Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.039381
Article

Enhancement of UAV Data Security and Privacy via Ethereum Blockchain Technology

Sur Singh Rawat[1,*], Youseef Alotaibi[2], Nitima Malsa[1] and Vimal Gupta[1]

[1]Department of Computer Science and Engineering, JSS Academy of Technical Education, Noida, 201301, India
[2]Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Makkah, 21955, Saudi Arabia

*Corresponding Author: Sur Singh Rawat. Email: sur.rawat@jssaten.ac.in

Received: 25 January 2023; Accepted: 01 June 2023; Published: 30 August 2023

Abstract: Unmanned aerial vehicles (UAVs), or drones, have revolutionized a wide range of industries, including monitoring, agriculture, surveillance, and supply chain. However, their widespread use also poses significant challenges, such as public safety, privacy, and cybersecurity. Cyberattacks, targeting UAVs have become more frequent, which highlights the need for robust security solutions. Blockchain technology, the foundation of cryptocurrencies has the potential to address these challenges. This study suggests a platform that utilizes blockchain technology to manage drone operations securely and confidentially. By incorporating blockchain technology, the proposed method aims to increase the security and privacy of drone data. The suggested platform stores information on a public blockchain located on Ethereum and leverages the Ganache platform to ensure secure and private blockchain transactions. The MetaMask wallet for Ethbalance is necessary for BCT transactions. The present research finding shows that the proposed approach's efficiency and security features are superior to existing methods. This study contributes to the development of a secure and efficient system for managing drone operations that could have significant applications in various industries. The proposed platform's security measures could mitigate privacy concerns, minimize cyber security risk, and enhance public safety, ultimately promoting the widespread adoption of UAVs. The results of the study demonstrate that the blockchain can ensure the fulfillment of core security needs such as authentication, privacy preservation, confidentiality, integrity, and access control.

Keywords: Unmanned aerial vehicles (UAVs); blockchain; data privacy; network security; smart contract; Ethereum

1 Introduction

Unmanned aerial vehicles (UAVs) are currently making inroads into a multitude of industries, increasing their market domination. There is now a lot of study being done on UAV communication issues and how to address their flaws. Due to a lack of physical infrastructure, it is frequently difficult to access certain locations. Drones enable us to do this. Drones are so often utilized in a range of industries, including agriculture, forestry, environmental protection, and security, for essential tasks like rescue, surveillance, and transportation. UAVs are becoming useful commercial instruments in the civilian sector thanks to recent developments in operation, network technology, communication, and manufacturing methods, which have allowed them to move beyond their defensive applications [1–5]. Both the public and private sectors of the economy are welcoming their introduction [6], and the industry is now presented with significant market opportunities [7]. However, as UAVs gain wider acceptance, their limitations are also becoming increasingly evident.

Since UAVs are now widely used, companies that sell items have developed a new mode of transportation that offers quicker delivery at less expensive prices for delivering goods to clients. As an example, Amazon has recognized the advantages of integrating drones and related technology into their current delivery process. This has led to quicker delivery times, as stated in [8,9]. This will benefit Amazon's supplychain management systems as the corporation has boosted its research and development spending on UAVs [10,11].

UAVs are less likely to be lost, physically taken over, or destroyed in open environments, but language hurdles impede attempts to attack the software that creates them [12–15]. UAV security, data management and storage, intra-UAV communication, and air data security are only a few of the issues with UAV networks that need to be handled because of the globalization of UAV technology.

A UAV ad-hoc network (UAANET) must be protected from hostile actors interfering with or disrupting data transmission and exchange since drones and ground control stations (GCS) interact by utilizing open wireless channels [16,17]. The usefulness of virtual circuit (VC)-based applications has significantly increased in the present era due to the inclusion of speed and altitude-supporting mechanisms. When deployed and operated appropriately, these technologies have the potential to be highly reliable and cost-effective wireless communication solutions for a range of issues, as referenced in [18,19]. For instance, many countries utilized UAV technology to monitor drone activity and track them, which can also function as Aerial User Equipment (AUE), which are surveillance drones designed to coexist with ground users and are sometimes referred to as cellular-connected UAVs [20,21].

However, it is vital to remember that modern UAV and drone systems, which entail diverse networking technologies and a high rate of utilization, must be well-protected to be used easily across many sectors of human life. The risk of VC-based devices (UAVs, drones, and Internet of Things (IoT) devices) is evaluated by considering the surrounding environment, weather, and geographical factors [22,23]. Additionally, there are technical factors to take into account, such as network protocols, communication privacy, and the use preventative measures [24–26]. When it comes to data security, UAVs and drones face comparable risks.

Various communication technologies have been developed to reduce the risks associated with network protocols used in these devices [27,28]. For drones and UAV systems, researchers have identified cryptography-based methods as potential solutions to reduce risks [29,30]. However, mitigating the risks of signal data compromise remains challenging, especially in adverse weather conditions. To determine the optimal technique for risk identification and data preservation, cutting-edge technologies such as machine learning, cryptography, network communication systems, and radar systems have been researched. As part of this study, BCT [31,32] has been proposed as a potential solution for risk reduction, data protection, and maintenance, especially in VC-based devices.

Different sectors have implemented applications based on blockchain to offer infrastructure for service, data, and business levels while also guaranteeing top-notch security. The usage of secure technology like blockchain can establish a protective system against the growing instances of cyber threats in the UAV network [33–35].

As a distributed ledger, blockchain ensures that every node in the network has a copy of all the data, and the blockchain network cannot be corrupted or destroyed even if a hacker attack or eliminates all the UAVs in it [36]. By employing blockchain, data security can be improved, and malicious nodes can be kept from joining the network. The current effort aims to enhance the privacy and security of the UAV network using blockchain technology.

In this study, the distributed, safe, and fair deep learning platform DeepChainis introduced. DeepChain offers a value-driven incentive mechanism that is based on the Blockchain to push players to behave properly. DeepChain, in the meantime, makes sure that each participant's data is secure and provides audibility during the entire training process. This work constructs a DeepChain prototype and conducts testing using a real dataset in a variety of circumstances; the results show that our DeepChain is promising [37,38].

The structure of the paper is as follows: Section 2 provides a thorough review of the literature. Section 3 explains the proposed approach and its related applications. The last paragraph of the Section 4 describes the findings and performance analysis. The paper concludes with a summary and suggestions for future research.

