energies

MDPI

Article

Energy-Aware UAV Based on Blockchain Model Using IoE Application in 6G Network-Driven Cybertwin

Atul B. Kathole [1], Jayashree Katti [1], Dharmesh Dhabliya [2], Vivek Deshpande [3], Anand Singh Rajawat [4], S. B. Goyal [5,*], Maria Simona Raboaca [6,7,8,*], Traian Candin Mihaltan [7], Chaman Verma [9] and George Suciu [10,*]

1 Department of Information Technology, Pimpri Chinchwad College of Engineering, Pune 411044, India
2 Department of IT, Vishwakarma Institute of Information Technology, Pune 411048, India
3 Computer Engineering Department, Vishwakarma Institute of Information Technology, Pune 411048, India
4 School of Computer Sciences & Engineering, Sandip University, Nashik 422213, India
5 Faculty of Information Technology, City University, Petaling Jaya 46100, Malaysia
6 ICSI Energy Department, National Research and Development Institute for Cryogenics and Isotopic Technologies, 240050 Ramnicu Valcea, Romania
7 Faculty of Building Services, Technical University of Cluj-Napoca, 400114 Cluj-Napoca, Romania
8 Doctoral School, University Politehnica of Bucharest, Splaiul Independentei Street, No. 313, 060042 Bucharest, Romania
9 Faculty of Informatics, University of Eötvös Loránd, 1053 Budapest, Hungary
10 R&D Department Beia Consult International Bucharest, 041386 Bucharest, Romania
* Correspondence: sb.goyal@city.edu.my (S.B.G.); simona.raboaca@icsi.ro (M.S.R.); george@beia.ro (G.S.)

check for updates

Citation: Kathole, A.B.; Katti, J.; Dhabliya, D.; Deshpande, V.; Rajawat, A.S.; Goyal, S.B.; Raboaca, M.S.; Mihaltan, T.C.; Verma, C.; Suciu, G. Energy-Aware UAV Based on Blockchain Model Using IoE Application in 6G Network-Driven Cybertwin. *Energies* **2022**, *15*, 8304. https://doi.org/10.3390/en15218304

Academic Editors: R. Maheswar, M. Kathirvelu and K. Mohanasundaram

Received: 19 September 2022
Accepted: 28 October 2022
Published: 7 November 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Abstract: Several advanced features exist in fifth-generation (5G) correspondence than in fourth-generation (4G) correspondence. Centric cloud-computing architecture achieves resource sharing and effectively handles big data explosion. For data security problems, researchers had developed many methods to protect data against cyber-attacks. Only a few solutions are based on blockchain (BC), but are affected by expensive storage costs, network latency, confidence, and capacity. Things are represented in digital form in the virtual cyberspace which is the major responsibility of the communication model based on cybertwin. A novel cybertwin-based UAV 6G network architecture is proposed with new concepts such as cloud operators and cybertwin in UAV. Here, IoE applications have to be energy aware and provide scalability with less latency. A novel Compute first networking (CFN) framework named secure blockchain-based UAV communication (BC-UAV) is designed which offers network services such as computing, caching, and communication resources. The focus of the blockchain was to improve the security in the cloud using hashing technique. Edge clouds support core clouds to quickly respond to user requests.

Keywords: 6G; cloud-computing; cybertwin; blockchain; UAV; IoE; CFN; BC-UAV

1. Introduction

Efficient and effective options for developing intelligent cities can be found in unmanned aerial vehicles (UAVs). They are broadly employed in civil and military domains, including data collecting, distribution of data, audio and video monitoring, aerial images, crop surveys, and real-time medical services. [1]. Due to the COVID-19 pandemic situation, several businesses are forced to do online. Ericsson predicted that 5Gwill be rapidly commercialized as numerous individuals embrace this change. As a result, using the Internet has become essential for better connectivity in order to meet the demands and requirements of a more stringent network. This is essential to simplify the emerging techniques to extend the reality, tactile, related independent systems [2], telemedicine, and Industrial Internet of Things (IIoT) [3], which has an impact on latency and data speed has to be high. Low latency and higher data speed minimize collision rates and provide more secure autonomous vehicles.

These applications must necessarily provide smart autonomous life, multisensory virtual experience, smart agriculture, smart cities, and even more. Unfortunately, 5G networks are not efficient enough to meet these emerging demands [4]. Thus, there has aroused a necessity to develop efficient 6G wireless communication networks which can upgrade social needs, thereby enabling Sustainable Development Goals (SDGs) [5].

Networks of the next generation may have a demand with people and devices connected. Hence, the network architecture in the future has to overcome the increasing traffic in mobile Internet along with the services and applications by the use of heterogeneous networks. It is considered that the future Internet of Everything (IoE) can intellectually connect humans, data, processes, and things [6]. For this, techniques related to artificial intelligence (AI) and mobile communication are used which makes the connections in the network more relevant, reliable, and valuable than the ones that is existing. This IoE architecture due to its revolutionary feature supports ubiquitous data collection, processing, aggregation, fusion, distribution, and service. There arouse several challenges and issues due to the disruptive change in designing IoE network architecture, providing mobility, scalability, availability, and security.

Security, dependability, flexibility, and extensibility are a few services offered by Nebula for Internet architecture with the use of more reliable routers and extendable control planes. Moreover, it enforces arbitrary policies using multiple paths. However, still, there exist limitations in scalability and performance as processing ability at the network edge is ignored. Moreover, issues related to the growing demands for resources and services are not considered. The CloNet is in a multi-administrative domain setup which helps network and data center domains to interact, thereby providing an elastic dynamic network to serve the customers on the cloud. Additionally, resources utilized for computing and storage are deployed for better end-user experience and to reduce network dependency.

A cloud-centric network architecture built on cybertwin is proposed to deal with scalability, availability, mobile, and safety for future networks. As an IoE helper, data recorder, and digital asset owner, Cybertwin operates. This architecture is designed using blockchain technology and fog computing. For device-devices, devices-to-FN, and FN-to-FN components, the resource provisioning model was used [7].

The main contribution of this research is sensitive applications and applications connected to end-users. There are several data security and data security problems, and worldwide researchers have provided many methods to protect data against cyber-attacks. Many of them have offered very computational cryptography solutions. Very few academics provide solutions based on blockchain (BC); however, their solutions may be affected by expensive storage costs, as well as problems in network latency, confidence, and capacity. This issue can be overcome by a novel cybertwin-based 6G network. The architectural design is proposed by introducing new concepts such as cloud operators and cybertwin. In the cybertwin-based UAV, IoE applications have to be energy aware and must provide scalability with less latency. A novel CFN framework is designed securely and blockchain-based UAV communication (BC-UAV).

In Section 2, the related works are presented. Section 3 shows the proposed model for CFN-based BC-UAV. Evaluation criteria are discussed in Section 4. Finally, the conclusion is presented in Section 5.

2. Literature Review

A peer-to-peer network utilized in many different types of technology was in charge of managing UAV communication based on the blockchain. The uses of DLT are mentioned to mitigate multiple cyber-threats which classified major cyber-attacks into four categories, namely scanning, power of root, local to remote, and denial of service [8]. The security issues in fog-enabled IoT applications were examined. Blockchain was considered to address these issues [9]. Moreover, this work failed to consider the ability of blockchain with AI. A detailed survey on reinforcement learning applications based on blockchain used in industrial IoT networks was presented [10]. It was revealed that the Q-learning algorithm,

one of the machine learning strategies, improved the network performance. A two-way convergence of blockchain with ML was discussed [11]. Blockchain with ML features provided security and reliability. ML was the tool used for optimizing blockchain networks.

The present blockchain based on AI techniques was examined for energy-cloud management, where the security and privacy issues were listed out [12]. A comprehensive study on blockchain-AI applications was presented along with their relationship in the IoT-enabled ecosystem. However, MEC which is a key technology of evolving 5G networks were not concentrated [13]. Blockchain techniques in 5G networks were discussed and a short survey was presented [14]. Three major challenges were identified, namely identity authentication, privacy, and trust management along with a few blockchain-based solutions. A short survey on the blockchain-enabled federated model was described [15]. In motivation to integrate MEC with blockchain was presented [16]. Edge computing was employed to enable mobile blockchains. Edge computing integrated with blockchain was examined. It was found that blockchain extended the ability of edge computing [17]. With this as the basis, the present work in this paper focuses on the blockchain-enabled distributed and decentralized ML approach. Anti-phishing approaches were used at different levels and has to meet a few predefined conditions. Random forest (RF) classifier was used for classifying the mails received on the basis of commonly known features set and the possible threats made known for which phishing incoming mails were required [18]. When an illegal mail received was redirected to a webpage, the level of similarity between legitimate and suspicious webpages was identified and classification was based on a content-based anti-phishing approach.

