Enhancing Data Security in IOT-based UAV Networks through Blockchain Integration

Vinod Kumar
Computer Science & Engineering, SGT University, Gurugram, India
vksmec@gmail.com (corresponding author)

Amit Asthana
Computer Science & Engineering, SGT University, Gurugram, India
amitasthana_feat@sgtuniversity.org

Gaurav Tripathi
M (SRS), Bharat Electronics Limited, Gurugram, India
gaurav.tripathy@gov.in

Received: 12 December 2024 | Revised: 11 January 2025 and 19 January 2025 | Accepted: 24 January 2025

 DOI: https://doi.org/10.48084/etasr.9922

ABSTRACT

There is great potential for utilizing Unmanned Aerial Vehicle (UAV) networks for commercial, military, and civil purposes. Therefore, as network volumes increase, communicating within UAV networks poses serious cybersecurity issues. Integrating Blockchain with UAV communication networks can offer a scalable and secure communication method. The proposed approach to a protected and accessible interaction method for peer-to-peer UAV networks integrates blockchain technology, allowing safe, decentralized, and cooperative communication between several entities. This study presents a new consensus-building technique to protect UAV network communications, integrating public key cryptography with blockchain Elliptic Curve Diffie-Hellman (ECDH) using the Secure Hash Algorithm (SHA) to preserve data integrity and secure key exchange to provide confidentiality.

Keywords-Internet of Things (IoT); UAV; blockchain; blockchain-enabled UAVs

I. INTRODUCTION

The ability of UAV networks to carry out hazardous and difficult tasks, including land surveying, traffic surveillance, shoreline monitoring, and search and rescue operations, has garnered a lot of interest in recent years. [1]. UAV communication is an innovative mode of Mobile Ad-hoc Network (MANET) where drones operate as nodes and accelerate the retransmission of communication to their definitive targets. This technology, after its military attention, has recently started to attract interest in civilian applications [2]. As the use of UAV networks continues to expand, UAVs are increasingly vulnerable to intrusions [3]. Therefore, ensuring the security of UAV communications is crucial, particularly during missions of greatest significance [4]. However, it is crucial to keep in mind that modern drone and UAV systems that integrate several communications have an excessive need to be sufficiently protected to be utilized in a variety of human life sectors [5]. Figure 1 depicts the risk estimation process for drones or UAVs [6]. Three crucial factors that must be considered for data protection are confidentiality, integrity, and availability. Threat analysis, unauthorized access, and environmental issues are also used in the risk assessment process. Data security concerns with drones and UAVs are similar to those with traditional airplanes [7]. Various communication solutions have been proposed to mitigate the risks in network procedures [8]. Cryptology-based methods have been recognized by investigators as feasible risk reduction strategies, especially regarding drones or UAVs [9, 10].

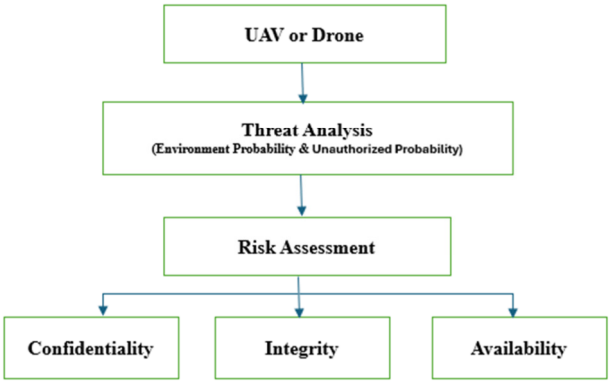

Fig. 1. Flow of risk assessment.

- Confidentiality relates to protecting private data that the UAV gathers or sends from unauthorized access.
- Integrity entails ensuring the accuracy and unaltered nature of the data collected by the UAV.
- Availability entails ensuring that the UAV remains operational and accessible for its intended uses.

Based on these factors, some noteworthy contributions are:

- This study suggests a blockchain-based method for safe communication among UAVs.
- The proposed method addresses important security aspects, such as Confidentiality, Integrity, and Availability (CIA), by incorporating suitable preventive measures.
- The Elliptic Curve Diffie-Hellman (ECDH) technique is applied to protect data stored in the cloud.
- SHA-256 is commonly used in generating digital signatures.

