABLE 2 Research challenges and matching solutions in UAV digital forensics.

S/n	Challenge	Solution
1	Lack of forensic readiness	Integrate secure logging, encryption, telemetry archiving from design
2	Poor standardization	Collaborate globally (ISO, IEEE, ICAO) on UAV forensic norms
3	Volatile/encrypted data issues	Use non-volatile memory and key escrow systems for access
4	Attribution difficulty	Use AI and PKI-based identity verification
5	Anti-forensics	Deploy blockchain/WORM logging and intrusion detection
6	Lack of forensic datasets	Create anonymized datasets for training and benchmarking
7	Jurisdictional/legal hurdles	Establish treaties and enforce UAV registration
8	Low stakeholder awareness	Conduct awareness campaigns and drone forensics training
9	Evolving threats	Promote AI-based detection and joint R&D initiatives
10	Weak real-time monitoring	Integrate forensic modules with health monitoring and cloud
11	High costs	Adopt modular design and promote open-source tools
12	Lack of experts	Launch specialized UAV forensic training and certifications
13	Complex threat landscape	Mandate layered defenses and UAV vulnerability assessments
14	Insufficient logging	Use non-volatile storage and standard logging formats
15	Encrypted/obfuscated firmware	Standardize forensic APIs and require key escrow
16	Legal gaps	Harmonize global laws and define lawful access protocols
17	Cloud forensic access	Design forensic-aware cloud storage with audit logs
18	Timeline reconstruction	Use timestamped logs and blockchain audit trails
19	Vendor non-cooperation	Mandate cooperation through compliance clauses
20	Closed protocols	Promote open interfaces and reverse engineering tools
21	Evidence contamination	Use write-protected extraction tools and standard kits

(Author's own processing).

and jurisdictional issues and proposes targeted interventions. Using a mixed-methods design, it reveals low stakeholder awareness, highlighting the urgent need for training, policy reform, and standardization. It further proposes a multi-layered architecture with AI-based threat detection and cloud-integrated telemetry handling, adaptable to dynamic UAV environments. Lastly, it advocates for global harmonization through open-source tools and regulatory cooperation, laying a strong foundation for secure, accountable, and forensically capable UAV ecosystems.

## 4 Research challenges

Despite advances in digital forensics, critical challenges persist, particularly in addressing UAV-specific cybersecurity threats. These span technical, legal, and operational areas, including volatile memory loss, lack of standardized protocols, real-time data constraints, and jurisdictional hurdles. The absence of unified forensic datasets, anti-forensic tactics, and cross-platform incompatibilities further complicate effective response. Tackling these challenges demands interdisciplinary collaboration among cybersecurity experts, legal practitioners, UAV manufacturers,

and policymakers. Only through such coordinated efforts can forensic capabilities evolve to address the complexity of emerging UAV threats. This study identifies twenty-one core challenges affecting UAV cyberattacks and their corresponding forensic solutions as presented in [Table 2](#).

These identified challenges highlight the need for interdisciplinary collaboration across UAV engineering, cybersecurity, digital forensics, and legal domains. [Section 5](#) discusses each challenge alongside its proposed forensic solution.

## 5 Digital forensic solution to the challenges of cyber-crimes against UAV systems

This study identifies 21 core challenges affecting UAV cybersecurity and digital forensic readiness. Resolving these issues requires a multidisciplinary approach involving technical innovation, legal reforms, standardized protocols, expert training, and increased public and institutional awareness. These efforts are crucial to ensure UAV systems remain secure, reliable, and legally accountable. The following subsections detail proposed forensic solutions to mitigate each challenge.

## 5.1 Lack of forensic readiness in UAV design

Most UAVs are not built with forensic capabilities in mind, compromising post-incident investigations (Studiawan et al., 2023; Alotaibi et al., 2022). A forensic-by-design approach should be adopted, integrating secure logging, tamper-resistant components, encrypted communications, and telemetry backups (Vassiliadis and Hedström, 2024). These measures are vital for evidence preservation, regulatory compliance, and building operational trust (Hadi et al., 2023).

### 5.1.1 Recommended forensic solution

A forensics-by-design approach should be embedded in UAV development to ensure accountability and forensic readiness. Main elements include secure, cryptographically protected logging of critical data; tamper-resistant hardware; continuous telemetry backups; encrypted communications; and audit-capable controllers that log key events. These measures support reliable forensic analysis, regulatory compliance, insurance assessments, and public trust.

## 5.2 Inadequate standardization in UAV forensics

UAV forensic practices lack consistency across jurisdictions and vendors. International bodies such as ISO, IEEE, and ICAO should establish unified forensic standards (Fakhouri et al., 2024; Mantas and Patsakis, 2022; McTurk, 2019). These standards must address evidence handling, logging formats, legal protocols, and investigator training to ensure global interoperability and evidentiary integrity (Dratwa, 2014). This inadequacy of uniformity of standard undermines the reliability and admissibility of forensic evidence, especially in legal proceedings. Unlike traditional digital devices with well-established forensic protocols, UAVs present greater complexity, integrating flight control systems, GPS, sensors, real-time communication, and payloads. Without universal standards, critical data may be missed, misinterpreted, or rendered inadmissible in court.

### 5.2.1 Recommended forensic solution

International bodies like ISO, IEEE, and ICAO must collaborate to create unified UAV forensic standards. These should cover evidence handling, standardized data logging, forensic imaging protocols, certified forensic tools, international cooperation, and specialized training. Such standards would improve legal defensibility, promote compliance, and enhance UAV forensic readiness. Currently, the absence of standardization hampers effective investigation and accountability. A global, harmonized framework is crucial for building a resilient and interoperable UAV forensic ecosystem.

## 5.3 Limited access to volatile or encrypted data

Critical UAV data is often stored in volatile memory or encrypted formats that are lost after crashes or power-offs (Viswanathan and

Baig, 2020). Forensic access can be improved using SSDs, key escrow systems, redundant storage, and secure decryption modules to ensure lawful and timely access to essential data. Encrypted data, while essential for security, can hinder investigations when decryption keys are unavailable post-incident. This limitation significantly impairs investigators' ability to reconstruct events or trace cyber intrusions, especially in high-stakes applications like military operations, border surveillance, or autonomous commercial drones, where accountability is paramount.

### 5.3.1 Recommended forensic solutions

A combined hardware-software strategy is essential to improve UAV forensic readiness. Key measures include: using SSDs or flash modules to capture memory snapshots during critical events; integrating secure, cryptographically protected forensic access points for authorized investigators; implementing trusted key escrow systems with hardware security modules for lawful decryption; enabling redundant storage or real-time cloud syncing to safeguard evidence; and enforcing time-bound, auditable forensic access governed by legal protocols. Therefore, these solutions enhance data preservation, support incident response, and strengthen legal and public trust in UAV systems.

## 5.4 Challenges in identifying and attributing cyber-attacks

UAV cyber-attacks are often anonymous and difficult to trace (Abbadi and Lachkar, 2025; Ly and Ly, 2021). These attacks including GPS spoofing, command hijacking, signal jamming, data injection, and firmware manipulation are often conducted remotely and anonymously using techniques that erase traces or mimic legitimate sources (Hartmann and Giles, 2016). Effective attribution requires real-time anomaly detection, PKI-based authentication, centralized UAV identity registries, and blockchain audit trails to verify activity and associate it with specific actors or devices.

### 5.4.1 Recommended forensic solutions

Advanced frameworks integrating AI, digital forensics, and secure communications are required, to improve UAV cyber-attack attribution. Main strategies include:

- (i) AI-driven behavioral and network forensics to detect anomalies and match attack patterns in real time.
- (ii) Real-time monitoring through embedded forensic agents that flag unusual activity and log data for investigation.
- (iii) PKI-based authentication to verify UAV communications and detect spoofing.
- (iv) Drone identity management systems to trace actions back to specific devices via centralized registration.
- (v) Cyber threat intelligence databases to match incidents with known threats and actors.
- (vi) Digital watermarking and immutable audit trails to preserve forensic evidence and system integrity.

Despite limitations such as attacker obfuscation and jurisdictional barriers, combining these tools enhances attribution

and deterrence. Long-term success depends on standardization and international cooperation.

## 5.5 Proliferation of anti-forensic techniques

Adversaries may deliberately erase, manipulate, or obscure UAV data to prevent investigation (Sinha, 2021). In UAVs, these may include wiping telemetry logs, encrypting flight data post-compromise, falsifying timestamps, spoofing GPS signals, or injecting false data (Horsman and Errickson, 2019). These tactics are especially problematic in critical domains such as defense, disaster response, and law enforcement, where accurate incident reconstruction is vital. UAVs should implement immutable storage such as WORM or blockchain, machine learning-based behavioral profiling, and tamper-evident logs to counter these anti-forensic tactics and ensure investigative reliability.

### 5.5.1 Recommended forensic solution

UAVs should implement tamper-resistant designs and strong data integrity measures to counter anti-forensic tactics. This includes using immutable storage such as blockchain, WORM, real-time intrusion detection systems (IDS), redundant log backups, and machine learning-based behavioral profiling. Legal frameworks should mandate forensic readiness and standardized logging. Together, these strategies enhance UAV security, accountability, and forensic reliability.

## 5.6 Lack of forensic datasets

The forensic community lacks access to standardized UAV datasets for tool validation, machine learning, and benchmarking. Developing anonymized, open-source datasets that simulate real-world UAV incidents is essential for training forensic systems and improving investigative consistency (Fakhouri et al., 2024; Studiawan et al., 2023).

### 5.6.1 Recommended forensic solution

However, to address the current gap, it is crucial to develop publicly accessible UAV cyber-attack datasets that are realistic and reflect diverse threat scenarios. These datasets should be created through collaboration between government, academia, drone manufacturers, and cybersecurity experts to ensure relevance and accuracy. A robust UAV forensic dataset should include:

- (a) **Multimodal Data Streams:** Integrating synchronized data such as GPS logs, telemetry, network traffic, control commands, camera footage, and sensor readings to support full-cycle forensic analysis.
- (b) **Labeled Attack Scenarios:** Clearly marked entries identifying the type of attack take for example spoofing, jamming, timeline, attacker behavior, and system response to aid in supervised model training and validation.
- (c) **Diverse Operational Environments:** Scenarios should reflect various settings urban, rural, maritime, and industrial with conditions like weather shifts or hardware constraints to mirror real-world operations.
- (d) **Synthetic and Real Data Fusion:** Due to ethical constraints on real attack data, synthetic data from simulations or digital twins should supplement real data to improve completeness and realism.
- (e) **Privacy Compliance:** Shared datasets must anonymize sensitive information and comply with relevant privacy laws and security standards.

## 5.7 Jurisdictional and legal barriers to evidence acquisition

UAVs often operate across national boundaries, creating legal obstacles to forensic data retrieval (Brown, 2015). Cross-border treaties, harmonized data access protocols, UAV registration requirements, and cooperation through international legal bodies like ICAO and UNODC are needed to streamline lawful evidence acquisition.

### 5.7.1 Recommended forensic solution

A unified global legal framework is essential for effective UAV digital forensics. This includes international treaties for evidence handling, legal harmonization through bodies like ICAO and UNODC, mandatory drone registration and data logging, and strict adherence to national laws and court oversight. Capacity building in developing regions and a standardized, secure evidence-sharing platform are also crucial. Together, these measures will enhance cross-border cooperation, ensure privacy, and improve global forensic readiness.

## 5.8 Poor public and stakeholder awareness

Many UAV operators, regulators, and security personnel are unaware of drone-specific cyber risks and forensic principles (Singh, 2024; Mohsan et al., 2023). Mandatory training, public education, and professional certifications are critical to fostering forensic-conscious drone ecosystems. Likewise, law enforcement personnel may lack the skills to handle UAV digital evidence (Gülataş and Baktur, 2018; Horsman, 2016), and policymakers frequently overlook forensic needs in drone regulations. This knowledge gap undermines effective incident response and weakens the resilience of UAV systems.

### 5.8.1 Recommended forensic solution

A comprehensive awareness and capacity-building strategy is needed to strengthen UAV cybersecurity and forensic readiness. This includes public education campaigns, mandatory training for drone operators, and specialized instruction for law enforcement and emergency responders. Academic programs should integrate UAV forensics into their curricula, while professional certifications can formalize expertise in the field. Collaboration with industry is vital to promote forensic-by-design principles, and policymakers must be engaged to support regulatory and funding initiatives. Overall, improving awareness through education, regulation, and cooperation is essential to enhance security and preparedness against UAV cyber threats.



## 5.9 Evolving nature of UAV cyber threats

The UAV threat landscape has become dynamic, with new attack vectors continuously emerging (Zaki et al., 2024). As drones become more complex, their attack surface widens exposing them to threats like GPS spoofing, command hijacking, malware injection, and DoS attacks. Threat actors, including state-sponsored groups, continue to exploit vulnerabilities, especially in high-risk domains such as surveillance, infrastructure monitoring, and disaster response. In such contexts, even minor cyber intrusions can lead to mission failure or safety risks. Traditional static defenses are no longer adequate, highlighting the need for adaptive and proactive security strategies.

### 5.9.1 Recommended forensic solution

Now, to address the rapidly evolving UAV cyber threat landscape, continuous research is essential for identifying new vulnerabilities and zero-day threats. AI-driven systems can enhance real-time threat detection and resilience through anomaly monitoring and self-healing mechanisms. Secure over-the-air patching ensures timely updates without service disruption. Cross-sector collaboration including industry, academia, and government is key to threat sharing and coordinated defense. Red team exercises and simulated attacks help uncover system weaknesses and improve forensic readiness. Dynamic risk assessments allow UAVs to adapt operations based on threat levels. Ongoing research into AI-driven anomaly detection, real-time monitoring, and joint academic-industry R&D initiatives is necessary to ensure forensic systems remain resilient and adaptive. Global policy harmonization and joint cybersecurity frameworks are vital to combat transnational drone threats. A multi-layered, adaptive approach is crucial to maintain UAV security and forensic accountability.

## 5.10 Limited integration with real-time monitoring systems

Without real-time forensic tools, critical evidence may be lost or altered during an incident (Choudhary et al., 2018). The lack of integration between real-time health monitoring, intrusion detection, and forensic tools limits prompt response and evidence collection (Salfati et al., 2022; Adel, 2020; Johansen, 2017; Alharbi et al., 2011).

