International Journal of Basic and Applied Sciences, 14 (SI-1) (2025) 22-25

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/vr9xzy19
Research paper

Cybersecurity Challenges in Autonomous Unmanned Aerial Vehicle Networks

Sumit Ramswami Punam [1] *, Manish Nandy [2]

[1] Department of Electrical and Electronics Engineering, Kalinga University, Raipur, India
[2] Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India
**Corresponding author E-mail: sumit.kant.dash@kalingauniversity.ac.in*

Received: May 2, 2025, Accepted: May 26, 2025, Published: July 7, 2025

Abstract

The use of autonomous unmanned aerial vehicles (UAVs) can offer innovative solutions to various problems, providing operational and financial benefits, as well as agricultural and military advantages in surveillance and logistics. Since they depend on wireless networks for real-time data processing and distributed control, UAVs have become so ubiquitous that they present serious cybersecurity risks. Poorly designed UAV systems offer hackers fresh possibilities to launch cyberattacks, while GIS spoofing opens channels for data breach exploits that result in communication failures. Critical applications needing exact data and control parameters suffer operational hazards on system performance, reliability, and safety standards, given the dependence on unmanned aerial vehicles. The different risks to UAV networks with respect to cybersecurity and their effects on operations are covered in this article. Using an analytical approach, researchers found risks and evaluated them to design security measures suitable for the unmanned aerial vehicle system. The research explains why unauthorized access to UAV communications and data accuracy must be defended by encryption algorithms, together with more rigorous authentication methods and intruder detection systems. The paper proposes a series of realistic security procedures that companies from several sectors can implement to counter growing threats and maintain UAV networks in a state of operational safety and system flexibility.

Keywords: *Vehicles; Cyber Security; Threats; UAV Network; Rick; Security.*

1. Introduction

Autonomous Unmanned Aerial Vehicle (UAV) networks help several sectors, from defense to agriculture, track environmental shifts, expedite logistics, and take advantage of defense features, helping them [1]. Their operational flexibility, as well as cost savings and efficiency gains, help many sectors to use UAVs [4]. When incorporated into crucial infrastructure, UAVs present major structural safety issues that can affect their performance readiness [2]. UAVs face several cyber assault threats due to wireless data transmission, including on-board sensors and cloud-based real-time computing [3]. These menaces consist of hacking attempts, communication jamming, GPS spoofing, and data falsification directed at drone safety and operational integrity [15]. The distributed nature of control centers operating UAVs is challenging because these assets perform surveillance tasks across military domains and infrastructure inspection and environmental monitoring [8]. Drone network success depends on establishing node-to-node connectivity and safe data transmission that upholds permanent operational safety metrics [5].

2. Problem statement

Modern UAVs are vulnerable to cyber threats due to unsecured communication protocols and data transfer, and control systems. Real-time data processing exposes UAVs to hacking and spoofing threats and jamming incidents, which are accelerated by their wireless communication systems and result in unauthorized access attacks. Autonomous UAVs operate with minimal human interface, yet are vulnerable to security threats because cyber-attacks can access and command these autonomous systems [14]. Security flaws in these critical applications, such as military operations, infrastructure surveillance, and environmental management, pose huge risks for unacceptable consequences [7]. Implementing security solutions is hard because UAV systems have distributed architecture components connecting multiple parts of their operational structure [6]. While many studies advocate GPS spoofing countermeasures such as antenna nulling or signal verification, few address their limitations in swarm UAV scenarios with shared GPS inputs. Furthermore, existing works rarely consider energy trade-offs in encryption frameworks. A critical gap is the underuse of real-time AI models trained on UAV-specific telemetry datasets. Foundational frameworks provided the first taxonomy of UAV networks but lacked cybersecurity dimensions, necessitating more integrated modern reviews.

3. Review of literature

The gaps identified in the literature—especially regarding real-time anomaly detection and blockchain feasibility—directly shaped the methodological approach of this study. Section 4 details how a multi-criteria evaluation framework was built to address these shortcomings. Spoofing Attacks: GPS spoofing and additional spoofing attacks manipulate UAV systems via manipulated navigation and communication data components specific to the operational environment [16]. A spoofing attack enables adversaries to manipulate UAV trajectories toward unexpected regions while also enabling them to acquire control of systems to modify aircraft flight paths. Due to exclusive GPS signal dependence for navigation, UAVs face serious operational challenges in response to GPS spoofing attacks. Through adjustments to crucial operational data, attackers produce mission failures and intense operational disruptions that have the strongest effect on military surveillance capabilities and commercial delivery services [9]. The prevention of spoofing needs accurate validation systems linked with protected communication standards to defend navigation channels.

