mathematics

MDPI

Article

Heterogeneous Blockchain-Based Secure Framework for UAV Data

Abdullah Aljumah [1,*], Tariq Ahamed Ahanger [2] and Imdad Ullah [1]

[1] College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia; i.ullah@psau.edu.sa
[2] Department of Management Information Systems, College of Business Administration, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia; t.ahanger@psau.edu.sa
* Correspondence: aljumah@psau.edu.sa

Abstract: Unmanned aerial vehicles, drones, and internet of things (IoT) based devices have acquired significant traction due to their enhanced usefulness. The primary use is aerial surveying of restricted or inaccessible locations. Based on the aforementioned aspects, the current study provides a method based on blockchain technology for ensuring the safety and confidentiality of data collected by virtual circuit-based devices. To test the efficacy of the suggested technique, an IoT-based application is integrated with a simulated vehicle monitoring system. Pentatope-based elliptic curve encryption and secure hash algorithm (SHA) are employed to provide anonymity in data storage. The cloud platform stores technical information, authentication, integrity, and vehicular responses. Additionally, the Ethbalance MetaMask wallet is used for BCN-based transactions. Conspicuously, the suggested technique aids in the prevention of several attacks, including plaintext attacks and ciphertext attacks, on sensitive information. When compared to the state-of-the-art techniques, the outcomes demonstrate the effectiveness and safety of the suggested method in terms of operational cost (2.95 units), scalability (14.98 units), reliability (96.07%), and stability (0.82).

Keywords: internet of things; security; blockchain; UAV

MSC: 68T05

Citation: Aljumah, A.; Ahanger, T.A.; Ullah, I. Heterogeneous Blockchain-Based Secure Framework for UAV Data. *Mathematics* **2023**, *11*, 1348. https://doi.org/10.3390/math11061348

Academic Editor: Ximeng Liu

Received: 29 December 2022
Revised: 7 March 2023
Accepted: 8 March 2023
Published: 10 March 2023

1. Introduction

Unmanned aerial vehicles (UAVs) are drones that have been combined with the internet of things (IoT) devices and are capable of autonomous flight. Since its inception in the market around 2010, its popularity has elevated as a result of technological developments and urbanization. Initially, UAVs appeared on the marketplace as commercial drones [1]. The widespread use of UAVs has given an edge to businesses that rely on product delivery. Due to cheaper costs and shorter transit times, it quickly replaced traditional transport methods for handling consumer demand. To increase its delivery speed, Amazon, for instance, acknowledged and publicized the benefits of incorporating drones and comparable technology into its existing delivery system [2]. Moreover, Amazon increased funding for research and development on UAVs that improve supply chain management [2]. Bluetooth-based WPANs, cellular networks using long term evolution (LTE) and 6G networks are all examples of communication technologies utilized in VC-based products [3]. In the design of drones, UAVs, and other IoT-based devices, state-of-the-art technologies serve a crucial supporting role in the monitoring of multimedia-streaming traffic over dynamic network segments. The exploitation that has occurred in some of these applications is a key cause for alarm and a driving force behind the current research. The built-in speed and altitude-supporting mechanisms of virtual circuit-based applications have greatly contributed to the use rate in the modern era. Such technologies have the potential to be extremely dependable and ensure cost-efficient wireless communication-based solutions to

a wide range of issues in the real world [4]. Most governments, for instance, employ UAV technology to track down and keep tabs on flying robots [5]. The aerial user equipment (AUE) refers to cellular-connected UAVs, which are surveillance drones designed to live with terrestrial users [6]. It is worth noting that companies such as Qualcomm want to use UAVs for widespread wireless communications in 5G networks [7]. These gadgets function in heterogeneous networks. Existing device-to-device (D2D) technologies have difficulties in the areas of cellular network frequency, planning, and resource usage [8–10]. Together, 5G-based environments and UAV-enabled flying base stations can address the aforementioned limitations of today's technology [11,12]. However, to be employed smoothly across many sectors of human life, UAVs, and drone systems comprising heterogeneous networking technologies, a high usage rate must be effectively protected. A representation of a procedure for evaluating potential dangers posed by UAVs or drones is shown in Figure 1. Specifically, confidentiality, integrity, and availability are three important parameters to be addressed for data protection. Moreover, the risk assessment is performed based on threat analysis, environmental parameters and unauthorized access. Drones and UAVs face similar threats to data security as any other type of aircraft. As a result, several methods of communication have been proposed to lessen the dangers caused by the network protocols [13]. Researchers have identified cryptology-based solutions [14,15] as possible risk-minimization strategies, particularly in the case of Drones and UAV systems. However, there are still obstacles to prevent the compromise of signal data. Many aspects of weather can pose threats to signal data. Machine learning, cryptography, network communication systems, and radar systems are some of the cutting-edge technologies that have been tested to identify the best method for risk identification and data upkeep. Research suggests that blockchain technology (BCN) [16] might be used to improve security, keep records safe, and keep VC-based devices running smoothly.

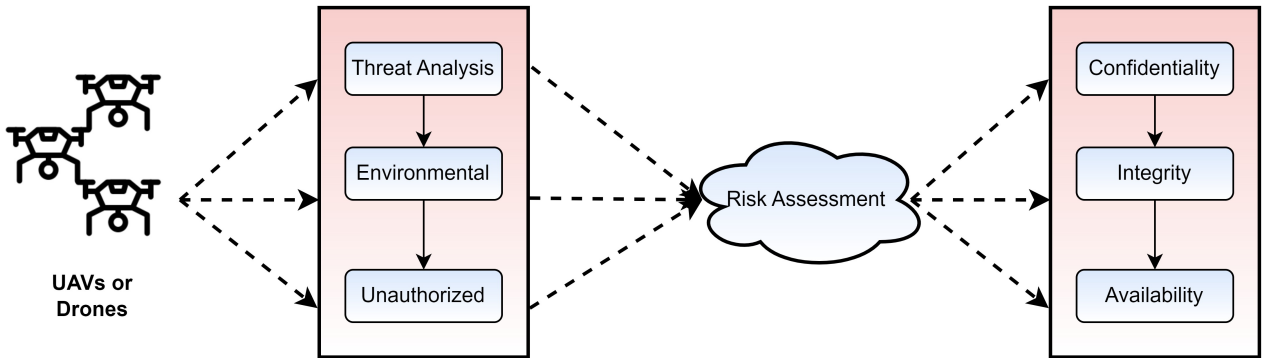

Figure 1. VC-based risk analysis.

