Vol 8, Issue 6, 2025 **Impact Factor: 8.535** DOI: https://doi.org/10.31426/ijamsr.2025.8.6.8426

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

# A Blockchain-Enabled Security Framework for Enhancing Data Integrity and Privacy in Drone Systems

**B. Saritha** [1]

[1] Research Scholar, Department of Computer Science, Mansarovar Global University, Sehore, M.P., India.

**Dr. Dhirendra Kumar Tripathi** [2]

[2] Supervisor, Department of Computer Science, Mansarovar Global University, Sehore, M.P., India.

**ABSTRACT**

Data integrity, privacy, and security are of the utmost importance due to the growing use of drones and Unmanned Aerial Vehicles (UAVs) in mission-critical applications. Problems with tampering, unauthorised access, and single-point failures are common in traditional centralised data storage technologies, which are problematic for UAV-based systems. This paper presents a security framework that may be implemented on top of blockchain technology. It combines many cryptographic methods to provide strong data protection, including Elliptic Curve Diffie-Hellman (ECDH), SHA-256 hashing, and distributed architectures that are hosted in the cloud. Drones and other unmanned aerial vehicles (UAVs) gather vital information from their sensors, encrypt it with PECC, and send it to a decentralised cloud system. While ECDH and SHA-256 offer secure communication and data integrity, blockchain guarantees immutability, transparency, and tamper resistance. With an 85% success rate for preservation, a 92% success rate for privacy, an 85% success rate for defence, and a 90% success rate for attack detection, the suggested strategy substantially outperforms current approaches across important parameters, according to performance tests. Based on these findings, the framework is appropriate for a variety of mission-critical applications due to its efficacy in improving UAV systems' security, privacy, and dependability.

***Keywords:*** *Blockchain, Drone, Privacy, Security, Attack.*

## I. Introduction

Drones, also known as unmanned aerial vehicles (UAVs), are seeing increased use in a wide variety of fields and industries, from logistics and emergency response to aerial surveys and agricultural monitoring. The use of digital technology for data gathering, transport, storage, and processing

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

brings up serious worries about data integrity and privacy, despite the fact that these systems provide unmatched flexibility and efficiency. Making ensuring that data acquired by drones is accurate, consistent, and reliable throughout its lifetime is crucial for data integrity. This means that the data must not be altered in any way, and must stay trustworthy. Critical applications like disaster management, urban planning, or defence operations are especially vulnerable to the consequences of inaccurate or corrupted data, which can include faulty decision-making, financial losses, operational failures, or even safety issues. Secure data storage, strong authentication procedures, and encryption are essential for drone systems to keep data intact in the face of threats such signal interference, communication flaws, cyberattacks, and software failures.

Concerns about privacy are as important as those about honesty. Drones can naturally cover vast areas, including private property and delicate ecosystems, and collect high-resolution images, audio, and location data. While there are numerous valid uses for this capacity, it does present serious threats to personal and company data. Legal repercussions, ethical breaches, and public mistrust might ensue from unauthorised monitoring, data leaking, or abuse of personal information. Technical, legislative, and administrative steps are all necessary to guarantee privacy during drone operations. Data anonymisation in real-time, geofencing to block access to limited regions, rigorous access control, and conformity with national and international data protection standards are all possible measures. There is a growing need for proactive privacy-preserving techniques due to the fact that the attack surface for possible breaches is expanding as drones interface with the Internet of Things (IoT), cloud computing, and artificial intelligence for real-time data analysis.

Data integrity and privacy are two sides of the same coin in drone systems; safeguards for one might have unintended consequences for the other. For instance, while robust encryption methods improve data security and integrity, they could make it harder to share data, make it work with other systems, or do real-time analyses—all of which are crucial to running operations efficiently. Drone system design must thus take a comprehensive approach, balancing practicality with strong privacy and security measures. Responsible and secure usage of drones while preserving sensitive data requires a concerted effort from researchers, developers, and lawmakers to solve these problems with new cybersecurity solutions, ethical standards, and legislative frameworks.