IoT devices performed edge computation on the resource owner nodes when required. A framework was developed in which in corporate blockchain technology in the applications based on IoT [19]. A Logchain system based on oneM2M which integrated IoT and blockchain technology was utilized which ensured block integrity. However, still, several security issues were not taken into account. To handle the inhibited nature of IoT, blockchain technology was integrated with Edge Computing in [20] which minimized the needs of the IoT device such as memory capacity. Moreover, the performance was improved and was satisfactory. The issues of this approach were addressed and one major issue evaluated was resource optimization which was not achieved. In [21], for enabling propitiation, techno-economic factors and normative assumptions were considered. However, data privacy was still low.

3. Cybertwin Based Network Architecture for 6G with Cloud-Fog Based Network (CFN) Block Chain Based UAV Communication (BC-UAV)

Cybertwin offers a few functions such as communication assistance, network behavior logger, and digital asset which satisfies several new design needs of the network. In end-to-end communication, an end-to-end connection to the server has to be established by the end devices to provide services. As depicted in Figure 1, in this cybertwin-based communication model, the things available in the physical network have to be initially connected with cybertwin which in turn obtains the necessary service from the network and then is delivered to the end-user. This is the most basic function termed as communication assistance function. During the network behavior logger function, while digital representation, cybertwin obtains and logs every data for users. In the digital asset function, cybertwin, after the removal of sensitive information, converts the behavior data of the user to a digital asset for sale. For obtaining improved performance with minimized latency, the technique for distribution assists in offering services based on demand. The standard of life for the citizens will improve as well as the residential expectations. The data processing can be speed-up by a pattern of fog computing which assists the elements of IoE through minimized latency [22].

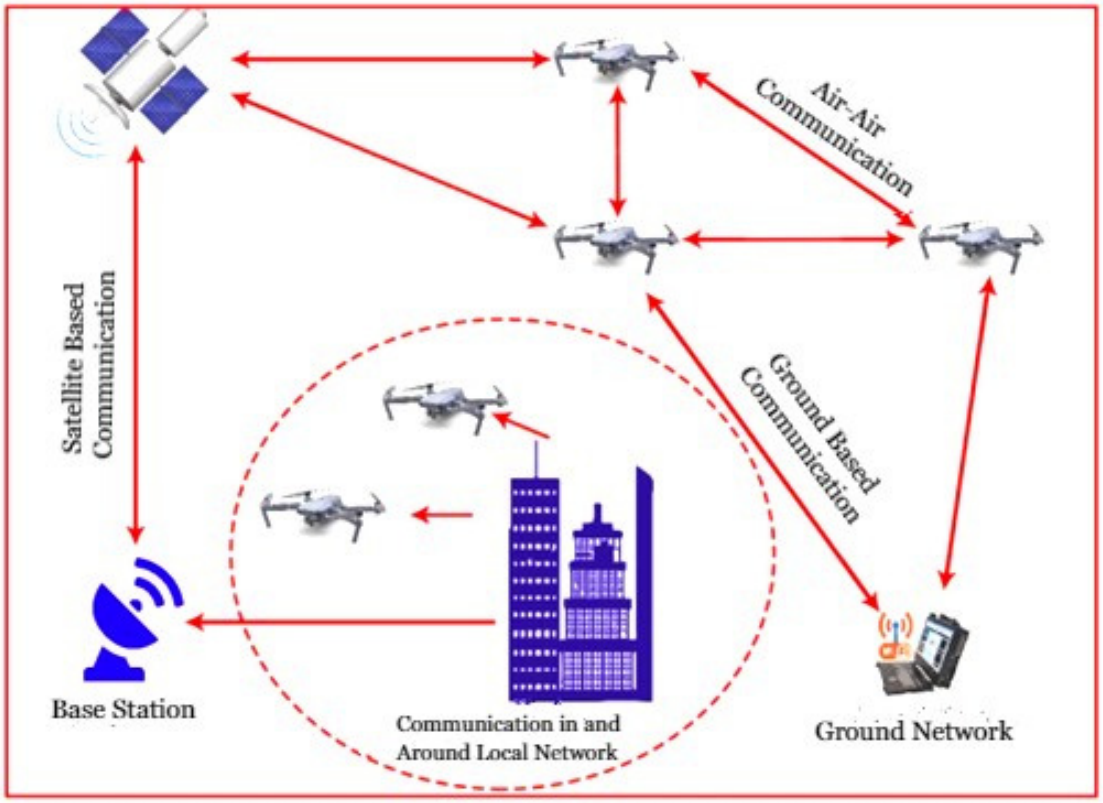

Figure 1. Cybertwin UAV-based communication.

3.1. Cybertwin Communication Model

It is already known that the recent Internet paradigm has no ability to satisfy the needs of the mobile network in the future. The IP address of the present Internet indicates the identity as well as the location information of the device. Due to this reason, the Internet faces difficulties in handling the growing needs of mobile devices as well as services thus causal ability challenges [23]. The network to be trustworthy and secure, the present Internet depends on the security measures of the end-to-end connection and adopts trustworthy users. No procedure is utilized for authenticating the users; hence several security issues are experienced. For ensuring the quality of service (QoS), the Internet considers the way communication resources are managed alone while the other entities are responsible for managing computing and caching resources. Thus, coordination among resources is not easily obtained. Hence, a novel cloud-centric Internet architecture following a cybertwin-based communication model is proposed which is better than using an end-to-end communication model [24].

3.2. Cloud-Centric Internet Architecture

This novel cloud-centric Internet architecture introduced here is depicted in Figure 2. The IP layer is still used as the "thin waist" of the stack in order to permit the developments in other layers and the continuous updates made in the infrastructure of legacy networks. In this architecture, there exist two new components in the network infrastructure which is the fog cloud above the IP layer. Many fully connected core clouds are present to offer network services such as computing, caching, and communication resources. In between core clouds and end users, edge clouds are present which support core clouds to respond to the requests of the end users quickly [25,26].

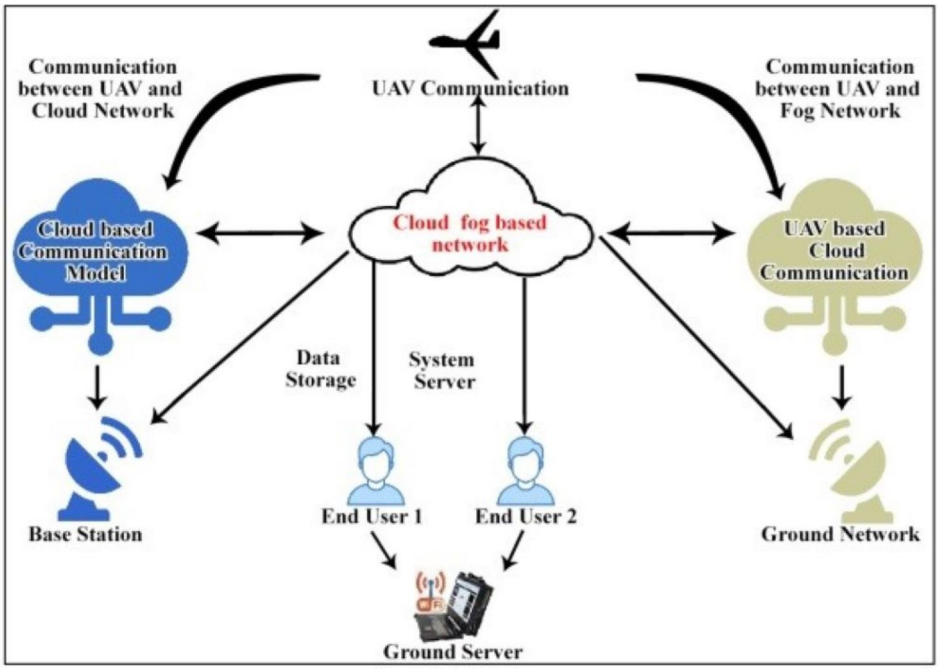

Figure 2. Cloud-fog architecture with IOT based on UAV.

In this Internet architecture, a new cloud operator is introduced to help in constructing an operating system for a cloud network, as illustrated in Figure 3. Services such as computing, caching, and communication resources are scheduled and coordinated accordingly. Moreover, a real-world trading environment for the end users is also established which helps in deploying more multi-purpose resources due to scarcity [27,28].

