Chapter 11
Blockchain-Powered Drone Surveillance: Enhancing Security and Transparency With IoT

B. Shaji
https://orcid.org/0000-0001-9688-6333
Department of Computer Science and Engineering, Mahaguru Institute of Technology, India

N. R. Ram Mohan
https://orcid.org/0000-0002-0624-145X
Department of Computer Science and Engineering, St. Thomas College of Engineering and Technology, India

K. L. Nisha
https://orcid.org/0000-0002-3495-4668
Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

ABSTRACT

Integrating blockchain and IoT with drone technology transforms surveillance by boosting security, transparency, and real-time monitoring. IoT-enabled drones access remote areas, while blockchain ensures tamper-proof data and secure communication. Features like autonomous navigation and smart payloads are enhanced through smart contracts and decentralized ledgers. Despite benefits, challenges such as blockchain's latency and high computational demand remain. Solutions include edge computing and lightweight cryptography to support resource-limited drones. This integration enables intelligent, reliable surveillance systems. Future research can focus on optimizing blockchain for drone communication and AI-driven decision-making. This interdisciplinary study will open the door towards the revolution of surveillance systems, ensuring reliability and trustworthiness in real-time applications.

DOI: 10.4018/979-8-3373-4277-1.ch011

1. INTRODUCTION

Drones are no longer just gadgets with cameras attached; they have become advanced surveillance tools. Modern models can capture not only clear photographs and videos but also thermal images that our eyes cannot normally detect. Some of the newer versions even come equipped with artificial intelligence, which helps them process the data they collect and sometimes act without constant human input. Since drones can be connected as part of the Internet of Things, they are able to cover large or difficult areas much faster than ground-based systems. This shift is already visible in fields such as agriculture, where farmers use them to monitor crops, and in urban security, where they support monitoring tasks that once relied only on people or fixed cameras (Branco et al.,2025).

Since drones can be linked through the Internet of Things, they act like moving network points that extend coverage to wide or hard-to-reach locations. In practice, this has improved both the speed and the accuracy of monitoring. The impact can be seen in different areas—farmers now use drones to track crop health, while cities rely on them for public safety. Compared with older systems that depended only on fixed cameras or manual observation, drones clearly provide a more flexible option (Yucesoy et al., 2025).

2. CURRENT CHALLENGES IN DRONE-BASED SURVEILLANCE SYSTEMS

One of the most pressing concerns with drones is security. In many setups today, drones are designed to take off from and return to a central control room. This creates a single point of weakness—if that control room is compromised, every connected drone can also be attacked. Even with time-stamping and other methods to ensure data integrity, there can be a delay of a few seconds or more before a drone makes it back to the control room, which can affect how quickly its data is confirmed as reliable evidence (Marek et al., 2025). Security risks also extend to the way drones communicate. Both the data they exchange and the commands they receive are attractive targets for hackers, who may try not only to disrupt the mission but also to take control of it without being noticed (Dorri et al, 2021).

Secondly, communication between drones is weak with today's technology. As drone technology advances, so does hacking technology (Wadhwa et al., 2025). A simple way for an attacking party to cause havoc would be signal jamming, cutting off some/all remote-control links between controllers on earth and drones close by. Another option would be intercepting either command signals or live video feeds to launch various types of attacks, such as Denial-of-Service Attacks against Drones, starving it for resources; spoofed commands leading to disaster or Grand Theft Auto-like crashes; drone-crashing packets-darknet DOS-ing if network congestion reveals data link information-security properties, etc. While traditional aircraft communicate via radio frequencies because these functions work without issue in un-segregated airspace, after millions of drones appear beside planes and helicopters, signaling interference makes this possibly unworkable (Wazid et al., 2025).

Thirdly, privacy becomes a critical concern whenever constant surveillance technologies are deployed, as seen years ago in Davos during the World Economic Forum. Police there experimented with advanced aerial monitoring tools, including China's civilian UAV (DJI Phantom) and Germany's Eagle's Lock system, capable of operating for hours at high altitudes while transmitting live video feeds (Odumbo & Onuma, 2025). While these tools helped detect certain incidents, they also highlighted a broader issue: widespread drone use by thousands of citizens raises pressing questions about regulation and the protection of private life.