## II. Review of Literature

Alqarni, Mohammed. (2024) Networks made up of several small unmanned aerial vehicles (UAVs) have recently attracted a lot of attention due to developments in wireless transceivers and robotics for the air. Although unmanned aerial vehicle (UAV) adhoc networks are ideal for some uses, they are susceptible to cyberattacks due to their dynamic topology and lack of centralised management. Unmanned Aerial Vehicles (UAVs) enrich and assist the ground network's sensor nodes and mobile nodes in data collecting and general network performance in several uses, including Internet of Things (IoT) networks and emergency failover networks. To achieve the goals of the network's purpose, it is critical to guarantee the safety of the adhoc UAV network and the data it contains. The blockchain-assisted security framework (BCSF) is a new method that we provide in this article for securing UAV adhoc networks. By adapting blockchain technology to the message's priority before transmission via the ad hoc UAV network, we show that the suggested approach offers network security without compromising speed. After conducting

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

a theoretical analysis using models from queuing theory to calculate average latency, we simulate the proposed BCSF approach and find that it performs better than the alternatives in terms of energy efficiency, data secrecy, data recovery, and transaction delay.

Kumar, Vinod. (2024) More and more, industries as varied as logistics, farming, surveillance, and emergency management are putting UAVs to use. Nevertheless, they are vulnerable to a range of cybersecurity risks because to their dependence on safe and effective communication networks. Blockchain technology (BCT) provides potential solutions to address these weaknesses due to its decentralised, irreversible, and transparent nature. This paper reviews unmanned aerial vehicle (UAV) communication networks, discusses blockchain's function in UAV communication, identifies and resolves critical security issues, and suggests a new consensus-building method to strengthen UAV network security. Create a trustworthy UAV communication system using a blockchain-based methodology by comparing the suggested method's results to those of current models according to privacy, security, attack rates, and dependability. So, both ciphertext and plaintext assaults may be better protected with the help of the proposed approach. When compared to the state-of-the-art, the results confirm the efficacy and security aspects of the proposed technique.

Gupta, Rajesh et al., (2021) Recent years have shown that Unmanned Aerial Vehicles (UAVs) have tremendous promise for improving healthcare, supply chain management, and video and surveillance while simultaneously reducing costs and increasing efficiency. There are a lot of privacy and security concerns with it, and experts from all around the world have come up with a lot of ways to keep sensitive information safe from hackers. A large number of them have proposed cryptographic-based approaches, which need substantial computational resources. While some academics have proposed blockchain-based solutions, these have raised concerns about the potential high costs of data storage and reliability/bandwidth/latency difficulties that may plague these systems. In this research, we offer a solution to these problems by proposing a secure UAV communication strategy over 6G network that uses the Inter Planetary File System (IPFS) and blockchain technology. The suggested method improves network performance, decreases data storage costs, and safeguards data privacy. After that, we outline the difficulties of the research and the ways forward for developing the system further.

Álvares, Paulo et al., (2021) It was anticipated that by 2020, there will be almost 26 billion Internet-connected gadgets, with a significant portion of those being automobiles. The term "Internet of Vehicles" (IoVa) describes a network of interconnected smart vehicles and other devices that work together to alleviate traffic, shorten travel times, increase comfort, and decrease pollution and accidents. Since attackers might utilise this data, it is necessary for the transmission of sensitive information (such position) to have specific security features in order to protect cars and drivers. In decentralised, untrustworthy settings, such as IoV networks, the relatively new technology known as blockchain ensures trust between nodes by use of cryptographic algorithms and consensus methods. Due to Blockchain's ability to address and resolve a wide range of issues plaguing the Internet of Vehicles (IoV), extensive study on its incorporation into the latter has shown promising results. One of the major drawbacks of Blockchain implementations in IoV is that they do not meet the computational and energy needs of traditional Blockchain systems. As a result, these implementations must contend with the difficulty of IoV node resource limits. One last purpose for these two technologies is to provide the groundwork for smart cities, which will open the door to new application models and improved outcomes for end users.

