


## Research Article

# Distributed Blockchain-Based Platform for Unmanned Aerial Vehicles

Tariq Ahamed Ahanger <sup>1</sup>, Abdulaziz Aldaej,<sup>1</sup> Mohammed Atiquzzaman,<sup>2</sup> Imdad Ullah,<sup>1</sup> and Muhammad Yousufudin<sup>1</sup>

<sup>1</sup>College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia

<sup>2</sup>School of Computer Science, University of Oklahoma, Norman, OK, USA

Correspondence should be addressed to Tariq Ahamed Ahanger; [t.ahanger@psau.edu.sa](mailto:t.ahanger@psau.edu.sa)

Received 18 April 2022; Revised 1 July 2022; Accepted 19 July 2022; Published 31 August 2022

Academic Editor: Le Sun

Copyright © 2022 Tariq Ahamed Ahanger et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Internet of Things (IoT)-inspired drone environment is having a greater influence on daily lives in the form of drone-based smart electricity monitoring, traffic routing, and personal healthcare. However, communication between drones and ground control systems must be protected to avoid potential vulnerabilities and improve coordination among scattered UAVs in the IoT context. In the current paper, a distributed UAV scheme is proposed that uses blockchain technology and a network topology similar to the IoT and cloud server to secure communications during data collection and transmission and reduce the likelihood of attack by maliciously manipulated UAVs. As an alternative to relying on a traditional blockchain approach, a unique, safe, and lightweight blockchain architecture is proposed that reduces computing and storage requirements while keeping privacy and security advantages. In addition, a unique reputation-based consensus protocol is built to assure the dependability of the decentralized network. Numerous types of transactions are established to characterize diverse data access. To validate the presented blockchain-based distributed system, performance evaluations are conducted to estimate the statistical effectiveness in the form of temporal delay, packet flow efficacy, precision, specificity, sensitivity, and security efficiency.

## 1. Introduction

Different industries use unmanned aerial vehicles (UAVs) for civilian, military, commercial, and governmental sectors [1]. There are several examples of environmental monitoring in the nonmilitary sector (such as pollution, plant health, and industrial accidents). After a natural catastrophe or a terrorist attack or other emergency situation, the military and government often use surveillance and delivery technologies to collect or convey data and/or distribute supplies. Products and supplies can be delivered in metropolitan regions as well as rural ones. Remote control and monitoring are made possible by UAVs' reliance on sensors, antennae, and embedded software, which makes them an integral element of the Internet of Things (IoT) [2]. Additionally, UAVs will be able to monitor essential infrastructure, such as power lines, when battery and quick charging technology

improves. Using UAVs to monitor the atmosphere from 2 to 3 kilometers above the ground is another applicability illustration. Weather forecasting algorithms can benefit from the pooled data, which includes temperature, wind and turbulence, and airspeed [3]. Using UAVs may lead to exposure to a variety of cyberattacks, including the Sybil attack, DoS/DDoS attack, and GPS spoofing. It could lead to the destruction of the entire system's data availability if the untrusted communication channel is breached [4]. As a result, device authentication and communication security are a major concerns. A central server or cloud or fog computing is used to process and store data in the UAV system. Because of the inherent flaws of conventional centralized design and cloud server manipulation, the integrity of data may be compromised when a server is hacked, which is also a concern with the conventional centralized architecture [5].

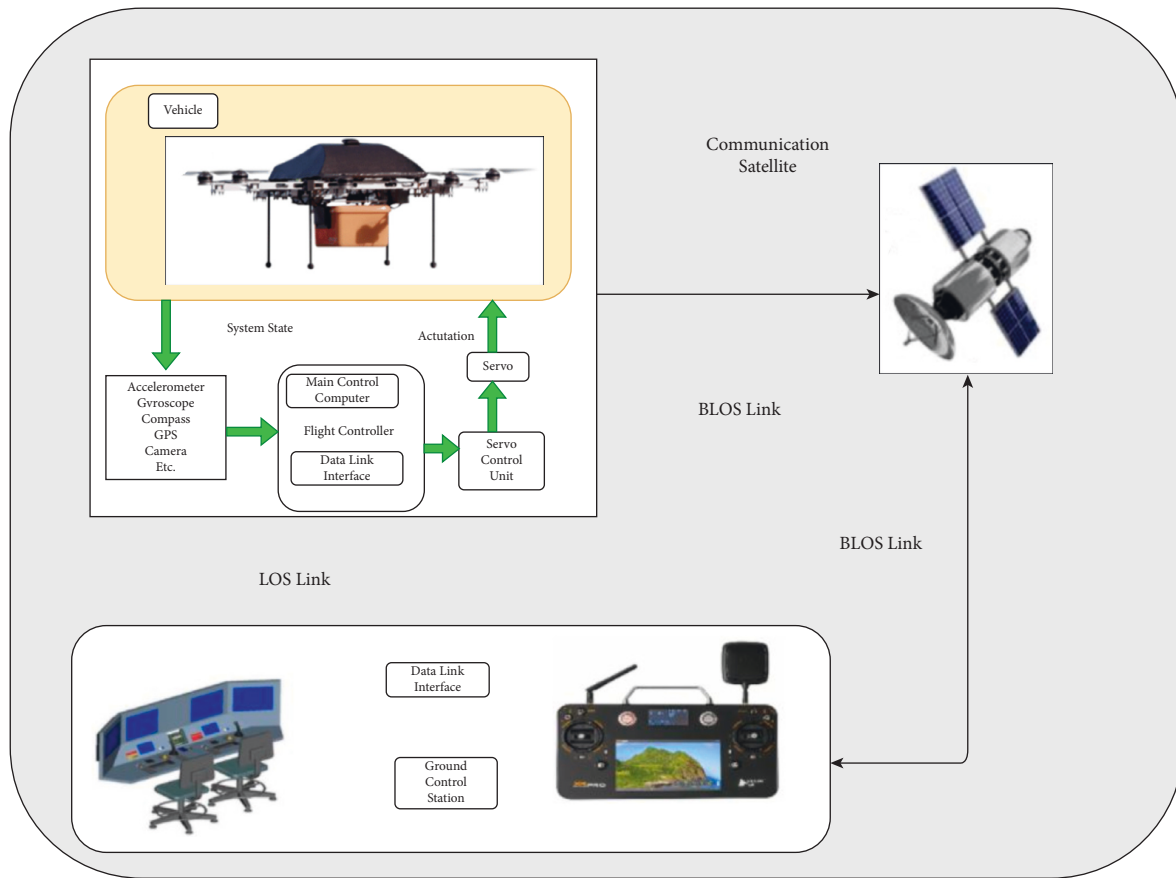


FIGURE 1: Conceptual overview of UAV architecture.

**1.1. Research Domain.** UAV technology is seeing a growing trend of autonomy, driven by developments in batteries, charging techniques, and embedded software that uses machine learning algorithms to learn [6]. It is being created and tested; however, there are currently no permitted autonomous UAV systems that may be used. Semiautonomous UAVs clearly show that a fleet of UAVs with advanced algorithms may be capable of handling a variety of human-defined tasks and developing issues with high levels of coordination by ensuring contact between UAVs and ground control station (GCS) [7]. Figure 1 shows the conceptual overview of the conventional UAV architecture (Source: <http://www.dronefromchina.com/new/drone-communicate-with-UAV-ground-stations.html>). Military planes have long used the term “a swarm of UAVs” to describe a large group of drones. Conspicuously, future UAVs will need a secure and private network system, as well as an integrated system that is responsive and sustainable to develop a trusted, integrated environment [8]. A huge number of linked devices, transaction processing, and coordination between many devices in the context of IoT may be achieved using blockchain (BC) technology, which is the rudimentary mechanism of Ethereum along with other cryptocurrencies [9]. Aside from being a tamper-proof, and immutable recording of data in a network (i.e., a log), BC is also a decentralized architecture that prevents a single point of failure, making it a more resilient and stable platform for IoT

execution. Figure 2 shows the illustration of the blockchain (Source: <https://github.com/rajibdpi/BlockChain>). The underlying cryptographic algorithm employed by BC, including hash functions, symmetric encryption, and digital signatures, is a key component of BC [10]. Many non-monetary situations for IoT security have already been used in BC, such as the protection of health care data, government democracy and legal enforcement, smart home, smart toy at the edge computing, and vehicle-to-infrastructure communication system [11, 12]. It is difficult to integrate blockchain technology with IoT because of the high resource consumption, high delays, and high memory overhead to store the records of billions of transactions [13]. When it comes to research on the integration of BC with UAVs, most of the studies focus on employing BC technology as a decentralized database [14].

A distributed blockchain-based architecture for UAVs is proposed in the current research to overcome the aforementioned security and privacy issues while also providing a high degree of operational autonomy. The following are the most significant contributions:

- (1) UAV applications are explored for vulnerability detection in the IoT domain for data security and protection.
- (2) The blockchain framework is designed to alleviate the demand for storage and calculation placed on

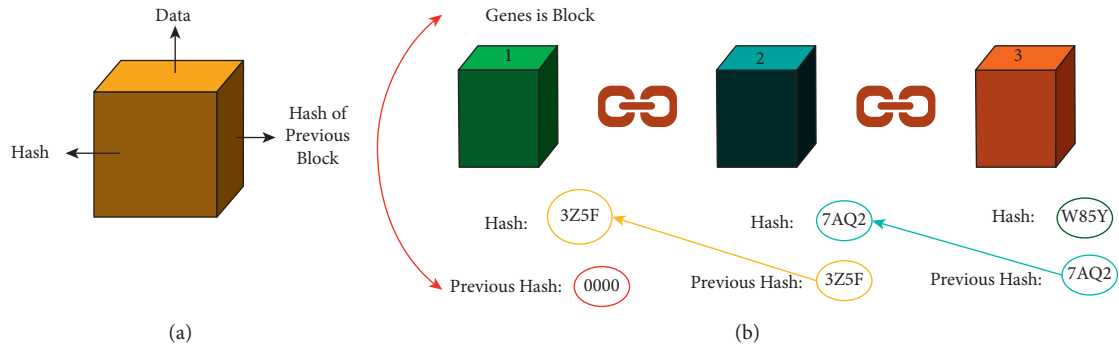


FIGURE 2: Illustration of blockchain architecture; (a) single block; (b) blockchain chain formulation.

each UAV by employing novel transaction and block structures over lightweight cryptography.