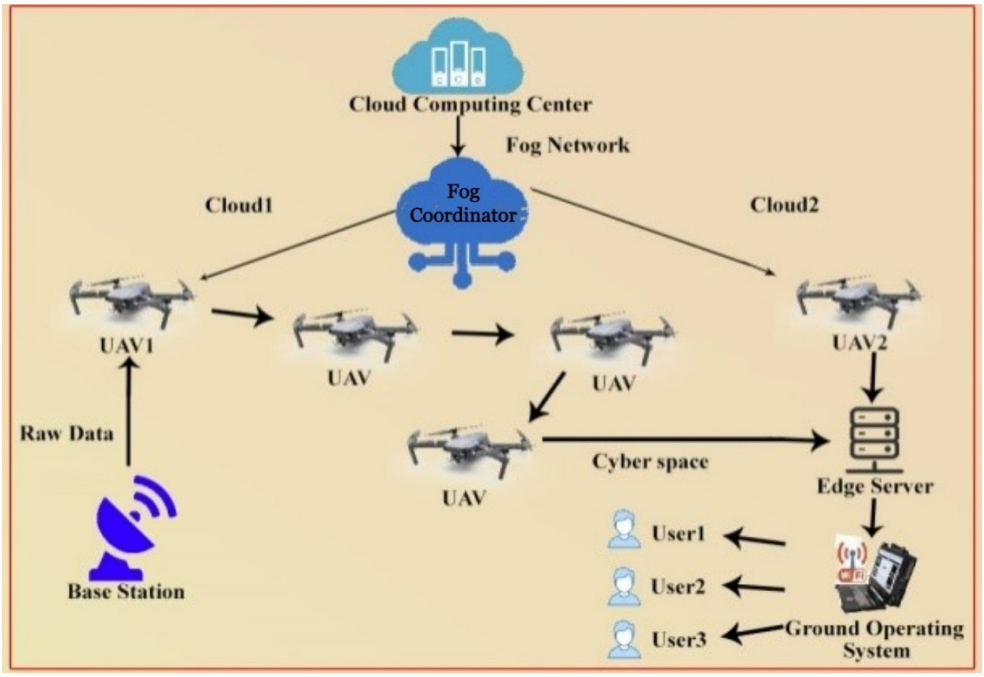

Figure 3. Cloud-fog network operating system with UAV.

According to the services provided by cloud operators in the network, the service providers of the application offer services to core clouds and edge thereby forming a service network. Due to this, the operational cost is reduced and no dedicated servers are required, thus offering the best QoS to the end users [29].

The proposed block chain-fog based network (BFN) connects to the Internet of Everything (IoE) and fog nodes of UAV. The distributed technology provides on-demand services thereby higher performance and less latency rate are achieved. From the citizen's point of view, their quality of life is improved and their expectations are met. Fog computing supports the components of IoE for quick data processing as latency is low [30]. By utilizing its unique features, such as immutability, effective cryptography, and distributed decentralized storage systems, the introduction of blockchain innovation will address these issues [31–36]. The authors [37] evaluated and organized all cryptographic ideas currently employed in blockchain technology in-depth. We also provide a list of cryptographic ideas that have not been used yet but could greatly enhance state-of-the-art blockchain solutions.

This BFN architecture comprises fog nodes. The fog nodes layer reduces the latency by processing the data received by fog nodes from the traffic of IoE. Expectations of the users are satisfied by providing faster services. In this architecture, the fog node layer denotes the devices connected with one another and with FN. The communication among the connected devices is secured as blockchain technology is employed.

3.3. Fog Node Layer

The users demand services that are met with IoE devices connected using fog computing for smart cities. Blockchain technology provides more reliability with the added new component. Several physical servers are integrated to form FN covering certain regions.

4. Block Chain Based UAV Communication (BC-UAV)

The physical UAVs fly in this layer to sense the data application/situation is used in the data sensing, that is, {S1, … Sn, … SN} for which UAV is used. For various applications with differing weights, capability of payload, elevation of the flight as well as choices to fly which has enormous dimensions of UAV. The UAVs are supposed to fly in a three-dimensional space having coordinates at time τ can be [x(τ), y(τ), z(τ)], are parallel to the ground and z(μ) are in a vertical height where UAVs can fly [23–26]. When the UAV is projected at an angle, the equations are given from the ground at the initial speed V at the following time as given in Equation (1):

$$\varnothing_{MN}^{ACn} = \varphi MN + \xi MN \sum_{f=1}^{Nf} \lambda_f \tag{1}$$

where λ_f is the bit rate of the flow f.

Range R of UAV attained has been represented by Equation (2)

$$\phi_{ABC}^{ACn} = N_s \cdot \varphi_{ABC} + \xi_{ABC} \sum_{f=1}^{Nf} \lambda_f \tag{2}$$

where R in particular is one of the elements that determines UAV deployment. For instance, the R should be high in the event of military use. In order to secure and reliable communication, communication of UAVs as well as data sharing between the UAVs in the B_{public} network UAV layer. A UAV can only store data in B public when the rules and criteria of SC are fulfilled. On the other hand, UAVs can also use B_{public} network to detect data from D_{SL} to assure confidentiality as well as secrecy of data. Every single UAV has a common ledger replica, thus reducing the latency of access to stored information. To reduce latency and boost system reliability, communication between UAVs and ground stations through a communication network of 6G. The blockchain-based UAV can be represented by Equations (3)–(6),

$$x_m = \frac{x}{a} \tag{3}$$

$$t = \frac{x_t}{x} \tag{4}$$

$$s_m = \frac{s}{a} \tag{5}$$

$$IDS = \frac{\sum a \epsilon X m_y}{x} \tag{6}$$

For exchange between UAVs, base stations, level of BC, and the x-layer, the communication system is a 6G system that delivers an enormously large range of information, ideal for latency-conscious applications. The features of the network layer of 6G communication include highly reliable (10−9), highly minimized latency (1 TB), and in elevation spectrum performance (3–10 P/M over 5G). The complete list of 6G functionalities compared to 5G can be found in Table 1. 6G provides software-defined networking (SDN) which isolates the control plane (CP) and the data plane (DP), allowing a centralized entity (controller) in the CP to configure the forwarding devices in the DP, enabling programmable and dynamic network setup, and network function virtualization (NFV) is a paradigm for network architecture where NFs that previously utilized specialized vendor-specific hardware [38]. SDN is a software prototype that splits the level of data from the controller to simplify and efficiently manage the UAV network. NFV virtualizes network infrastructure, including computer, memory as well as machinery components of the channel, in order to create a channel of UAV with more economic, effective and resistant. Since some of the UAV applications are crucial, even a 1 ms interval cannot be tolerated. The military and healthcare applications would be such. More latency of the network, the more chances of failure. Thus, latency (l) in UAV communication is a key parameter as given in Equation (7):

$$l_{M \to D}(d_{M,l}) = \mathbb{P}_{LOS}\left(d_{M,l,h_D}\right) L_0 d_{M,l}^{-\alpha A} + \left(1 - \mathbb{P}_{LOS}\left(d_{M,l,h_D}\right)\right) L_{NLOS} L_0 d_{M,l}^{-\alpha A} \tag{7}$$

Table 1. Network efficiency.

Number of Internet Things	CT-CNN [10]	DLT [8]	BAI_ECM [14]	CT-6G_CFN
10	92	92.1	92.3	92.4
20	92.5	93	94	95
40	93.8	93.8	95.8	96
60	94.3	94.2	96	97
80	95	95.1	96.5	98
100	96.5	96.8	97.1	98.5

Therefore, the energy for communication latency of UAV is given as Equations (8) and (9):

$$E_{tx}(l,d) = E_{tx-elec}(m) + E_{tx-amp}(l,d) \tag{8}$$

$$E_{tx}(l,d) = \begin{Bmatrix} m.E_{elec} + m \\ m.E_{elec} + d_{crossover} \end{Bmatrix} \tag{9}$$

Value l changes from channel to channel (end-to-end delay), i.e., from LTE-A to 6G, as shown in Equation (10):

$$\begin{gathered} \ell_{L\pi E-A} \leq 20 \text{ ms} \\ \ell_{5G} \leq 5 \text{ ms} \\ \ell_{B_{\mathrm{Fg}}md-5G} \leq 1 \text{ ms} \\ \ell_{6G} \leq 0.1 \text{ ms}. \end{gathered} \tag{10}$$

4.1. IoE Layer

This layer helps the users to deploy the application in a real-time environment with no limits. Clusters are formed based on the location and function of the IoT devices thus improving throughput and reducing energy consumption, time, and cost overheads. There is an increase in the workload of data centers as hardware and software services require processing by integration. Peer-to-peer (P2P) TCP/IP communication among IoT devices

takes place at a shorter distance. For longer distances, these devices make use of FN and communicate using technologies such as WIFI, ZigBee, and Bluetooth.