1.1. Major Contribution

Based on the aforementioned aspects, some of the major contributions are as follows:

1. Blockchain-based secure UAV communication technique is proposed in the current study.
2. Environment, weather, and geographical elements are taken for risk evaluation of VC-based UAV devices.
3. Network protocols, the confidentiality of communications, and appropriate preventative strategies are considered in the proposed technique for ensuring security.
4. The pentatope ECC (PECC) technique is used for securing data at cloud storage.
5. The proposed technique is validated based on comparative analysis with state-of-the-art techniques in terms of operational cost (2.95 units), scalability (14.98 units), reliability (96.07%), and stability (82.26%)

Abbreviations present the nomenclature used in the current study.

Paper Organization

Section 2 provides a comprehensive literature review. Section 3 outlines the suggested approach and its pertinent applications. Section 4 presents the findings and performance evaluation of the proposed model. Section 5 concludes the paper and outlines potential avenues for further study.

2. Literature Review

This section reviews some of the recent works in the current domain of study. Security concerns posed by drone use in society were the subject of a recent publication by Nassi et al. [1]. The risks, difficulties, and knowledge gaps associated with the items most important to technology's use were discussed. Problems with drone use are recognized, but the research does not attempt to provide evidence on how to fix them. The problems associated with UAVs, the internet of drones (IoD), and drones as a whole are all factored into the paradigm given by Karnik et al. [17]. Privacy and network administration are highlighted as key concerns in this analysis. The function of UAV-operating network devices, such as the 5th-generation (5G) network and the global positioning system (GPS), are discussed in detail. Wu et al. [18] also have similar ideas. However, the article fails to address the potential dangers and remedies for IoD and UAV deployments. Several aspects of UAVs, including the fact that they have been referred to as "Flying ad hoc networks (FANET)", were discussed by Muravskyi et al. [19] paper. As a part of a larger simulation study, the article analyzes topology-based routing protocols. The unique FANET characteristics—including its dynamic architecture, mobile nodes, reliance on cutting-edge network connectivity, and 3D spatial moment—make hacking and tampering exceedingly challenging. The study might benefit from including a description of the attacks [20] on the UAV data that were omitted. To detect the UAV device in the event of unwanted access including modification of the UAV signal, Majeed et al. [21] investigated the difficulties related to the detection and classification of UAVs implanted employing RF surveillance system boosted by wireless interference signals. Spiders in the sky is a term used to describe the unethical surveillance and control of UAVs through data, which is often carried out by unauthorized personnel [22]. The study emphasizes the BCN approach to data protection, which can ensure the confidentiality and integrity of data transmitted by UAVs and drones. Data privacy concerns in UAVs were discussed by Hasan et al. [23] along with various solutions to such concerns. Lightweight cryptographic methods and identity-based encryption (IBE) are highlighted in the study as an effective means of protecting users' confidentiality. The study foreshadows the potential for incoherent forces in society to launch plaintext, ciphertext, and denial of service/distributed denial of service attacks. According to Deepa et al. [24], blockchain technology can thwart these kinds of attacks by employing the suggested structure. Results, however, have been less than encouraging.

There have been several recent research projects utilizing blockchain technology, and an overview of comparative works is provided in Table 1. It depicts the distinguishing aspects of the proposed model in terms of major domain, BCN utilization, and crytographic technique used.

Table 1. Comparison analysis with state-of-the-art systems. NA: Not Applicable; Y: Yes; N: No.

Reference	UAV Category	Major Domain	BCN Used	Cryptographic Technique	Use Case	Cloud
[23]	Drone	Authentication	N	NA	NA	N
[1]	UAV	Authentication	Y	ECC	NA	N
[3]	Drone	Authentication	N	NA	NA	N
[25]	UAV	Authentication/ Confidentiality	N	NA	NA	N
[12]	Drone	Authentication/ Confidentiality	N	NA	NA	N
[26]	IoT Devices	Authentication	N	NA	NA	N
[27]	Drone-based	Privacy	Y	NA	Y	Y
[28]	Drone-based	Authentication/ Confidentiality	Y	Metaheuristic Technique	NA	Y
[29]	Drone-based	Authentication/ Confidentiality	Y	Fedrated Learning-based Technique	NA	Y
[30]	Drone	Authentication/ Confidentiality	Y	NA	COVID-19-based delivery	Y
This Paper	UAV/IoT/Drone	Authentication/ Confidential-ity/ Integrity	Y	PECC	Smart vehicular	Y

3. Proposed Model

To reduce the potential data loss in UAV and drone systems, the current research provides a BCN-based solution. Specifically, this method aims to deliver improved privacy and data storage techniques that include the following distinctive characteristics: *immutability, tamper-proofing, transparency, security, and efficient distribution mechanisms* Sensors are an integral part of drones, UAVs, and IoT devices, allowing users to accomplish a wide range of predetermined goals. Both local and distant control and monitoring of drones and UAVs are performed using network communication systems [31]. The main architecture for collecting data and managing drone or UAV components is shown in Figure 2. Specifically, data are acquired using a telecommunication network over drone platform. They are forwarded to the cloud network where encryption is performed in real time. With data security as their top priority, UAVs, drones, or virtually monitored vehicles (VMVs) store information in the cloud. Instead of storing unencrypted data on the cloud, cipher data created with the pentatope ECC (PECC) technique are kept there [32]. Benaya et al. [33] explain how SHA-based hash values may be used to assess the reliability of data and how these values can then be properly preserved inside the blockchain infrastructure. However, there are drawbacks to implementing BCN, such as high computing costs and excessive power consumption. In the presented study, we put a VC-based application's data on vehicles under surveillance through its paces. Whenever there is suspicious activity, the system records it and sends out a security warning. With the use of BCN and cloud computing, the authority may issue instructions to the system, and the cars' subsequent responses can be handled as transactions.

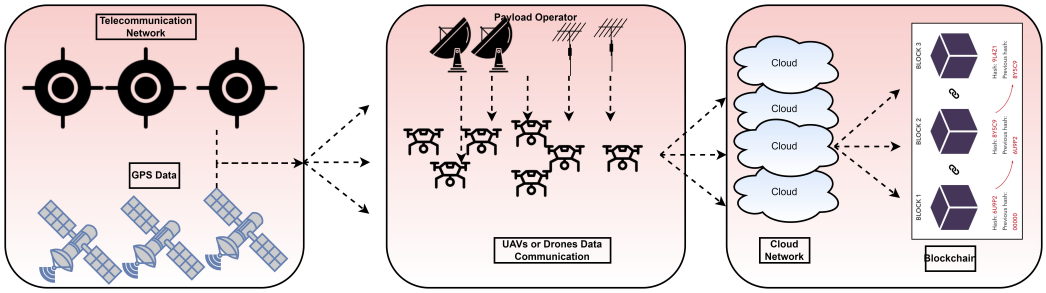

Figure 2. Proposed architecture of blockchain-based data security.