- (3) A novel consensus mechanism analogous to Delegated Proof of Stake (DPoS) paired with a reputation assessment system is implemented to achieve an agreement with the aggregated data amongst UAVs.
- (4) The blockchain-based decentralized architecture is validated for UAVs in which numerous tests are conducted to determine self-defense capabilities.

*1.1.1. Paper Structure.* Section 2 provides an overview of some of the important contributions in the related domain of study. Introduction to the UAV networks and BC technology is provided in Section 3. Block and transaction structures are shown in Section 4 to explain the system architecture required for the proposed semiautonomous BC-based UAV framework. Section 5 explains how the proposed framework for UAVs works. A security assessment and an efficiency assessment are included in the performance analysis presented in Section 6. Section 7 presents some of the open issues and challenges for future research. Finally, Section 8 concludes the paper.

## 2. Literature Review

*2.1. Internet of Things (IoT) Security.* Kanuparthi et al. [15] depicted that as the number of smart devices in IoT rises, the risk of cyber-attacks including buffer overflow attacks is also elevated. If the device is hacked, it might lead to a data leak and expose the server to attacks. Authors have incorporated hardware security primitives to address the security aspect. However, the presented technique takes a lot of computing power from the devices. According to Misra et al. [16], IoT devices did not evaluate security needs carefully; therefore, it can lead to enormous cyberattacks. For better privacy, several attempts are being made to analyze the security of UAV communication networks. Rudinskas et al. [17] examined the radio communication system and discussed radio-related challenges, harmful threats, and potential solutions for data transformation between various entities. The presented study focused on cryptography approaches while ignoring the limitations of UAVs in terms of space and power. To assist researchers and end-users in better grasping

the system's risk profile, Thing et al. [18] provided a clear and comprehensive security model for UAVs. Many UAV-related studies have focused on resisting GPS spoofing and jamming attempts due to the system's architecture as a GPS location system. A taxonomy of UAV cyberattacks and future research directions were provided by Krishna et al. [19] based on an in-depth examination of numerous GPS spoofing and jamming attacks. GPS spoofing attacks were researched in detail, including their design and impact. A new detection and mitigation approach was presented and tested on the most promising test platform. According to the technique presented by Javaid et al. [2], spoofing is caused by the lack of encryption of GPS information. MP-OLSR, the multi-path routing protocol introduced by Randu et al. [20] for FANET, aggregates dynamic data with high mobility in emergency scenarios. There is no discussion of a malicious node scenario for the technique in the simulation platform. A multilayer security framework for WiFi-based UAV systems was established by Hooper et al. [11]. Authors demonstrated how the proposed method mitigated three adversarial attacks: *Buffer-overflow attack*, *DoS attack*, and *ARP cache poison attack*. A different study by Zhang et al. [21] found that by simply relocating the UAV, the legal link could be created strongly than the eavesdropping link and that it may be used to combat eavesdropping in UAV-to-ground (U2G) and ground-to-UAV (G2U) communications.

*2.2. Blockchain Security for IoT.* The unchangeable and distributed ledger of the blockchain has drawn the interest of many academics [31]. However, the blockchain business has faced several difficulties as a result of the widespread use of IoT devices [32]. Tosh et al. [33] presented that consensus procedures in blockchain are a serious issue that might lead to a delay in the consensus of proof of work. Using a combination of private and public ledgers on local networks, a blockchain topology suitable for smart homes has been proposed by Dorri et al. [34]. Smart gadgets with edge computation and vehicle-to-infrastructure communication schemes were investigated by Yang et al. [35]. Numerous studies have been carried out to examine the success of integrating blockchain technology with UAV systems in many areas as blockchain may provide many benefits to various IoT situations. Using private blockchain to distribute and store group keys, as well as handle the dynamic list of

network members, Li et al. [36] suggested a mutual-healing group key distribution technique. Recovering an unmanned aerial vehicle (UAV) that has crashed is challenging; thus, Scarlato et al. [37] devised an authorized side chain with proof of authority consensus recording GPS coordinates and flying altitude for the avoidance and recovery of the wrecked UAVs. In an air-to-ground IoT network, Zhu et al. [38] studied trading and storage management difficulties and presented a novel consensus method based on Nash equilibrium to minimize resource usage. UAVs have limited processing resources; therefore, Kuzmin and Znak [39] introduced a unique proof-of-graph consensus mechanism for an autonomously running UAV network on the blockchain. To ensure data integrity, traceability, and unforgeability, Youssef et al. [40] developed a distributed payment system based on the blockchain between a UAV cloud and a sensor cloud. Rana et al. [41] focused on securing data sent and received between UAVs and the cloud, where GPS data are necessary to be included. Aslam and Shin [42] developed an effective method to verify user identity and identify malicious UAVs by employing a memory-efficient data structure known as the  $\pi$ -hash bloom filter. Based on the comprehensive overview, Table 1 has been formulated to depict the comparative analysis with the current work.

### 3. Fundamental Aspects

**3.1. UAV Communication.** UAV systems typically consist of 3 components: a single UAV (or fleet of them), ground control stations (GCS), and 3 different types of data transmission lines (satellite link, UAV-to-UAV link, and radio link) [43]. Each type of link has a particular purpose. GPS and meteorological data are transmitted between satellite and UAV through satellite connection, while the UAV-UAV link conveys messages of interaction between the two types of UAVs [2]. Finally, a radio communication link delivers GCS orders, audio/video, and other data to the UAVs [44]. In addition, a specific UAV is examined in the current research that has a flight controller, a cluster of sensors, and a set of actuators when discussing the building blocks. Moreover, the internal workings of a UAV are discussed [3]. In other words, UAV is piloted by a flight controller, which serves as a central processing unit for data acquired by different sensors and sent to the control units or relayed to GCS, depending on the mode of control [45]. Other acting actuators are influenced by GCS orders, which are regulated by the flight controller [19]. Drone photography, autonomous freight transport, precise crop monitoring, building surveillance, tracking unsafe circumstances, or providing essentials for emergency services are some of the uses for drones that have been documented in several studies [46]. UAVs exemplify how a multiscale technological ecosystem, such as WiFi, Zigbee, 4G/5G wireless cellular communications, and machine-to-machine (M2M) communication, as well as ancillary computational resources combine to form an embedded system (such as cloud computing and edge computing platform) [47]. Because cybersecurity was not prioritized in the early stages of design, modern UAV autopilot systems are vulnerable to a variety of cyberattacks [37].

**3.2. UAV Threats.** Three hostile cyberattacks aimed at attacking the distributed UAVs system are briefly discussed.

- (1) *Sybil Attack* peer-2-peer networks are vulnerable to Sybil attack, in which a hacker uses stolen or manufactured identities to represent numerous separate nodes in the network. There are a variety of harmful behaviors that the adversary might use to gain a disproportionate amount of control over data integrity, resource consumption, and overall network performance.
- (2) *DDoS (denial-of-service) attack* some requests may be prevented from being answered by making requests for the target device to become unavailable.
- (3) *GPS Spoofing* armed forces use encryption to ensure that GPS signals cannot be tampered with, while civilian GPS transmissions lack both encryption and authentication, making it possible for an adversary to produce or fake the original signals. As a result, the attacker can guide the UAV to a chosen destination that is different from the current intended course by manipulating the signals.

### 3.3. Blockchain Fundamentals

**3.3.1. Overview.** Although blockchain has been around for a few years now as Nakamoto et al. [48] coined the term in 2008. It is been widely regarded as an emerging technology for distributed and decentralized data sharing. Blockchain was initially designed to record money transactions, where each transaction is recorded and saved by all members of the peer-to-peer network, but it is increasingly being used in nonmonetary applications as well [49]. An important feature of blockchain is its ability to demonstrate that an uncensored group of users may form an agreement that can be recorded in a verifiable and safe manner [42].

**3.3.2. Structure of the Blockchain.** As shown in Figure 2, the chain is made up of blocks linked together by the hash value of the preceding block. To solve the complicated mathematical problem known as hash functions (i.e. hash functions), a nonce (target value) must be provided for each block in a sequence of transactions recorded in the current block [6]. The *proof of work* concept was developed for Ethereum to make block production computationally “hard” based on standard hash functions, thereby preventing the attackers from tampering with block information. For instance in Ethereum, only miners are responsible for creating blocks and broadcasting newly created blocks back to the blockchain. Once the newly created block has been validated by all parties, it should be added to the blockchain and validated along with the transactions it contains.