4.2. Blockchain for IoE

The proposed system uses blockchain for IoE due to its decentralized and tamper-proof nature. Thus, billions of devices in the network can be easily tracked. Moreover, the cost of managing and deploying the server is also reduced.

4.3. Data Transfer

This proposed CFN architecture helps in improving the mobility of the users in the applications based on IoE with fog nodes and cloud computing. Moreover, security is achieved to a greater extent using the blockchain technique where anonymous users are restricted to access IoE devices.

4.4. Cloud Network Layer Security

Assuming that the whole network is an R-circular region, where the characteristics of the network are analyzed in a huge R-based network. The received power in the Prx(xi, xj) main recipient, xj, should rise when increasing the primary transmitter P power and the Íh(xi, xj)Í amplitude of the complex fade coefficient of the primary link transmitter and the primary receptor in a quasi-static wireless environment. In addition, if the distance between primary transmitter xi and primary receiving xj rises, the received power would decrease. In addition, wireless transmission has to do with the trajectory loss exponent which, due to varying communication environments, fluctuates between 0.8 and 4. We explore situation a > 2 here to estimate the interference of primary users and eavesdroppers from the secondary users. The interference power on the primary recipient from the secondary user assumes that WP is the noise power introduced by the main receivers and IP. Now, we analyze a specific situation in the wireless environment where there is simply path loss h(xi,xj), and that is normalized to be one for everyone and not equal to j. Various antenna of the secondary receiver along with the eavesdropper have been prepared while the information of channel state is a channel of eavesdropper's and it is not available in the secondary transmitter [25]. To improve the security in the cloud the hash function is introduced. A hashing operation H is a function that converts an input of any size to an output of a specific size. There are some more characteristics of cryptographic hash functions, such as: Collision resistance: It is challenging to find two inputs a and b such that $H(x^i) = H(y^i)$; preimage resistance: It is challenging to find an input a such that $H(x^i)) = Y$ for a given output Y; and second preimage resistance: It is challenging to find an additional input yi such that $H(y^i) = Y$ for an input x^i and output = $H(x^i)$. The thermal power of the primary users and wafers is considered to be the same because this noise power can be presumed to be independent of a secondary user's location and they are both W. The powers received by the primary users and by the eavesdroppers can all be determined by wireless transmission propagation laws. This simplifies the secrecy capacity as shown in Equation (11):

$$C_s(x_i, x_j) = max\left\{ \begin{array}{l} \log_2\left(1 + \frac{P}{\|x_i - x_j\|^T (w + t_p)}\right) \\ -\log_2\left(1 + \frac{P}{\|x_i - e^*\|^\alpha (W + I_E)}\right), 0 \end{array} \right\} \quad (11)$$

The probability density function of IP and IE can first be derived. Then, the secrecy capacity *Cs*(*i,j*) is the probability density function from Equation (12):

$$f_{C_z(i,j)}(c) = \begin{cases} f_{C_P(i,j)}(c) * f_{C_E}(-c), & c > 0, \\ Pr_{0,j} \cdot \delta(c), & c = 0, \\ 0, & c < 0. \end{cases} \quad (12)$$

where I is the primary user's transmitter, j is the nearest neighbor j of transmitter I, and $f_{CP}(i,j)(c)$, $f_{CE}(c)$, $d(c)$, and Pr0,j denotes the primary user probability density, eavesdropper capacity probability function, and Dirac delta function and zero capability.

Depending upon the probability of secrecy, first-order expansion of $F_{\gamma_M|\{X\}}(\gamma)$ on X is represented by Equation (13),

$$F_{\gamma_M|\{X\}}(\gamma) = \begin{cases} \left(\frac{\gamma}{\overline{\gamma}_1}\right)^{n_B}, X \le \frac{\overline{\gamma}_p}{\overline{\gamma}_0} \\ \left(\frac{X}{\overline{\gamma}_1\sigma}\gamma\right)^{n_B}, X > \frac{\overline{\gamma}_p}{\overline{\gamma}_0} \end{cases} \tag{13}$$

the binomial expansion, the cloud network outage probability of secrecy is computed from Equation (14),

$$\begin{aligned} P_{out}^{\infty} = & \left(-1 - e^{-\frac{\overline{\gamma}_p}{\overline{\gamma}_0\Omega_0}}\right) \sum_{i=0}^{n_B} \binom{n_B}{i} \left(\frac{2^{R_s}-1}{\overline{\gamma}_1}\right)^{n_B-i} \left(\frac{2^{R_S}}{\overline{\gamma}_1}\right)^{i} \\ & \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} \frac{n_E}{\overline{\gamma}_2}(-1)^j \int_0^{\infty} (\gamma_E)^i e^{-\frac{(j+1)\sim E}{\overline{\gamma}_2}} d\gamma_E \\ & + \sum_{i=0}^{n_B} \binom{n_B}{i} \left(\frac{2^{R_S}-1}{\overline{\gamma}_1\sigma}\right)^{n_B-i} \left(\frac{2^{R_S}}{\overline{\gamma}_1\sigma}\right) \sum_{j=0}^{in_E-1} \binom{n_E-1}{j} \\ & \frac{n_E}{\overline{\gamma}_2\sigma}(-1)^j \frac{1}{\Omega_0} \int_{\frac{\pi_p}{\gamma_0}}^{\infty} e^{-\frac{x}{\Omega_0}} \int_0^{\infty} x^{n_B+1} (\gamma_E)^i e^{-\frac{(j+1)\gamma_E}{\overline{\gamma}_2\sigma}} d\gamma_E dx \end{aligned} \tag{14}$$

Employing Equation (14) given by $\int_0^{\infty} x^n e^{-\mu x} dx = \frac{1(n+1)^*}{\mu^{n+1}}$ integrally evaluated and the cloud network outage probability of secrecy is derived by Equation (15)

$$P_{out}^{\infty} = (G_a\overline{\gamma}_1)^{-G_i} + O\left(\overline{\gamma}_1^{-G_d}\right) \tag{15}$$

where the diversity order for secrecy is given by Equation (16):

$$zG_d = n_B \tag{16}$$

and the gain of secrecy array is given by Equation (17):

$$\begin{aligned} G_a = & \left[\left(1 - e^{-\frac{\sigma}{n_0}}\right) \sum_{i=0}^{n_B} \binom{n_B}{i} \left(2^{R_S}-1\right)^{n_B-i} 2^{R_s i} \right. \\ & \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} n_E \overline{\gamma}_2{}^i (-1)^j \frac{\Gamma(i+1)}{(j+1)^{i+1}} + \sum_{i=0}^{n_B} \binom{n_B}{i} \\ & \left(2^{R_S}-1\right)^{n_B-i} \sigma^{-n_B} 2^{R_s i} \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} n_E (\overline{\gamma}_2\sigma)^i \\ & \left. (-1)^j (\Omega_0)^{n_B-i} \frac{\Gamma(i+1)}{(j+1)^{i+1}} \Gamma\left(n_B - i + 1, \frac{\sigma}{\Omega_0}\right)\right]^{-\frac{1}{n_B}} \end{aligned} \tag{17}$$

where incomplete gamma function is represented by $\Gamma(\cdot, \cdot)$.

The CDF and PDF of Y are written by Equations (18) and (19):

$$F_Y(y) = \sum_{n=0}^{N} \binom{N}{n} (-1)^n e^{-\frac{nv}{n_Y}} \tag{18}$$

$$f_Y(y) = \sum_{n=0}^{N-1} \binom{N-1}{n} \frac{N}{\Omega_Y} (-1)^n e^{-\frac{(n+1)y}{n_Y}} \tag{19}$$

Let $u(X) = \min\left(\frac{\overline{\gamma}_p}{X}, \overline{\gamma}_0\right)$. Using the probability theory, for RV$\gamma = u(X)Y$ the conditional CDF and PDF of γ can be obtained as (19) and (20), respectively.