3.1. BCN-Based UAV Data Maintenance

Pentatope elliptic curve encryption is used to protect data in the cloud in the context of the proposed system. Drones and other UAVs have a distributed design in terms of data communication. The distributed design in drones and other unmanned aerial vehicles (UAVs) refers to the way data are communicated among different components of the drone. Instead of having a centralized system that processes and stores all data, the information is distributed across multiple units, each responsible for a specific task. For example, the flight control system, the sensors, and the communication module can all be separate units that communicate with each other using a network. This enables each component to process data in real time, leading to faster decision making and improved overall performance. Additionally, the distributed design can also improve reliability and safety by reducing the impact of a single component failure. If one unit fails, the other components can continue to operate, maintaining control of the drone and preventing a catastrophic failure. Overall, the distributed design is an important aspect of modern drone technology that enables improved functionality, performance, and reliability. When interacting with devices on the ground and in the air, it is important to keep the data being exchanged secure, which calls for the use of an anonymous technique, such as BCN. Each UAV requires its own Eth (Ethereum) balance, a temporary cryptocurrency, to conduct the transactions in its block. The MetaMask wallet is used in the present work. MetaMask is an extension for accessing Ethereum-enabled distributed applications. The extension injects the Ethereum web3 API into a JavaScript context so that apps can read from the blockchain. Using Metamask with a drone requires custom development work and integration of the Metamask software into the drone's hardware and software systems. The following steps were performed using Metamask with a drone:

1. Integration of the Metamask software: It involved integrating the Metamask code into the drone's operating system so that it can interact with the Ethereum network and perform transactions.
2. Connection of the drone to the Ethereum network: The drone was connected to the Ethereum network via a gateway to interact with dApps and perform transactions.
3. Interaction with dApps: Once the drone was connected to the Ethereum network, it interacted with decentralized applications (dApps) by sending transactions to them and receiving data from them.
4. Manage private keys: The drone securely stored its private keys, which are used to sign transactions and control access to its Ethereum account.

There is a cryptocurrency called EthGas that contributes to the creation of a block in the BCN ecosystem. A digital signature based on PECC is used to verify all data received from aerial devices. Figure 3 presents a diagram to keep track of every BCN block's one-of-a-kind transaction. Specifically, the data state is monitored and verified over a cloud network. Moreover, smart contracts and digital signatures are used for data security.

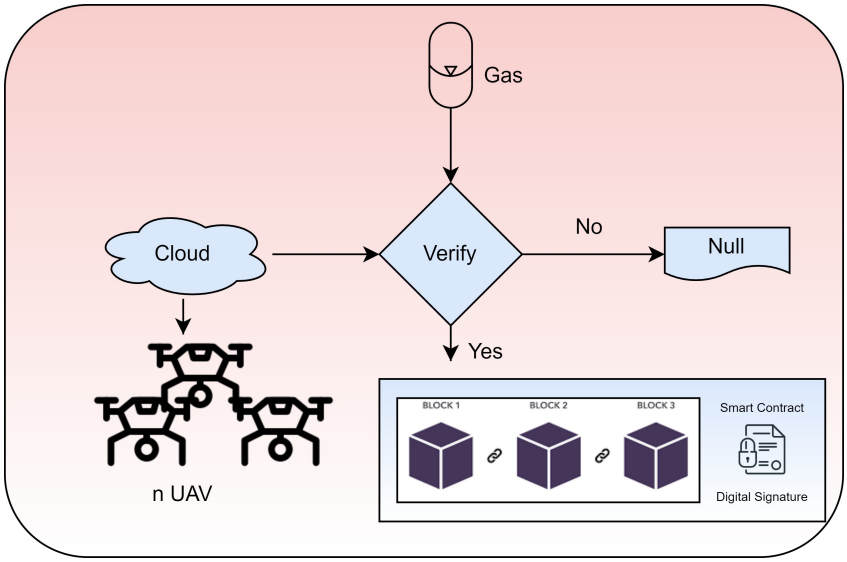

Figure 3. Proposed architecture: state chart diagram of proposed blockchain-based technique.

The BCN module's role in the block transaction process is outlined in Algorithm 1. In the proposed technique, the Ethereum balance is compared with the preferred threshold. If the value is greater than the threshold, then it is added to the BCN block. Similarly, the comparison is made with all the nodes (UAVs). Once the transaction is created, the EPECC is performed on the added device. There is no way to change or update the information that is stored in the block as a transaction because these records are immutable and transparent. Because the BCN is distributed, all participating devices are instantly updated whenever any changes are made. In this case, the proposed system is implemented in solidity using the MetaMask wallet and the Ganache platform. Open Stalk, a cloud platform, is integrated with Node MCU and ESP 32 to expand the framework even further.

Algorithm 1 Block transaction procedure

```
UAVs or Drone block Transaction
while n number of UAV devices do
    if ETH-balance is greater than Threshold then
        Allow the device to BCN Block
        Update ETH-balance
    else if Block transaction is not created then
        Device data privacy and preservation
        while n number of UAV devices do
            if Device[i] block transaction is created then
                Perform EPECC(in(Device [i])
                Add SHA of ETH-Balance
            end if
        end while
    end if
end while
```

3.2. Using BCN for Intelligent Vehicle Monitoring

The prototype is incredibly useful for keeping tabs on secure areas, where humans would have a difficult time keeping watch on their own. The prototype was created with the help of Arduino, Blynk IoT Platform, NodeMCU, and an ESP32 camera. The unmanned vehicle's special characteristics include voice-activated control and real-time visual feedback from the collected environment on a mobile device. Information obtained from vehicles is stored in a blockchain context. The car may be operated from a distance

using the touchscreen, the device's tilt sensor, and the accelerometers. The car is instructed via voice commands and the Blynk IoT Platform, and the servo module is utilized to position the camera at the desired angle. Users are first registered with the proposed system using the Blynk IoT Platform, which also verifies the users' identities later on. After the system has been validated, only the users are able to manipulate the servo motors and sliders within the software. The algorithm illustrates the steps involved in gathering information via surveillance and giving appropriate directions to the vehicle. Information about the vehicle is based on the commands it has received. The results of these directives are saved in the cloud for future reference. After the MetaMask wallet balance is confirmed to be accurate, the information is transmitted to the blockchain. To make a BCN transaction, the complete process is initiated on the Ganache platform.