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

## III. Proposed Framework

Improve the trustworthiness, confidentiality, and integrity of data in unmanned aerial vehicle (UAV) and drone systems using this study's proposed blockchain-enabled security architecture. Tampering, illegal access, and single-point failures are risks associated with traditional central data storage. The system incorporates cryptographic methods, blockchain technology, and a distributed architecture on the cloud to manage UAV data securely, therefore resolving these challenges.

Drones, Internet of Things (IoT) gadgets, and unmanned aerial vehicles (UAVs) gather vital information using in-built sensors and instantly upload it to the cloud. Data is protected from unauthorised access and disclosure by encrypting it using Pentatope Elliptic Curve Cryptography (PECC) prior to storage. Blockchain technology enhances trust and data governance by guaranteeing immutability, transparency, and tamper resistance.

Distributed architecture is used by the system to improve reliability, fault tolerance, and efficiency. UAV components like sensors, communication modules, and flight controllers work together in this design. Elliptic Curve Diffie-Hellman (ECDH) is used for secure key exchange and communication, while SHA-256 is used for data integrity and blockchain validation.

Unmanned Aerial Vehicles (UAVs) check their Ethereum (ETH) balance, generate and validate blockchain blocks, implement privacy protections, and use ECDH + SHA-256 to secure transactions, as shown in Figure 1, the workflow of the proposed framework. Applications that rely on UAVs benefit greatly from the strong privacy and security afforded by this integrated solution.

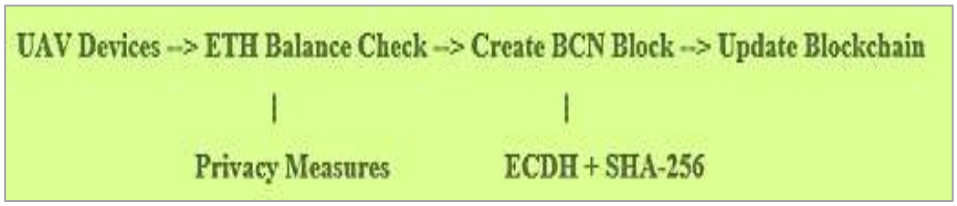


**Figure 1: Workflow of the Proposed Blockchain-Enabled UAV Security Framework**

## IV. Results and Discussion

The primary goal of the proposed system is to oversee, protect, and administer data collected by unmanned aerial vehicle (UAV) systems. The study's proposed BCN architecture ensures the secure storage of sensitive data acquired by UAVs and drones. Data acquired by unmanned aerial vehicles (UAVs) and drones is securely stored using the BCT framework that was proposed in the study.

**Table 1: Performance Evaluation of Preservation in the Proposed Method and Existing Methods**

| Technique Used | Preservation Success Rate (%) |
|---|---|
| Intelligent Omni-Surfaces | 50.0 |
| IFTTT Privacy Mitigation | 65.0 |
| Blockchain Authentication | 70.0 |
| Blockchain-Based UAV Framework | 80.0 |
| ECDH + SHA-256 | 85.0 |

