Advances in Nonlinear Variational Inequalities
ISSN: 1092-910X
Vol 28 No. 3s (2025)

A Blockchain-Based Solution for Securing UAV Communication

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: *30-09-2024*

Revised: *21-11-2024*

Accepted: *30-11-2024*

Abstract:

Unmanned Aerial Vehicles (UAVs) are increasingly being deployed across diverse applications, such as logistics, agriculture, surveillance, and disaster management. However, their reliance on secure and efficient communication networks exposes them to various cybersecurity threats. Blockchain technology (BCT), with its decentralized, immutable, and transparent nature, offers promising solutions to mitigate these vulnerabilities. This paper examines UAV communication networks and addressing the role of blockchain in UAV communication, addressing key security challenges and proposing a novel consensus-building mechanism to enhance the protection of UAV networks. Furthermore, analysis the result of proposed approach with existing models on the basis of privacy, security, attack rates and reliability to establish robust and secure UAV communication system through blockchain-based approach. Thus, the suggested methodology aids in safeguarding data against ciphertext attacks and plaintext attacks. The outcomes validate the effectiveness and security features of the suggested method when contrasted with the state-of-the-art.

Keywords: Blockchain, UAV, Blockchain-Aided UAVs, Security and Privacy.

1. Introduction

As more people take to the sky in the twenty-first century, UAVs, also referred to as drones, have developed significantly. Future smart cities will incorporate this technology due to its substantial advantages for both commercial and civil applications, including package delivery and hostage rescue. because of its streamlined appearance and adaptable mobility. Agriculture, the military, healthcare, monitoring, and surveillance are just a few of the numerous industries that use UAVs extensively. Communication networks that facilitate the control and data sharing of UAVs are essential to their efficient operation. These networks need to handle several security concerns to guarantee the reliable and safe operation of UAVs. It looks at the risks and vulnerabilities of UAV technology because there aren't sufficient trustworthy security solutions.

UAV technology is advancing quickly, and because of their great mobility, they can work together to accomplish a wide range of jobs. UAVs can be employed for military and commercial surveillance. They could also be used in civil applications such as search and rescue operations, which need a lot of

UAVs to send video streams and collect positional data. But in recent years, malicious UAV use has started to increase. These attacks, which can have catastrophic consequences, have become more frequent in recent years [1]. As a result, the pertinent sectors and standards organizations are looking into ways to safeguard UAV networks and systems [2].

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 communication technique and should be sufficiently protected since they have a high employment rate [3].

During UAV communications, it is crucial to make sure that no malevolent party can obstruct data flow. Now, the UAV is attacked by several technicians and has various vulnerabilities. One of the most potential approaches to enhancing user privacy and data security in interconnected networks of UAVis recently developed blockchain technology. Several things can be communicated in a safe, decentralized and fair way by using the blockchain. Distributed ledgers, consensus algorithms, and cryptography are all combined in blockchain technology to produce a trustworthy and decentralized platform. a blockchain-based security architecture that enhances UAV communications by combining smart contracts and cryptographic techniques.

Based on the aforementioned factors, a few noteworthy contributions are as follows:

- A comprehensive exploration of UAV communication networks, role of blockchain technology in UAVs communication is presented.
- The primary data security and privacy to UAV communication networks.
- The current approach suggests a blockchain-based method for safe communication amongst UAVs communication.

The paper is structured as follows: Section 2 described UAV communication and BCT. In section 3 presented data security and privacy in UAV network. Section 4 described the proposed approach. An explanation of the result analysis and presents the performance assessment factors explained in section 5, followed by conclusion and potential avenues for future investigation.

2. Background

2.1 Unmanned Aerial Vehicle

UAVs operate remotely through ground control systems (GCS), also referred to as ground cockpits or drones, and can function autonomously using systems like autopilot, eliminating the need for human intervention. Primarily, UAVs were initially designed for military and surveillance applications, but quick exploration and innovation lowered expense of producing UAVs. Consequently, UAVs technology is finding widespread use in both commercial and non-military domains. Examples of these include weather monitoring, surveillance, delivery services, agriculture, rescue, photography, filmmaking, and cutting-edge healthcare [4]. It attaches the airborne node. So, GCS, stationary nodes, infrastructure and communication networks is essential headed for UAV products. Hence, system possesses the ability to communicate from UAV-to-Ground, UAV-to-UAV, UAV-to-Satellites, and UAV-to-cellular [5,6].