In [11], the focus was on describing the particular security issues related to drone use in civilian applications. This study addressed several risks, difficulties, and gaps in scientific understanding related to the application of this technology. In [12], potential difficult problems with UAVs were discussed, suggesting solutions to protect data privacy. This study emphasized the use of Identity-Based Encryption (IBE) and low-tech cryptographic approaches to achieve anonymity. Attackers can trigger distributed or denial-of-service, ciphertext, and plaintext attacks. In [13], a Blockchain Technology (BCT) structure was proposed to prevent such attacks, but the results were not encouraging. BCT has been used in many recent studies, and Table I lists pertinent ones, illustrating the distinctions between the cryptographic technique, the use of BCT, and the core area of the suggested model.

TABLE I. SUMMARY OF LITERATURE SURVEY

Reference	Blockchain	Cryptography techniques	Primary domain
[11]	Yes	Elliptical Curve Cryptography	Authentication
[14]	Yes	Metaheuristic	Authentication and Confidentiality
[15]	Yes	Federated Learning-Based Technique	Authentication and Confidentiality
[16]	Yes	Elliptical Curve Cryptography	Authentication and Integrity
[17]	Yes	Attribute-Based Encryption	Authentication and Confidentiality
[7]	Yes	Pentatope Elliptic Curve Cryptography	Authentication, Confidentiality, and Integrity
Proposed	Yes	Elliptic Curve Diffie-Hellman	Authentication, Availability, Confidentiality, and Integrity

II. PROPOSED APPROACH

This study investigated a blockchain-integrated approach to reduce risks related to data in UAV and drone systems. UAVs, drones, and IoT devices through sensors allow handlers to achieve a variety of preset goals. Drones and UAVs are controlled using network link systems [18]. Blockchain-based solutions can reduce the hazards associated with drone and UAV systems' data. With special qualities, including immutability, security, transparency, tamper-proofing, and effective distribution methods, this approach specifically seeks to increase data integrity and privacy aspects. Depending on the application, UAVs, drones, and IoT devices typically have a variety of sensors that enable them to perform different functions.

A wireless communications network and a drone platform are used to collect information [7]. Cloud technology is used to store encrypted data created using the Pentatope ECC technique (PECC) [6]. In [19], it was stated that the hash value generated using SHA can be used to assess the accuracy of the data before it is properly recorded on the blockchain. Several obstacles are present in using BCT, including expensive processing expenses and extreme power utilization. Every time it notices an odd activity, the system records the event and issues a security alert.

The proposed method uses ECDH to protect cloud data. Figure 2 shows a state diagram for the BCT-aided proposed architecture. The key elements of the framework include:

- UAV devices: Commonly referred to as IoT gadgets or drones.
- Cloud server: Acts as the central hub for data processing.
- Verification module: Ensures energy and gas balance to validate or reject blockchain transactions.
- Blockchain: Comprises multiple blocks (Block 0, Block 1, …, Block *n*) linked together.
- Smart contracts: Facilitate automated transactions based on predefined conditions.
- Digital signatures: Ensure the authenticity and integrity of transactions.

EthGas is a cryptocurrency that contributes to the development of the BCT ecosystem. An ECDH-based digital signature is utilized to validate all the data acknowledged from aerial devices. Figure 2 displays a flowchart for monitoring every distinct transaction in a BCT block. The data status is tracked and validated through the cloud networks. Smart contacts and digital signatures are also employed to enhance data security.

A. Proposed Algorithm

This section outlines the proposed algorithm for the UAV block transaction protocol.

```
Algorithm 1: Proposed UAV Block
Transaction
while there are n UAVs:
  if the Ethereum balance of the UAV >
```

```
  a defined threshold value:
    Permit UAV to create a BCN Block.
    Modify the ETH balance of the UAV.
  else
    the block operation is not formed
  End if
End while

// To Ensure UAV data privacy and
// preservation.
while there are n UAVs :
  If the block transaction for Device[i]
  is formed:
    Execute ECDH on the data of
    Device[i].
    Add the SHA-256 hash of the updated
    ETH-balance to the block.
  End if
End while
```

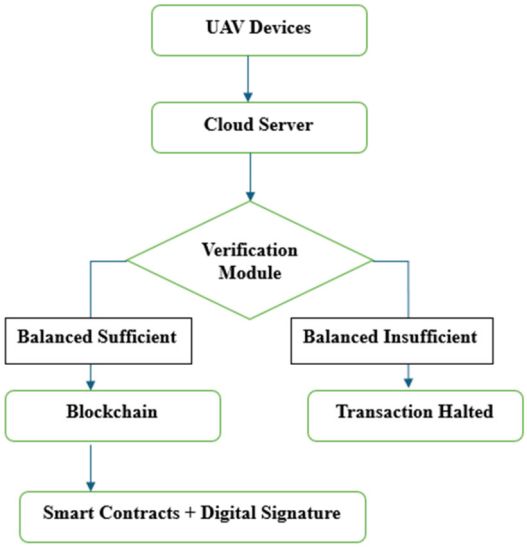

Fig. 2. State diagram for the Blockchain-aided proposed architecture.