### 5.10.1 Recommended forensic solution

Real-time forensic tools should be embedded into drone systems to enhance UAV cybersecurity. These tools detect anomalies, preserve evidence instantly, and log events with precise metadata for accurate incident reconstruction. Integrating forensics with health monitoring and intrusion detection systems (IDS) enables automated responses and links physical anomalies to cyber threats. Due to storage limits, UAVs should offload data to secure cloud platforms for backup and remote analysis. This integration bridges the gap between attack detection and investigation, enabling proactive, continuous threat monitoring. However, challenges such as computational limits, legal compliance, and standardization must be addressed through multi-stakeholder collaboration. UAVs should integrate embedded forensic agents,

health-monitoring systems, and secure cloud offloading to capture data continuously and preserve volatile evidence in real time.

## 5.11 High cost of implementation

Advanced forensic solutions can be financially prohibitive, especially for small-scale UAV operators (Henriques et al., 2024; Alsulami, 2022; Ganesh et al., 2022; Chen et al., 2019; Baig et al., 2017). These expenses include not only the procurement of specialized tools and software but also the need for skilled personnel, ongoing training, and system integration. For small-scale UAV operators such as independent drone service providers, research groups, startups, and hobbyists these financial demands can be overwhelming. As a result, the adoption of such advanced forensic capabilities remains limited in non-enterprise settings. This creates a significant disparity in the cyber resilience of UAV ecosystems, where only large organizations or government entities can afford robust forensic readiness, leaving smaller operators more vulnerable to cyber threats and less capable of investigating or responding to security incidents effectively.

### 5.11.1 Recommended forensic solution

The study proposes modular and scalable architectures that allow flexible adoption based on needs and budget, to make UAV digital forensics more accessible and cost-effective. Government incentives like subsidies and certification support can ease financial burdens. Open-source toolkits provide affordable, customizable forensic tools. Framing forensic readiness as a long-term cost-saving and trust-building measure further strengthens the case. However, affordability must not compromise reliability designs must maintain data integrity and compatibility. Overall, combining modular systems, public support, and open innovation can enable widespread, effective forensic integration in UAV operations. Adopting modular forensic architectures, incentivizing open-source development, and providing government support can lower barriers to adoption while preserving functionality.

## 5.12 Lack of skilled forensic experts in UAV domain

Investigating UAVs requires expertise beyond traditional digital forensics, including flight dynamics, wireless telemetry, and embedded systems (Sihag et al., 2023; Rugo et al., 2022). Unlike traditional digital forensics, UAV investigations require expertise in aerospace systems, embedded hardware, flight software, wireless communication, and real-time telemetry. As UAVs become more common in critical sectors like logistics, defense, and law enforcement, the demand for such skills is growing but the talent pipeline remains limited.

### 5.12.1 Recommended forensic solution

Nevertheless, to overcome legal barriers in UAV forensics, clear international frameworks, standardized evidence protocols, and cooperative agreements like MLATs are needed. These should support lawful data access, cross-border investigations, and protect privacy while ensuring forensic evidence is admissible

and collected ethically. Academic curricula and hands-on certification programs tailored to drone forensics are urgently needed to close this skills gap.

## 5.13 Understanding cyber threats to UAV systems

UAVs face attacks on multiple subsystems including GPS, IMUs, flight controllers, and data links (Wang et al., 2023; Oruc, 2022). These face attacks can lead to mission failure, data theft, or drone weaponization (Eltoukhy et al., 2025; Eltoukhy, 2025). A layered defense model combined with periodic UAV vulnerability assessments can improve threat resilience and ensure forensic traceability in multi-vector attack scenarios.

### 5.13.1 Common attack types include

UAVs face several critical cyber threats that compromise their safety and functionality. These include GPS spoofing, where fake signals misguide drone navigation; signal jamming, which disrupts control channels; and hijacking, which exploits unsecured links to seize control. Denial-of-Service (DoS) attacks overwhelm systems, rendering drones unresponsive (Xie et al., 2024). Malware injection can corrupt firmware or extract sensitive data, while Man-in-the-Middle (MITM) attacks allow real-time interception and manipulation of communications. Lastly, data tampering distorts telemetry or video feeds, hindering operational decision-making and forensic investigations. These threats are worsened by the complexity and fragmentation of UAV subsystems such as flight controllers, GPS, IMUs, and transceivers often built with proprietary protocols and lacking consistent security features. Many drones use outdated software, default passwords, and unsecured interfaces, particularly in commercial off-the-shelf (COTS) models. Weak encryption and poor authentication further expand the attack surface, allowing adversaries to hijack commands, inject malicious payloads, or clone devices. As drones are increasingly used in smart cities, emergency response, defense, and industrial automation, the consequences of cyber breaches grow significantly, including:

- (i) Exposure of sensitive surveillance data
- (ii) Operational disruption or physical destruction
- (iii) Unauthorized surveillance or targeting
- (iv) Espionage, sabotage, or terrorism

### 5.13.2 Recommended forensic solution

Mitigating these threats requires a layered defense approach that includes secure-by-design development, encryption, access controls, and real-time monitoring. Integrating digital forensics and standardized incident response protocols ensures accountability and strengthens system resilience. Given their growing role in critical domains, UAVs must be protected through proactive cybersecurity and forensic readiness to prevent malicious exploitation.

## 5.14 Volatile memory and limited logging

Many UAVs rely on volatile or cyclic logs that fail to capture comprehensively the data that can be used as evidence (Shakhatreh

et al., 2019; Xia et al., 2023; Shakeri et al., 2019; McEnroe et al., 2022). Critical data including telemetry, commands, and sensor inputs is often stored in volatile memory (RAM), which is lost if the UAV crashes, shuts down, or is disabled. This poses a major challenge for forensic investigations, as essential evidence may be permanently erased. In addition, many UAVs offer only basic or proprietary logging systems that capture minimal flight data such as speed, altitude, GPS, while omitting crucial security-relevant events such as unauthorized access attempts, spoofing, or communication anomalies. Logs may be encrypted, poorly formatted, or inaccessible to forensic tools. Onboard storage is often small, with logs overwritten cyclically unless data is offloaded in real time. These issues hinder cross-platform investigations and severely limit forensic visibility, especially in high-risk applications like law enforcement, infrastructure inspection, or military surveillance.

### 5.14.1 Recommended forensic solution

Systems should use non-volatile memory like SSDs or FRAM to retain data after power loss. Secure, tamper-resistant logging must be embedded in flight controllers to ensure audit trail integrity to enhance UAV forensic readiness. Real-time offloading of telemetry to cloud platforms helps preserve evidence if the UAV is compromised. By adopting a forensics-by-design approach during development, UAVs can support effective investigations and accountability. These measures address the critical weaknesses of volatile memory and limited logging through durable storage, secure standards, and proactive data preservation. Embedding tamper-proof, non-volatile memory and adopting standardized logging schemas can enhance data integrity and investigatory accuracy.

## 5.15 Encryption and obfuscation

While encryption is vital for UAV cybersecurity, it often impedes forensic access (Alenezi, 2024; Stoyanova et al., 2020). Encryption secures UAV telemetry, C2 signals, video, and onboard storage from unauthorized access especially in sensitive missions (Aissaoui et al., 2023; Hadi et al., 2023; Mekdad et al., 2023). However, it also creates significant challenges for digital forensics (Alenezi, 2024; Casino et al., 2022; Stoyanova et al., 2020). Without decryption keys often stored on UAVs, ground stations, or cloud server's investigators may be unable to access encrypted evidence (Shafique et al., 2021; Ever, 2020). This issue is exacerbated when keys are withheld by uncooperative vendors or involve criminal-controlled drones. Proprietary or undocumented encryption methods, along with obfuscation tactics like encrypted firmware and compressed logs, further hinder analysis. While these measures strengthen cybersecurity, they complicate forensic investigations, often requiring reverse engineering or specialized tools. Legal constraints and inadequate vendor support can delay access, risking the loss of critical evidence needed to trace attacks, detect malware, or reconstruct incidents.

### 5.15.1 Recommended forensic solution

UAVs should adopt forensic-friendly encryption frameworks, such as:



- (i) Key escrow mechanisms or forensic APIs allowing authorized access under legal orders.
- (ii) Documented encryption standards supported by manufacturers under controlled conditions.
- (iii) Cross-platform logging/encryption schemas to standardize data handling and reduce reliance on proprietary tools.

Balancing strong encryption with lawful forensic access is key to ensuring accountability and trust in UAV systems without compromising their security. Manufacturers should implement forensic-friendly encryption frameworks, key escrow mechanisms, and documented forensic APIs to enable lawful evidence decryption during investigations.

## 5.16 Legal and regulatory barriers

The lack of clear laws for UAV forensics complicates evidence handling and admissibility (Atkinson et al., 2021; Yeboah-Ofori and Brown, 2020). UAV digital forensics faces major legal and regulatory challenges (Mantas and Patsakis, 2022; Atkinson et al., 2021). As drones operate across borders and store data on foreign servers, jurisdictional conflicts hinder timely evidence access (Tyshchuk, 2024; Atrey, 2023; Yeboah-Ofori and Brown, 2020). Without mutual legal assistance treaties (MLATs), investigators may be denied critical data. Accessing encrypted logs often requires court orders, while proprietary systems or foreign ownership may block access entirely, risking the loss of volatile evidence. Privacy laws further complicate matters, as UAVs collect sensitive data like location, video, and biometrics. With legal protections varying by country, standardizing forensic protocols that respect civil rights is difficult. Data ownership and evidentiary admissibility add more hurdles—drone data may be protected as intellectual property, and improper handling can lead to legal rejection. Moreover, unclear laws on drone interception or remote evidence retrieval may classify forensic efforts as illegal hacking, limiting the use of proactive tools.

### 5.16.1 Recommended forensic solution

International legal harmonization, clear national policies on data retention and cooperation, and specialized training for law enforcement as well as forensic personnel are essential to overcome legal barriers in UAV forensics. Aligning global efforts will help balance security, privacy, and accountability in drone investigations. International regulatory bodies must define unified protocols for drone data access, retention, and admissibility across legal jurisdictions.

## 5.17 Limited forensic access to cloud-linked UAV data

UAVs increasingly store logs and telemetry on cloud platforms that are legally or technically inaccessible (Kuru, 2024; Ward, 2021; Stöcker et al., 2017). Legal restrictions and lack of prearranged access protocols can delay or prevent investigators from retrieving vital evidence.

### 5.17.1 Recommended forensic strategy

Organizations should establish cloud access agreements that allow timely data retrieval during authorized investigations, especially in criminal or national security contexts. Cloud services must incorporate forensic-readiness by enabling secure, logged, and legally compliant access to drone-stored data during authorized investigations.

## 5.18 Difficulty in reconstructing timeline of attacks

Attackers may tamper with or erase UAV logs to confuse investigations (Almusayli et al., 2024; Ceviz et al., 2024; Basan et al., 2022). Blockchain-based audit trails, timestamped event logs, and synchronized system clocks are vital for reliable, tamper-proof timeline reconstruction.

### 5.18.1 Recommended forensic strategy

UAVs should maintain tamper-proof logs with precise timestamps for every system event, using synchronized clocks (e.g., GPS time). Blockchain-based audit trails can ensure log integrity and order, enabling high-fidelity timeline reconstruction.

## 5.19 Absence of vendor cooperation during investigations

Some UAV vendors restrict access to proprietary data, hindering forensic analysis (Schiller et al., 2023; Anagnostis et al., 2024; Roberts, 2016). Without vendor assistance, investigators may be unable to access or interpret critical evidence.

### 5.19.1 Recommended forensic strategy

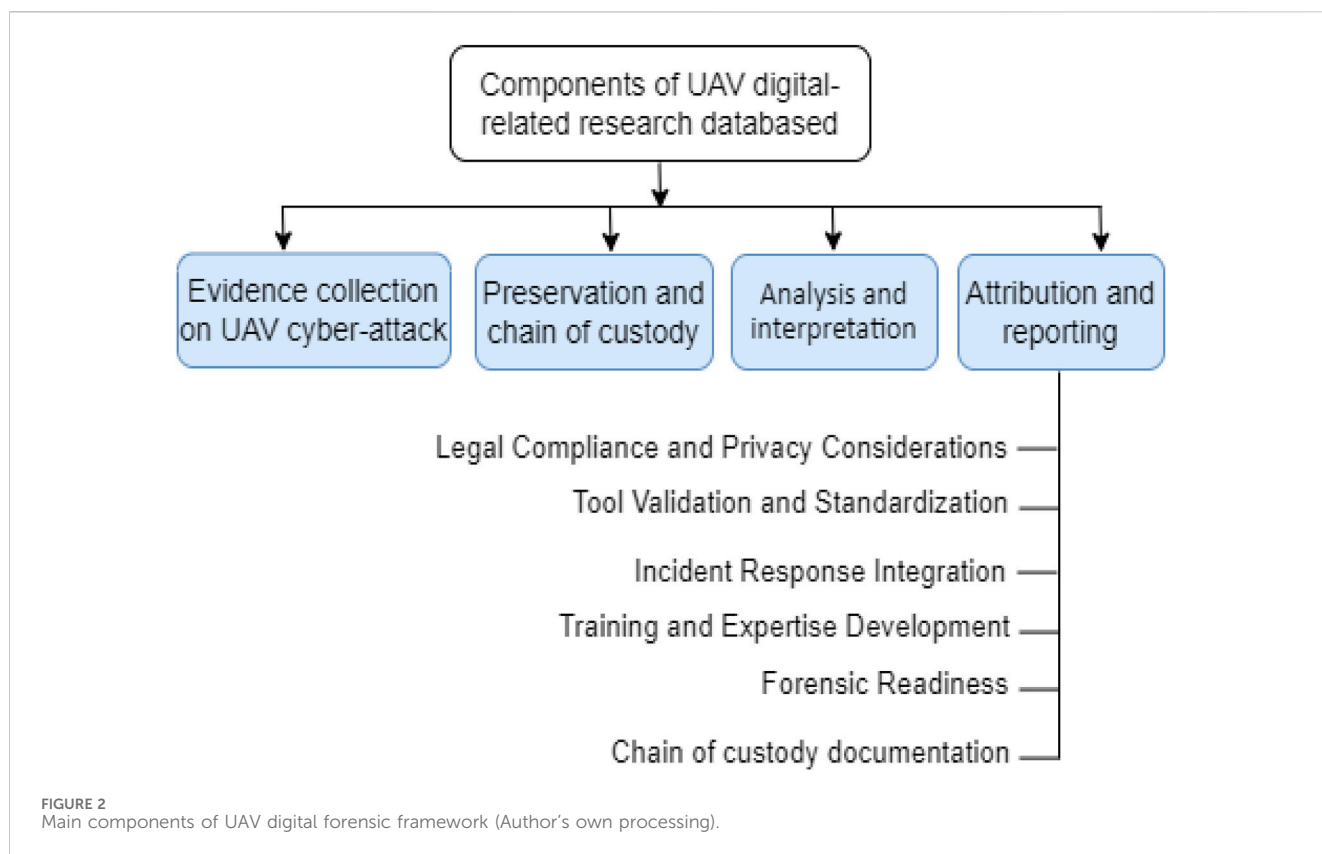
Regulatory frameworks should enforce vendor compliance through legal mandates, licensing conditions, and standardized cooperation clauses. These measures will ensure timely support for lawful forensic investigations.