1.1 Motivation

IoD, which stands out for its usability, adaptability, and mobility, is a vital component of the forthcoming Internet of Things. IoD applications are becoming more prevalent in both military and non-military domains. Drones, however, have limited resources and are extremely susceptible to various security concerns and assaults. IoD network security on the blockchain is getting more and more attention.

The study demonstrates that blockchain technology can fulfill fundamental security requirements, including authentication, privacy protection, and confidentiality, integrity, and access control. Drones are vulnerable to various hazards based on their characteristics and methods of operation. The attacks are classified into three categories: device-based attacks, network-based attacks, and software based attacks.

- **Attacks using devices** attempt to physically access drone parts, such as memory, to steal sensitive information or seize control of the drone.
- **Attacks that use networks** involve attacks where an attacker can intercept and change the sent data, such as man-in-the-middle, replay, eavesdropping, and modification attacks.
- **Attacks based on software** intent to introduce harmful data into drones and ground stationsto take advantage of software flaws. Denial of service/distributed denial of service (DoS/DDoS) attacks can be launched using them.

To defend against the aforementioned attacks, it is essential to provide the fundamental security properties of confidentiality, integrity, availability, authentication, and privacy preservation. By upholding confidentiality, communication is protected against unauthorized access and the potential for data leakage.

- Integrity ensures that data transmissions are free from tampering or modification.
- Access to resources or services offered to authorized drones or users is maintained by availability.
- Before data access or exchange, authentication requires confirming identification.

- Privacy protection stops malicious attackers from revealing personal information without consent.

The work proposes a technique for maintaining the integrity of acquired data while also safeguarding drone connectivity during data transmission and collection. The paper anchors the drone-collected hashed data records rather than simply adding the drone to the blockchain network. The paper suggests anchoring the hashed data records collected by drones rather than merely integrating the drones into the blockchain network. To ensure data integrity, the research recommends safeguarding the collection and communication of drone data when employing a public blockchain. The findings indicate that this approach creates a reliable, scalable, and decentralized system that guarantees drone data protection and resilience with minimal overhead.

1.2 Contribution

The contribution of the research effort is outlined as follows:

- To detect assaults, this paper keeps a watch on all blockchain transactions (data transmitted by each node, timestamp of each transaction, and routing table of each node). Transaction data cannot be altered because blockchains are immutable, maintaining data integrity.
- To establish confidence between participating network nodes, token transactions take place in the blockchain. Additionally, in exchange for ensuring the legality of the route to the originating node, the intermediary nodes pay ethers as a guarantee for successful transmission.
- The suggested model was experimentally evaluated and the findings revealed that it outperforms the referred state-of-the-art technique.

The remaining portions of this work are organized as follows: In Section 2 of the proposed design, the characteristics of blockchain and associated difficulties are discussed. The suggested strategy is highlighted in Section 3, which also discusses the notion of node registration in the UAV Network, the flow of data transactions and, contract functions in the blockchain. The implementation information and underlying algorithms for the planned system are described in Section 5. Section 6 discusses the detail of the outcomes and conclusions from the simulation of the suggested strategy. The paper's conclusion and possible next measures should be followed.

2 Related Work

This section presents the preliminary steps and the related work that isimportant for the suggested work.

2.1 Unmanned Aerial Vehicle Systems (UAVs)

The UAV system is composed of the GCS, components from the aircraft, and sensor payloads. UAVs can be flown using either ground-based control equipment or onboard electronics [39]. The UAVs cooperate to control and guide traffic, transfer data for transmission from source to destination, and remotely sense the UAVs and the GCS [40]. UAANET security can be improved by addressing the issues caused by the CIA trinity (Confidentiality, Integrity, and Availability).

2.2 Blockchain Technology

Blocks of transactional records are preserved in a blockchain, which is a decentralized, impermeable ledger [41]. A block is added to the blockchain permanently after transaction verification [42].

To link to the block preceding it, every block makes use of a unique identifier. Every time a data block is changed, a unique identity is altered, and all users are made aware of the change. The nodes disapprove of all such modified blocks. The blockchain network, a robust platform for collaborative record keeping, is challenging to alter or eliminate.

Its distributed, constant nature, absence of centralized approval, and security are increased. Blockchain technology and public key infrastructure (PKI) are used in this work to encrypt data [43]. As is done in the present study, automating dynamic UAV systems can be accomplished by utilizing consensus procedures and smart contracts. Traceability and automated business logic application properties of the blockchain serve as its driving forces [44,45]. Asymmetric encryption is used to guarantee the authenticity of the matching UAV's signature. Data alteration by malicious, illegal individuals is significantly less likely thanks to blockchain technology [46]. The unique security issues related to the use of drones in society were described in detail in a paper [47]. This paper addressed some of hazards, challenges, and scientific gaps in the use of this technology.

The study does not, however, focus on presenting practical answers to the raised issues with drone usage. Reference [48] have provided a model that takes drone, IoD, and unmanned aerial vehicle (UAV) considerations into account (UAV). The significance of privacy and network management has been emphasized in this study. The paper describes how network components like the 5G Network and the Global Positioning System, which are utilized to operate UAVs, work. Reference [49] refers to the unethical monitoring and control of UAVs utilizing data, which is often done by unauthorized individuals. The study puts a lot of focus on the BCT technique's ability to secure data privacy, preserve UAV, and drone communication data**.**

The blockchain network is a promising choice for trust management because it has been present and active in several research areas, including wireless networks [50] and the IoT [51–53]. The UAV ad-hoc network's resource restriction is essential for developing a trust management system that makes use of the decentralised blockchain. Drone delivery by Dorado Platform, Walmart's package tracking system, and drone package delivery are just a few of the well-known projects fusing drones and the blockchain technology that many researchers have even used. When adopting blockchain, security and, privacy of data are two important considerations. Studies on certain articles dealing with data security and privacy issues have been conducted.

The paper suggested a new methodology that reduces the number of operations required to produce secret keys by utilizing elliptic curve cryptography [54]. The next step has been the presentation of research difficulties and future directions for further developing the suggested system [55,56].

Blockchain is a technology that aims to improve product traceability and increase operational openness. However, there is not much discussion about blockchain usage, which suggests that its motivating factors need to be examined. The research identifies the drivers of blockchain adoption at a time when information technology is gaining attention. The Neutrosophic-based robust ranking analyses driving variables, giving drivers priority. Regarding the effect of the presented work on the adoption of blockchain operations in supply chain performance systems, the outcomes vastly outrank the drivers. It offers administrators a methodical strategy for integrating blockchain technology into supply chain operations. Table 1 provides the summary of the literature study in this work.