3.2.1. Monitoring Module

Figure 4 depicts the vehicle's numerous control components. By connecting to the L298N motor driver, the ESP8266 module relays the user's input to the motors. As time goes on, the vehicle's wheels begin turning in response to commands from the connected motors. At the same time, the camera's movement is put under the command of the servo module (Horizontal and Vertical). For live streaming, this is a must-have feature. The logic of the monitoring software is laid forth in Algorithm 2. The slider of the camera is moved horizontally and vertically, depending on the value. Once the data are acquired, they are forwarded to the cloud for further processing.

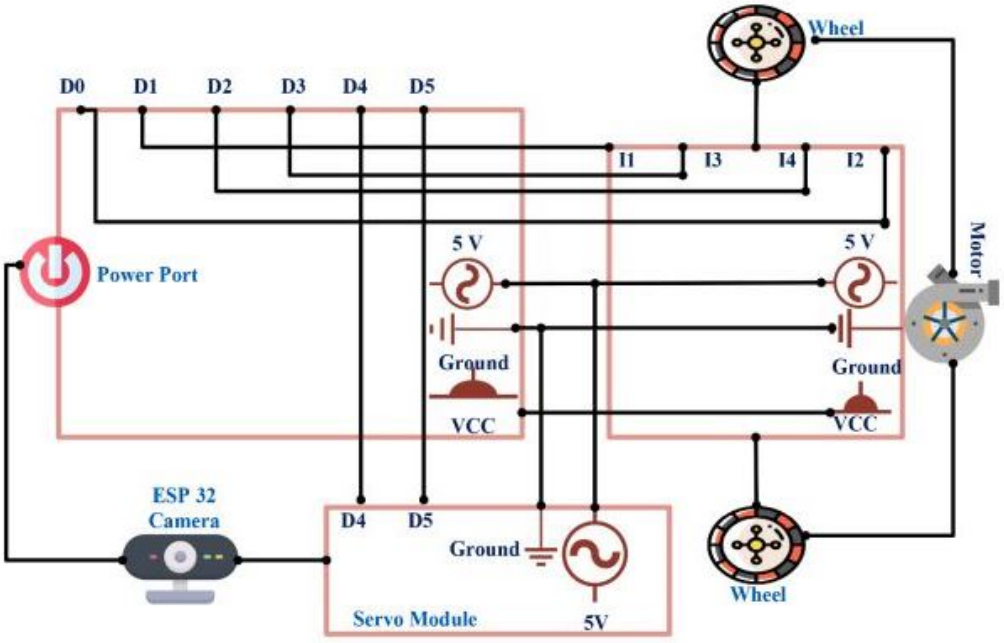

Figure 4. Intelligent vehicular system depicting vehicle's numerous control components.

Algorithm 2 Monitoring Component

Attach the camera to the tilt technique
Read the input from the Slider with Horizontal(Hi) and Vertical(Vi) Slider
if Slider is equal to Hi **then**
    The camera moves horizontally
else if Slider moves vertically **then**
    Read the input from the Slider Stream and forward it to cloud
end if

3.2.2. Voice Assist Subsystem

At first, the driver provides voice-over directions for the car on their mobile devices, indicating which way to turn, which way to go straight, and which way to go back. In the suggested system, the user's speech is verified using the *if this then That (IFTT) platform* [34], a freeware web-based service designed to improve automation and the quality of life. Following processing by Wi-Fi modules, these instructions eventually make it to the motor driver. Following this, the instructions are transmitted to the motors and the camera, which then begins live-streaming video recording. Here, PECC (pentatope elliptic curve cryptography) and SHA are used to protect the transmission of user instructions to the car and the resulting data in the cloud. The data from the vehicles are encrypted using a combination of the privacy enhancing cryptography standard and the secure hash algorithm. The logic behind the module's voice-assisted functionality is described in Algorithm 3. Specifically, based on the user's voice, the slider is moved horizontally. Finally, PECC is performed on the device to ensure security.

Algorithm 3 Voice Assistant Component

```
Read the user voice as input and store it in Yi
Verify Yi with horizontal slider
if Yi is equal to horizontal then
    Perform Yi
else
    Perform horizontal slider
    Perform PECC on Yi
    Store PECC of Yi in device
end if
```

3.2.3. Data Storage Using BCN

The verification of the balance at the MetaMask wallet transfers the data onto the blockchain [35]. Each user command given to the vehicle and its corresponding response are recorded as a transaction on the blockchain. The user-initiated video-streaming procedure begins when the vehicle receives instructions from the user. It is good knowledge that smart contracts contain security flaws of their own. Malware can be introduced into the system, leading to difficulties and 51% attacks in the blockchain. The set of programming principles might be used to defend against such attacks [36]. The blockchain protocol was built on the Ganache platform, using the 0.5.0+ commit compiler.

4. Experimental Implementation

The major goal of the proposed system is to manage, secure, and monitor information collected by UAV or drone systems. In this study, we put the suggested architecture through its paces on a BCN-based vehicle monitoring system that makes use of virtual circuits. The suggested BCN architecture in the study allows for the safe and secure storage of sensitive data gathered by UAVs and drones. The intruder alarm message created by the system is depicted, and the permitted alert message generated by the proposed application is depicted.

4.1. Simulation Environment

The suggested system is developed mostly on the Arduino IDE and the ESP32 camera. After running a shared Python program (between the IDE and the camera), the camera creates a connection that may be seen in the IDE serial monitor. Registration on the *ngrok* server is required for permitted users, after which a hash code is created. It allows people to use the system's features so they can drive the car. Users must initially enroll the suspicious or approved faces for the system to identify them as authorized or not. The camera then collects five samples of the user's face, which are then utilized for face recognition and validation in conjunction with the ongoing monitoring of the locations. The system

depicts the Hello Subject message being shown by the camera once the authorized person's face is detected. However, if the camera catches an illegal individual, the Intruder Alert message will appear, as illustrated in the system. The system can distinguish between permitted and unauthorized individuals and report any potential misidentifications to the appropriate authorities. Therefore, the system represents the situation in which the intruder or unauthorized person is discovered, even if he stays with a group of approved folks. Using gas cost on a MetaMask wallet to conduct a transaction without any hitches in the blockchain infrastructure is highlighted and explained in the system. There is no ambiguity for consumers as to the total cost, amount of gas used, gas price, or Ethereum involved in a transaction because all of this information is shown. The gas cost incurred by a MetaMask wallet to conduct a blockchain transaction is depicted in the system.