- **UAV-to-Ground Communication:** It refers to exchange of data and commands between an UAV and a GCS or the ground-based infrastructure. This communication typically involves

transmitting telemetry data, such as location, altitude, and system status, from the UAV to the ground, and sending control signals or mission updates from the ground to the UAV.

- **UAV-to-Ground Communication:** IT refers to the exchange of data and information between two or more unmanned aerial vehicles (UAVs). This communication enables UAVs to coordinate their movements, share sensor data, or collaborate on tasks, such as surveillance, mapping, or search and rescue operations
- **UAV-to-Satellite Communication:** It refers to the process of exchanging data and signals between an UAV and a satellite. This communication enables long-range or beyond-line-of-sight (BLOS) operations by acting as a relay between the UAV and ground control systems. It facilitates the transmission of telemetry, imagery, control commands, and other mission-critical data.
- **UAV-to-Cellular Communication:** It refers to the exchange of data and control signals between an UAV and a cellular network. This communication allows UAVs to connect to mobile networks, such as 4G or 5G, to transmit telemetry data, receive control commands, and upload or download other mission-related information. It is particularly useful for operations in urban areas or regions with established cellular infrastructure, enabling real-time, reliable communication over long distances without requiring dedicated radio frequencies.

UAVs have been used for several purposes recently, incorporating remote sensing, mapping, search and rescue, disaster relief, entertainment, and surveillance [7]. By 2025, it's expected that UAVs will become more prevalent and take up an important share of the market [8]. Furthermore, as UAV-assisted wireless networks are broadcast in nature, they are extremely vulnerable to security and privacy lapses such as malware infection, eavesdropping links, replay, impersonation, message injection, spoofing, & distributed denial-of-service (DDOS) attacks. There occur important privacy and security issues with UAV-assisted communication that need to be resolved [9].

2.2 Blockchain Technology

An immutable timestamped block representing each transaction is kept as part of a peer-to-peer electronic money technique called a blockchain. Every block in a blockchain has a hash, or cryptographic reference to the previous block, so seen in figure 1 [10]. Satoshi Nakamoto originally unveiled bitcoin, a cryptocurrency built on a blockchain, in 2008 [11]. Since then, multiple variations of blockchain and cryptocurrencies have been released.

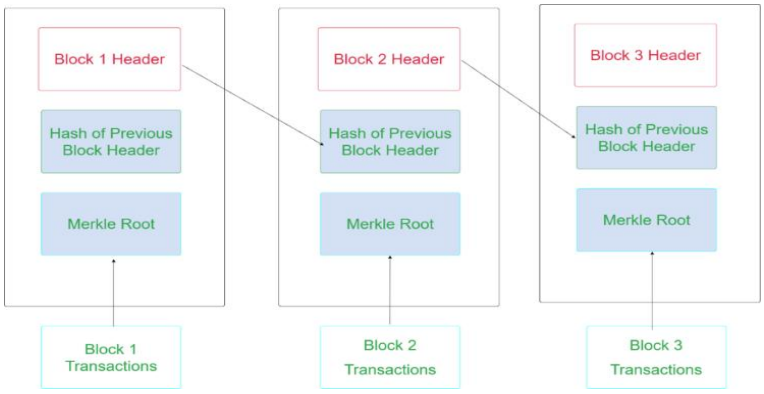

Figure 1: The blockchain structure.

Block-by-block transaction records are maintained on a blockchain, an open, impenetrable ledger. Following transaction verification, In the blockchain, a block becomes unchangeable. Every block connects to the block preceding it using a distinct identifier. Each change made to the data block changes a unique identity that is shared with all users. So, the blockchain network is a strong method of collaborative record keeping since it is hard to interfere with or eradicate. [12,13].