Data Integrity: UAV systems must retain perfect data integrity throughout their operational period because accurate real-time information continues to be vital for military reconnaissance operations in addition to environmental research initiatives. The transfer of UAV data between UAVs and control stations remains at risk for interception by man-in-the-middle attackers who then use their stolen data to create confusion in operational feedback and flight operational decision-making during continuous flight operations [10]. The application of UAV systems at national security and disaster response levels suffers critical consequences from any unauthorized alterations to collected data. Data validity alongside protocol encryption and algorithmic hashing, and monitoring protocols ensures information integrity protection against unauthorized alterations.

Denial of Service (DoS) Attacks: When operators launch Denial of Service (DoS) attacks, they overload UAV mechanisms with made-up network traffic, which disrupts their regular functioning procedures. RTL data and cloud-processing UAV systems are vulnerable to DoS attacks because excessive fake requests consume resources and cause system failures and shutdowns [11]. Technological event sequences caused by DoS attacks make UAV control unstable and result in uncontrolled states where UAVs deviate from their operational objective. Protection systems must prevent attacks first because attacks create operational risks during defense-critical moments, where maintenance cycles cause big operational disruptions.

4. Methodology

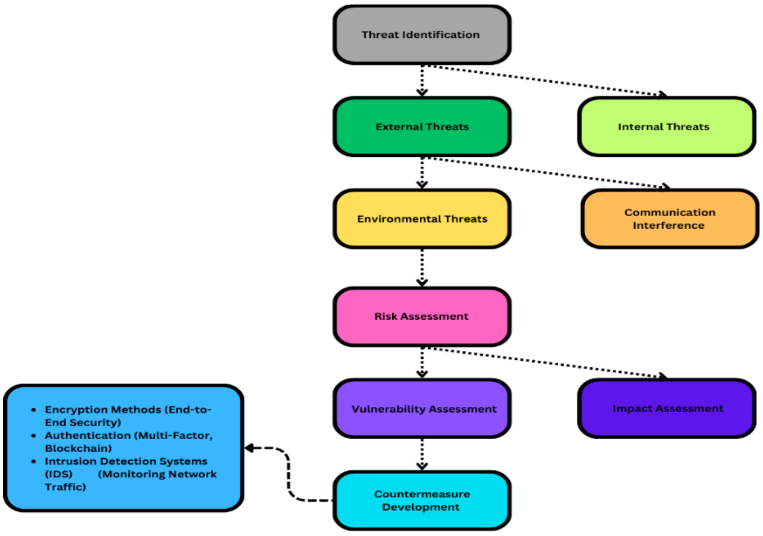
Threat Identification
External Threats
Internal Threats
Environmental Threats
Communication Interference
Risk Assessment
Vulnerability Assessment
Impact Assessment
Countermeasure Development
Encryption Methods (End-to-End Security)
Authentication (Multi-Factor, Blockchain)
Intrusion Detection Systems (IDS) (Monitoring Network Traffic)

Fig. 1: UAV Cybersecurity Methodology.

4.1. Threat identification

To protect the UAV network infrastructure, you need to know the major threats first. The three main external threats to UAVs are hackers who steal data and use it to disrupt operations and get valuable information from UAVs. Water supply operations face primary internal threats from system failures combined with intentional interference from authorized personnel who operate and maintain UAVs. System failures occur from equipment malfunction and authorized personnel taking unauthorized actions. Along with pollution, UAVs face two primary external threats: Weather instability creates unpredictable conditions and electromagnetic disturbances that break communication and control vehicle functions. Knowing the current threats means better security implementations to keep UAVs operational and safe. Threat Classification Matrix: This figure 1 categorizes common UAV vulnerabilities using impact vectors such as data integrity, control system takeover, and service disruption.

4.2. Countermeasure development

Many security measures have been proposed to address threat detection and risk assessment needs to protect UAVs. To protect data transmission between UAVs and their control stations, encryption methods provide end-to-end secure communication. MFA authentication systems and blockchain-based approaches should secure UAV system access as they verify that only authorized personnel manage UAV control systems. Threats were classified based on severity, exploitability, and impact, adapted from the Common Vulnerability Scoring System (CVSS v3.1). Ratings in Tables 1–3 were derived through a Delphi method involving cybersecurity experts and a review of case studies. Figures 1–4 illustrate the evaluation workflow, threat hierarchy, and rating criteria. For example, Image2.png outlines the threat classification matrix used during expert panel discussions.