## 4. Distributed BC-Based UAVs Framework

Distributed UAV framework based on blockchain technology works is presented in the current framework. Moreover, a customized blockchain structure for UAV



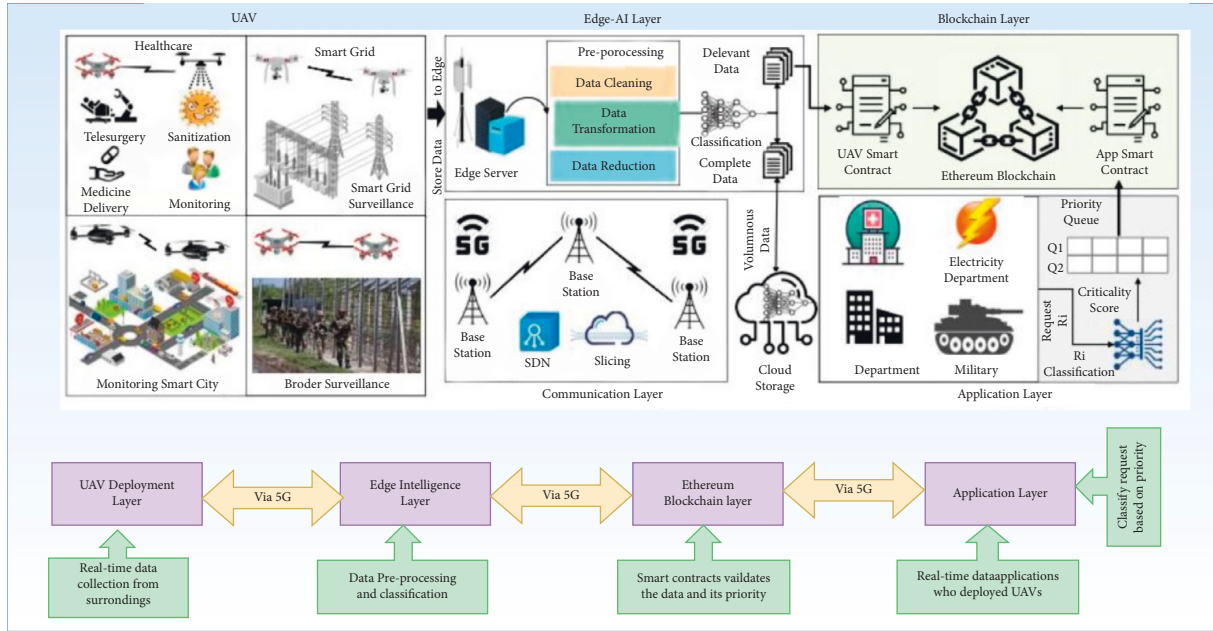


FIGURE 3: Blockchain-based UAVs framework: workflow analysis.

communication systems is proposed for secure data transmission.

**4.1. Overview.** Figure 3 shows a situation where healthcare surveillance UAVs are used to locate vulnerable patients to control disease outspread. Assuming the UAVs can identify the target individual with the use of identification, including facial recognition, it is assumed that any person walking outdoors in a region may be monitored by numerous surveillance UAVs. Ground control stations (GCS) are task control centers located on land that is responsible for managing UAVs to collect and process large amounts of data. In addition, the cloud server serves different purposes. Data from sensors, pictures, and videos, as well as the status and position of each UAV, may all be saved in the cloud as part of a single storage service. The cloud can handle a wide range of computation-intensive jobs due to the widespread use of high-quality computational tools. For example, UAVs may access the internet and obtain information on no-fly zones. A cloud server (either GCS or UAVs) must provide the hash value of the requested data to the requester.

**4.2. Blockchain Construction.** Expecting UAVs to have the same processing capacity as Ethereum miners makes the challenge of enabling distributed storage and security rather difficult for the IoT device-based network. As a result of these findings, a customized blockchain architecture is depicted in the suggested framework.

**4.3. Block-Level Information.** Reformatory blocks, like Ethereum's, may be broken down into 2 parts: the block header and the block body. The proposed block is tailored to the needs of lightweight IoT devices and UAV communications by employing lightweight cryptography technologies

TABLE 2: Block composition.

Contents	Description	Size (bits)
T_STAMP	Linux timestamp of the block	32
B_HASH	Hash value of current block header	78
P_LIST	Access rules of a fleet of O UAVs	$30 * O$
T_ROOT	Root of the transaction tree	78
P_HASH	Hash value of previous block header	78
R_ROOT	Root of the reputation tree	78

such as Keccak (i.e., a low-cost alternative to the standard version that was selected as the winner of SHA-3 by NIST) and redefining the functions of all transactions. Block headers are made up of the current block header's hash, the previous block header's hash, the root of a reputation tree, a policy list, and timestamp as shown in Table 2. Evaluation of reputation scheme is performed similarly to the fundamental idea of Delegated Proof of Stake (DPoS) to nominate a node to generate a new block, unlike Ethereum where the miners must find a solution to a hash puzzle to win the right of append to the main chain the new block. As a result, the reputation tree item is included in the block, and the block header records the tree's root. When adding new UAVs to the system during start-up, the GCS administrator generates a policy list, which is then included in Block 1. Each node in the network should refer to the most recent policy to process transactions because updating it is as simple as making a change to the policy list in the most recent block. A reputation tree and a transactions tree are therefore included in the block body. The reputation of a UAV can be affected by suspicious behaviors, such as checking privacy data against access policies provided in block headers and producing or relaying incorrect blocks. The reputation value for each UAV is stored using an MPT-based cryptographically authenticated data structure, which can be shown in Figure 4. This

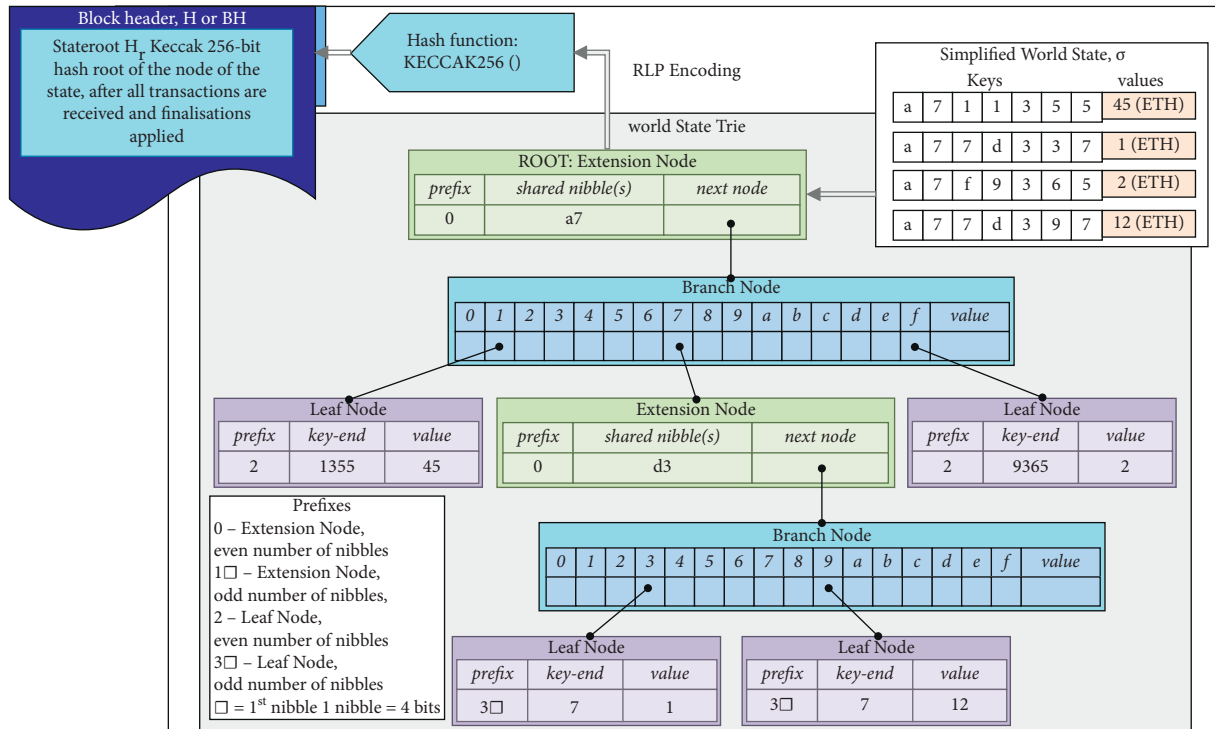


FIGURE 4: Example of the modified Merkle Patricia tree.

TABLE 3: Transaction composition.

Contents	Description	Size (bit)
T_TYPE	Transaction type	8
RV_ID	Device ID of the receiver	16
RQ_ID	Device ID of the sender	16
DATA	Additional information	1024
SIGNATURE	Signature/multi-signature	1024/2048

allows us to rapidly and efficiently detect data that have changed without retrieving the entire dataset to compare.

4.3.1. *Transaction Detail.* Transactions are defined as communications between GCS, UAVs, and cloud servers among the entire system. A microsized transaction structure, as indicated in Table 3, is recommended due to the limited storage capacity available in UAVs. A transaction’s details include the requester and recipient’s transaction type IDs (similar to blockchain addresses), the requester’s signature (i.e., the sender), and other data required. In contrast to the addresses used in the blockchain, shorter IDs are utilized to identify UAVs, and the extra data can range in length from 0 to 1024 bits.

4.3.2. *Handling Transactions.* Based on the distributed BC-based architecture presented in Figure 3, analysis is performed on how transactions are handled in the semiautonomous UAVs system.