Hence, the cloud network layer security in Equations (20)–(23) can be calculated as:

$$P_{\text{out}} = \underbrace{\int_0^{\frac{\overline{\gamma}_P}{\gamma_0}} \int_0^{\infty} F_{\gamma_M|\{X=x\}}(\epsilon(\gamma_E)) f_{\gamma E|\{X=x\}}(\gamma_E) f_X(x) d\gamma_E dx}_{\mathcal{J}_1} + \underbrace{\int_{\frac{\overline{\gamma}_P}{\gamma_0}}^{0} \int_0^{\infty} F_{\gamma_M|\{X=x\}}(\epsilon(\gamma_E)) f_{\gamma E|\{X=x\}}(\gamma_E) f_X(x) d\gamma_E dx}_{\mathcal{J}_2} \tag{20}$$

$$F_{\gamma u|\{X=x\}}(\epsilon(\gamma_{\text{E}})) = \sum_{i=0}^{n_{\text{B}}} \binom{n_{\text{B}}}{i} (-1)^i e^{-\frac{i\omega(\gamma_{\clubsuit})}{\gamma_0^{n_1}}}, f_{\gamma E|\{X=x\}}(\gamma_{\text{E}}) = \sum_{j=0}^{n\varepsilon-1} \binom{n_{\text{E}}-1}{j} \frac{n_{\text{E}}}{\overline{\gamma}_0 \Omega_2} (-1)^j e^{-\frac{(j+1)\sim_2}{F_0^{l_2}}} \tag{21}$$

$$\text{For } X > \frac{\overline{\gamma}_P}{\gamma_0}, \text{ we have}$$

$$F_{\gamma_M|\{X=x\}}(\epsilon(\gamma_E)) = \sum_{i=0}^{n_B} \binom{n_{\text{B}}}{i} (-1)^i e^{-\frac{i_k(\gamma_5)}{\overline{v}_p^{n_1} x}}, \tag{22}$$

$$f_{\gamma_Z|\{X=x\}}(\gamma_E) = \sum_{j=0}^{n_{\text{E}}} -1 \binom{n_{\text{E}}-1}{j} \frac{n_{\text{E}}}{\overline{\gamma}_p \Omega_2} (-1)^j x e^{-\frac{(j+1)\gamma_1}{T_p^{n_2} x}} \tag{23}$$

5. Performance Analysis

The performance of this proposed CFN model with its numerical simulation results from the iFogSim simulator is relatively examined with the existing ones. The real-time situation of smart city fog network is involved and considers traffic of web applications. The workload needs CPU and network resources.

The parametric analysis is given by graphs below.

The above Figures 4 and 5 show the average power consumption, and latency comparison between CFN with fog and cloud frameworks. In Figure 4 for 1s the power consumption stays constant for time without any minimal oscillations because of small variations vertically. Figure 5 shows fog computing architecture latency in which the event has been notified earlier for final users of cloud computing architecture. Here, the latency extends to second for cloud computing.

The above Tables 1 and 2 show a comparison of network efficiency, communication delay, and average power consumption, and Figures 6–12 show their graphical representation in comparison between existing and proposed techniques. From Figures 6–9 shows the network efficiency as well as the cloud computing layer delay has been initiated due to a delay in communication in cloud servers with edge servers. On one hand, this is on the grounds that the correspondence with a significant distance from end clients to the cloud server center may create high postponement. Then again, the limit of organization data transfer capacity builds the transmission delay from edge devices to cloud workers incredibly. As the measure of information increments consistently, the correspondence defers increments quicker. Figures 10–12 show communication latency, UAV mobility, and connectivity of UAVs. The bends turn 100% of responsibility in the cloud. This shows that the transmission rate acts simultaneously with the mist handling rate introduced. The dormancy at the mist will be improved as more work is moved to the cloud.

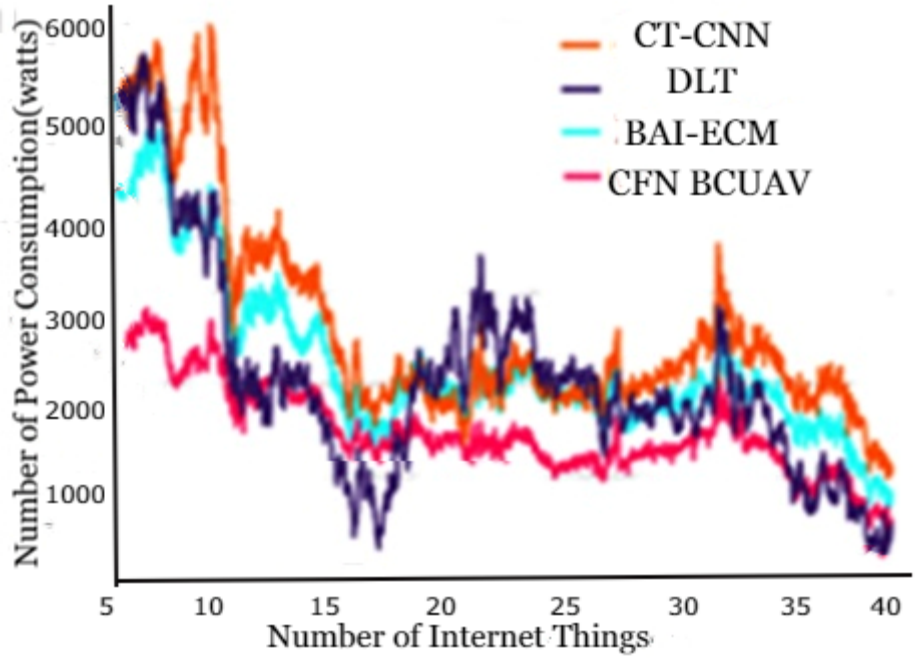

Figure 4. Average power consumption of UAV.

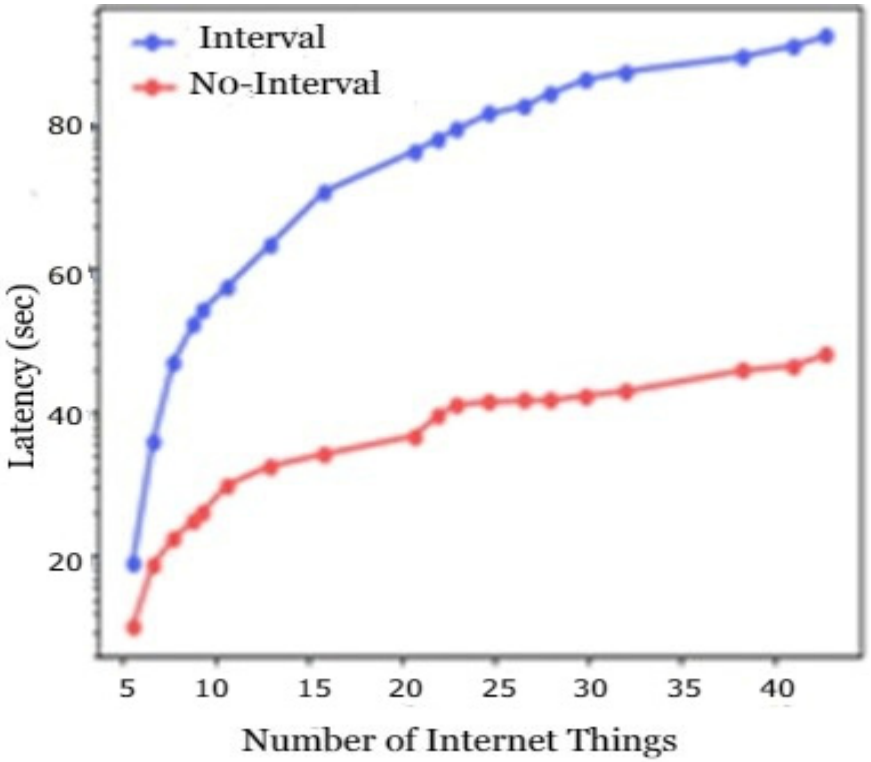

Figure 5. Comparison for latency of the proposed CFN with fog and cloud frameworks.

Table 2. Communication delay.