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

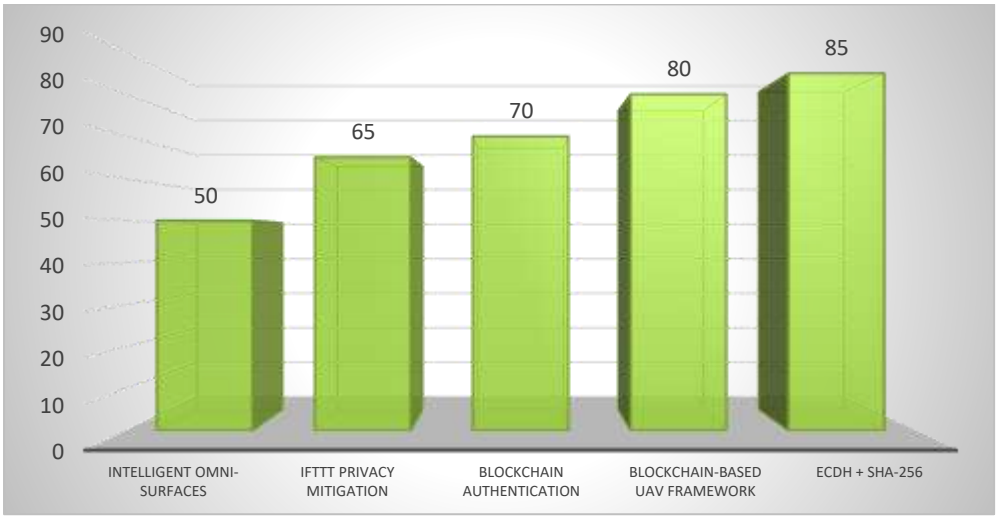


**Figure 2: Performance Evaluation of Preservation in the Proposed Method and Existing Methods**

Data preservation performance is significantly enhanced compared to existing approaches by the suggested strategy, as seen in the table. The success percentage for Intelligent Omni-Surfaces is 50%, IFTTT Privacy Mitigation is 65%, and Blockchain Authentication is 70%. An improved 80% success rate is achieved by the UAV Framework that is based on blockchain technology. With an 85% preservation success rate, the suggested ECDH + SHA-256 method outperforms the state-of-the-art methods in terms of data integrity and security.

**Table 2: Performance Evaluation of Privacy in the Proposed Method and Existing methods**

| Technique | Privacy Success Rate (%) |
|---|---|
| Intelligent Omni-Surfaces | 55 |
| IFTTT Privacy Mitigation | 75 |
| Blockchain Authentication | 78 |
| Blockchain-Based UAV Framework | 88 |
| ECDH + SHA-256 | 92 |

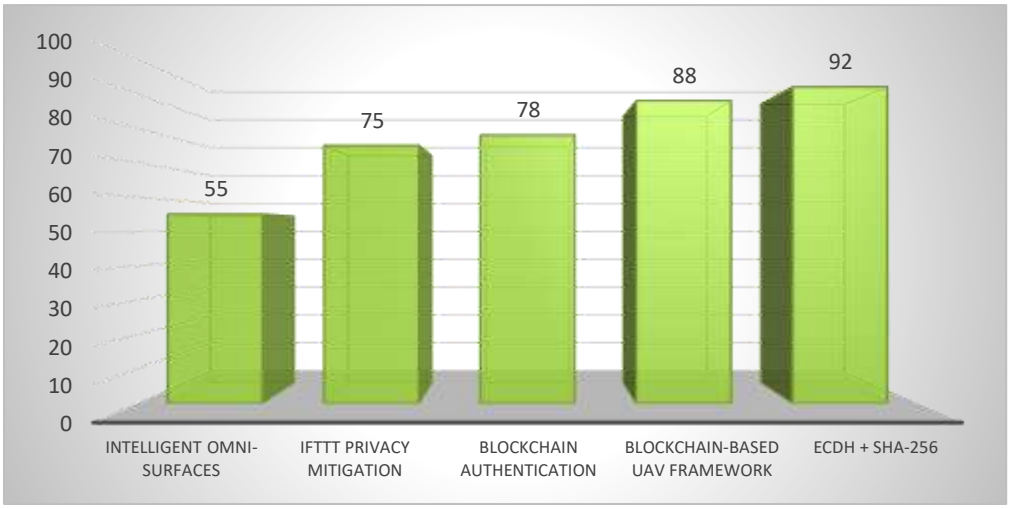


**Figure 3: Performance Evaluation of Privacy in the Proposed Method and Existing Methods**

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

Table 2 shows how the suggested solution stacks up against current privacy protection strategies. While IFTTT Privacy Mitigation offers a significant increase at 75%, Intelligent Omni-Surfaces have the lowest privacy success rate at 55%. As a result of the advantages of decentralised verification, Blockchain Authentication significantly improves privacy performance to 78%. With an impressive 88% success rate, the Blockchain-Based UAV Framework clearly preserves user privacy. With a privacy success rate of 92%, the suggested ECDH + SHA-256 solution proves to be more successful and resilient than any current strategy.