- (1) *Genesis:* genesis defines the process of adding additional devices before commencing the mission,

which should be established by GCS administrators after authentication, while each UAV is given a unique ID and a pair of public/private keys to allow it to sign transactions. Because each UAV has a starting reputation value of 69, which denotes its trustworthiness, and because the value fluctuates in response to the UAV’s bad behavior.

- (2) *Command:* to launch a command transaction, GCS must either request data from the UAV or send a control command to UAV equipment. There are several types of information that may be included: airborne GPS data (such as altitude and speed, for example), flight data (such as acceleration and deceleration), sensor data from UAVs (such as cameras), and picture data (such as photos and films taken with the camera). Command transaction is only applicable in the case where a large number of UAVs are within a short distance of the GCS. There is a DATA field in GCS’s transaction that specifies what sort of data was gathered. Command transactions are followed by time windows in which UAVs must follow through with the command. Another option is to use artificial means of capture, altering the policy list to prevent communications with that UAV, or lowering its reputation value to alert other UAVs in its network about the suspect.
- (3) *Inquiry:* some UAVs may require data from other UAVs following the specified policy. Some UAVs require information on the flight path of other UAVs to plan the route more accurately while modifying their respective direction. Note that the transaction

may only be initiated by UAVs. It is possible that with the presented technique, the requester may have to send a resend request within a time window  $\Delta t$ . The requester would launch a report transaction broadcasting the suspicious activity of a specific UAV if it did not receive a response in the context of a lawful query within  $\Delta t$ .

- (4) *Respond*: when a request is made that breaches an access restriction, the requesting party should make a report transaction detailing the infraction and disseminate it to punish the suspect UAV to some degree. Requestors would instead respond to requests according to the policy's satisfaction level, which is determined by the reputation value of the requestee. Diffie–Hellman shared key would be used by the receiver, and the answer would be sent back to the requester. The shared key is used to send the response back to the requester.
- (5) *Access*: the terms “access transaction” and “UAV/GCS cloud server interaction” are used interchangeably here. Transactions should be checked against the most recent policy list by any UAVs that receive them. To punish the person who requested access, the transaction should be discarded and a report should be published.
- (6) *Store*: it is the cloud server's job to store data from drones and ground control stations (GCS). To verify the transaction, the cloud server checks to see whether there is enough storage space available. The hash value of the received data is then calculated and compared to the received hash value. Once two hash values match, the data packets are stored in the cloud. This is followed by encoding the requested address with the Diffie–Hellman method and sending it back to the user.
- (7) *Report*: system-wide self-monitoring and semi-autonomy can be improved by the use of report transactions. If a hacked device is identified, either the UAV or GCS has the right to report it. Consequently, the reputation value will be lowered if the report is shown to be accurate. In circumstances of the dispute, such as the selection of a committee to mine the blocks and the acceptance or rejection of the report transaction, the transaction is meant to assure certain convergence towards a consensual conclusion. Voting in elections, for example, requires a single node to begin a vote transaction, and the other nodes answer with a response transaction that includes the candidate IDs and signatures of each node. Voting results are calculated after receiving the messages, and the new committee is announced to everyone.
- (8) *Alert*: all the information is identified to know about voting. There are ways to protect the system from future cyberattacks, such as having each UAV and GCS have alert transactions that sound an alarm if it detects a certain type of attack. It would help the

system as a whole defend itself and limit losses early on. In response to varied attacks, all of the UAVs in the network would take the same course of action.

## 5. Working Mechanism

A distributed ledger, consisting of connective blocks, is used to store all communications data in the current system. This ledger is present in both UAVs and GCS. Message transmission, message verification through a voting system, and mining all require accuracy guarantees to maintain data security. The presented framework's functioning mechanism as shown in Figure 5, including data processing, reputation evaluation, and consensus method, is explained in-depth ahead.

### 5.1. Processing of Data

*5.1.1. Registering a New account.* To join the network, any device (such as an unmanned aerial vehicle, or UAV) must first register using the genesis transaction. Based on its MAC address, the most recent timestamp, and random salt hash value, each device generates its private key before registration. Preloaded policies for each node will also outline what actions to do while receiving messages.

*5.1.2. Data Hashing.* Each node stores the public keys of all other nodes, its private key, and the next blocks in a sequence. Cryptography procedures like the hash function and digital signature must be performed on all devices before it delivers communications. In comparison to other lightweight hash functions (such as Quark, PHOTON, and SPONGENT), Keccak is a high-performance hash function in both code size and cycle count. Due to the extensive use of hash functions, such as block hash, prior hash, reputation root, transaction root, and the message digest for each transaction, the 160-bit output is shortened to 80-bit to conserve memory.

*5.1.3. Verification of the Data.* If two digests match, the data integrity and consistency of a transaction in a peer-to-peer network are verified. Whether the request is genuine, the policy list is checked to see whether it satisfies all of its requirements. Reputation values of individual UAVs are reduced if a transaction is rejected due to inaccuracies in data integrity or if it violates a set of policies, which are communicated to other UAVs via a report transaction issued by receivers of rejected transactions. As a result, the reputation worth of the person who correctly reports the hostile behavior rises. For example, each report transaction would trigger a voting procedure in which each node votes on its verification result and the reputation value of the suspected UAV in a distributed voting mechanism.

*5.2. Estimation of Reputation Measure.* To confirm the validity of the received blocks, a distributed reputation assessment mechanism is adopted that reduces the block



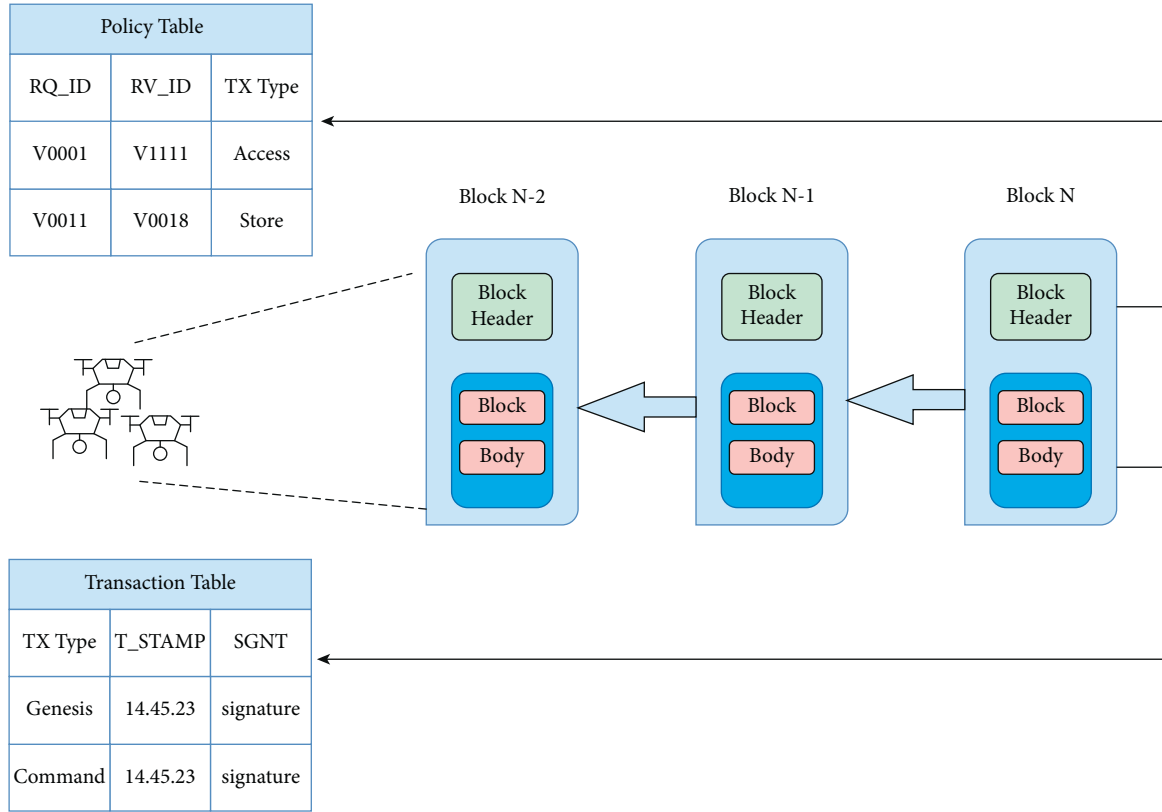


FIGURE 5: Proposed UAVs blockchain architecture.

verification cost. Merkle Patricia Trie is used to hold the reputation value of all nodes in the proposed architecture. Each group of UAVs is led by a master UAV and supported by a swarm of general UAVs. Using the reputation assessment, the system keeps track of each node's trustworthiness. For the most part, each UAV starts with a reputation value of 69, which may either be boosted or lowered depending on whether or not the UAV is successfully reported as suspicious. It is also vital to note that each UAV in the network can accept or relay transactions based on its reputation value, which is calculated using the following equations:

$$\begin{aligned} \mu &= 1, \text{ if } s > 99, \\ \mu &= \frac{\mu_1 * s}{\sum_{k=1}^O s_k * D_j}, \text{ if } 59 < s < 99, \\ \mu &= \frac{\mu_2 * s}{\sum_{k=1}^O s_k * D_j}, \text{ if } s < 59. \end{aligned} \quad (1)$$

If UAV  $V_j$ 's reputation value is more than 59 and its number of suspicious acts is greater than 59,  $\mu$  reflects the likelihood that UAV  $V_j$ 's request will be accepted. Conspicuously, a high reputation value encourages the acceptance and trustworthiness of its communications and vice versa. If the reputation value of the requester falls below 29, neighboring UAVs will refuse to transmit all of the transactions started by it. If UAVs are not programmed to transmit lots of spam or bad messages, it makes it harder for

them to take over the system. To compute the reputation of a connected node, a node takes into account the quality of service provided by its peers. Coefficients  $\mu_1$  and  $\mu_2$  are used to weigh the relevance of connections in the current system.