Table 1: Summary of the literature survey

Reference No.	Published year	Description
[39]	2010	1. This article discusses the performance analysis of mobile ad hoc unmanned aerial vehicle (UAV) communication networks with directional antennas. 2. The authors propose a new algorithm called Directional Routing Algorithm for Mobile Ad Hoc Networks with UAVs (DREAM). 3. The algorithm is designed to reduce the number of hops required for data transmission in a UAV network, improve the quality of service, and reduce power consumption
[40]	2020	1. The article discusses the potential benefits of using blockchain technology to enhance the security of unmanned aerial vehicle (UAV) communication networks. 2. The authors explore the various challenges and research issues related to the integration of blockchain and UAV technology.
[41]	2022	1. The article proposes the use of blockchain technology to improve the privacy and security of unmanned aerial vehicle (UAV) networks. 2. The authors present a blockchain-based protocol for UAVs that use smart contracts to manage the network's privacy and security policies
[42]	2017	1. The article proposes a rendezvous point estimation algorithm that considers drone speed and data collection delay for data gathering in UAV networks. 2. The algorithm aims to reduce the time taken to collect data and improve network performance.
[43]	2019	1. The article proposes an intelligent approach for UAV and drone privacy security using blockchain methodology. 2. The authors present a blockchain-based protocol that uses smart contracts and consensus algorithms to manage the security and privacy of UAV networks
[44]	2020	1. The article proposes a reinforcement learning approach for blockchain-enabled IoT monitoring applications. 2. The authors explore the potential benefits of using blockchain technology to enhance the security and reliability of IoT monitoring systems
[45]	2019	1. The article proposes an agent-based approach inspired by the principles of blockchain to enhance the security of networks of unmanned aerial vehicles (UAVs) for surveillance. 2. The authors present a security model that uses intelligent agents to detect and mitigate attacks on UAV networks

(Continued)

Table 1 (continued)

Reference No.	Published year	Description
[46]	2018	1. The article proposes the use of blockchain technology as a decentralized security framework for protecting IoT devices. 2. The authors explore the potential benefits of using blockchain technology to enhance the security and privacy of IoT networks
[47]	2019	1. The article presents a comprehensive review of the threats, challenges, solution mechanisms, and scientific gaps related to security and privacy in the age of drones. 2. The authors explore the potential benefits of using blockchain technology to address the security and privacy challenges posed by drones.
[48]	2020	1. The article presents a review of research relevant to emerging industry trends, including Industry 4.0, IoT, blockchain, and business analytics. 2. The authors explore the potential benefits of using these technologies to improve business operations and increase efficiency.
[49]	2021	1. The article proposes a blockchain-based soybean traceability system for agricultural supply chains. 2. The authors present a blockchain-based protocol that allows consumers to track the origin and quality of soybean products
[50]	2018	1. The article discusses the potential benefits of using blockchain technology as a decentralized security framework. 2. The authors explore the various applications of blockchain technology in enhancing the security and privacy of IoT networks
[51]	2021	1. This article proposes a blockchain based framework for Intelligent Transportation System(ITS) 2. With a focus on privacy preservation for secure and reliable communication.
[52]	2019	1. This article proposes a trust management framework, called Trustchain, for supply chains that are supported by blockchain and the Internet of Things (IoT) technologies. 2. The framework aims to provide a secure and trustworthy supply chain by ensuring the authenticity and integrity of the data exchanged among different parties. 3. The article presents a detailed design of the Trustchain framework and evaluates its effectiveness through simulation-based experiments.
[53]	2022	1. This article proposes an intelligent adaptive optimization method for enhancing information security in IoT-enabled environments.

(Continued)

Table 1 (continued)

Reference No.	Published year	Description
		2. The method aims to optimize the allocation of resources to enhance the security of IoT systems by using machine learning and optimization techniques. 3. The article presents a detailed design of the proposed method and evaluates its effectiveness through simulation-based experiments.
[54]	2022	1. This article proposes a Device Access Control and Key Exchange (DACK) protocol for the Internet of Things (IoT). 2. The protocol aims to provide a secure and efficient way for IoT devices to access each other while maintaining confidentiality and privacy. 3. The article presents a detailed design of the DACK protocol and evaluates its effectiveness through simulation-based experiments.
[55]	2021	1. This article discusses the potential of using blockchain technology to enhance the security of communication among Unmanned Aerial Vehicles (UAVs) in the 6G environment. 2. The article presents a detailed architecture for a blockchain-based UAV communication system and discusses the opportunities and challenges associated with its implementation.
[56]	2022	1. This article proposes an autonomous air combat decision-making framework for UAVs based on parallel self-play reinforcement learning. 2. The framework aims to enable UAVs to make independent decisions in air combat scenarios based on self-learning and decision-making. 3. The article presents a detailed design of the proposed framework and evaluates its effectiveness through simulation-based experiments

3 Proposed Work

The present study proposes using a smart contract to enhance security in the UAV network and mitigate various network threats. As smart contracts are decentralized and unchangeable, they provide a secure means for data transmission and communication in the UAV network. The proposed technology can help prevent threats like black holes, gray holes, DOD, and ensue confidentiality and integrity of the data.

The research proposes a Block chain technology (BCT)-based approach to minimize risks associated with data management in UAV and drone systems. The proposed method aims to enhance data storage and privacy measures through features like immutability, tamper proofing, transparency, security, and efficient distribution mechanisms. Drones, UAVs, and IOT devices are typically equipped with various sensors that facilitate the completion of pre-defined tasks according to the application chosen by user.

Drones or UAVs are used for these jobs, and they are controlled and observed locally or remotely using a network connection system. The proposed architecture of the proposed drone system as shown in Fig. 1 using the Ethereum blockchain consists of mainly four components as described below.