4.2. Evaluation of Results

The strengths of the suggested system in terms of privacy, preservation, attack rate, and defense rate are compared to those of the conventional state-of-the-art techniques, as shown in Figure 5. Attack rate and defense rate are computed using [37]. The comparisons place special emphasis on the assault rates, with a focus on the privacy and preservation elements. The significance of the suggested paradigm is further supported by taking into account other evaluation metrics including latency, response time, and data computation time. Unlike reaction time, latency can build up over time. Latency is the amount of time it takes for an IoT request to be processed and stored in a blockchain ledger. The term "response time" is used to describe how long it takes for the requested information to be returned to the requesting IoT device from the blockchain database. It is important to note that the suggested framework places equal weight on the system's non-functional needs. System performance parameters, such as operating cost, scalability for cloud infrastructure, scalability for applications, and fault tolerance rate, have been given careful consideration. The outcomes demonstrate the influence on attack rates owing to blockchain qualities, such as immutability, transparency, distribution, and security, and validate the superiority of the proposed technique above the outcomes provided by the conventional methodologies. Therefore, the suggested system has lower attack rates than the current methods. Nevertheless, there are still several restrictions that make full BCN implementation difficult. As an example of a drawback, reversible operations cannot be integrated into the BCN environment, and backup maintenance factors are notoriously difficult to implement in a blockchain setting. To get around these restrictions, developers have begun employing the cloud as a user interface rather than a database for user–app communication. To ensure system resilience, it is tested with data sizes ranging from 1 KB to 1 GB. As can be seen in Figures 6 and 7, the suggested system has effectively obtained higher performance outcomes in situations of all functional and non-functional aspects. Figure 6 shows the gas fee parameter, which is a blockchain transaction fee paid to network validators for their services to the blockchain. In Table 2, a comparative analysis is performed concerning state-of-the-art works. It depicts the comparison based on the functions and processing time. The immutable nature of the BCN, based on the hash value of the data created using SHA, allows it to thwart attacks that would otherwise compromise data integrity. Rather than storing data directly, the BCN method includes the use of the hash value of data being stored at blocks to record transactions, which makes the system transparent and immune to plaintext and ciphertext attacks. Latency and computation delay details for the function, right, left, and straight for the system with and without blockchain are shown in Table 2. This table demonstrates how the adoption of blockchain increases waiting times and processing times. Table 2 displays the outcomes of the smart contract deployment in Ethereum with Ganache IDE for tracking vehicle movements. Depending on the events specified in the smart contract, it depicts the exact amount of gas that must be consumed to complete the transactions. The added functionality of this method offers data on the Ether price of the necessary gas (units). The block's ID, mining time, and block size, as well as other transactional characteristics, such as the transaction's unique identifier (hash value),

are all detailed in detail. Information regarding a transaction's nonce size and its index inside the block is also included.

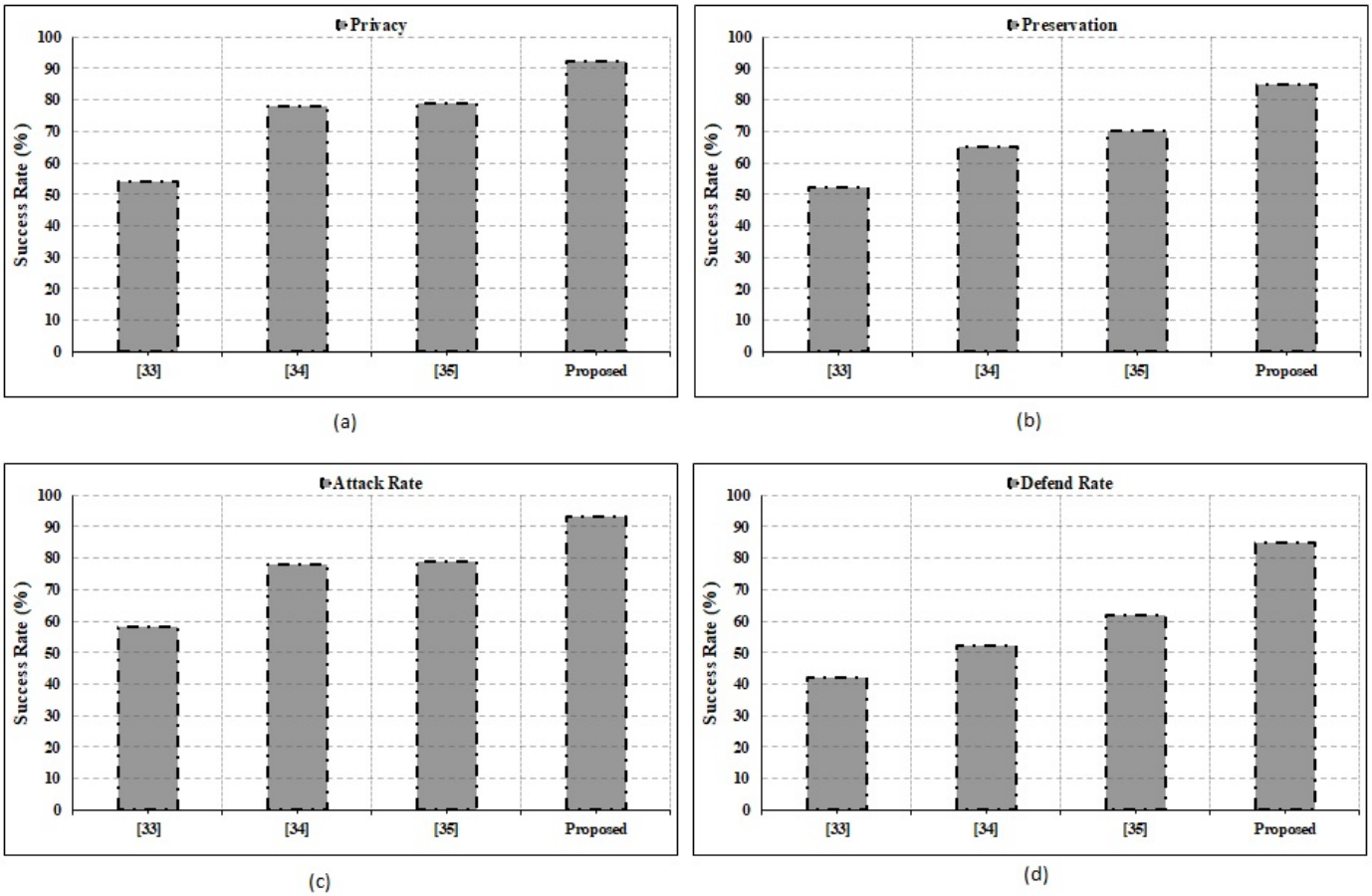

Figure 5. Performance assessment; (**a**) privacy (**b**) preservation (**c**) attack rate (**d**) defend rate.