**Table 3: Performance Evaluation of Defend Rate in the Proposed Method and Existing Methods**

| Technique | Defend Rate (%) |
|---|---|
| Intelligent Omni-Surfaces | 40 |
| IFTTT Privacy Mitigation | 50 |
| Blockchain Authentication | 60 |
| Blockchain-Based UAV Framework | 80 |
| ECDH + SHA-256 | 85 |

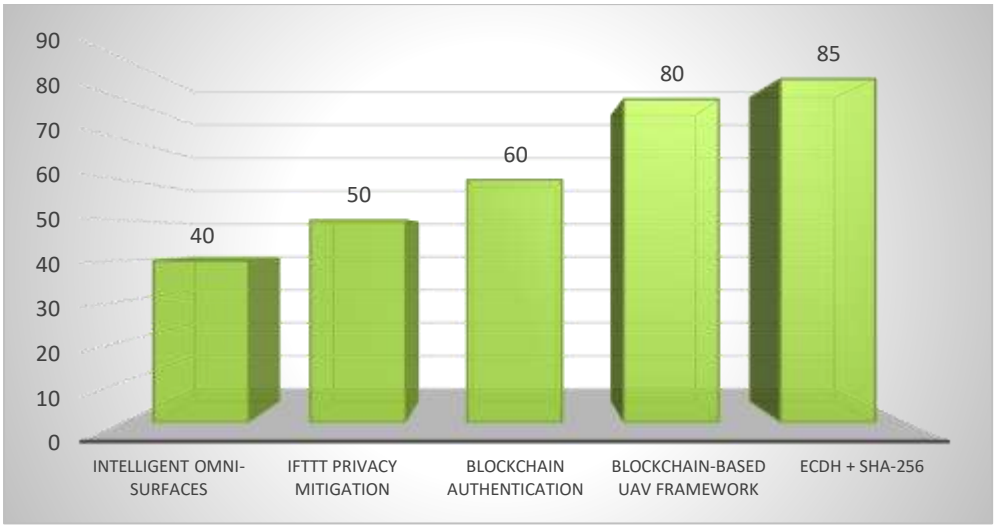


**Figure 4: Performance Evaluation of Defend Rate in the Proposed Method and Existing Methods**

Table 3 shows the results of comparing the suggested methods defend rate performance with those of current strategies. After IFTTT Privacy Mitigation, Intelligent Omni-Surfaces have the second-lowest defend rate at 40%. With blockchain authentication, the defend rate increases to 60%, showing that there is higher resistance to attackers. A far higher protect rate of 80% is achieved by the Blockchain-Based UAV Framework, indicating superior defensive capacity. With an impressive 85% defend rate, the suggested ECDH + SHA-256 approach proves to be the most effective defence for UAV systems against assaults.

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

**Table 4: Performance Evaluation of Attack Rate in the Proposed Method and Existing Methods**

| Technique | Attack Detection Rate (%) |
|---|---|
| Intelligent Omni-Surfaces | 50 |
| IFTTT Privacy Mitigation | 75 |
| Blockchain Authentication | 80 |
| Blockchain-Based UAV Framework | 85 |
| ECDH + SHA-256 | 90 |

