Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 3s (2025)

Blockchain-Aided Secure Communication Framework Intended for UAV Networks

Mr. Vinod Kumar[1], Dr. Amit Asthana[2], Dr. Gaurav Tripathi[3]
[1]Computer Science & Engineering, SGT University, Gurugram, India. vksmec@gmail.com
[2]Computer Science & Engineering, SGT University, Gurugram, India. amitasthana_feat@sgtuniversity.org
[3]M (SRS) Bharat Electronics Limited, Gurugram, India.gaurav.tripathy@gov.in

Article History:

Received: *26-09-2024*

Revised: *02-11-2024*

Accepted: *17-11-2024*

Abstract:

Networks of Unmanned Aerial Vehicles (UAVs) have a lot of promise for use in commercial, military, and civil applications. The communication of UAV networks presents significant cybersecurity challenges as network sizes increase. Including blockchain technology in peer-to-peer UAV networks is one way to offer a safe, scalable communication method. Blockchain enables safe, decentralized, and collaborative communication between several entities. To increase the security and privacy of UAV network communication, this article proposes a method based on Blockchain Technology (BCT). The proposed model employs Elliptic Curve Diffie-Hellman (ECDH) to ensure confidentiality through secure key exchange and utilizes the Secure Hash algorithm (SHA) to maintain data integrity. The cloud platform is used to store technical data, integrity, authentication, availability, and confidentiality. The data is then stored on a public blockchain based on Ethereum to enable seamless BCT transactions. The suggested approach improves in defending private information against a variety of threats, including plaintext and ciphertext attacks.

Keywords: UAV, Blockchain, Blockchain-enabled UAVs, Internet of things.

1. Introduction

In recent years, UAV networks have drawn a lot of attention due to their potential to perform complex and dangerous jobs like land surveying, traffic surveillance, coastline monitoring, and search and rescue missions [1]. These unmanned aerial vehicles are more susceptible to cyberattacks as the use of UAV networks keeps growing [2]. Therefore, it is essential to guarantee the security of UAV communications, especially during missions that are of utmost importance [3]. However, it is important to remember that to be used in a range of human life sectors, contemporary drone and UAV systems which incorporate a variety of networking technologies and have a high utilization percentage must be adequately safeguarded [4]. Figure 1 shows the flow of risk estimation for drones or UAVs [5]. Specifically, availability, confidentiality, and integrity are three important aspects that need to be considered for data protection. The risk evaluation is also carried out using environmental considerations, threat analysis, and illegal access. Drone and UAV data security issues are like those of conventional aircraft [6]. To reduce the hazards that network protocols present, several communication strategies have been proposed

[7]. Investigators have recognized cryptology-based solutions as feasible risk minimization schemes, particularly regarding drones or UAVs [8,9].

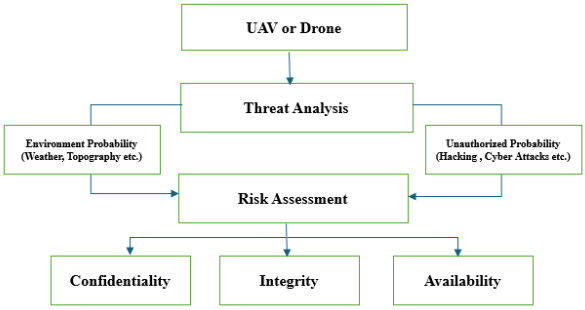


FIGURE 1. Risk Assessment Flow.

The key elements of the risk assessment model are outlined below:

- **UAV/Drone:** The initial point of reference for this risk analysis is drones, which are depicted by pictures of quadcopters.
- **Threat Analysis:** A threat analysis is carried out following the identification of the UAVs. The icons, which might stand for digital or physical threats, imply that possible risks like environmental hazards, hacking, or illegal access may be included in the study.
- **Environmental Probability:** This appears to indicate the possibility that the UAV will be impacted by environmental elements (such as weather, topography, or other external circumstances).
- **Unauthorized Probability:** This is the likelihood of unapproved actions, including hacking or unapproved UAV control.
- **Risk Assessment:** The gauge-style icon shows that an overall risk assessment is carried out following the consideration of unauthorized and environmental possibilities. This evaluation determines how serious the hazards are.
- **Effect on the Triad of Security:** The evaluation then correlates with the three cybersecurity pillars:
  - **Confidentiality:** This probably has to do with guarding against illegal access to private information that the UAV collects or transmits.
  - **Integrity:** Making certain that the data obtained by the UAV is correct and unaffected.
  - **Availability:** Making certain that the UAV continues to be functional and reachable for its designated purposes.