**5.2.1. Distributed Voting System.** ID-based vote distribution technique has several functions. DPOS-like distributed consensus protocol is proposed to agree with the acquired data. As a result, the committee that generates the block is elected by a vote. It is well known that a report transaction is used to alert authorities of suspicious activity by UAVs. However, the hacked UAV may undermine the system's availability by inventing report transactions to frame the conforming UAVs. As a result, the voting mechanism should assess the legitimacy of each report transaction. Moreover, the voting procedure is used to handle instances when there is a lot of disagreement. Vote transactions are used to compare the GPS of a UAV to those of other UAVs in a no-fly zone, for example, when one UAV unexpectedly finds itself in or near the no-fly zone without any anticipation. A GPS spoofing attack is extremely likely if it does not match, and the UAV should send out an alert to warn its neighbors so they can take precautions to reduce the danger. To further understand the voting process, assume a network of  $O$  UAVs. Each node in the network can cast a vote based on the outcome of its verification and its conclusion. If the total number of votes is less than or equal to  $O$ , then voting is permitted as  $(L/O) > \pi$ , where  $\pi$  denotes the threshold value.

To ensure that a result is accepted by the majority of nodes in the system, the threshold  $\pi$  must be larger than 50%.

**5.3. Consensus Protocol.** In distributed and multiagent systems like UAVs, the consensus method is critical for building trust and dependability in the network. A detailed explanation of how the system works, including the rules for generating committee selection blocks, is provided in the current section.

**5.3.1. Selection of Committee.** An ideal scenario for selection is one where GCS and UAVs are nearby, allowing for high-quality intersystem communications. Given that GCS can be trusted, it makes sense to designate GCS as the miner in charge of collecting all transactions, verifying the validity, and managing changes to reputation values in the block header, all of which relieves the UAVs from the computational burden. Instead, if the swarm of UAVs must coordinate independently on a mission without continuous connections to GCS, this technique, “Voted Nodes as Miners,” is more suited. The administrator of GCS should form a committee based on the roles assigned to UAVs during the system’s infancy, and the committee’s membership should be proportional to the entire number of UAVs. The reelection of the committee is triggered by any block generation or forks in the blockchain ledger that are not recorded. If this is the case, committee members are chosen based on their reputation value, with only the top 16% of nodes eligible to serve. To form the final committee, each node will vote for 3 of the top 5 candidates, and the master UAV will generate a vote transaction. The results of the voting will be shown to everyone on the whole network.

**5.3.2. Generation of Blocks.** The accumulative transactions in a block might generate communication delays or slow down the transmission rate among the network if the block generation rate is vague. Otherwise, the blockchain system’s nodes might become overburdened with processing if mining occurs too often. The presented design relies on blocks being generated at the right place; hence, a set block creation rate is recommended. Each block is generated at a certain time slot, which necessitates a regular rotation of the mining tasks. After the previous block is generated, the mining process immediately moves on to the next fresh round. Because various jobs have varying communication requirements, the time interval between two rounds of block creation may be customized. Time interval of mining, average block size, and time interval of periodic memory release are all variables that may be used to model an O-UAVs network’s data storage capacity. The following restriction applies to the current work;

$$\alpha * \text{floor} \left( \frac{t_0}{\beta} \right). \quad (2)$$

When rounding to the closest integer, floor (.) is used. Indeed, the restriction assures each device has enough memory to store data in the blockchain until its next

memory release. Figure 6 depicts the illustrative view of healthcare applications based on the presented model.

## 6. Performance Analysis

**6.1. Security Analysis.** This section details the performance analysis of the proposed model with respect to different attacks.

**6.1.1. Sybil Attack Protection.** In the suggested architecture, harmful requests are kept away from devices to boost availability by restricting the access privileges of each network participant by policy list to those entities that hold certain vital information of the system. To avoid message transformation, transactions received from other UAVs are authenticated by each device before being sent on to the neighbors.

**6.1.2. Mitigation of DoS/DDoS.** A DoS/DDoS attack is less likely to occur in our system because network nodes will not broadcast garbage information if the sender’s reputation value falls below a certain level. The packet flows between UAVs may be monitored by GCS, and as a result, GCS might reset the policy list to block all access permits, therefore decreasing the impact of a tampered UAV.

**6.1.3. Resistance against GPS Spoofing.** The proposed method has some resistance to GPS spoofing since the voting transaction may obtain other UAVs’ GPS information. As a general rule, it is hard for an attacker to take over all of the UAVs at the same time. Once a UAV identifies itself in or near a no-fly zone, it will transmit a vote transaction to claim its GPS data. Allowing participants to respond with true/false messages would be referred to as a vote function. As a result, the requester could verify that it had the correct GPS data.

**6.1.4. Consensus Protocol Security.** Blockchain-based UAV require high levels of security for the blockchain consensus mechanism that underpins them. Natoli et al. [50] summarized the security of consensus protocols under various attack models, including miner power attacks, strategic miner attacks, communication attacker attacks, hybrid attacker attacks combining strategic mining with communication attacks, and stake attacker attacks. As a result of the proposed consensus scheme’s reputation, attacks can be prevented from both mining power and strategic mining. However, the current system is vulnerable to communication attacks, strategic mining and communication attacks, and stake attacks.

**6.2. Evaluation of Efficacy.** The proposed distributed BC-based technique is deployed using an emulator for multi-agent UAVs networks termed as UB-ANC Emulator based on the technique of ns-3 [51]. The entire system configuration can be seen in Table 4. Moreover, the simulation parameters used in NS-3 are depicted in Table 5. The

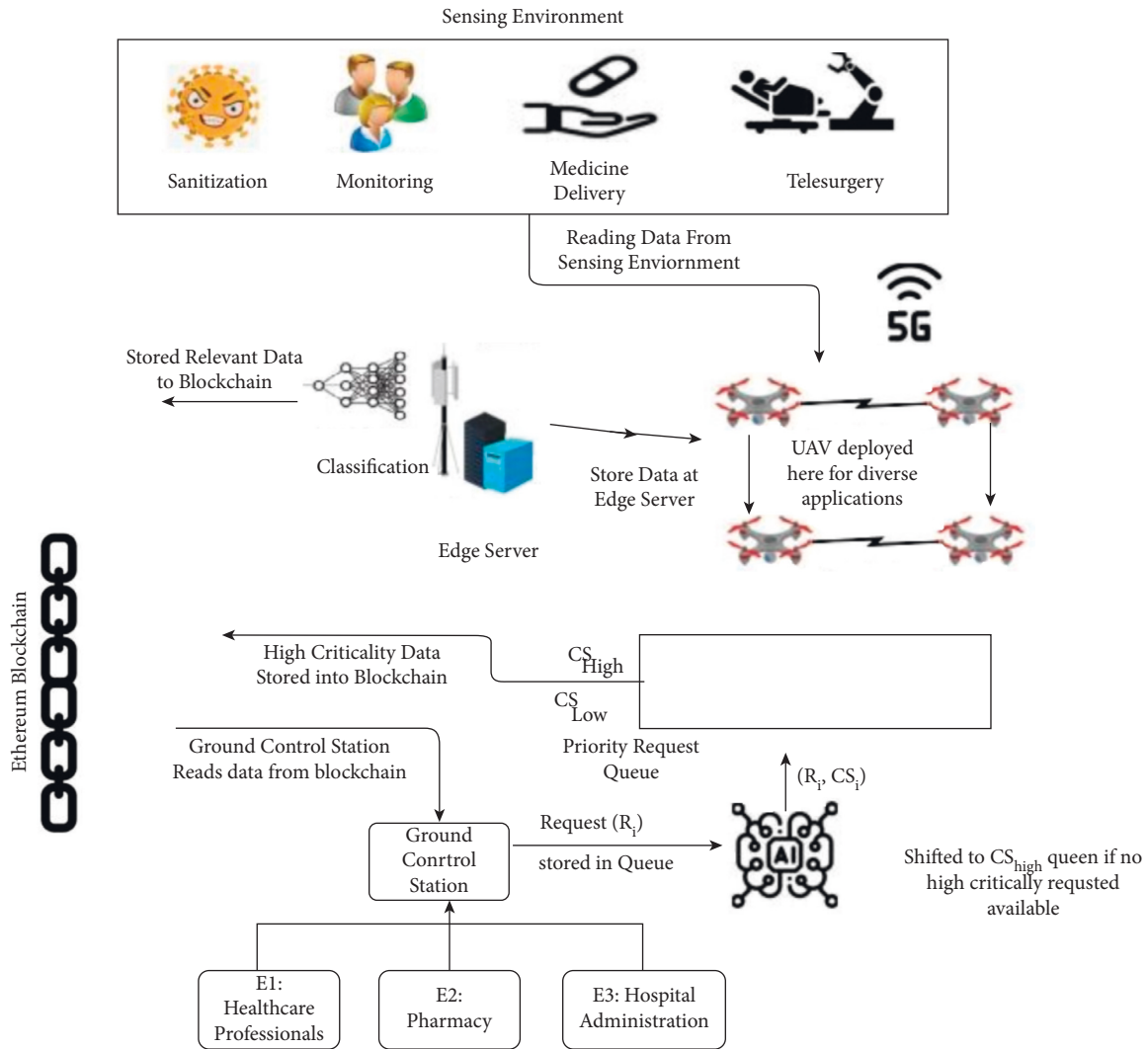


FIGURE 6: Blockchain-based intelligent surveillance: healthcare environment.