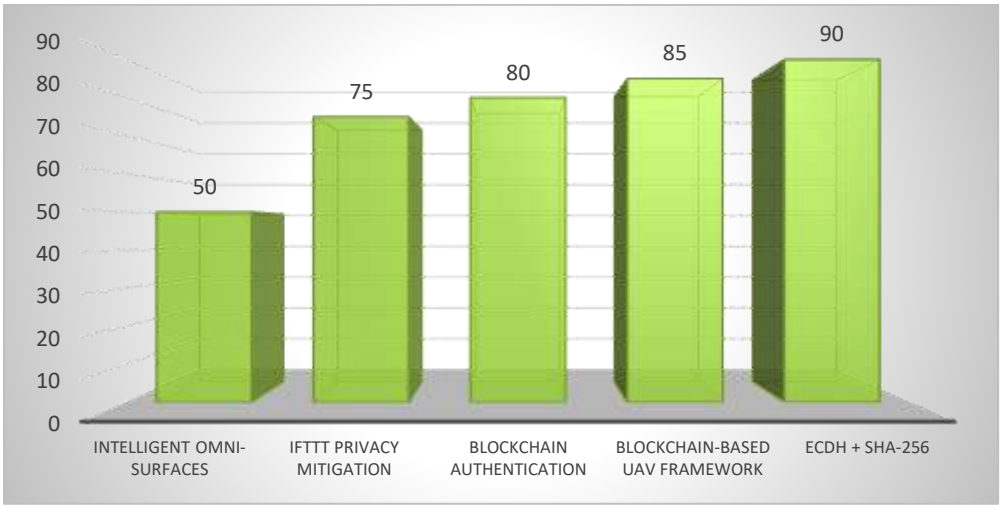


**Figure 5: Performance Evaluation of Attack Rate in the Proposed Method and Existing Methods**

Table 4 shows how well the suggested method detects attacks compared to other methods that are already in use. With a rate of only 50%, Intelligent Omni-Surfaces are the least successful at detecting assaults. The detection performance is improved to 75% with IFTTT Privacy Mitigation and even further to 80% with Blockchain Authentication. With an improved detection rate of 85%, the Blockchain-Based UAV Framework demonstrates its superior capacity to identify attacks. The higher efficiency of the suggested ECDH + SHA-256 approach in identifying and mitigating security risks in UAV systems is demonstrated by its maximum attack detection rate of 90%.

## V. Conclusion

When compared to older, more insecure methods of centralising data storage, the proposed blockchain-enabled UAV security architecture is light years ahead. The framework safeguards data integrity, privacy, and tamper resistance by integrating PECC encryption, ECDH-based secure communication, SHA-256 hashing, and blockchain technology. The suggested technique is more resilient against possible dangers than existing systems, as shown by comparative performance analysis, which shows that it outperforms existing methods in data preservation, privacy protection, defensive capabilities, and attack detection. Improved fault tolerance, reliability, and cooperative functioning of UAV components are other benefits of using a distributed cloud-based design.

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

## References

1. M. Alqarni, "Secure UAV adhoc network with blockchain technology," *PLOS ONE*, vol. 19, no. 5, pp. 1–16, 2024.
2. V. Kumar, "A Blockchain-Based Solution for Securing UAV Communication," *Advances in Nonlinear Variational Inequalities*, vol. 28, no. 3s, pp. 189–198, 2024.
3. A. Aljumah, T. Ahanger, and I. Ullah, "Heterogeneous Blockchain-Based Secure Framework for UAV Data," *Mathematics*, vol. 11, no. 6, pp. 1–14, 2023.
4. A. Aldaej, T. Ahanger, and I. Ullah, "Blockchain-Enabled M2M Communications for UAV-Assisted Data Transmission," *Mathematics*, vol. 11, no. 10, pp. 1–17, 2023.
5. S. Rawat, Y. Alotaibi, N. Malsa, and V. Gupta, "Enhancement of UAV Data Security and Privacy Via Ethereum Blockchain Technology," *Computers, Materials & Continua*, vol. 76, no. 2, pp. 1797–1815, 2023.
6. R. Gupta, A. Nair, S. Tanwar, and N. Kumar, "Blockchain-assisted Secure UAV Communication in 6G Environment: Architecture, Opportunities, and Challenges," *IET Communications*, vol. 15, no. 2, pp. 1352–1367, 2021.
7. P. Álvares, L. Silva, and N. Magaia, "Blockchain-Based Solutions for UAV-Assisted Connected Vehicle Networks in Smart Cities: A Review, Open Issues, and Future Perspectives," *Telecom*, vol. 2, no. 1, pp. 108–140, 2021.
8. Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and privacy issues of UAV: A survey," *Mobile Networks and Applications*, vol. 25, no. 1, pp. 95–101, 2020.
9. B. Li, Z. Fei, Y. Zhang, and M. Guizani, "Secure UAV communication networks over 5G," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 114–120, 2019.
10. D. He, S. Chan, and M. Guizani, "Drone-assisted public safety networks: The security aspect," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 218–223, 2017.