## 5.20 Obscured communication protocols and interfaces

UAVs often use undocumented or obfuscated protocols that resist forensic analysis (Tecedor Roa, 2024). These undocumented formats make it difficult to decode telemetry, detect spoofing, or investigate command injection attacks.

### 5.20.1 Recommended forensic solution

Developers should be encouraged to adopt open communication standards, while investigators should have access to vetted reverse-engineering toolkits and protocol libraries. Additionally, developing reverse-engineering toolkits and maintaining protocol libraries can help law enforcement decode proprietary data during investigations without vendor reliance.



### 5.21 Risk of evidence contamination during retrieval

Improper data extraction techniques may corrupt volatile UAV evidence (Brunty, 2023). Without proper tools or training, field personnel may unintentionally damage critical evidence, affecting its admissibility in court.

#### 5.21.1 Recommended forensic strategy

Standardized forensic kits featuring write-blockers, bit-by-bit imaging tools, and validated evidence handling procedures are essential to ensure admissibility in court. Personnel must also be trained in UAV evidence handling to preserve chain-of-custody and ensure evidence integrity during collection and analysis.

## 6 Components of UAV digital forensic framework

The growing frequency and sophistication of cyber-attacks on UAVs underscore the urgent need for specialized digital forensic frameworks. Unlike conventional computing systems, drones require tailored forensic mechanisms to accommodate their unique architecture, limited storage, and real-time data flow. A structured framework is essential to ensure accurate, tamper-proof evidence collection, preservation, and analysis during and after incidents. The core components of UAV digital forensics are organized into a structured investigative process, as depicted in Figure 2.

The components are to facilitate comprehensive evidence handling and ensure legal admissibility in diverse operational contexts. The key components commonly found in UAV-related research databases, particularly those focused on digital forensics, cybersecurity, data analysis, and AI applications is presented in Table 3.

Table 3 summarizes the critical components of UAV forensic systems drawn from recent research and practical implementations. These elements support essential functions such as evidence logging, anomaly detection, threat attribution, legal documentation, and AI-based behavior modeling. They collectively enable a complete, resilient forensic ecosystem tailored for UAV environments. For instance, the “UAV Metadata Repository” and “Communication Logs” are foundational for reconstructing incident timelines, while the “AI/ML Model Repository” and “Threat Pattern Database” enable real-time anomaly detection and proactive forensic insights. The inclusion of “Legal/Regulatory Archives” ensures that investigations adhere to jurisdictional and compliance requirements. These components serve as the foundation for the Enhanced UAV Forensic Framework (EUAVFF) introduced in the following sections, where technical design, implementation architecture, and validation are discussed in detail.

## 7 Literature review

The widespread adoption of UAVs across civilian and defense sectors has accelerated research into their cybersecurity vulnerabilities and forensic challenges. Initial studies primarily addressed general digital forensics without accounting for UAV-specific complexities,

TABLE 3 Key components of UAV digital Forensic research databases.

S/n	Component	Description
1	UAV Metadata Repository	Logs flight data: GPS, timestamps, altitude, speed, and direction
2	Sensor Data Archives	Stores outputs from onboard sensors (e.g., cameras, LiDAR, gyroscopes)
3	Communication Logs	Captures telemetry, C2 signals, and video transmissions
4	Firmware/Software Libraries	Includes firmware versions, updates, and patch history
5	Threat/Attack Pattern Database	Contains known malware and cyber-attack signatures
6	Component Fingerprint Database	Stores hashes/signatures for hardware/software integrity checks
7	Incident Case Repositories	Archives past forensic cases and outcomes
8	Network Traffic Database	Logs UAV communication traffic for anomaly detection
9	Legal/Regulatory Archives	Documents UAV laws, compliance, and airspace regulations
10	AI/ML Model Repository	Stores trained models for behavior prediction and anomaly detection

(Author's own processing).

but recent work has shifted toward tailored solutions involving AI, blockchain, and embedded systems (Mohay, 2005; Ruffell et al., 2014; Clark et al., 2017). Between 2018 and 2021, research began exploring advanced forensic mechanisms such as artificial intelligence for intrusion detection, authentication protocols, and electromagnetic watermarking to enhance data integrity (Fernández-Caramés et al., 2018; Singh et al., 2019). However, many of these approaches still lacked real-world applicability and legal integration.

But from 2023 onward, the literature has increasingly focused on adaptive, AI-driven UAV forensic frameworks capable of real-time anomaly detection, log protection, and autonomous evidence capture (Debas et al., 2024; Vajravelu et al., 2023). Despite these advances, most frameworks remain conceptual and lack large-scale validation across different UAV platforms. Overall, the research trajectory reflects a shift from foundational theory toward intelligent, UAV-specific forensic systems. Nevertheless, many studies are limited in scope, lacking encrypted data handling, standardized evidence protocols, or validation across multiple drone models. A summarize representative studies and their contributions, limitations, and focus areas is shown in Table 4.

As shown in Table 4, most existing works focus on conceptual frameworks, model-specific tools, or limited use-case validation. For example, studies like Wang et al. (2022) and Khelifi et al. (2021) provide useful insights but do not address encrypted firmware or spoofing detection. Even empirical case studies remain restricted to select commercial UAVs, ignoring broader forensic readiness requirements.

## 7.1 Analysis and synthesis

### 7.1.1 Evolution of forensic approaches

UAV forensic research has progressed through three major stages: generic digital forensics (pre-2015), drone-specific data extraction tools (2016–2020), and intelligent forensic frameworks (2021–present). Early work often treated UAVs like mobile devices, focusing on SD cards or GPS modules. More recent studies incorporate AI and blockchain, yet many solutions remain theoretical and lack standardized deployment across heterogeneous UAV systems.

### 7.1.2 Persistent gaps

Despite evolving methods, persistent gaps remain. Most tools target specific brands (e.g., DJI) and overlook encrypted logs, volatile memory capture, and cross-jurisdictional legal frameworks. Additionally, there is limited access to publicly available UAV forensic datasets to support reproducibility and benchmarking.

### 7.1.3 Emerging solutions

Emerging solutions emphasize modularity, AI integration, and compliance with international standards. Researchers are advocating for forensic-by-design architectures that embed tamper-proof logging, encrypted data capture, and chain-of-custody mechanisms. Concepts such as UAV Forensics-as-a-Service (UFaaS), blockchain-secured logging, and hybrid edge-cloud analytics are gaining traction to address both performance and admissibility constraints.

## 8 Emerging solutions and techniques in UAV digital forensics

As UAV technology becomes increasingly advanced and embedded in critical domains, drones are exposed to escalating cyber threats such as GPS spoofing, malware injection, and firmware manipulation. These evolving risks demand forensic responses that are equally sophisticated, real-time, and resilient to tampering (Aissaoui et al., 2023; Mekdad et al., 2023). Emerging forensic solutions focus on five strategic domains: forensic-by-design architectures, automation of evidence capture, cloud-enabled forensic processing, artificial intelligence for threat detection, and blockchain for log integrity. These innovations are revolutionizing UAV forensic readiness by enabling real-time monitoring, remote analysis, and legally defensible evidence preservation (Debas et al., 2024; Fernández-Caramés et al., 2018; Casino et al., 2022). Research is increasingly focused on proactive, integrated forensic methods as outlined in Figure 3.

The chart identifies and aligns 15 key innovations, each supported by peer-reviewed literature, that reflect a shift toward

TABLE 4 Summary of some selected UAV Forensic Studies.

S/n	Author(s)/Year	Focus	Key contributions	Limitations
1	Debas et al. (2024); Maqbool et al. (2024)	Conceptual frameworks	Proposed adaptive, multi-domain forensic strategies	No real-world validation
2	Vajravelu et al. (2023); Debs and Fayad (2023)	Systematic Review	ML-based taxonomy for UAV forensics	Lacks practical testing
3	Studiawan et al. (2023)	Literature Survey	Documented forensic tools, datasets, and trends	Descriptive, not implementation-based
4	Wang et al. (2022)	Defense Modeling	Honeypot game for collaborative UAV defense	Focused on prevention, not forensics
5	de Melo et al. (2021)	Identity Validation	UAVouch scheme for verifying drone identity/ location	Not designed for post-incident analysis
6	Khelifi et al. (2021)	Case Study	Extracted forensic data from 6 drone brands	Ignores encryption or spoofing detection
7	Abdalla et al. (2020)	Security Analysis	Detailed UAV threat and mitigation review	No forensic tool validation
8	Alshamsi (2020)	Parrot AR Drone case study	Artifact recovery techniques for Parrot drones	Model-specific; lacks encryption support
9	Renduchintala et al. (2019); Dumitrescu et al. (2019)	Hardware Forensics	GPS and telemetry extraction from DJI drones	Limited to non-encrypted memory
10	Esteves (2019)	EM Forensic Models	EM watermarking for data integrity	Complex hardware dependency
11	Fernández-Caramés et al. (2018)	IoT-UAV Surveillance	Showed traceability via sensor data	No legal or encryption consideration
12	Clark et al. (2017); Albrecht et al. (2017)	Tool Development	DROP parser for DJI log analysis	Model-locked and weak encryption support
13	Altawy and Youssef (2016)	Policy and Threat Survey	Covered UAV cyber/privacy risks	No forensic solutions proposed
14	Lee-Morrison (2015); KEBANDE (2017)	Visual Forensics	Cartographic evidence reconstructions	Lacks UAV-specific focus
15	Ruffell et al. (2014)	Forensic Mapping	Artifact recovery across 14 drone types	Industry-focused; lacks academic testing
16	Mohay (2005)	Foundational Theory	Early digital forensic framework design	Too generic; not UAV-focused

(Author’s own processing).

*proactive, real-time, and forensically capable* UAV architectures. Each innovation is assigned equal visual weight to emphasize their individual and collective importance rather than rank them hierarchically. It presents a comparative visual summary of emerging forensic technologies and architectural strategies proposed in UAV cybersecurity research and illustrates how various innovations collectively contribute to the next-generation of forensic readiness in drone systems. It illustrates modern UAV forensic technologies, highlighting proactive strategies such as AI-based behavior modeling, embedded intrusion detection, secure telemetry offloading, and tamper-proof blockchain logs. These tools allow forensic capture to begin during flight operations, minimizing data loss and enhancing response accuracy. Each item reflects a modern approach to strengthening UAV forensic capabilities amid growing cybersecurity threats. Collectively, these innovations support comprehensive forensic capability from onboard data collection to cloud-based analysis enabling investigators to reconstruct attacks, validate evidence, and maintain compliance with international legal standards. The outlines opportunities for applying UAV models across key sectors of socio-economic development is presented in Table 5.

Table 5 categorizes UAV applications across various socio-economic sectors, including healthcare, logistics, and disaster response, to contextualize forensic readiness beyond technical

settings. In each domain, drones play a mission-critical role, making forensic integrity essential for public trust, safety, and accountability. These emerging forensic techniques are redefining how UAV systems are secured and investigated. By embedding forensic capabilities into UAV architectures, stakeholders can respond more effectively to cyber incidents, conduct post-event analysis, and uphold the evidentiary standards required in legal or regulatory settings (Studiawan et al., 2023; Ntizikira et al., 2023).

## 9 Research methodology

This study adopted a mixed-method survey approach to assess the practicality, perceived importance, and readiness of digital forensic solutions in UAV environments. The survey was structured to validate the proposed Enhanced UAV Forensic Framework (EUAVFF) by collecting responses from stakeholders with backgrounds in cybersecurity, digital forensics, drone operations, and aviation regulation (Alenezi, 2024; Debas et al., 2024). Since this study does not involve human subjects, approval from a research ethics committee was not required. Participation was voluntary and anonymous, with informed consent obtained digitally from all respondents. A purposive sampling strategy was used to target professionals and researchers with UAV or forensic

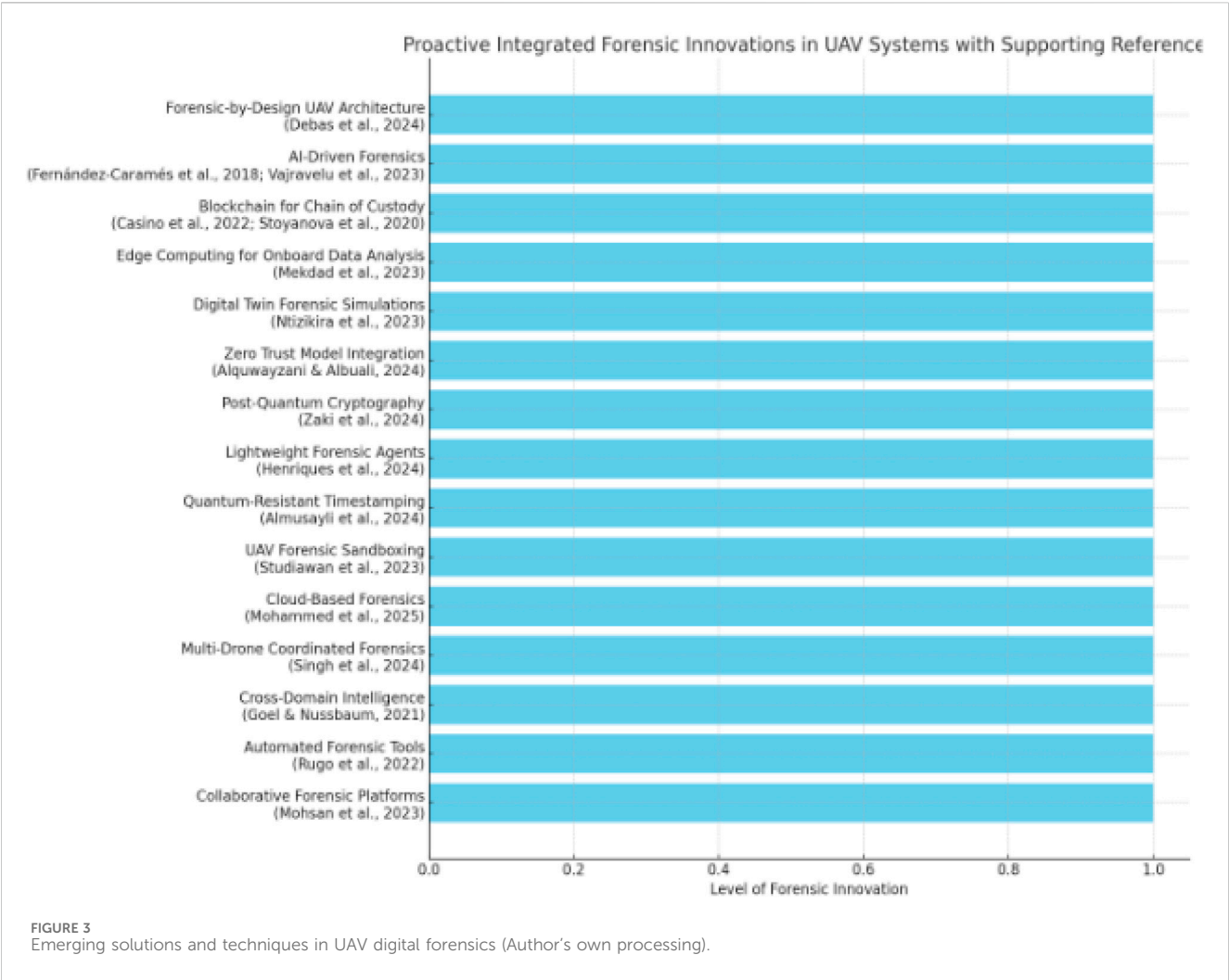


TABLE 5 UAV applications in socio-economic sectors.