TABLE 4: Simulation settings.

Operating platform	64-bit Linux
CPU	2.57 GHz intel i7 core
Network simulation tool	ns3
Ground control station tool	QGround-control

suggested architecture was compared to a base system that does not use a digital signature, hashing, or blockchain technology. The experiment excludes the average delay of transmission because of the limitations of the simulator. Figures 7–9 show the outcomes of the simulation trials. When it comes to drone networks, a novel method is presented in the current study that decreases computational and communication overhead while enhancing the security and privacy of drone systems. According to Figure 7, which shows the time overhead for various types of transactions, the most time-consuming portion is the store inquiry. Most transactions in the proposed system would take longer or cost more than they would in the current scheme. Inquiry transactions take less time in our solution because UAVs in the presented framework may choose more creditable

TABLE 5: Simulation parameters.

Simulation parameter	Measure
Radio link control (RLC) buffer size	150
Pkt size	998 bytes
Transmission control protocol (TCP) traffic type	Cubic
Application data rate	98 Mbps
Movement speed	18 m/s
Simulation area	6 km radius
Number of traffic source	8
Wired link delay	48 ms
Number of resource block	18
Mobility	Random walk 2D
Wired link capacity	8 Mbps

objects to collect information, saving a lot of time waiting for important replies. Reputation values for malicious nodes have been fluctuating over time as seen in Figure 8. The reputation value of the malicious node might be viewed as rising linearly over time if the other complying nodes are unable to identify any malicious behavior in the basic

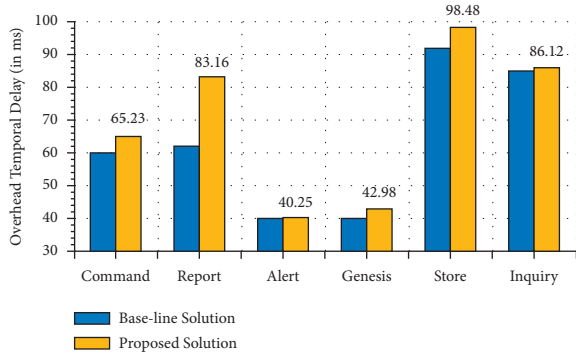


FIGURE 7: Overhead temporal delay.

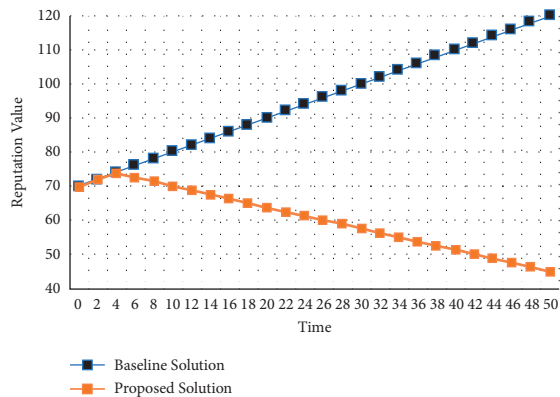


FIGURE 8: Reputation value estimation.

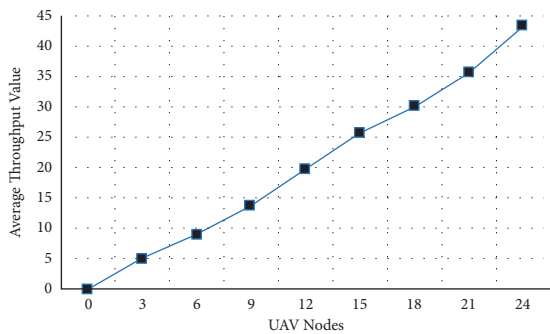


FIGURE 9: Throughput of proposed solution.

scheme without the reputation evaluation scheme This is not the case in our suggested method, whereby a hacked node's reputation quickly falls below the threshold value (59). It can be seen from the graph that the reputation of a rogue node deteriorates over time. Other nodes will not trust a malicious node when its reputation falls below a certain level. As a result, the UAV swarm's distributed autonomous decision-making may be assumed to be secure. The average throughput of the proposed BC-based framework increases as the number of UAVs in the network grows. Finally, Figure 9 depicts the cumulative throughput of the proposed model in comparison to the baseline techniques. Furthermore, Table 6 depicts the packet flow evaluation for the proposed model in comparison to the proposed approach.

TABLE 6: Packet flow evaluation.

Packet flow	Proposed	Baseline
From UAV to UAV	29	14
From UAV to cloud	39	19
From UAV to GCS	37	19
From GCS to cloud	63	59

**6.3. Statistical Performance.** In addition to the performance analysis mentioned before, the proposed model is deployed to determine the statistical performance in terms of precision, specificity, sensitivity, and f-measure. For comparative analysis, the baseline technique is used. Figure 10 shows the overall results of the proposed technique. It can be seen that in the current scenario, the proposed technique can register an enhanced precision measure of 92.15% (Figure 10(a)) concerning 83.15% of the baseline technique. Moreover, the specificity analysis shown in Figure 10(b) shows that the presented technique acquired a better measure of 93.65% in comparison to 88.45% for baseline. Furthermore, the enhanced measure of sensitivity (Figure 10(c)) and f-measure (Figure 10(d)) are registered for the presented technique showing that the proposed technique is more effective and efficient for detecting attacks in comparison to the baseline techniques.

**6.4. Stability and Reliability Estimation.** Stability refers to the normalized behavior of the proposed algorithm over the variable number of data events. In the current scenario, the stability is measured in terms of the mean stability measure (MSS), where the value of MSS lies between 0 and 1. 0 represents low stability and 1 indicates higher stability. Figure 11 shows the overall results for the proposed security technique over the variable number of data sets. Factually, the data instances are bootstrapped to 250000 for determining optimal results.

Reliability is another vital performance parameter in the current domain of study. Specifically, it deals with the durability of the proposed technique for attacks that can be carried out. In other words, the reliability performance is mapped using the failure rate, in case any data attack is performed in the current technique. Figure 12 shows the overall results of reliability for the proposed technique. It can be seen that in the current scenario, the proposed model can register enhanced reliability of 90.01% for different data instances in comparison to 85.26% for the baseline technique. It shows that the presented technique is more reliable for data security attacks variable attacks.

## 7. Open Issues

Blockchain, AI, and UAVs are being used in a wide range of applications, including healthcare, defense, smart cities, and the smart grid. Despite the many advantages of integrating drones with blockchain, AI, and 5G, there are still several issues that must be overcome. As seen in Figure 13, the main research problems of the suggested strategy are discussed below.

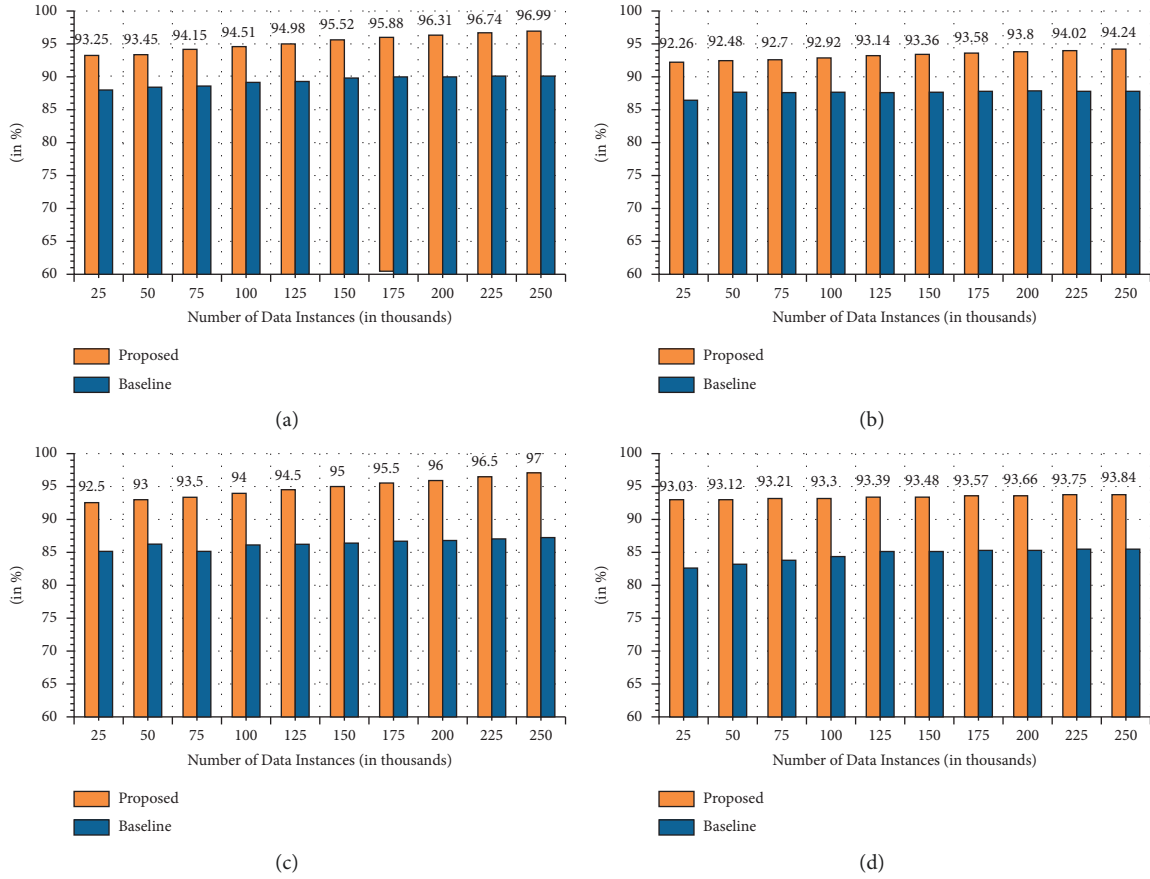


FIGURE 10: Statistical performance. (a) Precision. (b) Specificity. (c) Sensitivity. (d) *F*-measure.