1.1 Significant Contribution

Some of the significant contributions, based on the above listed aspects, are as follows: The current work proposes a secure UAV communication method based on blockchain.

- When evaluating the risk of UAVs or drones, environmental, meteorological, and geographic factors are considered.
- The current study proposes a blockchain-based approach for secure UAV communication.

- The proposed approach incorporates appropriate preventive strategies to address key security factors, including Confidentiality, Integrity, and Availability (CIA).
- To secure data at cloud storage, the Elliptic Curve Diffie-Hellman (ECDH) algorithm is employed.

1.2 Organization of Paper

The organization of the paper is as follows: Section 2 presents a comprehensive review of the literature. In Section 3 outlines the proposed model and algorithm. Results & analysis are explained in section 4. The paper's conclusion and possible directions for further research are described in Section 5.

2. Review of Literature

Nassi et al.'s study [10] focused on outlining the specific security concerns associated with drone use in society. This investigation addressed several hazards, challenges, and scientific knowledge gaps among items relevant to the use of this type of technology. The Hasan et al. [11] team talked about possible ways to achieve data privacy and potential challenging issues with UAVs. In order to achieve privacy, the study highlights the usage of Identity-Based Encryption (IBE) and low-tech cryptographic techniques. The study claims that erratic social factors may initiate ciphertext, plaintext, and distributed or denial-of-service attacks. By using the suggested structure, BCT can stop these kinds of attacks, according to Deepa et al. [12]. However, the results haven't been promising.

Numerous recent studies have made use of blockchain technology; a list of relevant studies is outlined in Table 1. It demonstrates differences between proposed model's core area, BCT usage, and cryptographic technique.

TABLE 1. Summary of the literature survey

Reference	Blockchain	Methods of Cryptography	Principal Domain
[10]	Yes	Elliptical Curve Cryptography	Authentication
[13]	Yes	Metaheuristic	Authentication and Confidentiality
[14]	Yes	Federated Learning- Based Technique	Authentication and Confidentiality
[6]	Yes	Pentatope Elliptic Curve Cryptography	Authentication, Confidentiality and Integrity
Proposed	Yes	Elliptic Curve Diffie-Hellman	Authentication, Availability Confidentiality and Integrity

3. Proposed Framework

In Present investigate offers a blockchain-based method to reduce the hazards related to data maintenance in drone and UAV systems. Thus, the most recent research indicates that it provides

a blockchain-based method to condense risk of data damage in drone and UAV systems. Sensors on IoT devices, UAVs, and drones allow handlers to achieve a number of predetermined objectives. Drones & UAVs are controlled and observed locally and remotely via network connection systems [15]. According to a recent study, blockchain-based solutions can reduce the risks related to data maintenance in drone and UAV systems. More specifically, this strategy aims to improve data storage and privacy features with unique features including immutability, security, transparency, tamper-proofing, and efficient distribution techniques. Drones, UAVs, and IoT devices usually feature a range of sensors that let them do various tasks, depending on the application [16].

The main blockchain-based data security system for gathering data for the component management of drones and UAVs. A wireless communications network and a drone platform are used to gather information. Wherever real-time encoding is done, they are received by a cloud network. Virtuality Monitored Vehicles (VMVs), UAVs, and drones all gather information in cloud with a primary focus on ensuring security. As an alternative of loading unencrypted information, Cloud is utilized to store encryption information created using pentatope ECC (PECC) technique [17,6].

We put the data from a VC-based application on UAVs through its paces in the study that was presented. The system logs and issues a security alert whenever it detects unusual activity. The authority can give commands to the system and handle the cars' following answers as transactions by using BCT and cloud computing [6]. Benaya et al. [18] states that hash value generated using SHA, It can be used to evaluate accuracy of information before being suitably recorded within the blockchain. There are a number of drawbacks to using BCT, such as expensive computing expenses and excessive power consumption. Every time it notices odd activity, The system records the event and issues a security alert. Using BCT and cloud computing, the authority can command system & manage the subsequent responses as transactions [6].