Table 2. Latency delay comparison.

Functions	BCN Platform	BCN Platform	Without BCN Platform	Without BCN Platform
	Latency Time (in Sec)	Processing Time (in Sec)	Latency Time (in Sec)	Processing Time (in Sec)
Left ()	5.26	38	2.15	16.25
Right()	4.26	6.05	3.25	7.01
Straight()	5.21	28.15	2.48	12.25

4.3. Reliability Analysis

There must be an evaluation of the dependability of the supplied framework. Results are compared to traditional techniques. The performance scale is determined by the degree to which the dependability value persists. The deployment used in actual implementation improves dependability. Figure 8 shows the numerical findings of the reliability analysis in terms of the percentage of correct result computation. It is concluded that the provided model achieves the highest reliability measure (96.07%) acquired for the proposed model as compared to the traditional technique [32] (85.15%), [33] (88.12%) and [34] (85.14%). In addition, the provided model is an effective tool for data storage.

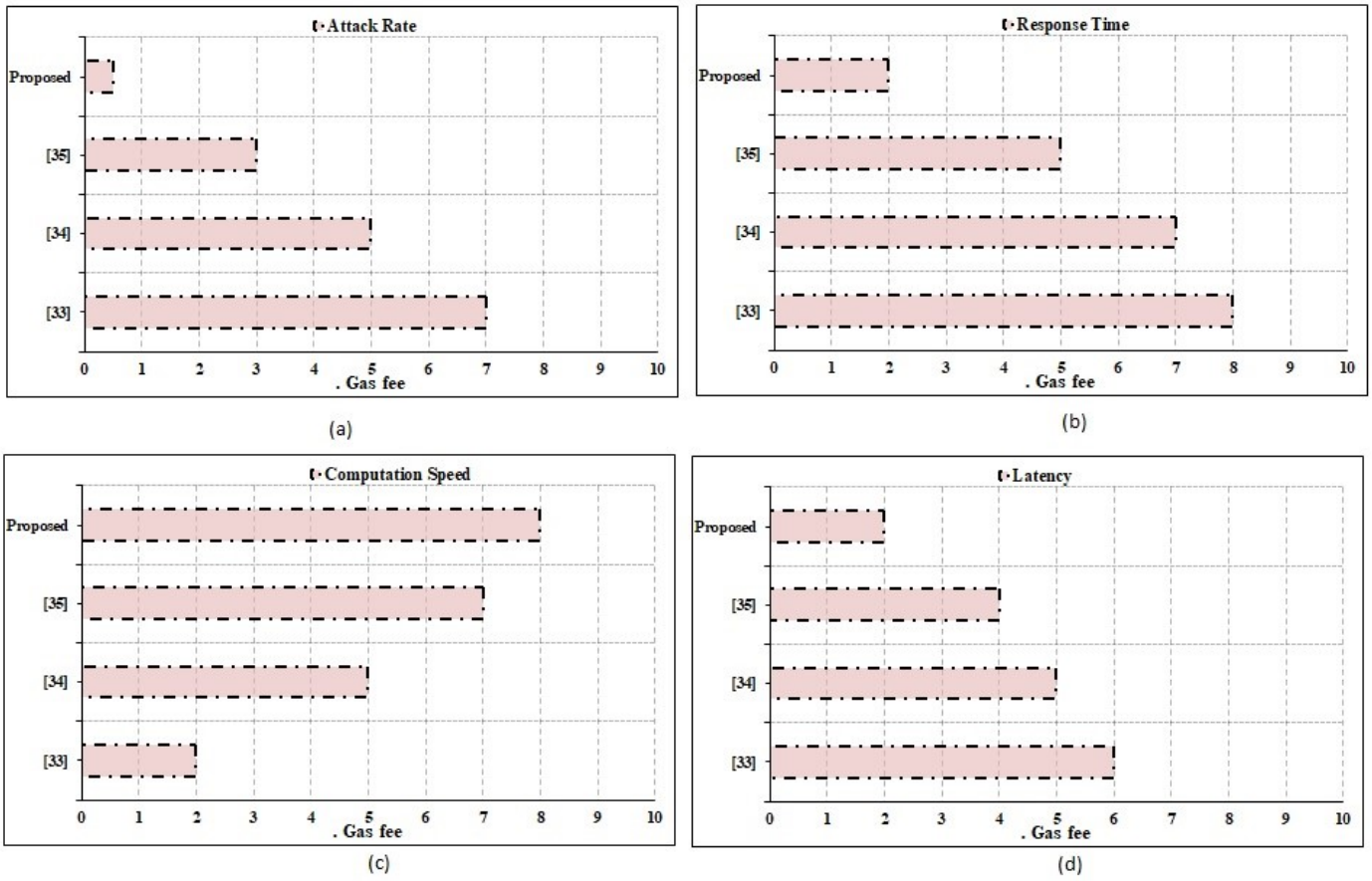

Figure 6. Performance analysis: transaction details.

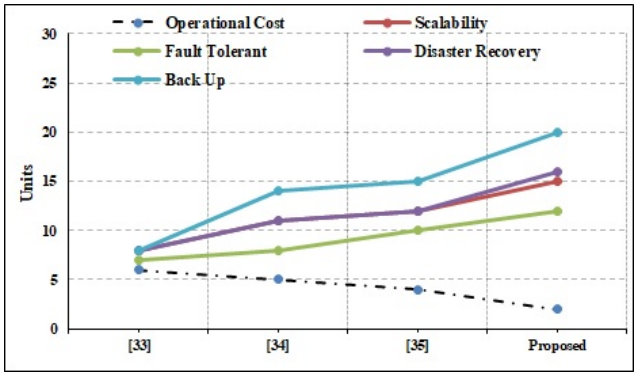

Figure 7. Performance analysis based on non-functional requirements.

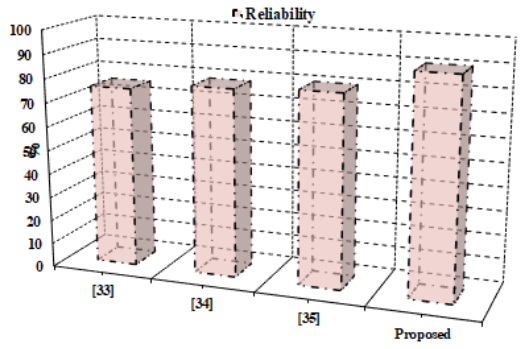

Figure 8. Reliability analysis.