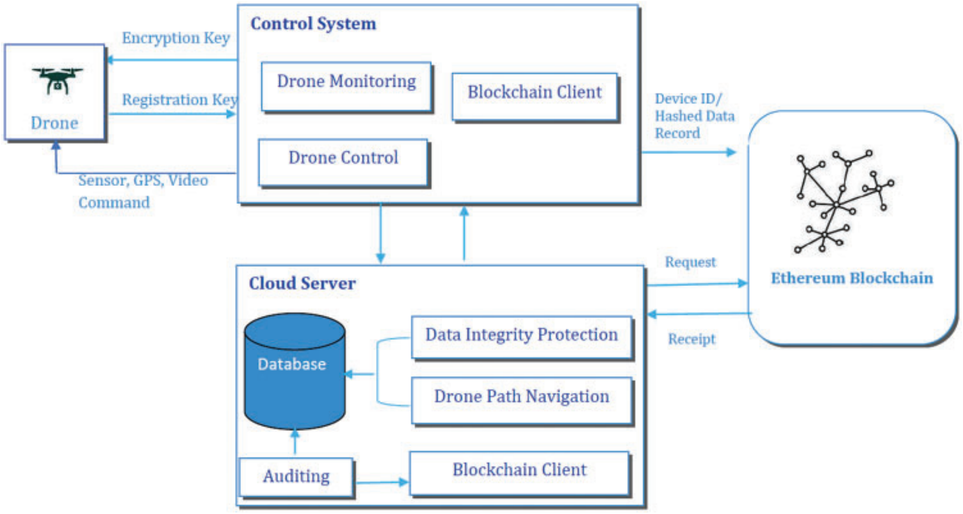


Figure 1: Proposed drone system architecture using Ethereum blockchain

3.1 Cluster of Drones

To order to do difficult tasks, one or more drones may band together to form a drone cluster. The cluster of drones can utilize sensors to collect physical data and embedded cameras to shoot photographs and films in the field. Drones need to be connected to a control system to transmit or receive commands and information about the state of their flight. Alternatively, by using a representative drone, this communication can happen directly.

3.2 Control System

A Control system can be allocated to and in communication with a drone cluster for the data gathering and command dissemination. The control system is in charge of giving drones instructions to adjust their flight route and various other physical parameters after receiving data from individual drones or drone clusters.

The control system functions as an intermediary that gathers information from drones, encrypts the data to ensure its authenticity, and transmits it to the blockchain network and cloud, both in its original and encrypted forms. The control system also follows the same process for its command data, creating an enduring log for monitoring purposes.

3.3 Cloud Server

The cloud server stores a vast amount of data gathered by the drones, and it conducts real-time processing and analysis to support future decision-making. The database on the cloud server is continuously updated with new information. It holds records of the original drone data, control system commands, cloud server data, and auditor data. Access to the data is monitored, and each entry is marked with a unique fingerprint that is logged in the database. To ensure accuracy, a daemon process checks the information stored in the database and the blockchain network at regular intervals.

Both the command and object data are trackable. Once a data breach or leak has been identified, the hostile entity can be traced and tracked down.

The cloud server is in charge of verifying the authenticity of data receipts by requesting a blockchain receipt from the blockchain network, which serves as a permanent record of data integrity. The cloud-based back-end system may also recover precise and quick feedback for additional drone manipulation, such as drone path routing, by utilizing machine learning algorithms. In the interim, advanced persistent threats (APTs) [6] and distributed denial of service (DDoS) attacks [7] can be early detected by analyzing the communication data between the server and the drone's control system as well as between those two systems.

3.4 Ethereum Blockchain

The blockchain is a decentralized network that is deployed for data validation and reliability. The blockchain network can be put to three different uses. For integrity protection and to ensure stability, each hashed data entry for the information gathered by drones and the instructions from the control system is uploaded to the blockchain network. Additionally, every database access and cloud server feedback transaction will be recorded on the blockchain for future auditing or study. Along with keeping the data records forever, a blockchain receipt will be given for data confirmation.

3.5 Data Security

Potential weaknesses have been examined for the implementation of Drone systems to provide a secure-aware architecture for drone data gathering and communication. The cloud server keeps a database to store data gathered by drones, but due to recognized flaws in cloud operating systems, it cannot ensure that data records will remain unmodified. Data security is done in two phases. In the first phase, data is encrypted using a hash function and then stored on the blockchain. Once the drone system is activated, the cloud server will be able to track the data, and the auditor will be given access to all the data operations, control orders, and monitoring data for the drones. The auditor, however, cannot be trusted. Hence, the gathered information or data can be altered.

Since the primary goal of a drone system employing blockchain is to safeguard the data. Hence, data is encrypted and stored in a chain of blocks, so that unauthorized users cannot access the data. To collect data through drones, they need to register first. **Algorithm 1** presents the Pseudo Code for Drone Registration smart contract for registering drones and control systems. For data storage on the cloud, encryption is done through encryption keys. Encryption keys are described as follows:

- ***Registration Keys***. The Drone needs to be registered with the system while collecting data. The Key for registration is denoted by KeyD. Every time a new data recordis generated, the registration key is needed. Similarly, the registration key for the control system is KeyC.
- ***Data Encryption Key (KeyE)***. Following registration, the drone creates the encryption key KeyE that will be used to encrypt all of the data. Drone encrypts data entries when they are made, allowing only authorized key holders to view the data. The hashed data entry will be stored on the blockchain each time a new data input is made.
- ***Data Access Public/Private Key Pair (KeyPB, and KeyPR)***. To access data, a public/private key pair is produced, designated as (KeyPB, KeyPR). In certain situations, the private key is utilized to produce an operator fingerprint that confirms the source of the data when recording data access activity on the blockchain. The public key is then used by the other parties to validate the stated origin.

The second phase of security is provided through a consensus algorithm embedded in the Ethereum blockchain itself. Proof of Work (PoW) consensus algorithm pseudo-code is presented in **Algorithm 2**. For hashing SHA256 hashing function is used which takes three inputs root node transaction, timestamp of the transaction, and previous node hash. Nonce (N_C) will be initialized by 0. Mining of the block will continue until the target difficulty (T_D) is greater than the new block. In this way, a new block can be added if 51% of nodes agree on that.

Algorithm 1: Pseudo Code for Drone Registration

```
// SPDX-License-Identifier: MIT
pragma solidity >= 0.5.22 < 0.9.0;
contract Drone{
structDroneR{
address owner;
string model;
uint256 registrationDate;}
mapping (address => Drone) public drones;
function registerDrone (string memory _model) public {
require(drones[msg.sender].isRegistered == false, “This address is already registered for a drone.”);
drones[msg.sender] = Drone(msg.sender, _model, block.timestamp, true); }
function unregisterDrone() public {
require(drones[msg.sender].isRegistered == true, “This address is not registered for a drone.”);
delete drones[msg.sender];}
function getDrone(address _owner) public view returns (address owner, string memory model, uint256 registrationDate, bool isRegistered) {
owner = drones[_owner].owner;
model = drones[_owner].model;
registrationDate = drones[_owner].registrationDate;
isRegistered = drones[_owner].isRegistered;}}
```

Algorithm 2: Pseudo Code for Proof of Work

```
Input X = SHA256hashFunction(TXR,TS , PR_hash)
Input NC = 0 //initial value for nonce
Start block Mining
Repeat NC++;
Until SHA256hashFunction(X, NC) < TD
End
```

The contract defines a DroneRstruct, which contains information about the drone’s owner, model, registration date, and whether or not it’s currently registered. The contract uses a mapping to associate each drone owner’s Ethereum address with their Drone struct.