Smart contracts, immutable data, and distributed ledgers are the three main building blocks for BCT. Furthermore, privacy & safety of data are guaranteed by blockchain innovation, fostering trust without the need for outside intervention. Additionally, the blockchain system resists monopolies, enabling every node to withstand the danger of monopoly and take part in decision-making, hence advancing blockchain's democratization [14].

2.3 Blockchain Key Attributes

The core attributes of blockchain technology are:

- **Decentralization:** Nothing like traditional databases controlled through a single entity, blockchain works on a peer-to-peer network. Every applicant has access to the entire database and its complete history.
- **Transparency:** All applicants in the network can examine transactions, but no one can alter them. This transparency fosters confidence between users.
- **Immutability:** When a transaction is recorded on the blockchain, it cannot be modified or removed. This feature confirms integrity & accurateness for data.
- **Security:** Blockchain uses cryptographic procedures to safe information. Every block is connected to previous one through a cryptographic hash, making it nearly impossible to alter without affecting the entire chain.
- **Consensus Mechanisms:** Blockchain networks ensure that all copies of the distributed ledger are similar by using consensus methods as Proof of Work (PoW) or Proof of Stake (PoS) to establish validity of operation.

3. Data Security and Privacy in UAV Network

The UAV business is expanding quickly, and the number of UAV-based products is rising. This development is challenged by various security attacks and constraints that need to be focused secure and secure drone products [15]. Cyberattacks are a major risk to internet-connected UAVs, raising serious concerns about data security and privacy. These threats can be classified into five main classes: confidentiality, integrity, availability, authenticity, and privacy attack [16]. The proportion of attacks gathered from latest surveys is shown in figure 2 [17]. The details of every intrusion are covered in the section that follows. The absence of security precautions for UAVs using national airspace increases the potential of both passive and aggressive attacks.

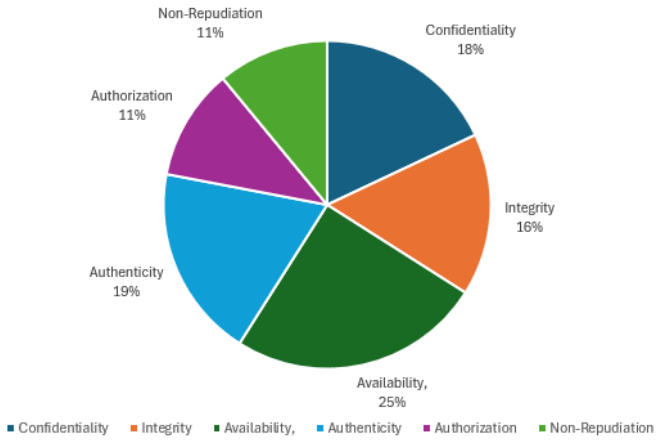

Figure 2: Proportion of different types of attacks on UAV networks.

Due to their nature and the setting in which they are deployed, UAVs are susceptible to a variety of threats. Device-based attacks, Network-based attacks, and Software-based assaults are the three main categories into which these attacks can be divided [18,19].

- **Device-Based Attacks:** It involves having physical access to drone parts, like memory, in order to retrieve private information or grab command of the aircraft.
- **Network-Based Attacks:** It includes attacks like replay, man-in-the-middle, eavesdropping, & alteration, in which a third party intercepts and modifies the data being delivered.
- **Software-Based Attacks:** It means to exploit software vulnerabilities by infecting drones and ground stations with malicious data. They can be used to launch various attacks like denial of service (DoS)/DDoS [20].

In order to avoid above-described attacks, It is necessary to guarantee the primary security characteristics, which include privacy-preserving, availability, integrity, and confidentiality [21].

- **Confidentiality:** Maintaining confidentiality lowers the possibility of data leakage and shields communication from unwanted access.
- **Integrity:** It ensures that any changes or tampering with the data during transmission can be found.
- **Availability:** It preserves the resources or services that are made available to authorized drone users.
- **Authentication:** Identity verification is a prerequisite for data exchange or access in authentication.
- **Privacy-Preserving:** It stops malevolent intruders from revealing personal information without consent.