5. Result

5.1. Agricultural UAVs

Agricultural UAVs perform three critical missions of growth monitoring, alongside soil assessment and irrigation determination. These system infrastructures remain at risk due to both data manipulation activities and unauthorized access attempts, thus leading to faulty statistical agricultural data and revenue losses. For lightweight encryption, symmetric key algorithms such as AES-128 and the SPECK cipher are often preferred due to their low computational overhead suitable for UAVs' limited resources. Public key cryptography (e.g., ECC) is occasionally deployed in hybrid models to enhance key exchange security. Regarding blockchain, its implementation in UAVs is limited by latency and energy constraints. However, permissioned blockchain frameworks like Hyperledger Fabric offer a more scalable approach. [15] proposed an AI-integrated blockchain architecture where anomaly detection is embedded within a distributed ledger framework, enhancing tamper-resistance while minimizing processing burden.

The following table displays the threat likelihood, impact, and efficacy of the recommended countermeasures:

Table 1: Threat Likelihood, Impact, and Countermeasure Effectiveness for Agricultural UAVs

Threat	Likelihood (1-5)	Impact (1-5)	Countermeasure Effectiveness (1-5)
Data tampering	4	5	4
Unauthorized access	4	4	5
Data interception	3	5	4
Sensor failure	3	3	4

5.2. Military UAVs

High-risk military UAV missions face two main security threats: GPS spoofing alongside illegal control attempts, which could cause mission failure or drone seizure incidents [12]. The table below summarizes the risk assessment for military UAVs:

Table 2: Threat Likelihood, Impact, and Countermeasure Effectiveness for Military UAVs.

Threat	Likelihood (1-5)	Impact (1-5)	Countermeasure Effectiveness (1-5)
GPS spoofing	5	5	5
Unauthorized control	4	5	4
Signal jamming	3	4	4
Network breaches	3	5	4

5.3. Logistics UAVs

Due to their susceptibility to denial-of-service attacks and data integrity issues, Logistics UAVs suffer operational instability and distribution breakdowns. The table below shows the severity of these dangers and the efficacy of countermeasures:

Table 3: Threat Likelihood, Impact, and Countermeasure Effectiveness for Logistics UAVs.

Threat	Likelihood (1-5)	Impact (1-5)	Countermeasure Effectiveness (1-5)
Denial of Service (DoS)	4	4	5
Data manipulation	3	4	4
Communication interference	3	5	4
Payload theft	2	5	4

1 = minimal impact or likelihood; 5 = critical impact or highly probable occurrence, based on expert consensus and literature trend analysis.

6. Conclusion

Strong cybersecurity measures have emerged as essential because UAV network adoption continues to expand into industrial sectors. Wireless network real-time processing requirements, when coupled with self-contained functionalities, generate particular security challenges for such systems. This includes data manipulation, defense against GPS hijacks, denial of service attacks, and unauthorized access incidents, and shows how to prevent them. By combining threat identification and defensive system development, this research provides a framework to build safer UAVs. This system structure protects vulnerabilities across UAV network systems for military and agricultural, and logistical use to ensure safe operation. Future UAVs need future cybersecurity solutions. Future research needs to combine modern security protocols, including blockchain, to ensure independent administration and complete data security. Artificial intelligence systems show immense potential for identifying anomalies in real-time, which helps security teams prevent upcoming cyber attacks [13]. Enhanced security methods through continuous threat-level adaptations will guarantee the reliability of UAV networks, which enables safe integration into critical operations. Future research should benchmark lightweight encryption schemes like LEA or PRESENT under various UAV processor loads. Moreover, real-time anomaly detection models such as federated learning-based LSTM networks must be tested on UAV telemetry data. Additionally, blockchain frameworks should be evaluated for real-world feasibility by measuring processing latency and energy overhead on UAV testbeds.

References

[1] Zhang, Z., & Shu, Z. (2024). Unmanned aerial vehicle (UAV)-assisted damage detection of wind turbine blades: A review. Energies, 17(15), 3731. https://doi.org/10.3390/en17153731.

[2] Santoso, J. T., Raharjo, B., & Wibowo, A. (2024). Combination of Alphanumeric Password and Graphic Authentication for Cyber Security. Journal of Internet Services and Information Security, 14(1), 16-36. https://doi.org/10.58346/JISIS.2024.I1.002.

[3] Babu, C. S., & Pal, A. (2024). Enhancing Security for Unmanned Aircraft Systems in IoT Environments: Defense Mechanisms and Mitigation Strategies. Unmanned Aircraft Systems, 429-476. https://doi.org/10.1002/9781394230648.ch11.

[4] Cvijić, R., Milošević, A., Čelebić, M., & Kovačević, Ž. (2018). Geological and Economic Assessment of the Perspective of the Mining in Ljubija Ore Region. Archives for Technical Sciences, 1(18), 1–8. https://doi.org/10.7251/afts.2018.1018.001C.