The register Drone function allows a drone owner to register their drone by providing the model of their drone. The function checks to make sure that the sender’s address is not already registered for a drone and then adds the new drone to the mapping.

The unregister Drone function allows a drone owner to unregister their drone by deleting the Drone struct associated with their Ethereum address. The getDrone function allows anyone to query the contract to get information about a particular drone owner's drone. The function takes an Ethereum address as input and returns the drone owner's address, model, registration date, and whether or not the drone is currently registered.

4 Implementation Results

The Drone implementation process consists of seven steps as described below:

4.1 Drone and Control System Registration

The drone must register in our system as a node to save data gathered from a specific place. After registration, the phase of data gathering begins, and each drone will be given a special ID. The device ID will be connected to each data record. The type of data could include measurements, videos, or pictures. Each data record is treated as an object for ease of use and hashed before uploading to the blockchain network. The original data is simultaneously saved in a local database for later retrieval. For the control system to forward hashed data on the blockchain, the drone must first be registered.

4.2 Data Transmission Through System Controller

The data entry can be created as a tuple consisting of the following elements: DeviceID, Time, Location, and Data for each data record that is acquired from the drone. The system controller will transmit the tuple to the blockchain network after receiving it. It will also reply with a few commands based on the facts and task at hand. The tuple "ControllerID, Time, Location, Command" will be used to store the commands together with other information on the blockchain.

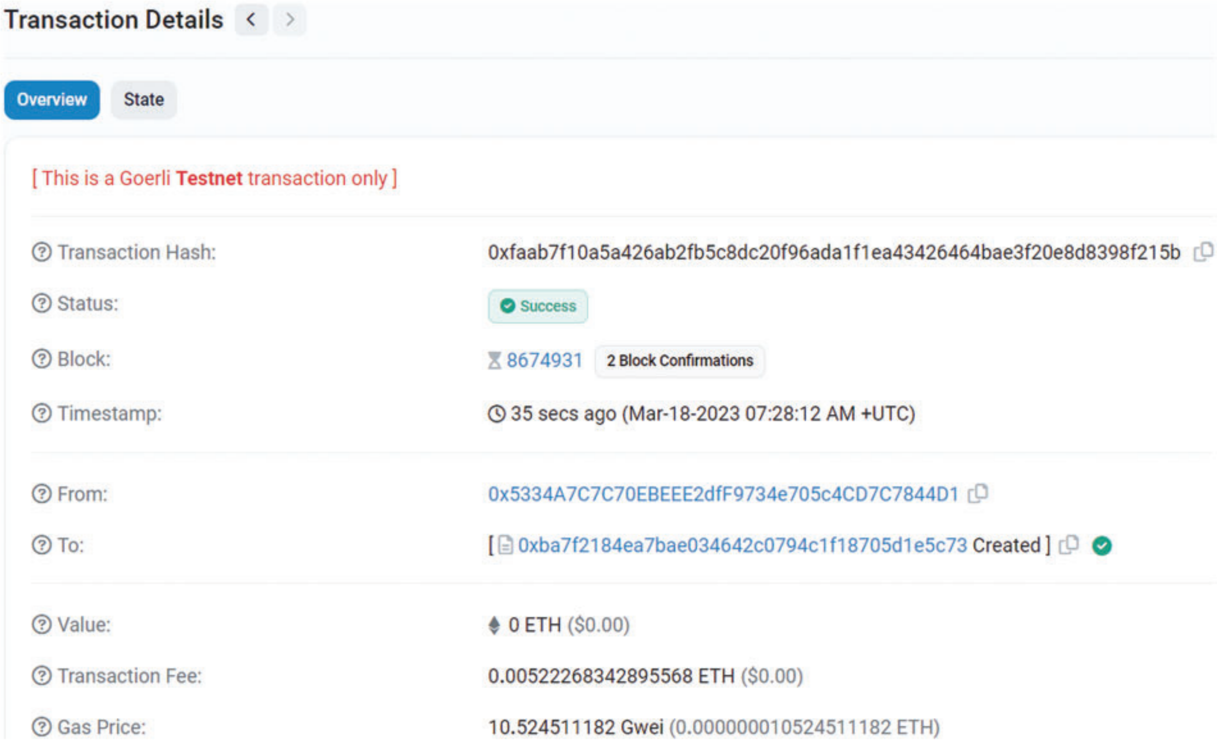
4.3 Blockchain Receipt Generation

A blockchain transaction will be created once a drone's acquired data record is transmitted to the network via the controller. The data management system can now perform future validation, tracking, and auditing thanks to this. The blockchainwill batch together some data items into a transaction. A new block will be created using a list of the transactions and confirmed by blockchain nodes. After the block has been verified, it will be included in the current blockchain and become a part of a tamper-proof ledger. Information regarding the blockchain transaction that was utilized to validate the transaction is included in the blockchain receipt. Fig. 2 displays a sample transaction details receipt.

4.4 Cloud Data Validation

As each record is instantly stored in the cloud, the integrity of the data can be regularly verified. This is done by comparing the computed hash to the target hash from the blockchain transaction detail receipt, which is obtained by regularly communicating with the blockchain network. This confirmation process applies to every record.

If an inconsistency is found, the record might be thought to have been compromised. Target hash, Merkle root, and the evidence from the blockchain details receipt are used as inputs to validate the data records. Reconstructing the Merkle tree from the blockchain receipt to calculate the Merkle root is the most crucial step [3]. In the blockchain network, each data record is kept alongside other records as one transaction. The evidence section of the receipt shows how each record from the same transaction is related to the others. For instance, the left node denotes that its record is anchored in the right node and that its record is collected earlier. The block index is represented by the transaction attribute height, and Block Explorer [4] provides the precise block.