4. Proposed Approach

A blockchain-aided methodology to lower the risks linked by records upkeep in drone and UAV networks are currently being investigated. Accordingly, the latest research suggests that it offers a blockchain-based approach to decrease risk of records loss in UAV and drone systems. Drones, UAVs, and IoT devices with sensors enable handlers to accomplish a variety of preset goals. Drones & UAVs are monitored & examined locally and remotely via network connection systems [22]. A recent study

found that blockchain-based solutions can lower the hazards associated with drone and UAV systems' data upkeep. With special qualities including immutability, security, transparency, tamper-proofing, and effective distribution methods, this approach specifically seeks to enhance data storage and privacy aspects. Depending on the application, drones, UAVs, and IoT devices typically have a variety of sensors that enable them to perform different functions [23].

The main blockchain-based data security system for gathering data for the component management of drones and UAVs [24]. A wireless communications network and a drone platform are used to gather information. Cloud is utilized to store encryption information created using pentatope ECC (PECC) technique [25]. Benaya et al. [26] 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 few drawbacks to using BCT, such as expensive computing expenses and excessive power consumption. Every time it notices odd action, System records the event & issues a security alert.

The ECDH is used in the proposed method to safeguard cloud data. EthGas is one of the cryptocurrencies that contributes to the development of the BCT ecosystem. An ECDH-based digital signature is utilized to validate whole data acknowledged from aerial devices. The data status tracked and validated through the cloud networks. Smart contacts and digital signatures are also employed to enhance data security and the proposed algorithm for the blockchain transaction process is provided below.

4.1 Proposed Algorithm for Blockchain Transaction Process

This section outlines the proposed algorithm for the UAV Block Transaction Protocol.

While there are n number of UAV devices:

- If the UAV's ETH-balance exceeds a predetermined threshold:
- Allow the UAV device to create a BCN Block (Blockchain Node Block).
- Permit the UAV to generate a Blockchain Node (BCN) Block.
- Update the UAV's ETH balance.
- Else the block transaction is not generated:
- Assure the privacy and preservation of device data.

While there are n number of UAV devices:

- If Device[i]'s block transaction is generated:
- Apply Elliptic Curve Diffie-Hellman (ECDH) to Device[i] data.
- Add the SHA-256 hash of the updated ETH-balance to the block.
- Else, Exit

5. Results and Performance Evalution

The primary aim of the proposed system is to monitor, secure, & handle data gathered by UAV systems or drones. The research's recommended BCN architecture permits for safe & secure storage of confidential information obtained by UAVs or drones. Confidential data gathered by drones and

UAVs is kept in an efficient storage system using the proposed BCT architecture in the study, ensuring security and privacy.

5.1 Performance Evaluation

Strong point of proposed system and the conventional state-of-art ethos in terms of preservation, privacy, defect effusiveness and attack frequency are contrasted in figure 3.

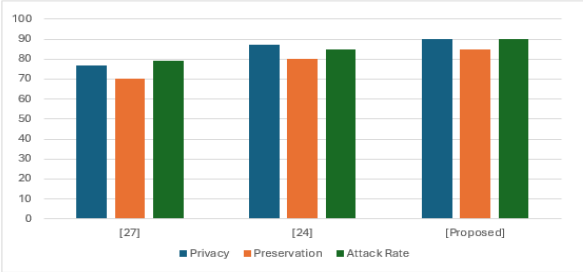

Figure 3: Performance evaluation of the proposed approach based on Privacy, Preservation and Attack rate.

The findings validate that the proposed method outperforms the results from conventional approaches and demonstrate how blockchain quality like as immutability, distribution, transparency, and security impact attack rates. As a result, the proposed system has lower attack rates than the existing methods.

In figure 4 displays gas fee parameter, which is a blockchain transaction fee gave to network validators for their services to blockchain.