4.4. Stability Analysis

Over numerous experiments, the suggested model's stability is analyzed. The stability metric is used to quantify the change. Its value can be anything from 0 to 1, where 0 represents the least stable state of the system and 1 represents the most stable state. Figure 9 shows a visual representation of the findings for the stability estimation for MAS. The range of stability is averaged to be 0.82, which is better than other techniques. The given framework is highly efficient and successful in securing data.

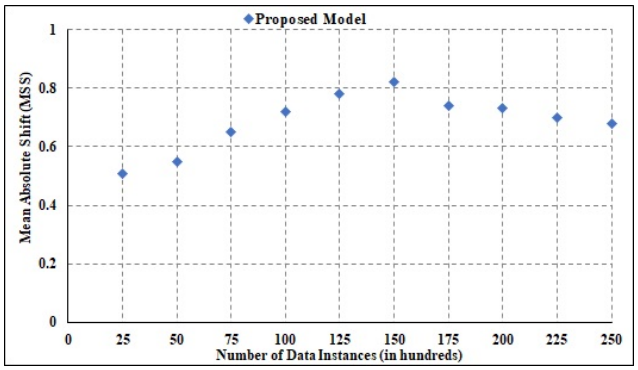

Figure 9. Stability analysis.

5. Conclusions

The UAV concerns of data privacy and preservation are addressed in the current research utilizing blockchain technology. Specifically, the current research focuses on incorporating the blockchain technique and PECC cryptography for ensuring data security during communication. Furthermore, a digital signature is used to verify the authenticity of all transactions in the proposed research, allowing for the highest level of confidentiality and security. Moreover, the proposed technique is deployed over smart vehicular communication as a use-case scenario. The proposed model can ensure transparent and secure data communication over the UAV platform. Experimental simulation results prove that the model is superior and effective in terms of operational cost (2.95 units), scalability (14.98 units), reliability (96.07%), and stability (82.26%). For future research, the current research can be extended to include local storage security over UAVs. Moreover, the battery effectiveness of UAVs is another aspect that can be explored in the future.

Author Contributions: Conceptualization, T.A.A.; Methodology, A.A. and T.A.A.; Software, A.A. and I.U.; Validation, A.A.; Formal analysis, I.U.; Investigation, T.A.A. and I.U.; Writing—original draft, T.A.A.; Writing—review & editing, A.A.; Visualization, I.U.; Supervision, A.A.; Project administration, A.A. All authors have read and agreed to the published version of the manuscript.

Funding: 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 IF2-PSAU-2022/01/22500.

Data Availability Statement: Data sharing does not apply to this article.

Conflicts of Interest: The authors declare no conflict of interest in this area.

Abbreviations

The following abbreviations are used in this manuscript:

UAV	Unmanned Aerial Vehicle
IoT	Internet of Things
BCN	Blockchain Technology
VC	Virtual Circuits

SHA	Secure Hash Algorithm
LTE	Long Term Evolution
AUE	Aerial User Equipment
ECC	Elliptical Curve Cryptography
PECC	Pentatope Elliptic Curve Cryptography
SHA	Secure Hash Algorithm

References

1. Nassi, B.; Bitton, R.; Masuoka, R.; Shabtai, A.; Elovici, Y. SoK: Security and privacy in the age of commercial drones. In Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP), Online, 24–27 May 2021; pp. 1434–1451.
2. Abkenar, F.S.; Ramezani, P.; Iranmanesh, S.; Murali, S.; Chulerttiyawong, D.; Wan, X.; Jamalipour, A.; Raad, R. A Survey on Mobility of Edge Computing Networks in IoT: State-of-the-Art, Architectures, and Challenges. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 2329–2365. [CrossRef]
3. Mozaffari, M.; Saad, W.; Bennis, M.; Nam, Y.H.; Debbah, M. A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2334–2360. [CrossRef]
4. Bhattacharya, P.; Tanwar, S.; Bodkhe, U.; Kumar, A.; Kumar, N. EVBlocks: A blockchain-based secure energy trading scheme for electric vehicles underlying 5G-V2X ecosystems. *Wirel. Pers. Commun.* **2022**, *127*, 1943–1983. [CrossRef]
5. Mohsan, S.A.H.; Khan, M.A.; Noor, F.; Ullah, I.; Alsharif, M.H. Towards the unmanned aerial vehicles (UAVs): A comprehensive review. *Drones* **2022**, *6*, 147. [CrossRef]
6. Salameh, A.I.; El Tarhuni, M. From 5G to 6G—Challenges, Technologies, and Applications. *Future Internet* **2022**, *14*, 117. [CrossRef]
7. Ji, Y.; Tang, H.; Sun, W. Coseismic Gravity Gradient Changes in a Spherical Symmetric Earth Model: Application to the 2011 Tohoku-Oki Earthquake. *J. Geophys. Res. Solid Earth* **2022**, *127*, e2021JB023560. [CrossRef]
8. Ueyama, Y.; Sago, T.; Kurihara, T.; Harada, M. An Inexpensive Autonomous Mobile Robot for Undergraduate Education: Integration of Arduino and Hokuyo Laser Range Finders. *IEEE Access* **2022**, *10*, 79029–79040. [CrossRef]
9. Aloqaily, M.; Hussain, R.; Khalaf, D.; Hani, D.; Oracevic, A. On the Role of Futuristic Technologies in Securing UAV-Supported Autonomous Vehicles. *IEEE Consum. Electron. Mag.* **2022**, *11*, 93–105. [CrossRef]
10. Diaz Linares, I.; Pardo, A.; Patch, E.; Dehghantanha, A.; Choo, K.K.R. IoT Privacy, Security and Forensics Challenges: An Unmanned Aerial Vehicle (UAV) Case Study. In *Handbook of Big Data Analytics and Forensics*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 7–39.
11. Elnabty, I.A.; Fahmy, Y.; Kafafy, M. A survey on UAV placement optimization for UAV-assisted communication in 5G and beyond networks. *Phys. Commun.* **2022**, *51*, 101564. [CrossRef]
12. Fotouhi, A.; Qiang, H.; Ding, M.; Hassan, M.; Giordano, L.G.; Garcia-Rodriguez, A.; Yuan, J. Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3417–3442. [CrossRef]
13. Akhloufi, M.A.; Couturier, A.; Castro, N.A. Unmanned aerial vehicles for wildland fires: Sensing, perception, cooperation and assistance. *Drones* **2021**, *5*, 15. [CrossRef]
14. Lee, W.; Lee, J.Y.; Joo, H.; Kim, H. An MPTCP-Based Transmission Scheme for Improving the Control Stability of Unmanned Aerial Vehicles. *Sensors* **2021**, *21*, 2791. [CrossRef] [PubMed]
15. Wu, Q.; Xu, J.; Zeng, Y.; Ng, D.W.K.; Al-Dhahir, N.; Schober, R.; Swindlehurst, A.L. A comprehensive overview on 5G-and-beyond networks with UAVs: From communications to sensing and intelligence. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 2912–2945. [CrossRef]
16. Li, G.; Ren, X.; Wu, J.; Ji, W.; Yu, H.; Cao, J.; Wang, R. Blockchain-based mobile edge computing system. *Inf. Sci.* **2021**, *561*, 70–80. [CrossRef]
17. Karnik, N.; Bora, U.; Bhadri, K.; Kadambi, P.; Dhatrak, P. A comprehensive study on current and future trends towards the characteristics and enablers of industry 4.0. *J. Ind. Inf. Integr.* **2022**, *27*, 100294. [CrossRef]
18. Wu, C.; Xiong, J.; Xiong, H.; Zhao, Y.; Yi, W. A Review on Recent Progress of Smart Contract in Blockchain. *IEEE Access* **2022**, *10*, 50839–50863. [CrossRef]
19. Muravskyi, V.; Zadorozhnyi, Z.M.; Lytvynenko, V.; Yurchenko, O.; Koshchynets, M. Comprehensive use of 6G cellular technology accounting activity costs and cyber security. *Indep. J. Manag. Prod.* **2022**, *13*, s107–s122. [CrossRef]
20. Rehman Javed, A.; Jalil, Z.; Atif Moqurrab, S.; Abbas, S.; Liu, X. Ensemble adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4088. [CrossRef]
21. Majeed, S.; Sohail, A.; Qureshi, K.N.; Iqbal, S.; Javed, I.T.; Crespi, N.; Nagmeldin, W.; Abdelmaboud, A. Coverage Area Decision Model by Using Unmanned Aerial Vehicles Base Stations for Ad Hoc Networks. *Sensors* **2022**, *22*, 6130. [CrossRef]
22. Salah, K.; Nizamuddin, N.; Jayaraman, R.; Omar, M. Blockchain-Based Soybean Traceability in Agricultural Supply Chain. *IEEE Access* **2019**, *7*, 73295–73305. [CrossRef]
23. Hasan, H.R.; Salah, K. Proof of Delivery of Digital Assets Using Blockchain and Smart Contracts. *IEEE Access* **2018**, *6*, 65439–65448. [CrossRef]
24. Deepa, N.; Pham, Q.V.; Nguyen, D.C.; Bhattacharya, S.; Prabadevi, B.; Gadekallu, T.R.; Maddikunta, P.K.R.; Fang, F.; Pathirana, P.N. A survey on blockchain for big data: approaches, opportunities, and future directions. *arXiv* **2022**, arXiv:2009.00858.