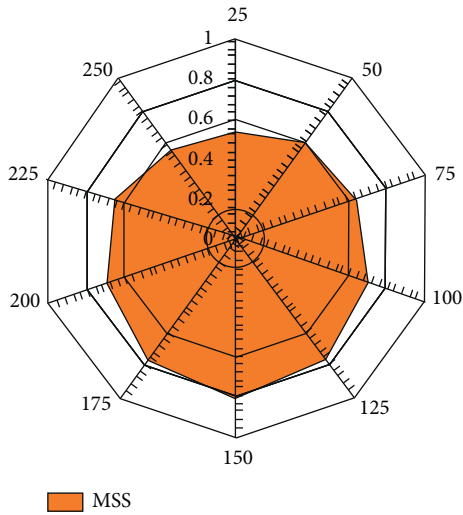


FIGURE 11: Stability analysis.

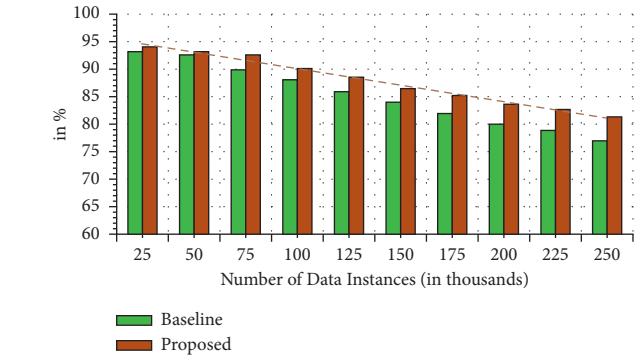


FIGURE 12: Reliability analysis.

(1) *Privacy*: to ensure the proposed scheme’s participants’ data privacy, the blockchain used in the proposed scheme is public and available to all of its participants. As a result, although data collection and storage on the blockchain increase security and improve UAV communication performance, sensitive information about users is also available. This

raises concerns about the privacy of blockchain data, and corporations are limiting the use of the blockchain as a result. There is a great deal of demand for blockchain privacy-preserving technologies.

(2) *Difficulty of computation*: UAV communication security and network performance will be improved with the proposed system’s usage of AI and 5G as an intermittent technology. Here, 5G enables tremendous data speeds and ultralow latency, resulting in massive amounts of data being generated. With so much data being created, the edge-AI algorithm (limited space and compute capacity) cannot manage it.

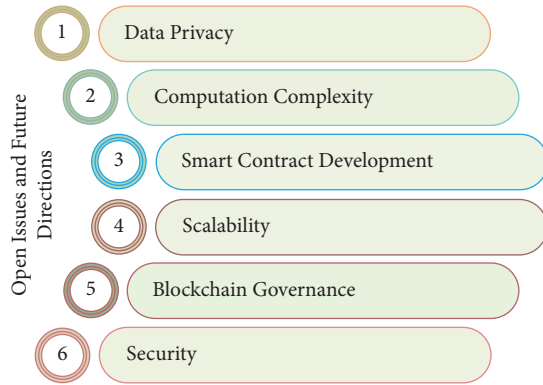


FIGURE 13: Open issues and challenges.

- (3) *Development of smart contracts* because smart contracts are immutable, it forces programmers to take extra care when creating them. The blockchain network can be severely damaged if a smart contract has a flaw or software vulnerability. To ensure the safety and security of the blockchain network, engineers must conduct a security and vulnerability evaluation.
- (4) *Ability to scale up* for the blockchain-aided UAV network, this is one of the most pressing issues to address. A blockchain conducts an average of 12 transactions per second, which is too slow for a 5G network. Blockchain's performance is appalling in comparison to social media platforms like Facebook, Instagram, and Twitter, which process millions of transactions every second. Because of this, the blockchain network must be made more scalable.
- (5) *Chain of command* in a public blockchain network that is completely decentralized and distributed, deploying and managing a distributed ledger (shared by several participants) is a difficult undertaking. Issues such as who oversees, manages, and troubleshoots the blockchain network emerge even in private/consortium blockchain. Other concerns include who is responsible for creating and deploying smart contracts, how disputes are resolved, and the rules and norms that govern blockchain. A strong and efficient blockchain governance paradigm is therefore required.
- (6) *Protection* using public-key cryptography, a blockchain network's data are protected from unauthorized access (digital signatures). Quantum computing, a futuristic notion, has the potential to decrypt public key encryption. By 2027, researchers predict that quantum computing will be able to compromise the blockchain's security. As a result, a quantum-secure blockchain network is required.
- (7) *Delay in data processing* many different sensors on UAVs can create a vast quantity of data, which can lead to suboptimal solutions due to the battery constraints of UAVs (not entirely correct).
- (8) *Standardization of the blockchain* companies have yet to settle on how to use blockchain technology. As

a result, the establishment of a real-time UAV network may impede its use.

## 8. Conclusion

IoT formulates a significant domain for provisioning real-time services in UAV applications. In the current research, security and privacy risks associated with the UAV system are addressed using a novel blockchain technique. With the proposed architecture, UAV-based applications can collect sensed data via a trustworthy platform. Specifically, the proposed framework is designed to remove storage constraints in the IoT environment. Moreover, a novel consensus algorithm is proposed with a reputation assessment system. Conspicuously, data gathering in real-time ensures integrity, confidentiality, and availability. Finally, a working prototype is proposed based on the proposed UAV system and tested in a real-world environment for performance enhancement. Based on the results, optimal results were registered in terms of statistical parameters of temporal efficacy, stability, reliability, and security analysis. For future works, research can be performed on communication-based data security. Moreover, network drop-constraint is another direction of research in the current domain.

## Data Availability

The data that support the findings of this study are available on request from the corresponding author.

## Conflicts of Interest

The authors declare that there are no conflicts of interest.

## Acknowledgments

The authors extend their appreciation to the Deputyship for Research and Innovation, Ministry of Education, in Saudi Arabia for funding this research work through the project number IF-PSAU-2021/01/17795.

## References

- [1] J. Won, Do-Y. Kim, Y.-Ik Park, and J.-W. Lee, "A Survey on Uav Placement and Trajectory Optimization in Communication Networks: From the Perspective of Air-To-Ground Channel Models," *ICT Express*, 2022.
- [2] Y. J Ahmad, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," in *Proceedings of the 2012 IEEE Conference on Technologies for Homeland Security (HST)*, pp. 585–590, IEEE, Waltham, MA, USA, November 2012.
- [3] I Lunsford and T. H. Bradley, "Evaluation of unmanned aerial vehicle tactics through the metrics of survivability," *The Journal of Defense Modeling and Simulation*, SAGE Publications Sage UK, London, England, 2021.
- [4] A. Wyatt, *The Disruptive Impact of Lethal Autonomous Weapons Systems Diffusion: Modern Melians and the Dawn of Robotic Warriors*, Routledge, Oxfordshire, England, UK, 2021.