3.1 Blockchain-Aided UAV Framework

The ECDH is used in the proposed method to safeguard cloud data. Drones and other unmanned aerial vehicles use distributed data connection architecture. The phrase distributed design refers to the way that information is shared among the different drone components in UAVs and drones. Instead of being processed and stored by a single system, the data is divided across multiple units, with each one responsible for a certain task. As an instance, flight control system, communication module, & sensors can all be distinct parts that are connected to each other via a network. It allows all components to process data quickly, which expedites judgement and improves efficiency. In addition, distributed design can improve safety & reliability by minimizing the effect of a single component failure. Even if one unit fails, the drone can still be controlled, and a catastrophic failure can be prevented because the remaining parts will continue to work. If one component fails, the remaining components can still work, allowing the drone to be controlled and preventing a catastrophic failure. All things considered, scattered architecture is a crucial element of recent drone technology that permits improved utility, reliability and performance. Using an anonymous method like BCT is necessary when working with both ground-based and airborne equipment since

protecting the transmitted data is essential. The Figure 2 shows state diagram for the blockchain technology-aided proposed architecture.

The key elements of a comprehensive 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.

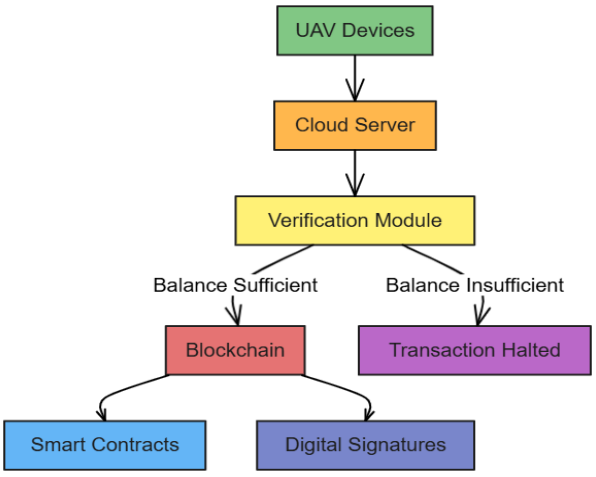


Figure 2. State Diagram for the Blockchain Technology-Aided Proposed Architecture

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

3.2 Workflow Diagram:

In figure 3 workflow demonstrates a secure process for UAV communication and blockchain integration.

UAV Devices → ETH Balance Check: UAVs check their Ethereum (ETH) account balance before proceeding.

ETH Balance Check → Create BCN Block: If the balance is sufficient, a block for the blockchain network (BCN) is created.

Create BCN Block → Update Blockchain: The newly created block is appended to the blockchain.

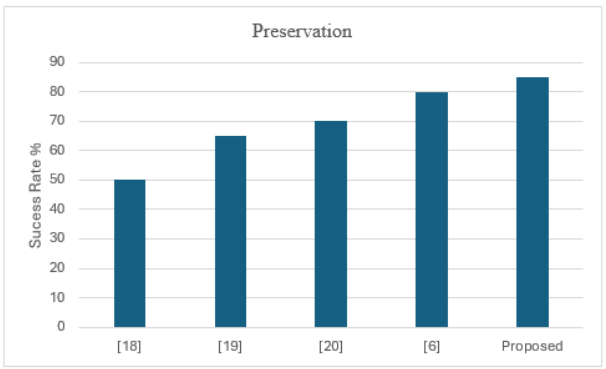
Privacy Measures: Implemented during or after the ETH balance check to ensure communication remains private.

ECDH + SHA-256: ECDH combined with SHA-256 hashing algorithm is used for secure communication and block integrity.

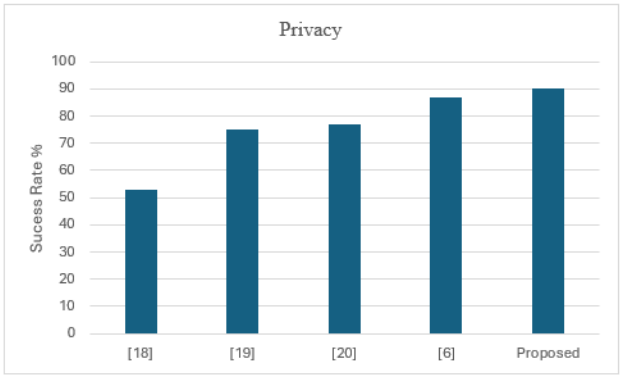
Figure 3. Workflow Diagram for the Blockchain Technology-Aided Proposed Model