Sector	Commercial	Hospitality and tourism	Healthcare	Emergency and disaster response
Automation and Labor	Food/grocery delivery, drone waiters	Food/beverage service, mobile hotels	Prescription, lab sample, and vaccine delivery	Medical/emergency supply drops, search and rescue
Risk Reduction	Replacing humans in hazardous jobs	–	Organ and blood transport	Damage inspection, restoring services (Wi-Fi, power)
Efficiency Gains	Fewer staff and steps, faster service	Entertainment delivery, facility maintenance	Drone ambulance, EMS support	Rapid assessment and logistics in disaster zones
Advanced Capabilities	–	Visual marketing, lifeguarding	Patient stay forecasting, telemedicine support	3D mapping, fire monitoring, power system surveillance
Special Functions	–	Security, material transport	Forensic analysis	Hydropower and infrastructure monitoring

(Author's own processing).

expertise. The survey link was distributed via academic mailing lists, professional drone networks, LinkedIn groups, and cybersecurity associations over a 6-week period in 2024. The questionnaire included 20 items across five sections: respondent demographics, awareness of UAV forensics, technical and legal barriers, framework relevance, and suggestions for improvement. It featured both Likert-

scale and open-ended questions to collect quantitative and qualitative feedback (Singh, 2024; Stoyanova et al., 2020). A total of 87 valid responses were received. Participants included digital forensic analysts (28%), cybersecurity professionals (24%), UAV pilots and engineers (20%), legal/regulatory officials (15%), and researchers (13%). This diversity ensured a well-rounded evaluation



of the framework across domains of relevance. Quantitative responses were analyzed using descriptive statistics in Microsoft Excel and SPSS, while qualitative responses were thematically coded to extract recurring patterns, challenges, and feedback themes. This dual analysis approach strengthened the triangulation and robustness of findings.

9.1 Literature review

A systematic review was conducted to map current advancements in UAV cybersecurity and digital forensics. Sources included peer-reviewed journals, conferences, white papers, and technical standards from databases such as Scopus, IEEE Xplore, ScienceDirect, SpringerLink, and Semantic Scholar. Studies from 2010 to 2025 that addressed UAV security threats, forensic tools, and evidence handling were included. Search terms used were: *UAV digital forensics*, *drone cyber-attacks*, *forensic readiness*, *GPS spoofing*, and *autonomous vehicle security*. The review identified 21 key challenges spanning technical, legal, and operational domains, which informed the framework requirements.

9.2 Empirical survey

A structured questionnaire was distributed online to UAV operators, aviation professionals, cybersecurity analysts, academics, and regulators. It evaluated:

- (i) Awareness of UAV cyber threats (e.g., command hijacking, firmware tampering)
- (ii) Knowledge of UAV forensic tools and principles
- (iii) Perceived need for UAV-specific forensic frameworks
- (iv) Assessment of existing forensic readiness

A total of 100 valid responses were analyzed using descriptive statistics. Results are presented in [Section 10](#).

10 Results and findings

This section presents the outcomes of the survey conducted among UAV operators, aviation professionals, cybersecurity analysts, academics, and regulators. Survey findings reveal strong consensus on the growing threat of cyberattacks against UAVs and the urgent need for embedded forensic capabilities. Respondents emphasized that without robust forensic mechanisms, UAV incidents may go unresolved, unprosecuted, or unprevented ([Singh, 2024](#); [Almusayli et al., 2024](#)).

10.1 Familiarity with UAV-specific cyber threats

Respondents’ awareness of UAV-specific threats such as command hijacking and firmware tampering is summarized in [Table 6](#).

Over 80% of participants endorsed the “forensic-by-design” concept, highlighting the importance of integrating logging, secure

TABLE 6 Stakeholders’ respondent familiarity with UAV-specific cyber threats.

Threat type	Familiar (%)	Unfamiliar (%)
Command Hijacking	32%	68%
Firmware Tampering	25%	75%
GPS Spoofing	38%	62%
Telemetry Interception	29%	71%
Onboard Sensor Manipulation	21%	79%

(Author’s own processing).

storage, and anomaly detection during UAV development. AI-driven intrusion detection (IDPS) and blockchain-based telemetry logging were frequently cited as critical technologies for proactive and tamper-proof investigations ([Debas et al., 2024](#); [Vajravelu et al., 2023](#)).

10.1.1 Interpretation

Most respondents showed limited awareness of UAV-specific cyber threats. GPS spoofing was the most recognized (38%), while onboard sensor manipulation was least known (21%). These findings underscore the need for targeted education, policy support, and forensic-by-design training in UAV operations, as illustrated in [Figure 4](#).

[Figure 4](#) demonstrates respondents’ familiarity with UAV-specific threats. GPS spoofing had the highest recognition (38%), while sensor manipulation was the least known (21%). In all cases, over 60% of participants were unfamiliar with these threats.

10.2 Awareness of UAV cybersecurity risks

The survey exposed a major knowledge gap: 72% of respondents reported low or no awareness of UAV-specific risks like GPS spoofing, command hijacking, firmware manipulation, and telemetry tampering as showed in [Table 7](#).

This 72% underscores a critical lack of cybersecurity awareness among UAV users, reinforcing the need for targeted education and policy initiatives.

10.3 Perceived need for UAV forensic solutions

When asked about the importance of digital forensics in UAV operations, 90% of respondents supported the need for specialized forensic frameworks, and 85% agreed that digital forensics is vital for UAV cybersecurity as presented in [Table 8](#).

These [Table 8](#) results underscore the importance of integrating forensic capabilities into UAV system architectures and support the relevance of the proposed EUAVFF model.

10.4 Evaluation of current UAV forensic readiness

Respondents assessed existing forensic capabilities in UAV systems. Results revealed a clear gap between security

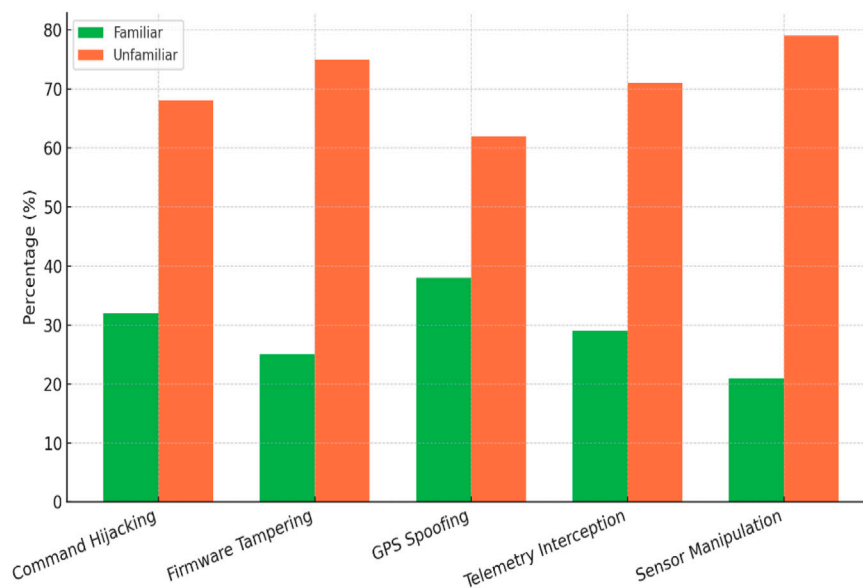


FIGURE 4  
Respondents' familiarity with UAV-specific cyber threats (Author's own processing).

TABLE 7 Respondents' awareness of UAV-specific cybersecurity risks.

Awareness level	Number of respondents	Percentage (%)
Aware of UAV cybersecurity risks	28	28%
Unaware of UAV cybersecurity risks	72	72%
Total	100	100%

(Author's own processing).

TABLE 8 Perceptions on UAV digital forensic readiness.

Statement	Agree (%)	Neutral (%)	Disagree (%)
Digital forensics is essential for securing UAVs against cyber threats	85%	10%	5%
Current UAVs are adequately equipped for forensic investigation	20%	18%	62%
There is a need for specialized forensic frameworks tailored to UAVs	90%	8%	2%

(Author's own processing).

expectations and the actual level of forensic integration, as shown in [Table 9](#).

#### 10.4.1 Interpretation

Over 50% of respondents disagreed that UAVs currently offer key forensic features like tamper-proof logs, real-time data preservation, or legally admissible evidence. Only 20% believed UAVs are adequately equipped for forensic investigations highlighting a major gap in readiness.

#### 10.4.2 Implications

These findings support the study's premise: UAVs are vulnerable due to limited cybersecurity awareness and weak forensic capabilities. Bridging this gap requires forensic-by-design

models, regulatory standards, and stakeholder training to ensure resilient and accountable drone operations.

### 10.5 Sample size and statistical basis

A total of 100 valid responses were analyzed using descriptive statistics. Participants included UAV operators, cybersecurity experts, aviation stakeholders, and academics. The survey assessed awareness of UAV threats, evaluated forensic readiness, and gauged perceptions on the need for enhanced forensic capabilities as displayed in [Table 10](#).

[Table 10](#) provides a consolidated snapshot of stakeholder perspectives on key focus areas related to UAV cybersecurity,

TABLE 9 Respondents' evaluation of UAV forensic readiness.

Statement	Agree (%)	Neutral (%)	Disagree (%)
UAVs are adequately equipped for forensic investigation	20%	18%	62%
Existing UAVs offer real-time data preservation for investigations	22%	20%	58%
Most UAVs have tamper-proof logging capabilities	19%	24%	57%
Forensic data in UAVs is legally admissible in most jurisdictions	17%	23%	60%

(Author's own processing).

TABLE 10 Descriptive summary.

S/n	Survey focus area	Agree (%)	Neutral (%)	Disagree (%)
1	Awareness of UAV cyber threats	28	-	72
2	Need for digital forensics in UAVs	85	10	5
3	Adequacy of current forensic capabilities	20	18	62
4	Real-time evidence preservation	22	20	58
5	Tamper-proof Logging	19	24	57
6	Legal admissibility of UAV Data	17	23	60

(Author's own processing).

forensic awareness, and system readiness. It synthesizes Likert-scale responses (Agree, Neutral, Disagree) across six dimensions, drawing from a diverse participant base of UAV operators, cybersecurity professionals, aviation regulators, and academics. Descriptive statistics like frequencies and percentages were used to analyze the survey responses, highlighting patterns in awareness and preparedness as revealing in Table 10. The data validates the forensic gaps outlined in earlier sections, including insufficient real-time readiness, insecure logging, and poor legal integration. There is a clear divergence between operational adoption and forensic preparedness, suggesting a misalignment between drone functionality and forensic needs.

**Awareness of UAV Cyber Threats (28% Agree, 72% Disagree):** A striking 72% of respondents reported low or no awareness of UAV-specific threats such as GPS spoofing, command hijacking, or firmware tampering. This underscores a significant educational and informational gap, especially given the growing use of drones in sensitive domains.

**Need for Digital Forensics in UAVs (85% Agree):** A large majority recognized the necessity for integrating digital forensic capabilities in UAV systems. This validates the foundational motivation for developing the Enhanced UAV Forensic Framework (EUAVFF), showing strong stakeholder demand for proactive forensic readiness.

**Adequacy of Current Forensic Capabilities (20% Agree, 62% Disagree):** Over 60% of participants expressed skepticism about the current forensic capacity of UAVs. This highlights that while UAV usage is increasing, their ability to support incident investigation remains insufficient.

**Real-Time Evidence Preservation (22% Agree, 58% Disagree):** Only 22% agreed that existing UAVs support real-time data

capture or secure log offloading. This confirms the critical need for real-time telemetry logging, cloud integration, and embedded evidence capture mechanisms like those proposed in the EUAVFF.

**Tamper-Proof Logging (19% Agree, 57% Disagree):** The low agreement rate indicates that most UAVs lack secure logging features such as immutable audit trails or hash-chained logs. This finding justifies the inclusion of blockchain-based evidence tracking in the proposed framework.