B. Workflow

The workflow in Figure 3 demonstrates a secure process for UAV communication and blockchain integration.

1) Device Registration

- UAVs register in the network with initial ETH balances.
- Threshold check.
- Continuously monitor UAV ETH balances.

2) Block Creation

- If eligible, create BCN blocks.
- Encryption and hashing:

  Secure data with ECDH:

  $(a * G) * b = (b * G) * a$

  If two parties have their own secret numbers, a and b (private keys), and an elliptic curve defined with a generator point G, they can exchange their public keys, $(a * G)$ and $(b * G)$, over an unsafe channel. Utilizing public keys, they can then calculate a shared secret:

  $secret = (a * G) * b = (b * G) * a$

  Then hash is balanced using SHA-256.

3) Ledger Update

- Add the BCN block to the blockchain.

4) Privacy Assurance

- Encrypt and secure data for ineligible UAVs

Fig. 3. Workflow diagram for the Blockchain-aided proposed model.

III. RESULTS AND ANALYSIS

The proposed approach was tested on a Rinkeby Ethereum network to evaluate its effectiveness in UAV device validation. Rinkeby provides a thorough development ID to SC compiling and execution platform, facilitating the prototype procedure for blockchain-assisted schemes. Specifically, Remix configuration with compiler version 0.8.7. com mit.228d28d was used. ETH gas cost analysis was used during the solidity SC code, implemented on a configured Remix setup. ETH gas price represents the cost of running an Ethereum blockchain. The system was tested on an Ubuntu 18.04 LTS, Intel Core i5-1135G7 processor at 2.40GHz 1.38 GHz, and 16 GB RAM, and a Raspberry PI 4 Model B, Quad-Core ARM Cortex-A72 at 1.5 GHz, and 16 GB RAM.

The primary objective of the proposed system is to monitor, protect, and handle data collected via UAV or drone systems. The proposed BCN architecture permits for cautious and protected storage of restricted data assembled using UAVs and drones. Confidential data collected by drones and UAVs are kept in an efficient storage system using the proposed BCT architecture, ensuring security and privacy. Figure 4 demonstrates the strong focus of the proposed system regarding preservation, attack rate, privacy, and defend rates.

The reliability of the proposed approach was confirmed through experiments that covered data sizes from 1 KB to 1 GB. The fault-resistant BCN operates through SHA-generated hash values for protection against attacks that could potentially affect data integrity. The hash values of block-stored data drive the BCN technique instead of direct storage because this method ensures transparent transaction tracking and prevents plaintext and ciphertext attacks. Table I shows system functionality measurements.

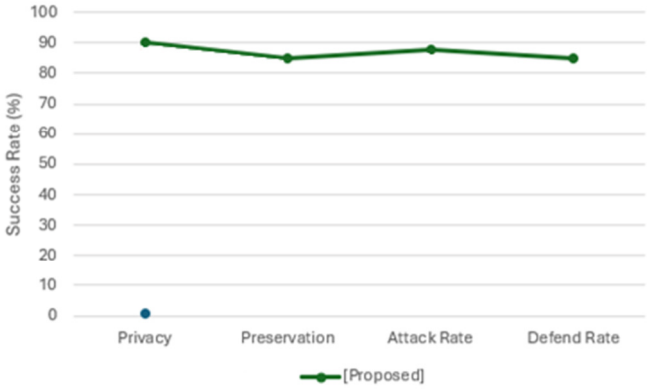

Fig. 4. Performance evaluation of the proposed system based on preservation, privacy, attack rate, and defend rate attributes.

TABLE II. COMPARISON OF LATENCY AND PROCESSING TIME

Functions	Latency time (s)	Processing time (s)
Left()	4.16	37
Right()	4.06	5
Straight()	5.24	29

The findings validate the proposed method, demonstrating how blockchain abilities such as transparency, distribution, immutability, and security reduce attack rates. Particular attention is paid to attack rates and privacy and preservation aspects. When considering additional evaluation measurements, such as response time, latency, and data computation time, the importance of the proposed paradigm is further reinforced. Latency is the time required to process and store an IoT request in a blockchain ledger. The response time is the time it takes the blockchain database to return the requested data to the IoT device. Latency can accumulate over time, in contrast to response time.