Transaction Details

Overview State

[This is a Goerli **Testnet** transaction only]

Transaction Hash:	0xfaab7f10a5a426ab2fb5c8dc20f96ada1f1ea43426464bae3f20e8d8398f215b
Status:	✓ Success
Block:	8674931 2 Block Confirmations
Timestamp:	35 secs ago (Mar-18-2023 07:28:12 AM +UTC)
From:	0x5334A7C7C70EBEEE2dfF9734e705c4CD7C7844D1
To:	[0xba7f2184ea7bae034642c0794c1f18705d1e5c73 Created] ✓
Value:	0 ETH ($0.00)
Transaction Fee:	0.00522268342895568 ETH ($0.00)
Gas Price:	10.524511182 Gwei (0.000000010524511182 ETH)

Figure 2: Transaction details receipt

4.5 *Auditing of Data and Decision Making*

Data auditing and decision-making can be initiated based on the trustworthy data set once the cloud data is accessible for validation. The data records are kept in chronological order and are traceable to a reliable data source. Depending on the drones' application circumstances, either synchronously or asynchronously. Data auditing is essential for spotting irregularities in the command records from the cloud server and control system. Effective actions to prevent and mitigate APT assaults or DDoS attacks can be made based on the auditing results.

4.6 *Experimental Environment*

Remix Ethereum IDE environment setting

1. Environment: Javascript VM
2. Account: Administrator's account (0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c)
3. GAS Limit: 3000000
4. Value: in wei (100)
5. Contract: Solidity Contract (Drone)
6. Address: deploy address of contract (0x14723A09ACff6D2A60DcdF7aA4AFf308FDDC160C)
7. Solidity: Version of solidity (>= 0.5.22 < 0.9.0)

4.7 Gas Optimization for Smart Contract

In this section, the gas optimization for smart contracts is shown below in Tables 2 and 3. The execution of programmable code on a blockchain is made easier by smart contracts. Gas is a resource that is metered according to the cost of executing smart contract code; the precise quantity depends on how computationally intensive the underlying smart contract is. Therefore, it is crucial to optimize smart contract codes to cut down on gas usage and, in some cases, even prevent harmful assaults.

Table 2: Unoptimized smart contract code

Unoptimized code	// SPDX-License-Identifier: MIT
	pragma solidity >= 0.5.22 < 0.9.0;
	contract Drone{
	address[] public drone;
	address[] public controlSystem;
	address public manager;
	constructor(){
	manager = msg.sender; }
	event registered(string registered);
	function drone_register(address _droneAddress) public {
	uint flag = 1;
	for(uint128 j = 0;j < drone.length;j++)
	if(drone[j] == _droneAddress){flag = 0; }
	if(flag == 1){ emit registered("You have been registered");
	drone.push(_droneAddress); }
	else
	revert("You have already registered");}
	function control_system(address_systemAddress) public{uint flag = 1;
	for(uint128 j = 0;j < controlSystem.length;j++)
	if(controlSystem[j] == _systemAddress){flag = 0; }
	emit registered("You have been registered");
	controlSystem.push(_systemAddress); }
	else
	evert("You have already registered"); }}

Bug	Using extra "flag" variable& using uint128data type
Transaction cost	515341 gas
Execution cost	515341 gas
Total cost	1030682 gas

As the Ethereum platform is being used for the implementation of the application, Ethers will be consumed. Cost of 1 Ether = 1,548.95 USD (as of date 15/02/23). Hence, a 5.69% reduction in GAS will be reduced much in amount. It can be observed from Table 3 that a small registration smart contract code saves 5.69% on gas cost, hence more gas cost can be saved for smart contracts by applying different methods of optimization.

Table 3: Code optimized smart contract

Optimized code	// SPDX-License-Identifier: MIT
	pragma solidity >= 0.5.22 < 0.9.0;
	contract Drone{
	address[] public drone;
	address[] public controlSystem;
	address public manager;
	constructor(){manager = msg.sender;}
	event registered(string registered);
	function drone_register(address
	_droneAddress) public {
	for(uint256 j = 0;j < drone.length;j++){
	if(drone[j] == _droneAddress)
	revert("You have already registered");

Change	Removed "flag" variable and added a better approach to find the duplicacy & Replaced uint128 with uint256 data Type
Transaction cost	486000 gas
Execution cost	486000 gas
Total cost	972000 gas

4.8 Discussions

In this work, a drone system architecture has been built. Registration for drone systems, and control systems, a smart contract has been created as shown in **Algorithm 1** required transaction details have been shown in **Algorithm 2**, Tables 3 and 4 presents the optimized and un-optimized code for smart contract. In the optimized code, the variable flag has been removed and replaced uint128 data type with uint256 which in turn reduced the gas cost by 5.69%.

Table 4: Gas cost comparison for optimized and unoptimized smart contract

S. No.	Total GAS		Cost reduction after applying optimization techniques
	Optimized code	Unoptimized code	
1.	972000 gas	1030682 gas	5.69%

As the Ethereum platform is being used for the implementation of the application, Ethers will be consumed. Cost of 1 Ether = 1,548.95 USD (as of date 15/02/23). Hence, a 5.69% reduction in GAS will be reduced much in amount. It can be observed from Table 4 that a small registration smart contract code saves 5.69% on gas cost, hence more gas cost can be saved for smart contracts by applying different methods of optimization.

5 Conclusions

The potential applications for UAVs keep growing. UAVs will play an important role in the growth and operation of smart cities in the future. It can result in service improvements from companies and franchisors. However, after realizing the amazing things that drones are capable of, many have even begun to utilize this technology. UAV networks are vulnerable to numerous threats since they transmit important data. Their implementation necessitates secure and resilient UAV networks since it demands private and dependable UAV communications.

This study suggests a blockchain-based approach to enhance the security and reliability of the UAV ad-hoc network. By leveraging blockchain technology, data security is ensured, and the network is safeguarded against malicious nodes attempting to infiltrate it. Moreover, both GCS and UAV nodes can detect any attempts at manipulating the data. A smart contract implemented in the Ethereum network can address a variety of issues in the UAV network, including blackhole and grey hole attacks, as well as data eavesdropping. Potential future enhancements for the system include developing different response mechanisms for each type of attack. The proposed method proved to be more effective that the existing approaches available.

Acknowledgement: The authors extend their appreciation to the Deanship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through project number: IFP22UQU4281768DSR205.