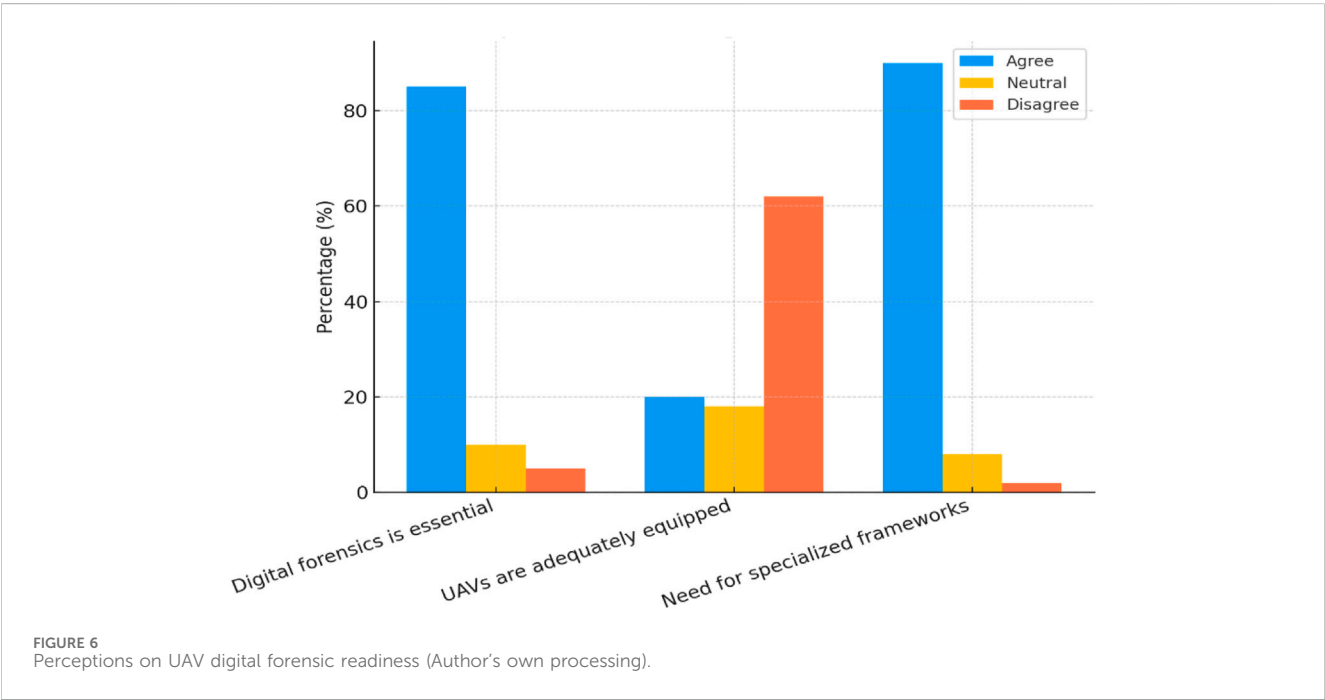
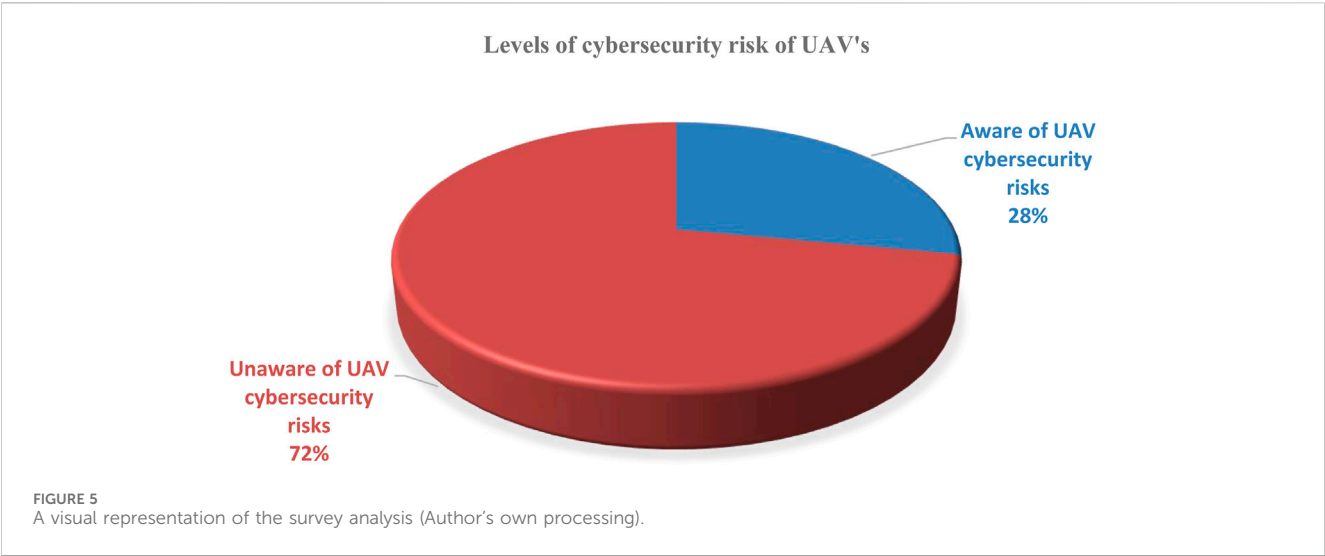
**Legal Admissibility of UAV Data (17% Agree, 60% Disagree):** A majority expressed concern that UAV-derived forensic data may not hold up in court due to inconsistencies in formatting, incomplete metadata, or lack of chain-of-custody documentation. This strongly supports the study's emphasis on compliance with ISO/IEC standards and policy harmonization.

The results justify the core components of EUAVFF, particularly its emphasis on forensic-by-design architecture, legal compliance, and modular deployment across diverse UAV systems.

This evidence-based approach reflects real stakeholder perspectives. A visual summary of the findings is presented in Figure 5.

Figure 5 shows that 72% of respondents lacked awareness of UAV-specific cybersecurity risks, highlighting a significant knowledge gap. An illustration of the stakeholder perceptions of UAV forensic readiness is shown in Figure 6.

Figure 6 shows strong support for forensic integration, with 85%–90% of respondents affirming the need for UAV-specific forensic solutions. However, 62% disagreed that current UAVs are adequately equipped, indicating a gap between threat perception and system readiness. Both Figures 5, 6 highlight the urgency for adopting forensic-by-design frameworks like EUAVFF.



10.6 Validation of the proposed EUAVFF

A structured online survey was conducted with 100 respondents, including UAV operators, cybersecurity experts, aviation professionals, and academics to validate the EUAVFF and assess stakeholder awareness as summarized in Table 11.

Table 11 provides a descriptive summary of the methodology used to gather stakeholder input on UAV digital forensics and validate the proposed Enhanced UAV Forensic Framework (EUAVFF). This table is pivotal to understanding how the empirical findings in the manuscript were obtained and why they are relevant to the broader goals of the research. Table 11 directly supports the credibility of the survey findings presented in

Figures 5, 6 and discussed in Sections 10.6, 10.8. It justifies the conclusions about gaps in UAV forensic awareness and validates the practical necessity of a proactive forensic framework like EUAVFF.

These insights substantiated the practical relevance and urgency of the proposed solution.

**10.7 Design validation: mapping challenges to EUAVFF components**

Validation was conducted through expert input and theoretical mapping. A matrix aligned the 21 identified forensic challenges with

TABLE 11 Structured online survey description.

Survey attribute	Description
Survey type	Structured online survey
Platform Used	GDPR-compliant online tool like Google Forms, Microsoft Forms
Number of Questions	25 (Multiple-choice and Likert scale)
Question Categories	Demographics, Cybersecurity Awareness, Forensic Readiness, Framework Validation
Sample Size	100 respondents
Sampling Technique	Purposive sampling via professional networks (LinkedIn, ResearchGate, email)
Participant Profiles	UAV pilots, cybersecurity analysts, regulators, academics
Participation Model	Voluntary, anonymous, informed consent
Data Analysis Method	Descriptive statistics (frequency, percentage)
Objective	Validate EUAVFF design and assess UAV forensic awareness and readiness

(Author’s own processing).

relevant components of the EUAVFF to ensure coverage and practical applicability as presented in Table 12.

As summarized in Table 12, each forensic component in the EUAVFF received high relevance scores from respondents. For example, 94% rated the secure data capture module as “critical,” while 87% rated blockchain logging as “highly relevant.” This strong support reinforces the framework’s practical viability and perceived importance among stakeholders.

10.8 Practical implications and application pathways of EUAVFF

The Enhanced UAV Forensic Framework (EUAVFF) was developed to address the real-world deficiencies of UAV cybersecurity and forensic readiness. This section presents clear, measurable, and applicable implications of the framework across different operational domains, followed by validation strategies and a structured adoption roadmap.

1. Concrete Use Cases of EUAVFF
- a. Law Enforcement and Border Security: In crime scene investigations involving drones (e.g., smuggling,

TABLE 12 Mapping UAV Forensic challenges to EUAVFF components.

S/n	Forensic challenge	EUAVFF component	Coverage
1	Volatile memory loss	Real-time telemetry offload; Cloud sync	Technical
2	No standard protocols	Forensic-by-design; Modular design	Legal/Technical
3	Weak tamper-proof logging	Blockchain audit trails; Secure logs	Technical
4	No real-time evidence captures	Edge-based autonomous logging	Technical
5	Legal jurisdiction issues	Cross-border handling protocols	Legal
6	Poor encryption	Forensic-friendly encryption (e.g., keyed hash)	Technical
7	Poor documentation	Auto-logging; Chain-of-custody metadata	Legal/Technical
8	User unawareness	Education modules; Risk dashboards	Human
9	No onboard forensics	Embedded forensic firmware tools	Technical
10	No recovery after attack	Blockchain audit recovery; Fail-safe logging	Technical
11	Hardware incompatibility	Modular support for all UAV types	Technical
12	GPS spoofing	AI anomaly detection; Signal validation	Technical
13	Firmware tampering	Integrity checks; Signed logs	Technical
14	Developer unawareness	Forensic-by-design policy guidance	Organizational
15	Evidence inadmissibility	ISO/IEC-compliant data schema	Legal/Technical
16	Limited log storage	Log compression; Prioritized recording	Technical
17	No forensic datasets	Open-source dataset contributions	Research
18	Real-time limits	Edge analytics; Load shedding	Technical
19	Lack of validation tools	Verification interface; Blockchain checks	Technical
20	Anti-forensic methods	Tamper detection; Log anchoring	Technical
21	Integrity verification issues	Hash chains; Timestamped logs	Legal/Technical

(Author’s own processing).



unauthorized surveillance), EUAVFF enables forensic-grade evidence acquisition from flight logs, onboard videos, and command telemetry. Its tamper-proof blockchain-based audit trails ensure legal admissibility during prosecution (Henriques et al., 2024).

- b. Disaster Response and Emergency Services: Drones used for post-disaster surveillance often operate in volatile environments. EUAVFF's real-time anomaly logging and remote cloud sync allow secure evidence offloading during missions crucial for tracing failures, miscommunication, or system compromise during humanitarian deployments (Mohsan et al., 2023).
- c. Critical Infrastructure Surveillance: Energy, transportation, and telecommunications sectors rely on drones for inspection. A compromised drone can disrupt services or leak sensitive data. EUAVFF facilitates attribution of malicious activity and helps recover forensic data from telemetry, communication logs, and embedded sensors (Goel and Nussbaum, 2021; Clark et al., 2017).
- d. Regulatory and Aviation Safety Compliance: The framework supports aviation authorities in auditing drone operations. Its ISO/IEC-compliant forensic schema and cross-border compatibility protocols help assess violations and certify UAV airworthiness during investigations (Yeboah-Ofori and Brown, 2020).

## 2. Performance Metrics for Real-World Validation

EUAVFF performance should be validated using the following metrics to transition from concept to practical deployment:

- (i) Forensic Accuracy: Precision and recall in attributing events using AI-based threat detection models.
- (ii) Latency: Time elapsed between anomaly detection and evidence capture; critical for in-flight incidents.
- (iii) Tamper Resistance: Resilience against log manipulation or unauthorized data overwrite, tested via red-teaming and adversarial simulations.
- (iv) Chain-of-Custody Integrity: Capability to maintain end-to-end audit trails for legal admissibility.
- (v) Storage Efficiency: Ability to optimize log data using compression and cloud offloading without loss of evidentiary value.

## 3. Adoption Roadmap and Tool Integration Pathways

Step 1: Modular Deployment: Each forensic tool like, secure logger, anomaly detector, metadata encryptor can be deployed as plug-and-play modules on UAVs of varying size and mission profiles.

Step 2: API and Firmware-Level Integration: Manufacturers can adopt the framework's APIs to embed forensic hooks within UAV firmware.

Step 3: Regulatory Alignment and Standardization: The framework encourages collaboration with regulatory bodies (e.g., ICAO, ISO, NIST) for policy-compliant digital evidence handling.

Step 4: Open-Source Toolkit Development: A community-led open-source development approach will facilitate academic and commercial contributions.

Step 5: Cross-Border Use Cases and Interoperability: EUAVFF supports international missions via multi-language logging and forensic schema aligned with MLATs.

## 10.9 Discussion of results

Three dominant themes emerged from the open-ended responses: (1) legal admissibility concerns due to lack of standardization, (2) difficulty accessing encrypted or proprietary logs, and (3) the absence of training among UAV operators on forensic procedures. These themes reinforce earlier literature gaps and validate the need for a standardized, modular forensic framework (Fernández-Caramés et al., 2018; Mohay, 2005; Clark et al., 2017). The Enhanced UAV Forensic Framework (EUAVFF) was designed using a forensic-by-design approach, drawing from literature, stakeholder surveys, and secure systems best practices. Its core features include:

- Blockchain-based secure logging
- Forensic-friendly encryption and telemetry offloading
- Modular support for different UAV types
- Real-time evidence captures via cloud sync

Respondents viewed the proposed Enhanced UAV Forensic Framework (EUAVFF) as a significant step toward solving key challenges particularly its inclusion of modular forensic tools, AI analytics, secure storage, and regulatory alignment. Many highlighted the framework's potential to serve in court-admissible investigations if adopted globally and tested across real UAV systems (Stoyanova et al., 2020; Henriques et al., 2024).

### 10.9.1 Comparative analysis

EUAVFF was benchmarked against current UAV forensic and cybersecurity models. It outperformed others in forensic readiness, real-time processing, legal admissibility, AI integration, and standards compliance. This demonstrates EUAVFF's comprehensive and scalable capabilities for UAV cybercrime investigation.

### 10.9.2 Ethical compliance

Participants gave informed consent, and no personal data was collected. Responses were anonymized, and data was securely stored, following institutional research ethics.

### 10.9.3 Limitations

While this study contributes to the body of knowledge in UAV forensic readiness, several limitations must be acknowledged. First, the proposed Enhanced UAV Forensic Framework (EUAVFF) remains conceptual and has not yet been tested on live or deployed UAV systems. As such, its performance under real-world cyberattack conditions, resource constraints, and operational stressors is yet to be empirically validated (Henriques et al., 2024).

Second, the survey data may reflect sample bias due to its purposive sampling strategy. While efforts were made to diversify participants across technical, legal, and operational domains, the

responses may not fully capture the perspectives of law enforcement agencies or small-scale drone operators in underrepresented regions (Yeboah-Ofori and Brown, 2020).

Third, legal and regulatory insights were drawn largely from open-source documents and participant responses rather than formal governmental data-sharing partnerships. Consequently, this study may not fully address access restrictions related to proprietary logs, jurisdictional barriers, or classified UAV operations (Atkinson et al., 2021; Tecedor Roa, 2024). Findings rely on self-reported data, which may not reflect actual practices. Also, EUAVFF has not yet been field-tested. Future work will focus on live implementation and real-world performance validation.