The results show how blockchain properties such as distribution, transparency, immutability, and security affect attack rates and confirm that the suggested method performs better than the results from traditional approaches. Consequently, compared to the existing techniques, the proposed system has reduced attack rates.

A. Performance Assessment Factors

The proposed approach can provide important security services at an affordable cost. The key benefits of the proposed method are:

- Confidentiality: The confidentiality of UAV communication data is preserved using the ECDH technique, which ensures secure key exchanges.
- Integrity: All messages in the proposed system were encrypted using SHA-256 hashes, which ensure data integrity by detecting any data modifications. Thus, the integrity of the message has been confirmed.
- Availability: Blockchain's decentralized structure ensures the high availability of the network. The system's functionality is maintained by the remaining active nodes, thus even if certain UAVs or nodes fail, the network is up and running and UAV services are not interrupted.
- Authentication: The encrypted transaction confirms the identity of UAVs, and Blockchain offers built-in authentication procedures. Every message in the proposed technique has the sender's digital signature attached to it. To ensure message authentication, an attacker cannot provide a legitimate signature for a modified message.
- Energy efficiency: A node's energy serves as a gauge for the strength and longevity needed to survive in the network. Energy consumption is the communication overhead of nodes when a specific amount of erroneous information is introduced into a network. Numerous energy-efficient routing techniques have been put forth in recent years. Energy-efficient functioning is ensured by optimizing computational operations and balancing ETH usage.
- Throughput: Multiple UAVs can process transactions in parallel, increasing system throughput and facilitating effective block formation and verification management.
- Computational efficiency: Low computational overhead and effective use of resources during block creation and verification.

IV. CONCLUSION

This study presented a blockchain solution for improving security in IoT-based UAV networks since current privacy and security measures are sensitive to these issues. UAV networks are essential in today's applications, including disaster response, delivery, security, and sensing, due to vulnerabilities such as data tampering, intrusion, and single points of failure. Analyzing the literature, this study identified blockchain as a solution due to its attributes, such as decentralization, immutability, and transparency, which are key components to strong UAV communication security. Secure communication channels between UAVs are essential to preserve CIA characteristics in UAV networks in various applications. As the network increases, BCT can provide transparency and security. The study highlights several key advances: consensus algorithms developed especially for UAV needs, ensuring privacy, security, confidentiality, integrity, availability, and low latency. Compared to traditional techniques such as encryption or key management that require centralized control, deficiency or absence of which leads to attacks, blockchain-based solutions offer significantly better attack resilience while avoiding dependence on a single point of control.

This work's critical contribution is the identification and resolution of key knowledge gaps, including the lack of privacy, security, authentication, integrity, scalable, lightweight consensus mechanisms specifically suited for resource-constrained UAVs, and the need for seamless interoperability between IoT devices and blockchain networks. The proposed framework introduces a consensus mechanism that improves security and makes it suitable for UAV deployments. The proposed approach offers the highest level of security and confidentiality using a digital signature to confirm the legitimacy and integrity of every transaction. The model outperforms other models in terms of operational cost (2.85

units), scalability (15.01 units), reliability (96.10%), and stability (82.36%).

Future research could broaden the method to include UAV scalability and local storage security. The hyperledger fabric platform can also be used to develop the system. Additionally, it would be great to broaden the focus of the proposed approach to include other relevant IoT domains outside UAVs.

REFERENCES

[1] A. Islam and S. Y. Shin, "BHMUS: Blockchain Based Secure Outdoor Health Monitoring Scheme Using UAV in Smart City," in *2019 7th International Conference on Information and Communication Technology (ICoICT)*, Kuala Lumpur, Malaysia, Jul. 2019, pp. 1–6, https://doi.org/10.1109/ICoICT.2019.8835373.

[2] A. Kout, B. Bouaita, A. Beghriche, S. Labed, S. Chikhi, and E. B. Bourennane, "A Hybrid Optimization Solution for UAV Network Routing," *Engineering, Technology & Applied Science Research*, vol. 13, no. 2, pp. 10270–10278, Apr. 2023, https://doi.org/10.48084/etasr.5661.

[3] M. R. Manesh and N. Kaabouch, "Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions," *Computers & Security*, vol. 85, pp. 386–401, Aug. 2019, https://doi.org/10.1016/j.cose.2019.05.003.