Funding Statement: This research was supported by the Deanship for Research & Innovation, Ministry of Education in Saudi Arabia with the Grant Code: IFP22UUQU4281768DSR205.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Sharma, P. Vanjani, N. Paliwal, C. M. W. Basnayaka, D. N. K. Jayakody *et al.,* "Communication and networking technologies for UAVs: A survey," *Journal of Network and Computer Applications*, vol. 168, pp. 102739, 2020.

[2] N. M. Noor, A. Abdullah and M. Hashim, "Remote sensing UAV/drones and its applications for urban areas: A review," in *IOP Conf. Series: Earth and Environmental Science*, Kuala Lumpur, Malaysia, vol. 169, no. 1, 012003, 2018.

[3] J. P. Yaacoub, H. Noura, O. Salman and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet of Things*, vol. 11, 100218, 2020.

[4] U. R. Mogili and B. B. V. L. Deepak, "Review on application of drone systems in precision agriculture,"*Procedia Computer Science*, vol. 133, pp. 502–509, 2018.

[5] F. Outay, H. A. Mengash and M. Adnan, "Applications of unmanned aerial vehicle (UAV) in road safety, traffic and highway infrastructure management: Recent advances and challenges," *Transportation Research Part A: Policy and Practice*, vol. 141, pp. 116–129, 2021.

[6] L. Zhang and J. Bai, "An Ethereum-based wind power energy network contract management solution," *International Journal of Communication Networks and Distributed Systems*, vol. 28, pp. 43–60, 2022.

[7] Y. Alotaibi, "A new database intrusion detection approach based on hybrid meta-heuristics," *Computers, Materials & Continua*, vol. 66, no. 2, pp. 1879–1895, 2021.

[8] J. Sharma, M. Tyagi, A. Sachdeva, S. Dhingra and M. Ram, "Prediction of mutual interdependencies among the drivers of block-chain for enhancing the supply chain dynamics," *Journal of Computational and Cognitive Engineering*, vol. 1, pp. 1–12, 2022.

[9] P. K. Sharma and D. I. Kim, "Coverage probability of 3-D mobile UAV networks," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 97–100, 2018.

[10] V. Sharma, "Advances in drone communications, state-of-the-art and architectures," *Drones*, vol. 3, no. 1, 21, 2019.

[11] M. Abdel-Basset, G. Manogaran and M. Mohamed, "Internet of things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems," *Future Generation Computer Systems*, vol. 86, no. 9, pp. 614–628, 2018.

[12] T. Rana, A. Shankar, M. K. Sultan, R. Patan and B. Balusamy, "An intelligent approach for UAV and drone privacy security using blockchain methodology," in *2019 9th Int. Conf.*, Noida, India, pp. 162–167, 2019.

[13] B. Ly and R. Ly, "Cybersecurity in unmanned aerial vehicles (UAVs)," *Journal of Cyber Security Technology*, vol. 5, no. 2, pp. 120–137, 2021.

[14] Y. Mekdad, A. Aris, L. Babun, A. Fergougui, M. Conti *et al.,* "A survey on security and privacy issues of UAVs," *Computer Networks*, vol. 224, pp. 109626, 2023.

[15] X. C. Zheng and H. M. Sun, "Hijacking unmanned aerial vehicle by exploiting civil GPS vulnerabilities using software-defined radio," *Sensors and Materials*, vol. 32, no. 8, pp. 2729–2743, 2020.

[16] B. Bera, D. Chattaraj and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled internet of drones deployment,"*Computer Communications*, vol. 153, pp. 229–249, 2020.

[17] M. T. Lwin, J. Yim and Y. B. Ko, "Blockchain-based lightweight trust management in mobile ad-hoc networks," *Sensors*, vol. 20, no. 3, 698, 2020.

[18] A. Jindal, G. S. Aujla and N. Kumar, "Survivor: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment," *Computer Networks*, vol. 153, pp. 36–48, 2019.

[19] Y. Lu, "Security in 6G: The prospects and the relevant technologies," *Journal of Industrial Integration and Management*, vol. 5, no. 3, pp. 271–289, 2020.

[20] P. K. R. Maddikunta, S. Hakak, M. Alazab, S. Bhattacharya, T. R. Gadekallu *et al.,* "Unmanned aerial vehicles in smart agriculture: Applications, requirements, and challenges," *IEEE Sensors Journal*, vol. 21, no. 16, pp. 17608–17619, 2021.

[21] Y. Lu and X. Ning, "A vision of 6G—5g's successor," *Journal of Management Analytics*, vol. 7, pp. 301–320, 2020.

[22] C. Fan, S. Bao, Y. Tao, B. Li and C. Zhao, "Fuzzy reinforcement learning for robust spectrum access in dynamic shared networks," *IEEE Access*, vol. 7, pp. 125827–125839, 2019.

[23] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir and I. Guve, "Detection and classification of UAVs using RF fingerprints in the presence of Wi-Fi and Bluetooth interference," *IEEE Open Journal of the CommunicationsSociety*, vol. 1, pp. 60–76, 2019.

[24] L. Zhou, Z. Yang, S. Zhou and W. Zhang, "Coverage probability analysis of UAV cellular networks in urban environments," in *2018 IEEE Int. Conf. on Communications Workshops (ICC Workshops)*, MO, USA, pp. 1–6, 2018.

[25] C. Iwendi, Z. Jalil, A. R. Javed, T. Reddy, R. Kaluri *et al.,* "Keysplitwatermark: Zero watermarking algorithm for software protection against cyber-attacks,"*IEEEAccess*, vol. 8, pp. 2650–2660, 2020.

[26] R. Ch, T. R. Gadekallu, M. H. Abidi and A. Al-Ahmari. "Computational system to classify cyber crime offenses using machine learning," *Sustainability*, vol. 12, 4087, 2020.

[27] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Transactions on Cyber-Physical Systems*, vol. 1, no. 2, pp. 1–25, 2016.

[28] V. Chang, P. Chundury and M. Chetty, "Spiders in the sky: User perceptions of drones, privacy, and security," in *Proc. of the 2017 CHI Conf. on Human Factors in Computing Systems*, Denver, Colorado, USA, pp. 6765–6776, 2017.

[29] S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, M. Guizani *et al.,* "Securing smart cities through blockchain technology: Architecture, requirements, and challenges," *IEEE Network*, vol. 34, pp. 8–14, 2020.

[30] Y. Lu, “A survey on functions, applications and open issues,” *Journal of Industrial Integration and Management*, vol. 3, no. 4, 1850015, 2018.