## 11 Future directions of UAV cybersecurity and digital forensics

As UAVs become more autonomous and integral to critical infrastructure, the demand for resilient cybersecurity and forensic solutions will increase (Aissaoui et al., 2023; Kuru, 2024). Emerging directions in this field are shaping a future where UAVs are not only secure but also forensic-ready by design.

### (i) UAV-Specific Forensic Toolkits:

New toolkits are being developed to extract and analyze UAV-specific data such as flight logs, GPS data, and sensor inputs tailored to embedded systems and real-time OS, offering features like tamper detection and automated response (Debas et al., 2024).

### (ii) Regulatory and Legal Frameworks:

Bodies like ICAO are expected to enforce policies on forensic readiness, mandating built-in logging, encryption, and access controls. These will also help define liability and support cross-border investigations (Atkinson et al., 2021).

### (iii) Interdisciplinary Collaboration:

Stronger cooperation among cybersecurity experts, aerospace engineers, and legal professionals is vital for embedding secure and legally compliant forensic functions into UAVs (Stoyanova et al., 2020).

### (iv) Autonomous Forensics:

AI-driven systems onboard UAVs will detect and respond to anomalies, securing data in real-time even in remote or high-risk areas (Fernández-Caramés et al., 2018).

### (v) Integration with Smart Cities:

UAVs embedded in smart infrastructure must exchange data securely with urban systems, requiring forensic mechanisms to reconstruct actions in case of incidents (Eltoukhy, 2025).

### (vi) Blockchain for Evidence Integrity:

Blockchain ensures immutable, verifiable logs with tamper-proof timestamps, supporting chain-of-custody and cross-agency investigations (Alenezi, 2024; Casino et al., 2022).

### (vii) AI-Powered Threat Prediction:

Machine learning models trained on attack patterns can predict threats, trigger preventive actions, and ensure forensic logging (Xie et al., 2024).

### (viii) Digital Twin and Simulation Environments:

Simulated UAV environments allow for safe forensic testing, tool evaluation, and personnel training without risking operational drones (Rugo et al., 2022).

### (ix) UAV Forensics-as-a-Service (UFaaS):

Cloud-based forensic services will offer remote analysis tools such as malware detection and log reconstruction, enabling access for resource-limited organizations (Anagnostis et al., 2024).

### (x) Global Monitoring Centers:

International UAV cybersecurity hubs could facilitate attack data collection, threat advisories, and cross-border forensic cooperation (Tyshchuk, 2024).

### (xi) 5G/6G and Edge Forensics:

High-speed networks will enable real-time forensic processing at the edge, minimizing data loss and enabling rapid responses (Mekdad et al., 2023).

### (xii) Ethical and Legal Considerations:

Future frameworks must balance forensic needs with privacy laws like GDPR, ensure lawful data collection, and define admissibility standards for drone-acquired evidence (Yeboah-Ofori and Brown, 2020).

### (xiii) Advancing UAV Forensic Readiness:

Building on the findings of this study, future research should advance UAV forensic readiness through multi-dimensional strategies involving technical development, policy integration, legal standardization, and field-based validation. The following subsections outline key trajectories for continued exploration and implementation.

### (xiv) Tool Development and Technical Validation:

There is a pressing need to translate the EUAVFF into deployable, modular forensic tools. Future efforts should focus on developing prototype software/hardware modules for secure telemetry capture, encrypted log extraction, and real-time anomaly detection as well as cloud-based evidence capture modules. Field testing these tools across different UAV models

and cyberattack scenarios will provide empirical evidence of their effectiveness and scalability (Debas et al., 2024; Vajravelu et al., 2023).

#### (xv) Public Awareness and Forensic Literacy

Increasing awareness among UAV operators and developers about forensic responsibilities is critical. Future work should develop educational materials, certification programs, and awareness campaigns to encourage forensic-by-design principles in both commercial and civilian drone sectors (Mohsan et al., 2023; Singh, 2024).

#### (xvi) Policy Collaboration and Legal Readiness

Policymakers must be engaged to ensure UAV forensic tools align with national and international regulatory frameworks and to draft UAV-specific forensic compliance policies and evidence admissibility guidelines. Future work should explore stakeholder workshops, joint law enforcement simulations, and formal inclusion of UAV forensics in aviation safety protocols. Legal experts should co-develop guidelines for evidence collection, privacy preservation, and international chain-of-custody transfer (Yeboah-Ofori and Brown, 2020; Atkinson et al., 2021).

#### (xvii) International Standardization and Compliance

Global standardization is essential for cross-border collaboration in UAV cyber investigations. Researchers and regulatory bodies should co-create international standards on forensic logging, data retention, UAV audit trails, and cloud-based evidence repositories. Engagement with ISO, ICAO, IEEE, and INTERPOL can help drive the institutionalization of UAV forensic norms (Clark et al., 2017; Oruc, 2022).

#### (xvii) Dataset Generation and Benchmarking

The lack of publicly available UAV forensic datasets hampers comparative analysis. Researchers should focus on generating synthetic and anonymized datasets that represent various attack vectors, operational contexts, and forensic scenarios. These resources will support tool benchmarking, AI training, and reproducibility (Studiawan et al., 2023; Fakhouri et al., 2024).

#### (xviii) Interdisciplinary Education and Training

Academic programs should integrate UAV forensics into cybersecurity and engineering curricula to build a skilled forensic workforce. That is, to support the evolving needs of UAV forensic readiness, academic institutions must embed interdisciplinary training in their curricula. UAV forensics sits at the intersection of computer science, electrical engineering, criminal justice, and aviation safety, and thus requires holistic knowledge across these domains. Universities and technical institutes should introduce dedicated courses and modules that cover topics such as forensic-by-design UAV architecture, embedded systems security, anomaly detection, chain-of-custody principles, and legal admissibility of drone-captured evidence.

Laboratory simulations, case study-based learning, and collaborations with drone manufacturers or law enforcement can further enhance the practical skillset of students. Certification programs, hackathons, and forensics-focused drone competitions may also foster innovation and interest in this niche field. By investing in such interdisciplinary education, the academic sector can help build a robust pipeline of professionals equipped to handle the forensic challenges of next-generation UAV systems, ultimately contributing to safer skies and more accountable drone operations.

## 12 Comparison with existing state-of-the-art studies

This study was systematically compared with relevant prior research to highlight its unique contributions to UAV cybersecurity and digital forensics. Unlike earlier works, which often focused on conceptual models or single UAV types, this study introduces the Enhanced UAV Forensic Framework (EUAVFF) with practical, modular, and legally admissible forensic features. The comparison emphasizes EUAVFF's advancements in:

- Real-time evidence acquisition,
- Forensic-by-design architecture,
- Cross-platform compatibility, and

A summary of these novel contributions, demonstrating how this work addresses persistent gaps in UAV forensic capabilities and cyber-attack response is presented in Table 13.

Table 13 highlights this study's distinct contributions compared to existing literature. It introduces the Enhanced UAV Forensic Framework (EUAVFF) a structured, comprehensive solution tailored to UAV cyber threats. The framework addresses UAV-specific limitations by enabling real-time forensic readiness through continuous evidence capture, anomaly detection, and secure cloud offloading.

A central innovation is the forensic-by-design approach, integrating forensic capabilities during UAV development. The framework incorporates AI for behavior analysis, blockchain for log integrity, and supports standardized practices for legal admissibility and cross-border data handling. Moreover, the study emphasizes implementation through the creation of UAV-specific forensic datasets, awareness programs, and training modules. Unlike earlier works that focused on either technical or conceptual aspects, this study delivers a multidisciplinary roadmap that bridges technical, legal, and operational gaps in UAV digital forensics.

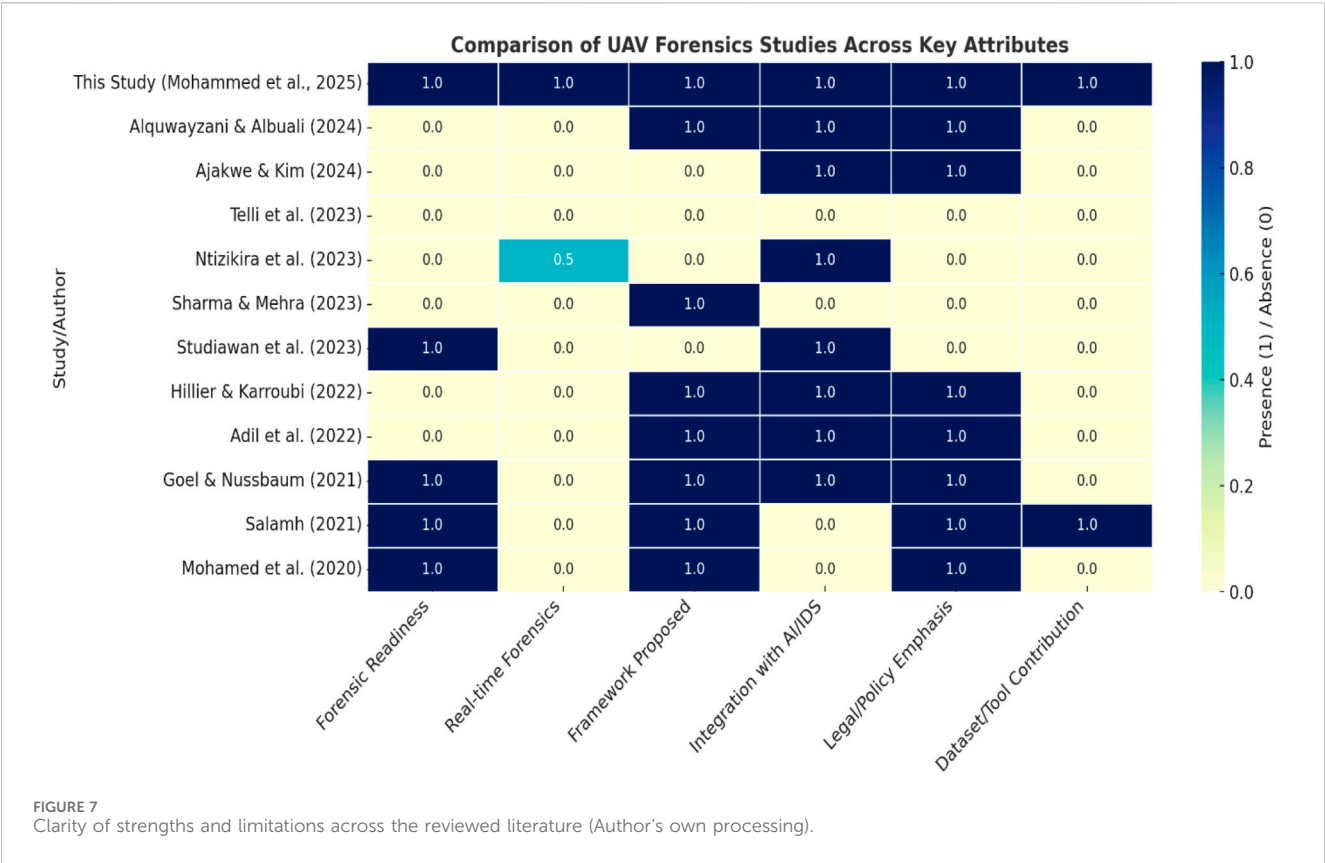
A heatmap was used to present a structured summary of the strengths and limitations identified across the reviewed literature, aiding in the comparison of studies shown in Table 13. It also illustrates how this new study Ajakwe and Kim (2024) demonstrates the most extensive forensic coverage, as depicted in Figure 7.

A visual comparison heatmap of Table 13 that clearly illustrates how each study performs across key attributes such as: Forensic Readiness, Real-time Forensics, Framework Proposed, Integration

TABLE 13 Comparison of study with other state-of-the-arts.

S/n	Study/ Author	Focus area	Forensic readiness	Real-time forensics	Framework proposed	Integration with AI/IDS	Legal/Policy emphasis	Dataset/Tool contribution	Study's unique contribution
1	This Study	UAV digital forensic framework and safety	Forensics-by-design	✓ Yes	✓ Enhanced UAV Forensic Framework	✓ AI + Blockchain-based readiness	✓ Strong legal and standardization call (Strong Global Scope)	✓ Highlights need for datasets (Proposed + Training Need)	Holistic forensic model tailored to UAVs, bridging real-time evidence capture, legal compliance, and technical constraints. First study to integrate real-time forensics, legal, policy, AI, and cloud solutions in UAVs
2	Alquwayzani and Albuali (2024)	Zero Trust for UAVs in IoBT	✗ No	✗ No	✓ ZTA Model	✓ Trust-based AI	✓ Yes	✗ No	Focus on access control and security architecture; lacks forensic mechanisms
3	Ajakwe and Kim (2024)	Smart aerial mobility and logistics security	✗ No	✗ No	✗ No	✓ Context-aware paradigms	✓ Yes	✗ No	Broader aerial transport safety model; limited forensic utility
4	Telli et al. (2023)	Review of UAV applications and trends	✗ No	✗ No	✗ No	✗ No	✗ No	✗ No	Wide-ranging survey; lacks forensic or security framework
5	Ntizikira et al. (2023)	IDS for UAV communications	✗ No	✓ Partial	✗ No	✓ IDS-based	✗ No	✗ No	Effective at threat detection; lacks forensic evidence handling
6	Sharma and Mehra (2023)	Secure communications in IoT-based UAVs	✗ No	✗ No	✗ No	✓ Cryptographic protocols	✗ No	✗ No	Cryptographic protocols for communication, not designed for forensic traceability
7	Studiawan et al. (2023)	UAV forensics overview	✓ Thematic insights	✗ No	✗ No	✗ No	✓ Yes	✗ No	Identifies UAV forensic gaps, but lacks practical solution or framework
8	Hillier and Karroubi (2022)	Threat hunting lifecycle for digital systems	✗ No	✗ No	✓ General Lifecycle	✓ Adaptive detection	✓ Yes	✗ No	Valuable threat hunting model; not UAV-specific or forensically integrated
9	Adil et al. (2022)	UAV-IoT security threats and taxonomy	✗ No	✗ No	✗ No	✓ IDS + policy view	✓ Yes	✗ No	Comprehensive taxonomy; not tailored for forensic or incident response
10	Goel and Nussbaum (2021)	Cyberattack attribution across domains	✓ Attribution logic	✗ No	✗ No	✓ Pattern recognition	✓ Yes	✗ No	Cross-domain attribution analysis; lacks UAV-specific evidence protocols
11	Salamh (2021)	UAV forensic taxonomy (U-FIT)	✓ Yes	✗ No	✓ Taxonomy	✗ No	✓ Moderate	✓ Taxonomy tool	Provides theoretical forensic taxonomy, limited real-time or technical application
12	Mohamed et al. (2020)	Forensics in cyber-physical systems	✓ General CPS	✗ No	✓ Conceptual model	✗ No	✓ Yes	✗ No	General CPS model; not directly applicable to UAV ecosystems

(Author's own processing).



with AI/IDS, Legal/Policy Emphasis, and Dataset/Tool Contribution. This heatmap provides a structured overview of strengths and gaps across the literature and highlights how “This study (Mohammed et al., 2025)” stands out with the most comprehensive forensic scope. This heatmap not only validates the comprehensiveness of this study (Mohammed et al. (2025)), but also highlights clear research gaps in the broader UAV forensic literature. Most existing work either targets UAV security in general or offers narrow technical contributions that lack forensic readiness, legal support, or deployable tools. Hence, the visual summary strongly supports the novelty and necessity of a unified, AI-integrated, and legally aware UAV forensic framework as proposed in this current study.