[5] Shah, I. A. (2024). Privacy and security challenges in unmanned aerial vehicles (UAVs). Cybersecurity in the Transportation Industry, 93-115. https://doi.org/10.1002/9781394204472.ch5.

[6] Juma, J., Mdodo, R. M., & Gichoya, D. (2023). Multiplier Design Using Machine Learning Algorithms for Energy Efficiency. Journal of VLSI Circuits and Systems, 5(1), 28–34. https://doi.org/10.31838/jvcs/05.01.04.

[7] Mykytyn, P., Brzozowski, M., Dyka, Z., & Langendoerfer, P. (2024). A Survey on Sensor-and Communication-Based Issues of Autonomous UAVs. CMES-Computer Modeling in Engineering & Sciences, 138(2). https://doi.org/10.32604/cmes.2023.029075.

[8] Papadopoulos, N. A., & Konstantinou, E. A. (2025). SoC solutions for automotive electronics and safety systems for revolutionizing vehicle technology. Journal of Integrated VLSI, Embedded and Computing Technologies, 2(2), 36–43.

[9] Chen, J., & Zhang, C. (2024, September). A UAV Communication System with Anti-Interference and Covert Communication Capabilities Using Two Antennas. In 2024 AIAA DATC/IEEE 43rd Digital Avionics Systems Conference (DASC) (pp. 1-4). IEEE. https://doi.org/10.1109/DASC62030.2024.10748965.

[10] Talaei Khoei, T., Al Shamaileh, K., Devabhaktuni, V. K., & Kaabouch, N. (2025). Performance analysis of capsule networks for detecting GPS spoofing attacks on unmanned aerial vehicles. International Journal of Information Security, 24(1), 62. https://doi.org/10.1007/s10207-024-00978-x.

[11] Kostopoulos, N., Stamatiou, Y. C., Halkiopoulos, C., & Antonopoulou, H. (2025). Blockchain Applications in the Military Domain: A Systematic Review. Technologies, 13(1), 23. https://doi.org/10.3390/technologies13010023.

[12] Tychola, K. A., & Rantos, K. (2025). Cyberthreats and Security Measures in Drone-Assisted Agriculture. Electronics, 14(1), 149. https://doi.org/10.3390/electronics14010149.

[13] Prasath, C. A. (2023). The role of mobility models in MANET routing protocols efficiency. National Journal of RF Engineering and Wireless Communication, 1(1), 39-48.

[14] Abdullahi, S. M., & Lazarova-Molnar, S. (2025). On the adoption and deployment of secure and privacy-preserving IIoT in smart manufacturing: a comprehensive guide with recent advances. International Journal of Information Security, 24(1), 53. https://doi.org/10.1007/s10207-024-00951-8.

[15] Tlili, F., Ayed, S., & Fourati, L. C. (2024). Advancing UAV security with artificial intelligence: A comprehensive survey of techniques and future directions. Internet of Things, 101281. https://doi.org/10.1016/j.iot.2024.101281.

[16] Usikalu, M. R., Alabi, D., & Ezeh, G. N. (2025). Exploring emerging memory technologies in modern electronics. Progress in Electronics and Communication Engineering, 2(2), 31–40. https://doi.org/10.1109/TSUSC.2024.3443256.

[17] Pasdar, A., Koroniotis, N., Keshk, M., Moustafa, N., & Tari, Z. (2024). Cybersecurity Solutions and Techniques for Internet of Things Integration in Combat Systems. IEEE Transactions on Sustainable Computing.

[18] Wheeler, M. (2024). Warming Wars: The Role of Climate Change in Future National Security Challenges (Doctoral dissertation, Georgetown University).

[19] Sindhu, S. (2025). Comparative Analysis of Battery-Supercapacitor Hybrids for Fast EV Charging Infrastructure. Transactions on Energy Storage Systems and Innovation, 1(1), 26-33.

[20] Achehboune, M., Sani, A., & Boukdir, M. (2025). A note on maximal regularity in relation with measure theory. Results in Nonlinear Analysis, 8(1), 193-203.

[21] S. K. Ghosh, E. Kepros, Y. Chu, B. Avireni, B. Wright and P. Chahal, "Terahertz Metasurfaces on Flex Using Aerosol Jet Printing and a Novel Parylene Lift-off Process," *2024 IEEE 74th Electronic Components and Technology Conference (ECTC)*, Denver, CO, USA, 2024, pp. 760-764, https://doi.org/10.1109/ECTC51529.2024.00124.