[31] N. Malsa, V. Vyas, J. Gautam, R. N. Shaw and A. Ghosh, “Framework and smart contract for blockchain enabled certificate verification system using robotics,” in *Machine Learning for Robotics Applications*. Singapore: Springer, pp. 125–138, 2021.

[32] N. Malsa, V. Vyas, J. Gautam, R. N. Shaw and A. Ghosh, “CERTbchain: A step by step approach towards building a blockchain based distributed appliaction for certificate verification system,” in *2021 IEEE 6th Int. Conf. on Computing, Communication and Automation (ICCCA)*, Arad, Romania, pp. 800–806, 2021.

[33] L. Zhou, Z. Yang, S. Zhou and W. Zhang, “Coverage probability analysis of UAV cellular networks in urban environments,” in *2018 IEEE Int. Conf. on Communications Workshops (ICC Workshops)*, Kansas City, MO, USA, pp. 1–6, 2018.

[34] T. Alladi, V. Chamola, N. Sahuand and M. Guizani, “Applications of blockchain in unmanned aerial vehicles: A review,” *Vehicular Communications*, vol. 23, 100249, 2020.

[35] S. Das, B. K. Mohanta and D. A. Jena, “State-of-the-art security and attacks analysis in blockchain applications network,” *International Journal of Communication Networks and Distributed Systems*, vol. 28, pp. 199–218, 2022.

[36] J. Moubarak, E. Filiol and M. Chamoun, “On blockchain security and relevant attacks,” in *2018 IEEE Middle East and North Africa Communications Conf. (MENACOMM)*, Jounieh, Lebanon, pp. 1–6, 2018.

[37] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang *et al.,*“Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive,” *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2438–2455, 2019.

[38] G. Xu, J. Zhang, U. G. Cliff and C. Ma, “An efficient blockchain-based privacy-preserving scheme with attribute and homomorphic encryption,” *International Journal of Intelligent Systems*, vol. 37, pp. 10715–10750, 2022.

[39] A. I. Alshbatat and L. Dong, “Performance analysis of mobile ad hoc unmanned aerial vehicle communication networks with directional antennas,” *International Journal of Aerospace Engineering*, vol. 2010, pp. 1–14, 2010.

[40] S. Sharma and S. Saxena, “Blockchain and UAV: Security, challenges and research issues,” in *Proc. of UASG 2019: Unmanned Aerial System in Geomatics*, Roorkee, India, Springer Cham, vol. 51, pp. 99–107, 2020.

[41] H. Sachdeva, S. Gupta, A. Misra, K. Chauhan and M. Dave, “Improving privacy and security in unmanned aerial vehicles network using blockchain,” *arXiv preprint arXiv*:2201.06100, 2022.

[42] K. Jo, J. Heo, J. Jung, B. Kim and H. Min, “A rendezvous point estimation considering drone speed and data collection delay,” in *2017, 4th Int. Conf. on Computer Applications and Information Processing Technology (CAIPT)*, Kuta Bali, Indonesia, pp. 1–4, 2017.

[43] T. Rana, A. Shankar, M. K. Sultan, R. Patan and B. Balusamy, “An intelligent approach for UAV and drone privacy security using blockchain methodology,” in *2019, 9th Int. Conf. on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, pp. 162–167, 2019.

[44] N. Mhaisen, N. Fetais, A. Erbad, A. Mohamed and M. Guizani, “To chain or not to chain: A reinforcement learning approach for blockchain-enabled IoT monitoring applications,” *Future Generation Computer Systems*, vol. 111, pp. 39–51, 2020.

[45] I. García-Magariño, R. Lacuesta, M. Rajarajan and J. Lloret, “Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain,” *Ad Hoc Networks*, vol. 86, pp. 72–82, 2019.

[46] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos and C. Yang, “The blockchain as a decentralized security framework,” *IEEE Consumer Electronics Magazine*, vol. 7, pp. 18–21, 2018.

[47] B. Nassi, A. Shabtai, R. Masuoka and Y. Elovici, “SOK-security and privacy in the age of drones: Threats, challenges, solution mechanisms, and scientific gaps,” *arXiv preprint arXiv*:190305155, 2019.

[48] C. Zhang and Y. Chen, “A review of research relevant to the emerging industry trends: Industry 4.0, IoT, blockchain, and business analytics,” *Journal of Industrial Integration and Management*, vol. 5, no. 1, pp. 165–180, 2020.

[49] R. J. K. Salah, K. Nizamuddin and M. Omar, “Blockchain-based soybean traceability in agricultural supply chain,” *IEEE Access*, vol. 7, pp. 73295–73305, 2021.

[50] D. Puthal, D. N. Malik, S. P. Mohanty, E. Kougianos and C. Yang, “The blockchain as a decentralized security framework [future directions],” *IEEE Consumer Electronics Magazine*, vol. 7, pp. 18–21, 2018.

[51] S. S. Panda, D. Jena, B. K. Mohanta and S. Patnaik, “A blockchain-based ITS framework with privacy preserving for secure and reliable communication,” *International Journal of Communication Networks and Distributed Systems*, vol. 27, pp. 366–387, 2021.

[52] S. Malik, V. Dedeoglu, S. S. Kanhere and R. Jurdak, “Trustchain: Trust management in blockchain and IoT supported supply chains,” in *2019 IEEE Int. Conf. on Blockchain*, Atlanta, GA, USA, pp. 184–193, 2019.

[53] S. P. Singh, Y. Alotaibi, G. Kumar and S. S. Rawat, “Intelligent adaptive optimisation method for enhancement of information security in IoT-enabled environments,” *Sustainability*, vol. 14, pp. 13635, 2022.

[54] M. A. Haque, N. Almrezeq, S. Haque and A. Abd El-Aziz, “Device access control and key exchange (DACK) protocol for internet of things,” *International Journal of Cloud Applications and Computing (IJCAC)*, vol. 12, no. 1, pp. 1–14, 2022.

[55] R. Gupta, A. Nair, S. Tanwar and N. Kumar, “Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges,” *IET Communications*, vol. 15, no. 10, pp. 1352–1367, 2021.

[56] B. Li, J. Huang, S. Bai, Z. Gan, S. Liang *et al.,* “Autonomous air combat decision-making of UAV based on parallel self-play reinforcement learning,” *CAAI Transactions on Intelligence Technology*, vol. 8, pp. 64–81, 2022.