Number of Internet Things	CT-CNN [10]	DLT [8]	BAI_ECM [14]	CT-6G_CFN
20	4.2	3.9	3.5	3.2
40	6	6.3	6.5	5.7
60	7.3	7.5	7.8	6.8
80	8.2	6.7	7.9	8.2
100	12	11.5	11	10.8

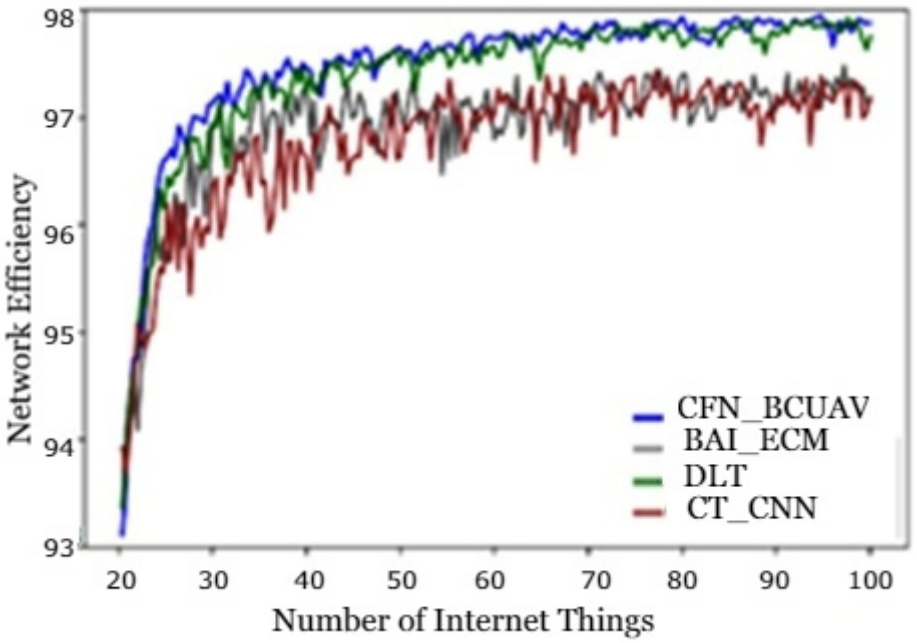

Figure 6. Network efficiency.

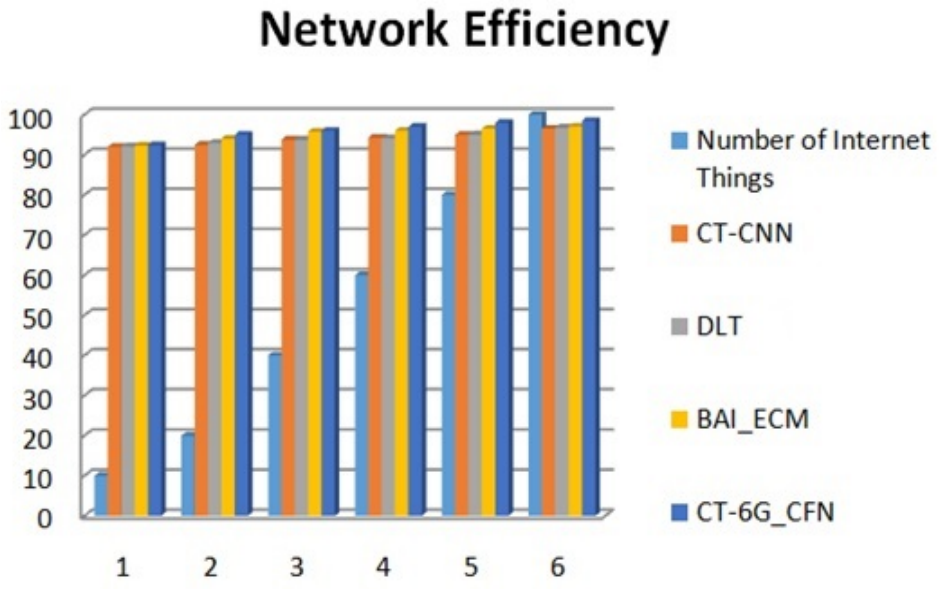

Figure 7. Comparison chart—network efficiency.

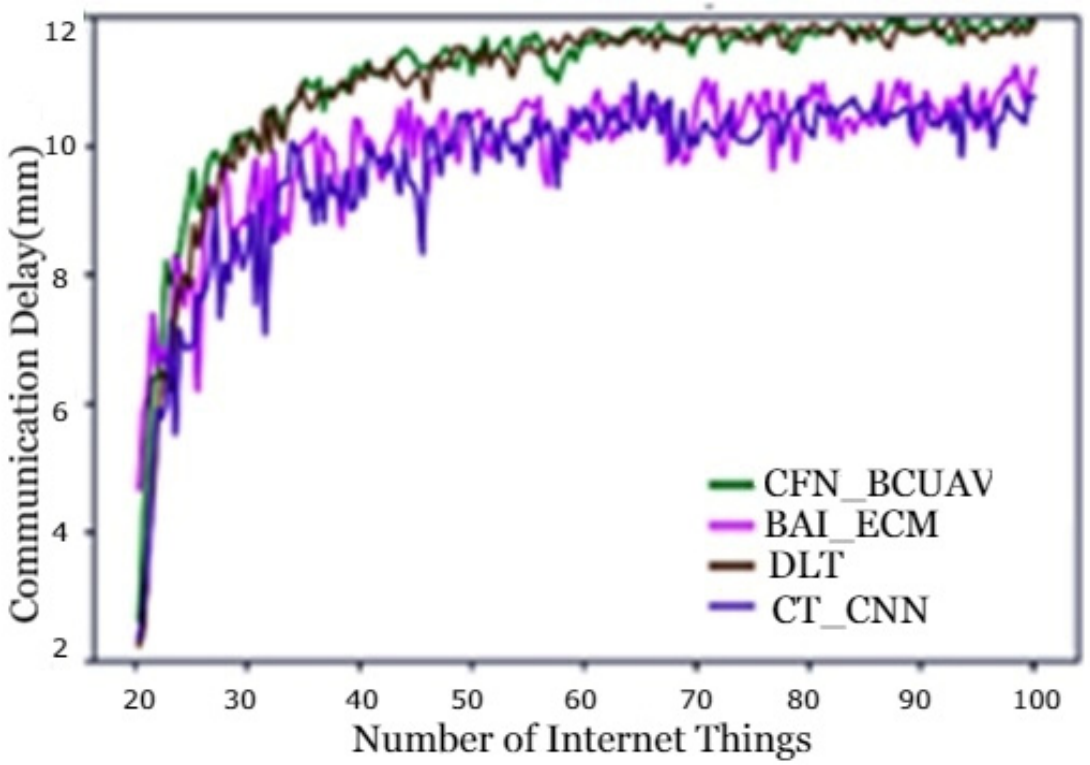

Figure 8. Communication delay.

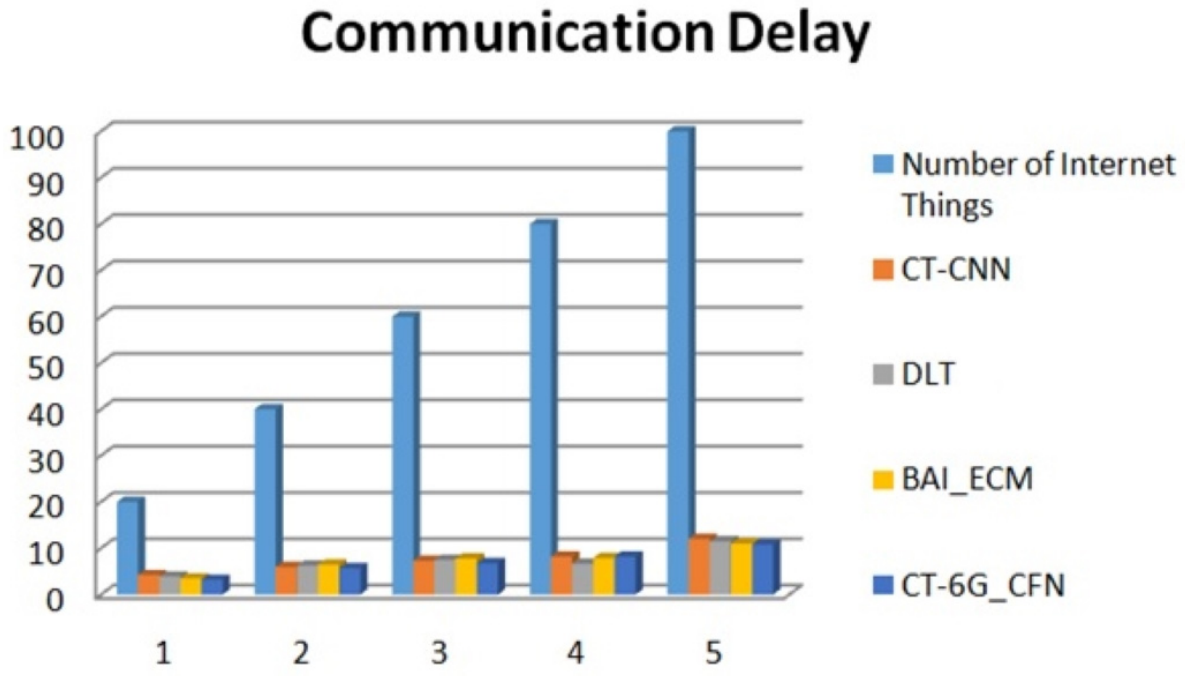

Figure 9. Comparison chart—communication delay.