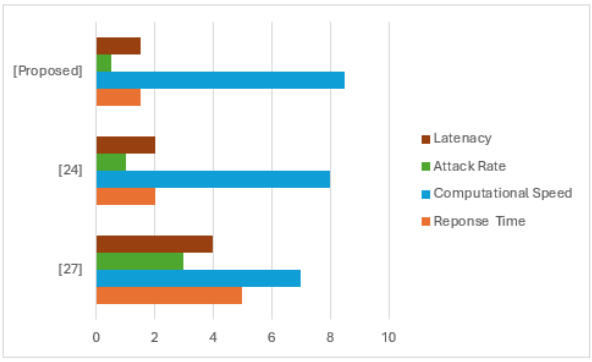

Figure 4: Performance evaluation of the proposed approach-based gas fee parameter.

The reliability of the proposed model must be assessed. The outcomes are contrasted with conventional methods. The degree of persistence of reliability value determines performance scale. Reliability is increased by deployment employed in real implementation. The reliability analysis's numerical results, expressed as the proportion of correctly calculated results, are displayed in figure 5. It is determined that, in comparison to conventional model [26] and [27], the given model attains the maximum reliability measure obtained for the suggested model.

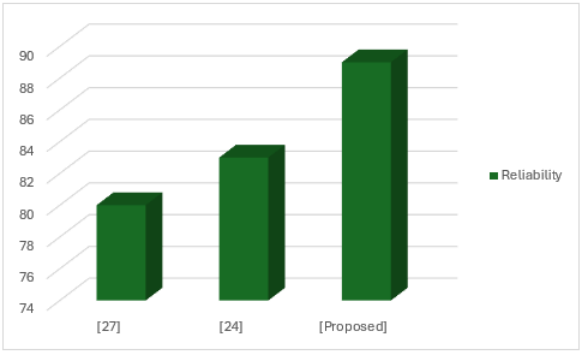

Figure 5: Reliability analysis of the proposed approach

5.2 Performance Assessment Factors

The cryptography system of every network determines its security performance. This section will assess our suggested approach and show that it can provide significate security services at an affordable cost. Here are the key benefits of the proposed method.

- **Confidentiality:** The confidentiality of UAV communication data is preserved using the ECDH technique, which guarantees secure key exchanges.
- **Integrity:** All messages in the suggested system were encrypted using SHA-256 hashes, which ensure data integrity by detecting any data modifications. Thus, the message's integrity has been confirmed.
- **Availability:** Blockchain's decentralized structure guarantees the network's high availability. 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 suggested 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. The communication overhead of nodes when a specific quantity of erroneous information is introduced into a network is known as energy consumption. 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.

6. Conclusion

As the usage of UAV networks in a variety of applications increases, secure communication routes between UAVs are crucial to maintaining CIA features. Blockchain technology can offer security and transparency as the network expands. The current study mainly focuses on utilizing ECDH cryptography in conjunction with blockchain technology to ensure data security and secrecy during

communication. The suggested method uses digital signature to validate authenticity and integrity of each transaction, providing the maximum level of security and confidentiality.

The methodology could be expanded in future studies to incorporate local storage security and UAV scalability. The system can also be developed using the Hyperledger Fabric platform. It would also be fantastic to expand the scope of the study discussed here to encompass additional pertinent IoT topics.