**Trends and Gaps Identified:** most studies ignore the need for in-flight forensic logging or volatile memory protection, which is a major gap, therefore the gap lie within underutilization of real-time forensics which was addressed by this current study (Mohammed et al. (2025). With the exception of Mohammed et al. (2025) and Salamh (2021), no other studies proposed reusable datasets or tools a concern for reproducibility and benchmarking, hence, this study also makes sparse dataset/tool contribution. Less than half the studies meaningfully address legal admissibility, standardization, or jurisdictional constraints limiting their real-world applicability, thus, this study lay more emphases on legal and policy than other studies. AI/IDS is common but often shallow among other studies, although, several papers mention AI or threat

detection, but without deep integration into forensic workflows or evidence validation.

13 Conclusion

In conclusion, the survey confirms alignment between current UAV forensic challenges in literature and real-world stakeholder perspectives. Participants validated both the structure and necessity of the proposed framework, reinforcing its relevance to law enforcement, UAV developers, and policy bodies alike (Alsulami, 2022; Yeboah-Ofori and Brown, 2020). This study provides a comprehensive evaluation of UAV cybersecurity risks and presents the EUAVFF to enhance forensic readiness and incident response. Key innovations include modular forensic components, blockchain-secured logs, and AI-enabled threat detection, addressing deficiencies in existing UAV platforms. Survey findings showing over 70% of respondents unaware of UAV cyber threats reinforce the need for stakeholder education, standardization, and forensic integration. The study identifies persistent challenges such as encryption, volatile memory loss, and jurisdictional barriers, calling for multidisciplinary collaboration to resolve them.

EUAVFF offers a scalable, forward-looking solution adaptable to diverse UAV types, including micro-drones and VTOL systems. Future work should expand on real-world implementation, improve UAV model coverage, and adapt to emerging attack vectors. As UAV



adoption grows across sectors, embedding forensic-by-design principles will be vital to ensuring security, accountability, and resilience. Future iterations of this work should incorporate real-world forensic case studies, involve legal practitioners in co-design, and validate framework components through cross-platform field testing.

## Author contributions

UM: Funding acquisition, Visualization, Writing – review and editing. AEO: Data curation, Funding acquisition, Investigation, Methodology, Validation, Writing – review and editing. OI: Conceptualization, Funding acquisition, Writing – original draft, Writing – review and editing. JR: Funding acquisition, Visualization, Writing – review and editing. OO: Funding acquisition, Resources, Writing – review and editing. PL: Investigation, Supervision, Writing – review and editing. PA: Supervision, Visualization, Writing – review and editing. AGO: Formal Analysis, Writing – review and editing.

## Funding

The author(s) declare that financial support was received for the research and/or publication of this article. Funding provided by Tertiary Education Trust Fund (TetFund), Institutional Based Research Grant, Nigeria.

## References

- Ab Rahman, N. H., and Choo, K. K. R. (2015). A survey of information security incident handling in the cloud. *Comput. and Secur.* 49, 45–69. doi:10.1016/j.cose.2014.11.006
- Abbadi, D., and Lachkar, A. (2025). The cybersecurity risks threatening drones: innovative solutions in the digital age.
- Abdalla, A. S., Powell, K., Marojevic, V., and Geraci, G. (2020). UAV-assisted attack prevention, detection, and recovery of 5G networks. *IEEE Wirel. Commun.* 27 (4), 40–47. doi:10.1109/mwc.01.1900545
- Adel, A. (2020). *Developing a digital forensic capability for critical infrastructures: an investigation framework*. New Zealand: Auckland University of Technology. Available online at: <https://www.aut.ac.nz/researchethics/guidelines-and-procedures/exceptions-to-%20activities-requiring-autec-approval-6>
- Adil, M., Jan, M. A., Liu, Y., Abulkasim, H., Farouk, A., and Song, H. (2022). A systematic survey: security threats to UAV-aided IoT applications, taxonomy, current challenges and requirements with future research directions. *IEEE Trans. Intelligent Transp. Syst.* 24 (2), 1–19. doi:10.1109/tits.2022.3220043
- Aissaoui, R., Deneuville, J. C., Guerber, C., and Pirovano, A. (2023). A survey on cryptographic methods to secure communications for UAV traffic management. *Veh. Commun.* 44, 100661. doi:10.1016/j.vehcom.2023.100661
- Ajakwe, S. O., and Kim, D.-S. (2024). Facets of security and safety problems and paradigms for smart aerial mobility and intelligent logistics. *IET Intelligent Transport Systems* 18 (S1), 2827–2855. doi:10.1049/itr2.12579
- Albrecht, F. G., König, D. H., Baucks, N., and Dietrich, R. U. (2017). A standardized methodology for the techno-economic evaluation of alternative fuels—A case study. *Fuel* 194, 511–526. doi:10.1016/j.fuel.2016.12.003
- Alenezi, A. M. (2024). Cloud security assurance: strategies for encryption in digital forensic readiness. *arXiv Prepr. arXiv:2403.04794*.
- Alharbi, S., Weber-Jahnke, J., and Traore, I. (2011). “The proactive and reactive digital forensics investigation process: a systematic literature review,” in *Information Security and Assurance: international Conference, ISA 2011, Brno, Czech Republic, August 15–17, 2011. Proceedings* (Springer Berlin Heidelberg), 87–100.
- Almusayli, A., Zia, T., and Qazi, E. U. H. (2024). Drone forensics: an innovative approach to the forensic investigation of drone accidents based on digital twin technology. *Technologies* 12 (1), 11. doi:10.3390/technologies12010011
- Alotaibi, F. M., Al-Dhaqm, A., and Al-Otaibi, Y. D. (2022). A novel forensic readiness framework applicable to the drone forensics field. *Comput. Intell. Neurosci.* 2022 (1), 1–13. doi:10.1155/2022/8002963
- Alquwayzani, A. A., and Albuali, A. A. (2024). A systematic literature review of zero trust architecture for UAV security systems in IoT. *Comput. Sci. Math.* 1 (1), 1–33.
- Alshamsi, Y. (2020). *Digital forensic investigation framework on commercial drones*. Doctoral dissertation, Pittsburgh, PA, United States Khalifa University of Science.
- Alsulami, H. (2022). Implementation analysis of reliable unmanned aerial vehicles models for security against cyber-crimes: attacks, tracebacks, forensics and solutions. *Comput. Electr. Eng.* 100, 107870. doi:10.1016/j.compeleceng.2022.107870
- Altawy, R., and Youssef, A. M. (2016). Security, privacy, and safety aspects of civilian drones: a survey. *ACM Trans. Cyber-Physical Syst.* 1 (2), 1–25. doi:10.1145/3001836
- Anagnostis, I., Kotzanikolaou, P., and Douligeris, C. (2024). Understanding and securing Unmanned Aerial Vehicle (UAV) services: a comprehensive tutorial. *Authorea Prepr.* doi:10.36227/techrxiv.170975064.43115762/v1
- Atkinson, S., Carr, G., Shaw, C., and Zargari, S. (2021). Drone forensics: the impact and challenges. *Digital forensic investigation Internet Things (IoT) devices*, 65–124. doi:10.1007/978-3-030-60425-7\_4
- Atrey, I. (2023). Cybercrime and its Legal Implications: analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence. *Int. J. Res. Anal. Rev.* doi:10.1729/Journal.35277
- Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., et al. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digit. Investig.* 22, 3–13. doi:10.1016/j.diin.2017.06.015
- Basan, E., Basan, A., Nekrasov, A., Fidge, C., Abramov, E., and Basyuk, A. (2022). A data normalization technique for detecting cyber attacks on UAVs. *Drones* 6 (9), 245. doi:10.3390/drones6090245
- Brown, C. S. (2015). Investigating and prosecuting cyber crime: forensic dependencies and barriers to justice. *Int. J. Cyber Criminol.* 9 (1), 55. doi:10.5281/zenodo.22387
- Brunty, J. (2023). Validation of forensic tools and methods: a primer for the digital forensics examiner. *Wiley Interdiscip. Rev. Forensic Sci.* 5 (2), e1474. doi:10.1002/wfs2.1474
- Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., et al. (2022). Research trends, challenges, and emerging topics in digital

## Conflict of interest

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

## Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

## Publisher's note

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

forensics: a review of reviews. *Ieee Access* 10, 25464–25493. doi:10.1109/access.2022.3154059

Ceviz, O., Sen, S., and Sadioglu, P. (2024). A survey of security in uavs and fanets: issues, threats, analysis of attacks, and solutions. *IEEE Commun. Surv. and Tutorials*, 1. doi:10.1109/comst.2024.3515051

Chaikin, D. (2006). Network investigations of cyber attacks: the limits of digital evidence. *Crime, Law Soc. Change* 46, 239–256. doi:10.1007/s10611-007-9058-4

Chen, L., Takabi, H., and Le-Khac, N. A. (2019). *Security, privacy, and digital forensics in the cloud* (John Wiley and Sons).

Choudhary, G., Sharma, V., You, I., Yim, K., Chen, R., and Cho, J. H. (2018). “Intrusion detection systems for networked unmanned aerial vehicles: a survey,” in *2018 14th international wireless communications and mobile computing conference (IWCMC)* (IEEE), 560–565.

Clark, D. R., Meffert, C., Baggili, I., and Breitering, F. (2017). DROP (DRone Open source parser) your drone: forensic analysis of the DJI phantom III. *Digit. Investig.* 22, S3–S14. doi:10.1016/j.diin.2017.06.013

Cosar, M. (2022). Cyber attacks on unmanned aerial vehicles and cyber security measures. *Eurasia Proc. Sci. Technol. Eng. Math.* 21, 258–265. doi:10.55549/epstem.1226251

de Melo, C. F. E., e Silva, T. D., Boeira, F., Stocchero, J. M., Vinel, A., Asplund, M., et al. (2021). UAVouch: a secure identity and location validation scheme for UAV-Networks. *IEEE Access* 9, 82930–82946. doi:10.1109/access.2021.3087084

Debas, E., Albuli, A., and Rahman, M. H. (2024). Forensic examination of drones: a comprehensive Study of frameworks, challenges, and machine learning applications. *IEEE Access* 12, 111505–111522. doi:10.1109/access.2024.3426028

Debs, P., and Fayad, L. M. (2023). The promise and limitations of artificial intelligence in musculoskeletal imaging. *Front. Radiology* 3, 1242902. doi:10.3389/fradi.2023.1242902

Dratwa, J. (2014). “Ethics of security and surveillance technologies,” in *Book Ethics of security and surveillance technologies* EGE Opinion Report.

Dumitrescu, C., Minea, M., and Ciotirnae, P. (2019). “UAV detection employing sensor data fusion and artificial intelligence,” in *International conference on information systems Architecture and technology* (Cham: Springer International Publishing), 129–139.

Eltoukhy, A. E., Kolotylo, I., and Hashim, H. A. (2025). Electronic warfare cyberattacks, countermeasures, and modern defensive strategies of UAV Avionics: a Survey. *IEEE Access* 13, 68660–68681. doi:10.1109/access.2025.3561068

Esteves, J. L. (2019). “Electromagnetic Watermarking: exploiting IEMI effects for forensic tracking of UAVs,” in *2019 international symposium on electromagnetic Compatibility-EMC EUROPE* (IEEE), 1144–1149.

Ever, Y. K. (2020). A secure authentication scheme framework for mobile-sinks used in the internet of drones applications. *Comput. Commun.* 155, 143–149. doi:10.1016/j.comcom.2020.03.009

Ezeji, C. L. (2024). Cyber policy for monitoring and regulating cyberspace and cyber security measures for combating technologically enhanced crime in South Africa. *Int. J. Bus. Ecosyst. Strategy* (2687-2293) 6 (5), 96–109. doi:10.36096/ijbes.v6i5.670

Fakhouri, H. N., AlSharaiah, M. A., Alkalaileh, M., and Dweikat, F. F. (2024). “Overview of challenges faced by digital forensic,” in *2024 2nd international conference on Cyber resilience (ICCR)* (IEEE), 1–8.

Fernández-Caramés, T. M., Blanco-Novoa, O., Suárez-Albela, M., and Fraga-Lamas, P. (2018). “A UAV and blockchain-based system for industry 4.0 inventory and traceability applications,” *Proceedings Basel, Switzerland: MDPI*. 4. 26. doi:10.3390/eca-5-05758

Fisher, B. S., and Schnittger, S. (2012). *Autonomous and remote operation technologies in the mining industry*. Australia: BAEconomics Pty Ltd.

Ganesh, N. G., Venkatesh, N. M., and Prasad, D. V. V. (2022). A systematic literature review on forensics in cloud, IoT, AI and blockchain. *Illumination of Artificial Intelligence in Cybersecurity and Forensics*, 197–229.

Giannaros, A., Karras, A., Theodorakopoulos, L., Karras, C., Kranias, P., Schizas, N., et al. (2023). Autonomous vehicles: sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions. *J. Cybersecurity Priv.* 3 (3), 493–543. doi:10.3390/jcp3030025

Goel, S., and Nussbaum, B. (2021). Attribution across cyber-attack types: network intrusions and information operations. *IEEE Open J. Commun. Soc.* 2, 1082–1093. doi:10.1109/ojcoms.2021.3074591

Gülataş, İ., and Bakır, S. (2018). Unmanned aerial vehicle digital forensic investigation framework. *J. Nav. Sci. Eng.* 14 (1), 32–53.