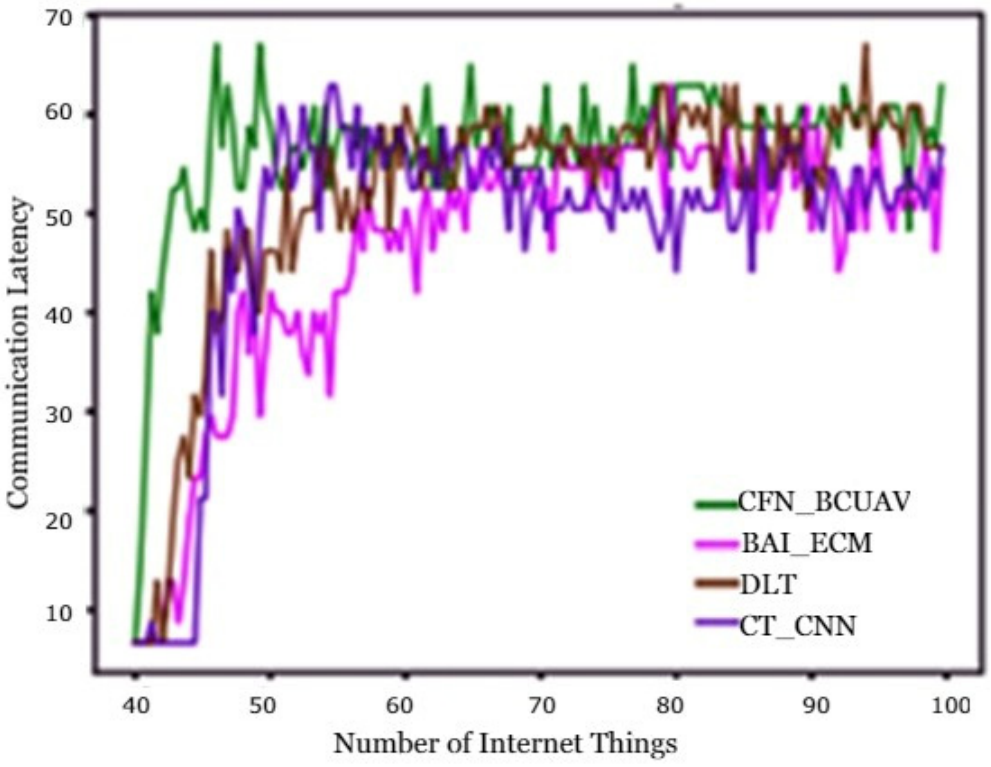

Figure 10. Communication latency.

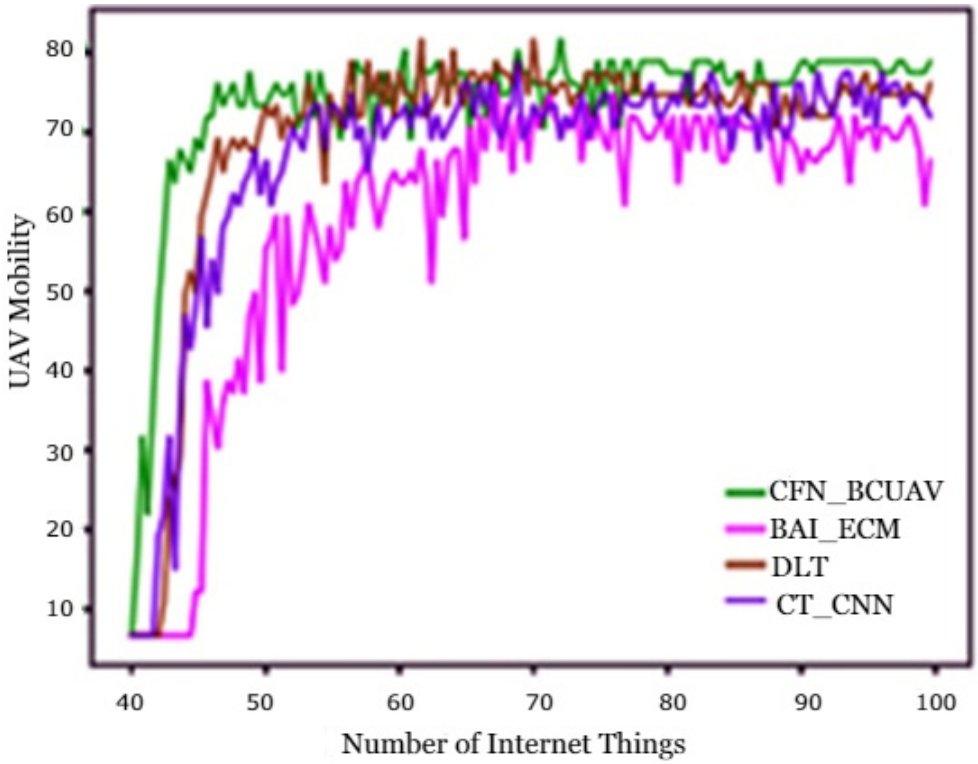

Figure 11. UAV mobility.

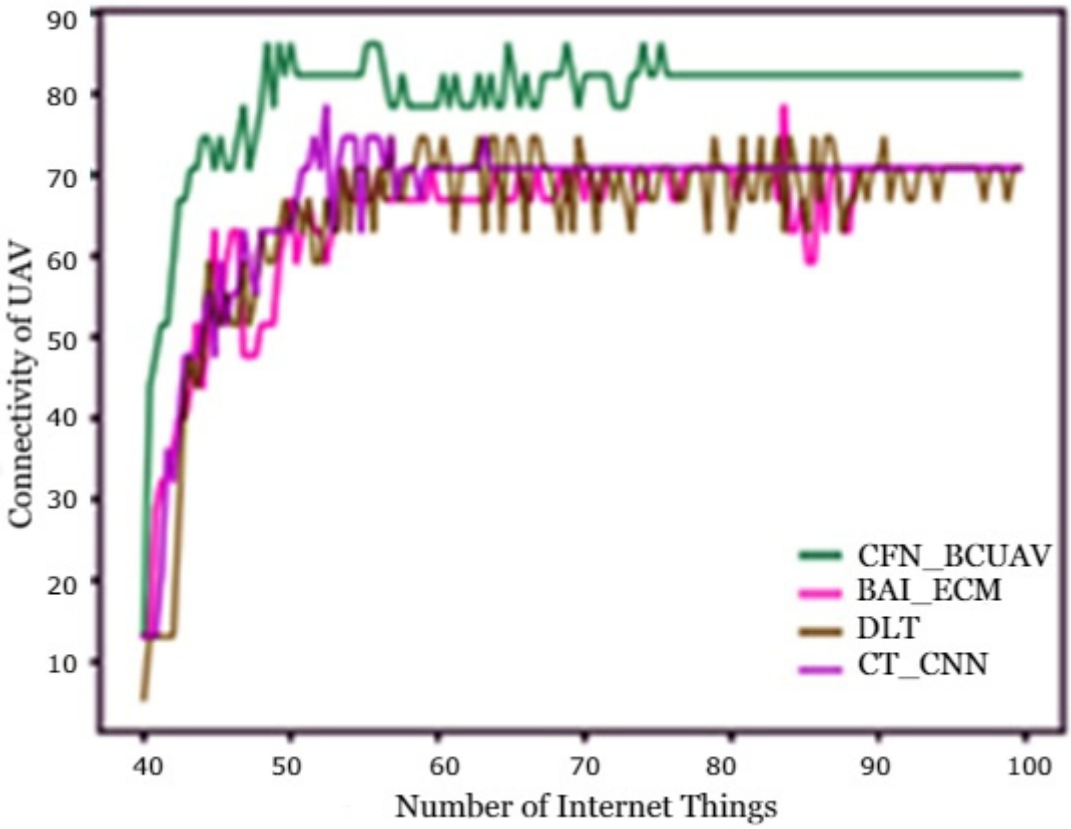

Figure 12. Connectivity of UAV.