4. Results and Analysis

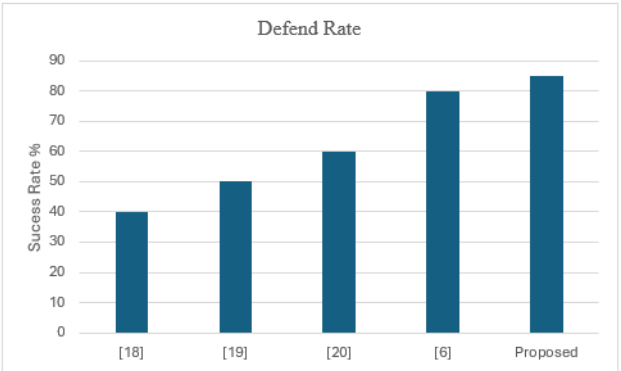
The suggested system's main objective is to monitor, secure, and manage data gathered by drone or UAV systems. Sensitive data collected by drones and UAVs can be safely and securely stored according to the study's recommended BCN architecture. Using the suggested BCT framework in the research, confidential information collected by UAVs and drones is maintained in an effective storage system, guaranteeing privacy and security. Figure 4 compares the strengths of the proposed system with the Conventional state-of-the-art methos regrading privacy, preservation, attack rate and defend effusiveness.



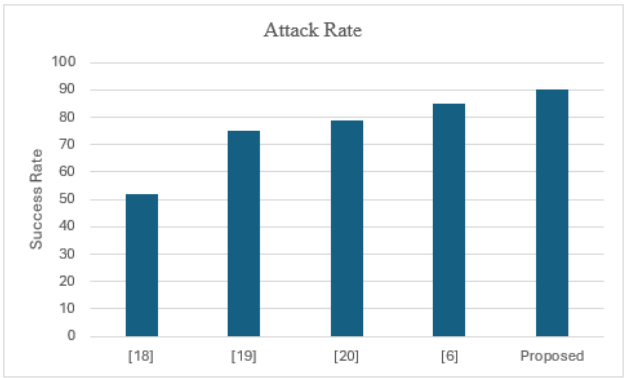
(a) Preservation



(b) Privacy



(c) Defend Rate



(d) Attack Rate

Figure 4. Performance evaluation: (a) Preservation (b) Privacy (c) Defend Rate (d) Attack Rate

As illustrated in Figure 4, the proposed system's preservation, privacy defect frequency and attack frequency are contrasted with those of traditional state-of-the-art methods. Particular attention is paid to the assault rates in the comparisons, with particular attention to the privacy and preservation aspects. By considering additional evaluation metrics like latency, reaction time, and data computation time, the importance of the proposed paradigm is further reinforced. Latency can accumulate over time, in contrast to reaction time. The time it takes to process and store an IoT request in a blockchain ledger is known as latency. The time it takes for the blockchain database to return the requested data to the requesting IoT device is referred to as the response time. It is noteworthy that the non-functional requirements of the system are given equal weight in the proposed framework. Operating cost, cloud infrastructure scalability, application scalability, and fault tolerance rate are among the system performance metrics that have been carefully examined.

The results show how blockchain properties like immutability, transparency, distribution, 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. However, several limitations still exist that make complete BCN implementation challenging. One disadvantage is that backup maintenance features are scandalously hard to implement in a blockchain context, and reversal processes cannot be integrated into the BCN ecosystem. Developers have started using cloud as a user interface instead of a database for user-app interaction designed to overcome this limitation.

5. Conclusion

As the use of UAV networks in a variety of applications increases, secure communication routes between UAVs are crucial to maintaining Confidentiality, Integrity, and Availability (CIA) attributes. Blockchain technology can offer security and transparency as the network expands.

Blockchain technology is being used in the current study to address privacy and preservation issues with UAV data. The current study specifically focuses on utilizing ECDH cryptography in conjunction with the blockchain technology to ensure data security and confidentiality during communication. The suggested method uses a digital signature to verify the integrity and validity of each transaction to provide the maximum level of security and confidentiality. In future studies, methodology may be expanded to incorporate local storage security for UAVs. The battery efficiency of UAV is another topic that might be looked at in the future.

References

[1] Anik, and S. Y. Shin, “Bhmus: Blockchain Based Secure Outdoor Health Monitoring Scheme Using UAV in Smart City,” International Conference on Information and Communication Technology (ICoICT), pp. 1-6. 2019.

[2] Manesh, Mohsen Riahi, and Naima Kaabouch. "Cyber Attacks on Unmanned Aerial System Networks: Detection, Countermeasure, and Future Research Directions." Computers & Security (2019).