- [5] M. A. Akhlofi, A. Couturier, and N. A. Castro, "Unmanned aerial vehicles for wildland fires: sensing, perception, cooperation and assistance," *Drones*, vol. 5, no. 1, p. 15, 2021.
- [6] S. Zudaire, F. Gorostiaga, C. Sánchez, G. Schneider, and S. Uchitel, "Assumption monitoring using runtime verification for uav temporal task plan executions," in *Proceedings of the 2021 IEEE International Conference on Robotics and Automation (ICRA)*, pp. 6824–6830, IEEE, Xi'an, China, May 2021.
- [7] P. Alemany, R. Vilalta, R. Muñoz, R. Casellas, and R. Martínez, "Evaluation of the abstraction of optical topology models in blockchain-based data center interconnection," *Journal of Optical Communications and Networking*, vol. 14, no. 4, pp. 211–221, 2022.
- [8] S. Alsamhi, F. Afghah, R. Sahal et al., "Green internet of things using uavs in b5g networks: a review of applications and strategies," *Ad Hoc Networks*, vol. 117, Article ID. 102505, pp. 1–15, 2021, <https://reader.elsevier.com/reader/sd/pii/S1570870521000639?token=703434D7A18035BA8917A0858D4266353ACF9089355D96F71284F46488B98223733C165FB0FA1515D62D6C4F2546E9B4&xoriginRegion=eu-west-1&xoriginCreation=20220818194053>.
- [9] Y. Chen, W. Feng, and G. Zheng, "Optimum placement of uav as relays," *IEEE Communications Letters*, vol. 22, no. 2, pp. 248–251, 2018.
- [10] C. Ge, C. Yin, Z. Liu, L. Fang, J. Zhu, and H. Ling, "A privacy preserve big data analysis system for wearable wireless sensor network," *Computers & Security*, vol. 96, no. 1–10, p. 101887, 2020.
- [11] M. Hooper, Y. Tian, R. Zhou et al., "Securing commercial wifi-based uavs from common security attacks," in *Proceedings of the MILCOM 2016-2016 IEEE Military Communications Conference*, pp. 1213–1218, IEEE, Baltimore, MD, USA, November 2016.
- [12] C. Ge, Z. Liu, J. Xia, and L. Fang, "Revocable identity-based broadcast proxy re-encryption for data sharing in clouds," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1214–1226, 2021.
- [13] C. Ge, W. Susilo, J. Baek, Z. Liu, J. Xia, and L. Fang, "Revocable attribute-based encryption with data integrity in clouds," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1214–1226, 2021.
- [14] C. Ge, W. Susilo, J. Baek, Z. Liu, J. Xia, and L. Fang, "A verifiable and fair attribute-based proxy re-encryption scheme for data sharing in clouds," *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2021.
- [15] A. Kanuparthi, K. Ramesh, and S. Addepalli, "Hardware and embedded security in the context of internet of things," in *Proceedings of the 2013 ACM Workshop on Security, privacy & dependability for cyber vehicles*, pp. 61–64, Berlin, Germany, November 2013.
- [16] S. Misra, P. V. Krishna, H. Agarwal, A. Saxena, and M. S. Obaidat, "A learning automata based solution for preventing distributed denial of service in internet of things," in *Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, pp. 114–122, IEEE, Dalian, China, October 2011.
- [17] D. Rudinskis, Z. Goraj, and J. Stankūnas, "Security analysis of uav radio communication system," *Aviation*, vol. 13, no. 4, pp. 116–121, 2009.
- [18] L. L. T. Vrizlynn and J. Wu, "Autonomous vehicle security: a taxonomy of attacks and defences," in *Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE green Computing and Communications (Greencom) and IEEE Cyber, Physical and Social Computing (Cpscom) and IEEE Smart Data (Smartdata)*, pp. 164–170, IEEE, Chengdu, China, December 2016.
- [19] C. G. L. Krishna and R. R. Murphy, "A review on cyber-security vulnerabilities for unmanned aerial vehicles," in *Proceedings of the 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*, pp. 194–199, IEEE, Shanghai, China, October 2017.
- [20] D. Radu, A. Cretu, P. Benoit, J. Yi, C. Avram, and A. Astilean, "Flying ad hoc network for emergency applications connected to a fog system," *International Conference on Emerging Internetworking, Data & Web Technologies*, vol. 17, pp. 675–686, 2018.
- [21] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing uav communications via joint trajectory and power control," *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 1376–1389, 2019.
- [22] P. Alemany, R. Vilalta, R. Muñoz, R. Casellas, and R. Martínez, "Blockchain-based connectivity provisioning in multiple transport sdn domains," in *Proceedings of the 2021 International Conference on Optical Network Design and Modeling (ONDM)*, pp. 1–3, IEEE, Gothenburg, Sweden, July 2021.
- [23] M. Singh, G. S. Aujla, A. Singh, N. Kumar, and S. Garg, "Deep-learning-based blockchain framework for secure software-defined industrial networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 606–616, 2021.
- [24] M. Saalim Jamal, A. Hirwe, and K. K. Vibhajan, "A lightweight and scalable control plane management for multi-controller sdn," in *Proceedings of the 2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, November 2018.
- [25] K. Tolga Bagci and A. Murat Tekalp, "Sdn-enabled distributed open exchange: dynamic qos-path optimization in multi-operator services," *Computer Networks*, vol. 162, no. 1–10, p. 106845, 2019.
- [26] P. Fernando and W. Jin, "Blockchain-powered software defined network-enabled networking infrastructure for cloud management," in *Proceedings of the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, January 2020.
- [27] D. Chattaraj, S. Saha, B. Bera, and A. K. Das, "On the design of blockchain-based access control scheme for software defined networks," in *Proceedings of the IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 237–242, IEEE, Toronto, ON, Canada, July 2020.
- [28] D. Tan, L. D. Nguyen, T. Q. Duong, S. R. Khosravirad, and H. Claussen, "Joint optimisation of real-time deployment and resource allocation for uav-aided disaster emergency communications," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 11, pp. 3411–3424, 2021.
- [29] L. Xiao, H. Zhu, S. Xiang, and P. Cong, "Modeling and verifying sdn under multi-controller architectures using csp," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 2, 2021.
- [30] Z. Yao, W. Cheng, W. Zhang, and H. Zhang, "Resource allocation for 5g-uav-based emergency wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 11, pp. 3395–3410, 2021.
- [31] A. Dhar Dwivedi, R. Singh, S. Dhall, G. Srivastava, and K. Saibal, "Tracing the source of fake news using a scalable blockchain distributed network," in *Proceedings of the 2020 IEEE 17th International Conference on Mobile Ad Hoc and*

- Sensor Systems (MASS)*, pp. 38–43, Delhi, India pages, December 2020.
- [32] G. Srivastava, J. Crichigno, and S. Dhar, “A light and secure healthcare blockchain for iot medical devices,” in *Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, pp. 1–5, Edmonton, AB, Canada, May 2019.
- [33] K. T Deepak, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and N. Laurent, “Security implications of blockchain cloud with analysis of block withholding attack,” in *Proceedings of the 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, pp. 458–467, IEEE, Madrid, Spain, May 2017.
- [34] D. Ali, S. S. Kanhere, and J. Raja, “Blockchain in Internet of Things: Challenges and Solutions,” 2016, <https://arxiv.org/abs/1608.05187>.
- [35] J. Yang, Z. Lu, and J. Wu, “Smart-toy-edge-computing-oriented data exchange based on blockchain,” *Journal of Systems Architecture*, vol. 87, pp. 36–48, 2018.
- [36] X. Li, Y. Wang, P. Vijayakumar, D. He, N. Kumar, and J. Ma, “Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11309–11322, 2019.
- [37] M. Scarlato, C. Perra, M. Yaseen Jabarulla, G. Jung, and H. No Lee, “A Blockchain for the Collision Avoidance and the Recovery of Crashed Uavs,” *Proceedings of the Korean Institute of Electronics Engineers Conference*, pp. 463–467, 2019.
- [38] Y. Zhu, G. Zheng, and K.-K. Wong, “Blockchain-empowered decentralized storage in air-to-ground industrial networks,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3593–3601, 2019.
- [39] A. Kuzmin and E. Znak, “Blockchain-base structures for a secure and operate network of semi-autonomous unmanned aerial vehicles,” in *Proceedings of the 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, pp. 32–37, IEEE, Singapore, July 2018.
- [40] S Bel Hadj Youssef, S. Rekhis, and N. Boudriga, “A blockchain based secure iot solution for the dam surveillance,” in *Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, IEEE, Marrakesh, Morocco, April 2019.
- [41] T. Rana, A. Shankar, M. Kamran Sultan, R. Patan, and B. Balusamy, “An intelligent approach for uav and drone privacy security using blockchain methodology,” in *Proceedings of the 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, pp. 162–167, IEEE, Noida, India, January 2019.
- [42] A. Islam and S. Y. Shin, “BUS: a blockchain-enabled data acquisition scheme with the assistance of UAV swarm in internet of things,” *IEEE Access*, vol. 7, pp. 103231–103249, 2019.
- [43] N. Fatima, P. Saxena, and M. Gupta, “Integration of multi access edge computing with unmanned aerial vehicles: current techniques, open issues and research directions,” *Physical Communication*, vol. 52, Article ID 101641, 2022.
- [44] M. S. Rahman, I. Khalil, and M. Atiqzaman, “Blockchain-powered policy enforcement for ensuring flight compliance in drone-based service systems,” *IEEE Network*, vol. 35, no. 1, pp. 116–123, 2021.
- [45] I. A. Elnabty, Y. Fahmy, and M. Kafafy, “A survey on uav placement optimization for uav-assisted communication in 5g and beyond networks,” *Physical Communication*, vol. 51, Article ID 101564, 2022.
- [46] J. Lee, K. Kim, H. Kim, and H. Kim, “Devising geographic diffusion for drone networks,” in *Proceedings of the 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 76–78, IEEE, Vienna, Austria, July 2016.
- [47] R. Karem, M. Ahmed, and F. Newagy, “Resource allocation in uplink noma-iot based uav for urlcc applications,” *Sensors*, vol. 22, no. 4, p. 1566, 2022.
- [48] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system,” *Decentralized Business Review*, 2008, [https://www.researchgate.net/publication/228640975\\_Bitcoin\\_A\\_Peer-to-Peer\\_Electronic\\_Cash\\_System](https://www.researchgate.net/publication/228640975_Bitcoin_A_Peer-to-Peer_Electronic_Cash_System).
- [49] X. Xu, X. Zhang, H. Gao, Y. Xue, L. Qi, and W. Dou, “Become: blockchain-enabled computation offloading for iot in mobile edge computing,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4187–4195, 2020.
- [50] C. Natoli, J. Yu, V. Gramoli, and P. Esteves-Verissimo, “Deconstructing Blockchains: A Comprehensive Survey on Consensus, Membership and Structure,” arXiv preprint arXiv:1908.08316, 2019.
- [51] J. Modares, N. Mastronarde, and K. Dantu, “Ub-anc emulator: an emulation framework for multi-agent drone networks,” in *Proceedings of the 2016 IEEE International Conference on Simulation, Modeling, and Programming for Autonomous Robots (SIMPAN)*, pp. 252–258, IEEE, San Francisco, CA, USA, December 2016.