Hadi, H. J., Cao, Y., Nisa, K. U., Jamil, A. M., and Ni, Q. (2023). A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs. *J. Netw. Comput. Appl.* 213, 103607. doi:10.1016/j.jnca.2023.103607

Hartmann, K., and Giles, K. (2016). “UAV exploitation: a new domain for cyber power,” in *2016 8th international conference on cyber conflict (CyCon)* (IEEE), 205–221.

Henriques, J., Caldeira, F., Cruz, T., and Simões, P. (2024). A survey on forensics and compliance auditing for critical infrastructure protection. *IEEE Access* 12, 2409–2444. doi:10.1109/access.2023.3348552

Hillier, C., and Karroubi, T. (2022). Turning the hunted into the hunter via threat hunting: life cycle, ecosystem, challenges and the great promise of AI. *arXiv Prepr. arXiv:2204.11076*.

Horsman, G. (2016). Unmanned aerial vehicles: a preliminary analysis of forensic challenges. *Digit. Investig.* 16, 1–11. doi:10.1016/j.diin.2015.11.002

Horsman, G., and Errickson, D. (2019). When finding nothing may be evidence of something: Anti-forensics and digital tool marks. *Sci. and Justice* 59 (5), 565–572. doi:10.1016/j.scijus.2019.06.004

Johansen, G. (2017). *Digital forensics and incident response*. Birmingham, UK: Packt Publishing Ltd.

Kebande, V. R. (2017). *A novel cloud forensic readiness service model*. South Africa: University of Pretoria.

Khan, A., Gupta, S., and Gupta, S. K. (2022). Emerging UAV technology for disaster detection, mitigation, response, and preparedness. *J. Field Robotics* 39 (6), 905–955. doi:10.1002/rob.22075

Khelifi, A., Ciccone, G., Altaweel, M., Basmaji, T., and Ghazal, M. (2021). Autonomous service drones for multimodal detection and monitoring of archaeological sites. *Appl. Sci.* 11 (21), 10424. doi:10.3390/app11210424

Kouros, K. D. (2025). The use of space-based assets for enhancing EU’s security: an analysis of the role of satellites in detecting internal security threats.

Krishna, C. L., and Murphy, R. R. (2017). “A review on cybersecurity vulnerabilities for unmanned aerial vehicles,” in *2017 IEEE international symposium on safety, security and rescue robotics (SSRR)* (IEEE), 194–199.

Kumar, M. S., and Thampi, S. M. (2025). “From ground to cloud: integrated multi-attack detection in IoT-Driven UAV security frameworks,” in *Securing the connected world: exploring emerging threats and innovative solutions* (Cham: Springer Nature Switzerland), 381–419.

Kuru, K. (2024). Technical report: big data-concepts, infrastructure, analytics, challenges and solutions.

Lee-Morrison, L. (2015). “The Forensic Architecture Project: virtual imagery as evidence in the contemporary context of the war on terror,” in *Workshop: virtual zones of peace and conflict*.

Ly, B., and Ly, R. (2021). Cybersecurity in unmanned aerial vehicles (UAVs). *J. cyber Secur. Technol.* 5 (2), 120–137. doi:10.1080/23742917.2020.1846307

Mantas, E., and Patsakis, C. (2022). “Who watches the new watchmen? The challenges for drone digital forensics investigations,” *Array* (N. Y.). 14, 100135. doi:10.1016/j.array.2022.100135

Maqbool, A., Slimane, J. B., Khediri, N., Ben, M., Ammar, A. K., and Alshammari, A. (2024). Proactive cyber defense and forensic investigation techniques for drone operation: a holistic approach. *J. Of Theor. Appl. Inf. Technol.* 102 (18).

Marinoni, M., Facchinetti, T., Buttazzo, G., and Franchino, G. (2006). “An embedded real-time system for autonomous flight control,” in *Proc. of the 50th int. Congress of ANIPLA on methodologies for emerging technologies in automation (ANIPLA 2006)*, 1237–1242.

McEnroe, P., Wang, S., and Liyanage, M. (2022). A survey on the convergence of edge computing and AI for UAVs: opportunities and challenges. *IEEE Internet Things J.* 9 (17), 15435–15459. doi:10.1109/jiot.2022.3176400

McTurk, B. (2019). *Forensic professionals’ views on the lack of standards in the digital forensic field: a generic qualitative inquiry*. Minneapolis, MN, USA: Capella University.

Mekdad, Y., Aris, A., Babun, L., El Fergougui, A., Conti, M., Lazzaretto, R., et al. (2023). A survey on security and privacy issues of UAVs. *Comput. Netw.* 224, 109626. doi:10.1016/j.comnet.2023.109626

Mohamed, N., Al-Jaroodi, J., and Jawhar, I. (2020). Cyber-physical systems forensics: today and tomorrow. *J. Sens. Actuator Netw.* 9 (3), 37. doi:10.3390/jsan9030037

Mohay, G. (2005). “Technical challenges and directions for digital forensics,” in *First international workshop on systematic approaches to digital forensic engineering (SADFE’05)* (IEEE), 155–161.

Mohsan, S. A. H., Othman, N. Q. H., Li, Y., Alsharif, M. H., and Khan, M. A. (2023). Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends. *Intell. Serv. Robot.* 16 (1), 109–137. doi:10.1007/s11370-022-00452-4

Ntizikira, E., Lei, W., Alblehai, F., Saleem, K., and Lodhi, M. A. (2023). Secure and privacy-preserving intrusion detection and prevention in the internet of unmanned aerial vehicles. *Sensors* 23 (19), 8077. doi:10.3390/s23198077

Oruc, A. (2022). Potential cyber threats, vulnerabilities, and protections of unmanned vehicles. *Drone Syst. Appl.* 10 (1), 51–58. doi:10.1139/juvs-2021-0022

Renduchintala, A., Jahan, F., Khanna, R., and Javadi, A. Y. (2019). A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework. *Digit. Investig.* 30, 52–72. doi:10.1016/j.diin.2019.07.002

Roberts, G. A. (2016). Open-source unmanned aerial vehicles: vulnerabilities, exploits, and risk. *Master’s thesis, Utica Coll.*

- Rowlingson, R. (2004). A ten step process for forensic readiness. *Int. J. Digital Evid.* 2 (3), 1–28.
- Ruffell, A., Pringle, J. K., and Forbes, S. (2014). Search protocols for hidden forensic objects beneath floors and within walls. *Forensic Sci. Int.* 237, 137–145. doi:10.1016/j.forsciint.2013.12.036
- Rugo, A., Ardagna, C. A., and Ioini, N. E. (2022). A security review in the UAVNet era: threats, countermeasures, and gap analysis. *ACM Comput. Surv. (CSUR)* 55 (1), 1–35. doi:10.1145/3485272
- Salamh, F. E. (2021). *A 3-Dimensional UAS forensic intelligence-led taxonomy (U-FIT)*. Doctoral dissertation, West Lafayette, IN, USA: Purdue University.
- Salamh, F. E., Mirza, M. M., and Karabiyik, U. (2021a). UAV forensic analysis and software tools assessment: DJI Phantom 4 and Matrice 210 as case studies. *Electronics* 10 (6), 733. doi:10.3390/electronics10060733
- Salamh, F. E., Karabiyik, U., Rogers, M. K., and Matson, E. T. (2021b). A comparative uav forensic analysis: static and live digital evidence traceability challenges. *Drones* 5 (2), 42. doi:10.3390/drones5020042
- Salfati, E., Salfati, E., and Pease, M. (2022). *Digital forensics and incident response (dfir) framework for operational technology (ot)*. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.
- Schiller, N., Chlosta, M., Schloegel, M., Bars, N., Eisenhofer, T., Scharnowski, T., et al. (2023). Drone security and the mysterious case of dJI's DroneID. *NDSS*. doi:10.14722/ndss.2023.24217
- Shafik, W., Matinkhah, S. M., and Shokoor, F. (2023). Cybersecurity in unmanned aerial vehicles: a review. *Int. J. Smart Sens. Intelligent Syst.* 16 (1), 20230012. doi:10.2478/ijssis-2023-0012
- Shafique, A., Mehmood, A., and Elhadef, M. (2021). Survey of security protocols and vulnerabilities in unmanned aerial vehicles. *IEEE Access* 9, 46927–46948. doi:10.1109/Access.2021.3066778
- Shakeri, R., Al-Garadi, M. A., Badawy, A., Mohamed, A., Khattab, T., Al-Ali, A. K., et al. (2019). Design challenges of multi-UAV systems in cyber-physical applications: a comprehensive survey and future directions. *IEEE Commun. Surv. and Tutorials* 21 (4), 3340–3385. doi:10.1109/comst.2019.2924143
- Shakhatreh, H., Sawalmeh, A. H., Al-Fuqaha, A., Dou, Z., Almaita, E., Khalil, I., et al. (2019). Unmanned aerial vehicles (UAVs): a survey on civil applications and key research challenges. *Ieee Access* 7, 48572–48634. doi:10.1109/access.2019.2909530
- Sharma, J., and Mehra, P. S. (2023). Secure communication in IOT-based UAV networks: a systematic survey. *Internet Things* 23, 100883. doi:10.1016/j.iot.2023.100883
- Sihag, V., Choudhary, G., Choudhary, P., and Dragoni, N. (2023). Cyber4drone: a systematic review of cyber security and forensics in next-generation drones. *Drones* 7 (7), 430. doi:10.3390/drones7070430
- Singh, B. (2024). Unmanned Aircraft Systems (UAS), surveillance, risk management to cybersecurity and legal regulation landscape: unraveling the future analysis, challenges, demand, and benefits in the high sky exploring the strange new world. *Unmanned Aircr. Syst.*, 313–354. doi:10.1002/9781394230648.ch8
- Singh, K. S., Irfan, A., and Dayal, N. (2019). “Cyber forensics and comparative analysis of digital forensic investigation frameworks,” in *2019 4th international conference on Information Systems and computer networks (ISCON)* (IEEE), 584–590.
- Sinha, M. (2021). Radically reimagining forensic evidence. *Ala. L. Rev.* 73, 879. Available online at: <https://ssrn.com/abstract=3891788>
- Stöcker, C., Bennett, R., Nex, F., Gerke, M., and Zevenbergen, J. (2017). Review of the current state of UAV regulations. *Remote Sens.* 9 (5), 459. doi:10.3390/rs9050459
- Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., and Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Commun. Surv. and Tutorials* 22 (2), 1191–1221. doi:10.1109/comst.2019.2962586
- Studiawan, H., Grispos, G., and Choo, K. K. R. (2023). Unmanned aerial vehicle (UAV) forensics: the good, the bad, and the unaddressed. *Comput. and Secur.* 132, 103340. doi:10.1016/j.cose.2023.103340
- Tang, J., Chen, G., and Coon, J. P. (2019). Secrecy performance analysis of wireless communications in the presence of UAV jammer and randomly located UAV eavesdroppers. *IEEE Trans. Inf. Forensics Secur.* 14 (11), 3026–3041. doi:10.1109/tifs.2019.2912074
- Tecedor Roa, J. (2024). Ground command unit to DRONE radio control and telemetry.
- Telli, K., Kraa, O., Himeur, Y., Ouamane, A., Boumehraz, M., Atalla, S., et al. (2023). *A Compr. Rev. Recent Res. Trends Unmanned Aer. Veh. (UAVs). Syst.* 11, 400. doi:10.3390/systems11080400
- Tyshchuk, V. V. (2024). A review of legal regulation regarding the use of unmanned aerial vehicles for border security and the impact of global technologies. *Int. Comp. Jurisprud.* 10 (1), 61–81. doi:10.13165/j.icj.2024.06.005
- Vajravelu, A., Ashok Kumar, N., Sarkar, S., and Degadwala, S. (2023). “Security threats of unmanned aerial vehicles,” in *Wireless networks: cyber security threats and countermeasures* (Cham: Springer International Publishing), 133–164.
- Vassiliadis, T., and Hedström, J. (2024). The challenges and opportunities in incident response for companies.
- Verma, M. (2024). The crucial role of flight data recorders in modern aviation.
- Viswanathan, S., and Baig, Z. (2020). “Digital forensics for drones: a study of tools and techniques,” *Appl. Tech. Inf. Secur. 11th Int. Conf.* 11, 29–41. doi:10.1007/978-981-33-4706-9\_3
- Wang, Y., Su, Z., Benslimane, A., Xu, Q., Dai, M., and Li, R. (2022). “A learning-based honeypot game for collaborative defense in UAV networks,” in *GLOBECOM 2022-2022 IEEE global communications conference* (IEEE), 3521–3526.
- Wang, Z., Li, Y., Wu, S., Zhou, Y., Yang, L., Xu, Y., et al. (2023). A survey on cybersecurity attacks and defenses for unmanned aerial systems. *J. Syst. Archit.* 138, 102870. doi:10.1016/j.sysarc.2023.102870
- Ward, E. D. (2021). *The influence of Mobile technology advancements on digital forensics investigations practices and procedures: a generic qualitative inquiry*. Minneapolis, MN, United States Capella University.
- Whelan, J., Sangarapillai, T., Minawi, O., Almeahadi, A., and El-Khatib, K. (2020). “Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles,” in *Proceedings of the 16th ACM symposium on QoS and security for wireless and Mobile networks*, 23–28.
- Xia, X., Fattah, S. M. M., and Babar, M. A. (2023). A survey on UAV-Enabled edge computing: resource management perspective. *ACM Comput. Surv.* 56 (3), 1–36. doi:10.1145/3626566
- Xie, L., Yuan, B., Yang, H., Hu, Z., Jiang, L., Zhang, L., et al. (2024). MRFM: a timely detection method for DDoS attacks in IoT with multidimensional reconstruction and function mapping. *Comput. Stand. and interfaces* 89, 103829. doi:10.1016/j.csi.2023.103829
- Yaacoub, J. P. A., Noura, H. N., Salman, O., and Chehab, A. (2022). Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. *Int. J. Inf. Secur.* 21 (1), 115–158. doi:10.1007/s10207-021-00545-8
- Yeboah-Ofori, A., and Brown, A. D. (2020). Digital forensics investigation jurisprudence: issues of admissibility of digital evidence. *J. Forensic, Leg. and Investigative Sci.* 6 (1), 1–8. doi:10.24966/flis-733x/100045
- Zaki, A. M., Abdelhamid, A. A., Ibrahim, A., Eid, M. M., and El-Kenawy, E. S. M. (2024). Securing the skies: a study of cybersecurity measures in unmanned aerial vehicles. *Int. J. Wirel. and Ad Hoc Commun.* 8 (1), 51–55. doi:10.54216/ijwac.080106