[3] Manesh, Mohsen Riahi, and Naima Kaabouch. "Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system." International Journal of Critical Infrastructure Protection 19 (2017): 16-31.
[4] Vinod Kumar, Amit Asthana and Saneh Lata Yadav, "A Comprehensive Review on Security Issues in UAV Communication Networks", Journal of Network Security Computer Networks, Vol. 9 No. 3, 2023.
[5] Rupa Ch, Gautam Srivastava, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, Sweta Bhattacharya, Security and privacy of UAV data using blockchain technology, Journal of Information Security and Applications, Volume 55, 2020, 102670, ISSN 2214-2126.
[6] Abdullah Aljumah, Tariq Ahamed Ahanger, Imdad Ullah, " Heterogeneous Blockchain-Based Secure Framework for UAV Data", Analytical Frameworks and Methods for Cybersecurity, Mathematics 2023, 11(6), 1348
[7] Akhloufi, M.A.; Couturier, A.; Castro, N.A. Unmanned aerial vehicles for wildland fires: Sensing, perception, cooperation and assistance. Drones 2021, 5, 15.
[8] Lee, W.; Lee, J.Y.; Joo, H.; Kim, H. An MPTCP-Based Transmission Scheme for Improving the Control Stability of Unmanned Aerial Vehicles. Sensors 2021, 21, 2791.
[9] Wu, Q.; Xu, J.; Zeng, Y.; Ng, D.W.K.; Al-Dhahir, N.; Schober, R.; Swindlehurst, A.L. A comprehensive overview on 5G-and-beyond networks with UAVs: From communications to sensing and intelligence. IEEE J. Sel. Areas Commun. 2021, 39, 2912–2945.
[10] Nassi, B.; Bitton, R.; Masuoka, R.; Shabtai, A.; Elovici, Y. SoK: Security and privacy in the age of commercial drones. In Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP), Online, 24–27 May 2021; pp. 1434–1451.
[11] Hasan, H.R.; Salah, K. Proof of Delivery of Digital Assets Using Blockchain and Smart Contracts. IEEE Access 2018, 6, 65439–65448.
[12] Deepa, N.; Pham, Q.V.; Nguyen, D.C.; Bhattacharya, S.; Prabadevi, B.; Gadekallu, T.R.; Maddikunta, P.K.R.; Fang, F.; Pathirana, P.N. A survey on blockchain for big data: approaches, opportunities, and future directions. arXiv 2022, arXiv:2009.00858.
[13] Khan, A.A.; Laghari, A.A.; Gadekallu, T.R.; Shaikh, Z.A.; Javed, A.R.; Rashid, M.; Estrela, V.V.; Mikhaylov, A. A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment. Computers & Electrical Engineering. 2022, 102, 108234.
[14] Islam, A.; Al Amin, A.; Shin, S.Y. FBI: A federated learning-based blockchain-embedded data accumulation scheme using drones for Internet of Things. IEEE Wireless Communications Letters. 2022, 11, 972–976.
[15] Gupta, M.; Varma, S. Optimal placement of UAVs of an aerial mesh network in an emergency situation. J. Ambient. Intell. Humaniz. Comput. 2021, 12, 343–358.
[16] Vinod Kumar, Dr. Amit Asthana, Dr. Gaurav Tripathi, "Blockchain-Based Secure Communication Approach for UAV Networks", International Conference on Recent Advancements in Communication, Computing and Artificial Intelligence, 2024

[17]Ch, R.; Srivastava, G.; Gadekallu, T.R.; Maddikunta, P.K.R.; Bhattacharya, S. Security and privacy of UAV data using blockchain technology. J. Inf. Secur. Appl. 2020, 55, 102670.
[18]Benaya, A.; Ismail, M.H.; Ibrahim, A.S.; Salem, A.A. Physical Layer Security Enhancement via Intelligent Omni-Surfaces and UAV-Friendly Jamming. IEEE Access 2023, 11, 2531–2544.
[19]Xu,R.; Zeng, Q.; Zhu, L.; Chi, H.; Du, X.; Guizani, M. Privacy leakage in smart homes and its mitigation: IFTTT as a case study. IEEE Access 2019, 7, 63457–63471.
[20]Choi, N.; Kim, H. A Blockchain-based user authentication model using MetaMask. Journal of Internet Computing and Services, 2019, 20, 119–127.