25. Chen, Y.; Feng, W.; Zheng, G. Optimum placement of UAV as relays. *IEEE Commun. Lett.* **2017**, *22*, 248–251. [CrossRef]
26. Fatima, N.; Saxena, P.; Gupta, M. Integration of multi access edge computing with unmanned aerial vehicles: Current techniques, open issues and research directions. *Phys. Commun.* **2022**, *52*, 101641. [CrossRef]
27. Alsamhi, S.H.; Shvetsov, A.V.; Shvetsova, S.V.; Hawbani, A.; Guizan, M.; Alhartomi, M.A.; Ma, O. Blockchain-empowered security and energy efficiency of drone swarm consensus for environment exploration. *IEEE Trans. Green Commun. Netw.* **2022**, *7*, 328–338. [CrossRef]
28. Khan, A.A.; Laghari, A.A.; Gadekallu, T.R.; Shaikh, Z.A.; Javed, A.R.; Rashid, M.; Estrela, V.V.; Mikhaylov, A. A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment. *Comput. Electr. Eng.* **2022**, *102*, 108234. [CrossRef]
29. Islam, A.; Al Amin, A.; Shin, S.Y. FBI: A federated learning-based blockchain-embedded data accumulation scheme using drones for Internet of Things. *IEEE Wirel. Commun. Lett.* **2022**, *11*, 972–976. [CrossRef]
30. Singh, M.; Aujla, G.S.; Bali, R.S.; Batth, R.S.; Singh, A.; Vashisht, S.; Jindal, A. CovaDel: A blockchain-enabled secure and QoS-aware drone delivery framework for COVID-like pandemics. *Computing* **2022**, *104*, 1589–1613. [CrossRef]
31. Gupta, M.; Varma, S. Optimal placement of UAVs of an aerial mesh network in an emergency situation. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 343–358. [CrossRef]
32. Ch, R.; Srivastava, G.; Gadekallu, T.R.; Maddikunta, P.K.R.; Bhattacharya, S. Security and privacy of UAV data using blockchain technology. *J. Inf. Secur. Appl.* **2020**, *55*, 102670. [CrossRef]
33. Benaya, A.; Ismail, M.H.; Ibrahim, A.S.; Salem, A.A. Physical Layer Security Enhancement via Intelligent Omni-Surfaces and UAV-Friendly Jamming. *IEEE Access* **2023**, *11*, 2531–2544. [CrossRef]
34. Xu, R.; Zeng, Q.; Zhu, L.; Chi, H.; Du, X.; Guizani, M. Privacy leakage in smart homes and its mitigation: IFTTT as a case study. *IEEE Access* **2019**, *7*, 63457–63471. [CrossRef]
35. Choi, N.; Kim, H. A Blockchain-based user authentication model using MetaMask. *J. Internet Comput. Serv.* **2019**, *20*, 119–127.
36. Almadhoun, R.; Kadadha, M.; Alhemeiri, M.; Alshehhi, M.; Salah, K. A user authentication scheme of IoT devices using blockchain-enabled fog nodes. In Proceedings of the 2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA), Aqaba, Jordan, 28 October–1 November 2018; pp. 1–8.
37. Erola, A.; Agrafiotis, I.; Nurse, J.R.; Axon, L.; Goldsmith, M.; Creese, S. A system to calculate cyber-value-at-risk. *Comput. Secur.* **2022**, *113*, 102545. [CrossRef]