Refrences

[1] S. Hayat, E. Yanmaz, and R. Muzaffar, "Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint," IEEE Communications Surveys and Tutorials, vol. 18, no. 4, pp. 2624–2661, 2016.
[2] L. Gupta, R. Jain, and G. Vaszkun, "Survey of Important Issues in UAV Communication Networks," IEEE Communications Surveys and Tutorials, vol. 18, no. 2, pp. 1123–1152, 2016.
[3] 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.
[4] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6G: Challenges, opportunities and research directions," in Proc. IEEE 2nd 6G Wireless Summit, 2020, pp. 1–5.
[5] S. Hafeez et al., "Blockchain-Assisted UAV Communication Systems: A Comprehensive Survey," in IEEE Open Journal of Vehicular Technology, vol. 4, pp. 558-580, 2023.
[6] M. Ghamari, P. Rangel, M. Mehrubeoglu, G. S. Tewolde, and R. S. Sherratt, "Unmanned aerial vehicle communications for civil applications: A review," IEEE Access, vol. 10, pp. 102492–102531, 2022.
[7] Esraa M. Ghourab , Wael Jaafar , Lina Bariah , et al. Interplay between Physical Layer Security and Blockchain Technology for 5G and Beyond: A Comprehensive Survey. TechRxiv. November 30, 2022.
[8] J. Li et al., "Joint optimization on trajectory, altitude, velocity, and link scheduling for minimum mission time in UAV-Aided data collection," IEEE Internet Things Journal., vol. 7, no. 2, pp. 1464–1475, Feb. 2020.
[9] Z. Ullah, F. Al-Turjman, U. Moatasim, L. Mostarda, and R. Gagliardi, "UAVs joint optimization problems and machine learning to improve the 5G and beyond communication," Comput. Netw., vol. 182, 2020, Art. no. 107478.
[10] G. K. Pandey, D. S. Gurjar, H. H. Nguyen, and S. Yadav, "Security threats and mitigation techniques in UAV communications: A comprehensive survey," IEEE Access, vol. 10, pp. 112858–112897, 2022.
[11] Harbi, Y., Medani, K., Gherbi, C. et al. , "A Systematic Literature Review of Blockchain Technology for Internet of Drones Security", Arabian Journal for Sciecne and Engineering. 48, 1053–1074, 2023.
[12] NIST, Information technology, Blockchain. https://www.nist.gov/topics/blockchain. (accessed June 22, 2020).
[13] Jo, K., Heo, J., Jung, J., Kim, B., & Min, H. (2017, August). A rendezvous point estimation considering drone speed and data collection delay. In 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT) (pp. 1-4). IEEE.
[14] Sana Hafeez, Ahsan Raza Khan, Mohammad Al-Quraan, Lina Mohjazi, Ahmed Zoha, Muhammad Ali Imran, Yao Sun, "Blockchain-Assisted UAV Communication Systems: A Comprehensive Survey" IEEE Open Journal of Vehicular Technology (Volume: 4) pp. 558 – 580, 2023.
[15] R. Majeed, N. A. Abdullah, M. F. Mushtaq, and R. Kazmi, "Drone security: Issues and challenges," Parameters, vol. 2, 2021, Art. no. 5GHz.
[16] Herbadji, A.; Goumidi, H.; Harbi, Y.; Medani, K.; Aliouat, Z.: Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications. 1, 159–197 (2020).
[17] Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H.: Blockchain technologies for the Internet of Things: research issues and challenges. IEEE Internet of Things Journal. 6(2), 2188– 2204 (2018).
[18] Ferrag, M.A.; Shu, L.: The performance evaluation of blockchainbased security and privacy systems for the Internet of Things: a tutorial. IEEE Internet of Things Journal. 8(24), 17236–17260 (2021).
[19] Yaacoub, J.P.; Noura, H.; Salman, O.; Chehab, A.: Security analysis of drones systems: attacks, limitations, and recommendations. Internet Things 11, 100,218 (2020).
[20] Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N.: Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials. 21(3), 2702–2733 (2019).

[21] Harbi, Y.; Aliouat, Z.; Harous, S.; Bentaleb, A.; Refoufi, A.: A review of security in Internet of Things. Wireless Personal Communications. 108(1), 325–344 (2019).
[22] Gupta, M.; Varma, S. Optimal placement of UAVs of an aerial mesh network in an emergency situation. Journal of Ambient Intelligence and Humanized Computing. 2021, 12, 343–358.
[23] 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
[24] 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.
[25] Ch, R.; Srivastava, G.; Gadekallu, T.R.; Maddikunta, P.K.R.; Bhattacharya, S. Security and privacy of UAV data using blockchain technology. Journal of Information Security and Applications. 2020, 55, 102670.
[26] 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.
[27] Choi, N.; Kim, H. A Blockchain-based user authentication model using MetaMask. Journal of Internet Computing and Services, 2019, 20, 119–127.