[4] M. R. Manesh and N. Kaabouch, "Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system," *International Journal of Critical Infrastructure Protection*, vol. 19, pp. 16–31, Dec. 2017, https://doi.org/10.1016/j.ijcip.2017.10.002.

[5] V. Kumar, A. Asthana, and G. Tripathi, "A Systematic Literature Review of Blockchain-Assisted UAV Communication Systems," in *2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON)*, New Delhi, India, Nov. 2024, pp. 1–9, https://doi.org/10.1109/DELCON64804.2024.10866634.

[6] C. Rupa, G. Srivastava, T. Reddy Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "Security and privacy of UAV data using blockchain technology," *Journal of Information Security and Applications*, vol. 55, Dec. 2020, Art. no. 102670, https://doi.org/10.1016/j.jisa.2020.102670.

[7] A. Aljumah, T. A. Ahanger, and I. Ullah, "Heterogeneous Blockchain-Based Secure Framework for UAV Data," *Mathematics*, vol. 11, no. 6, Jan. 2023, Art. no. 1348, https://doi.org/10.3390/math11061348.

[8] M. A. Akhloufi, A. Couturier, and N. A. Castro, "Unmanned Aerial Vehicles for Wildland Fires: Sensing, Perception, Cooperation and Assistance," *Drones*, vol. 5, no. 1, Mar. 2021, Art. no. 15, https://doi.org/10.3390/drones5010015.

[9] W. Lee, J. Y. Lee, H. Joo, and H. Kim, "An MPTCP-Based Transmission Scheme for Improving the Control Stability of Unmanned Aerial Vehicles," *Sensors*, vol. 21, no. 8, Jan. 2021, Art. no. 2791, https://doi.org/10.3390/s21082791.

[10] Q. Wu *et al.*, "A Comprehensive Overview on 5G-and-Beyond Networks With UAVs: From Communications to Sensing and Intelligence," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 10, pp. 2912–2945, Jul. 2021, https://doi.org/10.1109/JSAC.2021.3088681.

[11] B. Nassi, R. Bitton, R. Masuoka, A. Shabtai, and Y. Elovici, "SoK: Security and Privacy in the Age of Commercial Drones," in *2021 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, May 2021, pp. 1434–1451, https://doi.org/10.1109/SP40001.2021.00005.

[12] H. R. Hasan and K. Salah, "Proof of Delivery of Digital Assets Using Blockchain and Smart Contracts," *IEEE Access*, vol. 6, pp. 65439–65448, 2018, https://doi.org/10.1109/ACCESS.2018.2876971.

[13] N. Deepa *et al.*, "A survey on blockchain for big data: Approaches, opportunities, and future directions," *Future Generation Computer Systems*, vol. 131, pp. 209–226, Jun. 2022, https://doi.org/10.1016/j.future.2022.01.017.

[14] A. A. Khan *et al.*, "A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment," *Computers and Electrical Engineering*, vol. 102, Sep. 2022, Art. no. 108234, https://doi.org/10.1016/j.compeleceng.2022.108234.

[15] A. Islam, A. Al Amin, and S. Y. Shin, "FBI: A Federated Learning-Based Blockchain-Embedded Data Accumulation Scheme Using Drones for Internet of Things," *IEEE Wireless Communications Letters*, vol. 11, no. 5, pp. 972–976, Feb. 2022, https://doi.org/10.1109/LWC.2022.3151873.

[16] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and M. Alazab, "Blockchain-Envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled Internet of Drones Environment," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9097–9111, Dec. 2020, https://doi.org/10.1109/TVT.2020.3000576.

[17] C. Feng *et al.*, "Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach," *IEEE Network*, vol. 35, no. 1, pp. 130–137, Jan. 2021, https://doi.org/10.1109/MNET.011.2000223.

[18] M. Gupta and S. Varma, "Optimal placement of UAVs of an aerial mesh network in an emergency situation," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 343–358, Jan. 2021, https://doi.org/10.1007/s12652-020-01976-2.

[19] A. M. Benaya, M. H. Ismail, A. S. Ibrahim, and A. A. Salem, "Physical Layer Security Enhancement via Intelligent Omni-Surfaces and UAV-Friendly Jamming," *IEEE Access*, vol. 11, pp. 2531–2544, 2023, https://doi.org/10.1109/ACCESS.2023.3233947.

[20] N. Choi and H. Kim, "A Blockchain-based User Authentication Model Using MetaMask," *Journal of Internet Computing and Services*, vol. 20, no. 6, pp. 119–127, 2019, https://doi.org/10.7472/jksii.2019.20.6.119.