6. Conclusions

The concept of blockchain technology, cybertwins (CTs) with UAV assumes a protuberant part in business use, convoluted security basic missions alongside numerous other assorted scopes of uses. UAVs ought to have the option to give wide inclusion and availability to distant regions under all conditions. Besides, conventional UAV correspondence is not satisfactory to manage the high-versatility and dynamic highlights of UAVs. Along these lines, there is a requirement for an effective and secure organization of UAVs as they have been broadly utilized in antagonistic conditions. So, this paper proposed that cybertwin-based UAVs and IoE applications have to be energy aware and must provide scalability with less latency. A novel CFN framework is designed securely and blockchain-based UAV communication (BC-UAV). The overall results reveal that the performance of this proposed CFN_BC-UAV architecture is better for cyber-based security in 6G techniques. Since applications were designed based on the fog computing environment which provides scalability, energy efficiency as well as security. In some current works, the information privacy and trustworthiness levels additionally stay low. The examination difficulties and open issues in joining blockchain with the 6G correspondence network are investigated. Then, at that point, the future exploration rules toward blockchain-empowered IoT with 6G correspondence are given. Security and protection issues of 5G advancements are to be diminished contingent upon requests and prerequisites.

Author Contributions: Conceptualization, A.B.K.; supervision, J.K. and S.B.G.; original draft and review and editing, D.D. and V.D.; validation, A.S.R. and S.B.G.; writing—review and editing, A.S.R., S.B.G., M.S.R., T.C.M., C.V. and G.S.; proposed the new method or methodology, D.D. and A.B.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data will be shared for review based on the editorial reviewer's request.

Acknowledgments: This paper was partially supported by UEFISCDI Romania and MCI through BEIA projects NGI-UAV-AGRO, SOLID-B5G, I-DELTA, STACK, ENTA, IMMINENCE and by European Union's Horizon 2020 research and innovation program under grant agreement No. 883522 (S4ALLCITIES). This work is supported by Ministry of Research, Innovation, Digitization from Romania by the National Plan of R & D, Project PN 19 11, Subprogram 1.1. Institutional performance-Projects to finance excellence in RDI, Contract No. 19PFE/30.12.2021 and a grant of the National Center for Hydrogen and Fuel Cells (CNHPC)—Installations and Special Objectives of National Interest (IOSIN).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Yu, Q.; Ren, J.; Zhou, H.; Zhang, W. A Cybertwin based Network Architecture for 6G. In Proceedings of the 2020 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 17–20 March 2020; IEEE: Piscataway, NJ, USA, 2020.
2. Yu, Q.; Zhou, H.; Chen, J.; Li, Y.; Jing, J.; Zhao, J.J.; Qian, B.; Wang, J. A fully-decoupled RAN architecture for 6G inspired by neurotransmission. *J. Commun. Inf. Netw.* **2019**, *4*, 15–23. [CrossRef]
3. Yu, Q.; Ren, J.; Fu, Y.; Li, Y.; Zhang, W. Cybertwin: An origin of next generation network architecture. *IEEE Wirel. Commun.* **2019**, *26*, 111–117. [CrossRef]
4. Fernandez-Caram, T.M.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access* **2018**, *6*, 32979–33001. [CrossRef]
5. Nawaz, S.J.; Sharma, S.K.; Wyne, S.; Patwary, M.N.; Asaduzzaman, M. Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future. *IEEE Access* **2019**, *7*, 46317–46350. [CrossRef]
6. Shafi, M.; Molisch, A.F.; Smith, P.J.; Haustein, T.; Zhu, P.; de Silva, P.; Tufvesson, F.; Benjebbour, A.; Wunder, G. 5G: A tutorial overview of standards, trials, challenges, deployment, and practice. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 1201–1221. [CrossRef]
7. Zhao, J. A survey of reconfigurable intelligent surfaces: Towards 6G wireless communication networks with massive MIMO 2.0. *arXiv* **2019**, arXiv:1907.04789.
8. Yang, R.; Yu, F.R.; Si, P.; Yang, Z.; Zhang, Y. Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1508–1532. [CrossRef]
9. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for 5G and beyond networks: A state of the art survey. *J. Netw. Comput. Appl.* **2020**, *166*, 102–693. [CrossRef]
10. Kumari, A.; Gupta, R.; Tanwar, S.; Kumar, N. Blockchain and AI amalgamation for energy cloud management: Challenges, solutions, and future directions. *J. Parallel Distrib. Comput.* **2020**, *143*, 148–166. [CrossRef]
11. Fernández-Caramés, T.M.; Fraga-Lamas, P. Towards next generation teaching, learning, and context-aware applications for higher education: A review on blockchain, IoT, fog and edge computing enabled smart campuses and universities. *Appl. Sci.* **2019**, *9*, 4479. [CrossRef]
12. Liu, Y.; Yu, F.R.; Li, X.; Ji, H.; Leung, V.C.M. Blockchain and Machine Learning for Communications and Networking Systems. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1392–1431. [CrossRef]
13. Gui, G.; Liu, M.; Tang, F.; Kato, N.; Adachi, F. 6G: Opening New Horizons for Integration of Comfort, Security and Intelligence. *IEEE Wirel. Commun.* **2020**, *27*, 126–132. [CrossRef]
14. Wang, M.; Zhu, T.; Zhang, T.; Zhang, J.; Yu, S.; Zhou, W. Security and privacy in 6G networks: New areas and new challenges. *Digit. Commun. Netw.* **2020**, *6*, 281–291. [CrossRef]
15. Kim, H.; Park, J.; Bennis, M.; Kim, S. Blockchained On-Device Federated Learning. *IEEE Commun. Lett.* **2020**, *24*, 1279–1283. [CrossRef]
16. Mao, Y.; You, C.; Zhang, J.; Huang, K.; Letaief, K.B. A Survey on Mobile Edge Computing: The Communication Perspective. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2322–2358. [CrossRef]
17. Jiang, X.; Yu, F.R.; Song, T.; Ma, Z.; Song, Y.; Zhu, D. Blockchain-Enabled Cross-Domain Object Detection for Autonomous Driving: A Model Sharing Approach. *IEEE Internet Thing. J.* **2020**, *7*, 3681–3692. [CrossRef]
18. Rahim, R.; Murugan, S.; Mostafa, R.R.; Dubey, A.K.; Regin, R.; Kulkarni, V.; Dhanalakshmi, K.S. Detecting the Phishing Attack Using Collaborative Approach and Secure Login through Dynamic Virtual Passwords. *Webology* **2020**, *17*, 524–535. [CrossRef]
19. Fourati, M.; Najeh, B.; Idriss, A. Blockchain Towards Secure UAV-Based Systems. In *Enabling Blockchain Technology for Secure Networking and Communications*; IGI Global: Hershey, PA, USA, 2021; pp. 149–174.
20. Gupta, R.; Shukla, A.; Anwar, S. BATS: A Blockchain and AI-empowered Drone-assisted Telesurgery System towards 6G. *IEEE Trans. Netw. Sci. Eng.* **2020**, *8*, 2958–2967. [CrossRef]
21. Pokhrel, S.R. Federated learning meets blockchain at 6g edge: A drone-assisted networking for disaster response. In Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, London, UK, 25 September 2020; pp. 49–54.
22. Singh, P.; Nayyar, A.; Kaur, A.; Ghosh, U. Blockchain and fog based architecture for internet of everything in smart cities. *Future Internet* **2020**, *12*, 61. [CrossRef]

23. Rametta, C.; Schembra, G. Designing a softwarized network deployed on a fleet of drones for rural zone monitoring. *Future Internet* **2017**, *9*, 8. [CrossRef]
24. García-Magariño, I.; Lacuesta, R.; Rajarajan, M.; Lloret, J. Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain. *Ad Hoc Netw.* **2019**, *86*, 72–82. [CrossRef]
25. Hattab, G.; Cabric, D. Energy-efficient massive IoT shared spectrum access over UAV-enabled cellular networks. *IEEE Trans. Commun.* **2020**, *68*, 5633–5648. [CrossRef]
26. Monir, M.B.; Mohamed, A.A. Energy aware routing for wireless sensor networks. *Int. J. Commun. Netw. Inf. Secur. IJCNIS* **2022**, *14*, 70–75. [CrossRef]
27. Aljarrah, I.A.; Alshare, E.M. Improved Residual Dense Network for Large Scale Super-Resolution via Generative Adversarial Network. *Int. J. Commun. Netw. Inf. Secur. IJCNIS* **2022**, *14*, 118–125. [CrossRef]
28. Osama, I.; Rihan, M.; Elhefnawy, M.; Eldolil, S.; Abd El-AzemMalhat, H. A review on Precoding Techniques For mm-Wave Massive MIMO Wireless Systems. *Int. J. Commun. Netw. Inf. Secur. IJCNIS* **2022**, *14*, 26–36. [CrossRef]
29. Paliwal, R.; Khan, I. Design and Analysis of Soft Computing Based Improved Routing Protocol in WSN for Energy Efficiency and Lifetime Enhancement. *Int. J. Recent Innov. Trends Comput. Commun.* **2022**, *10*, 12–24. [CrossRef]
30. Degambur, L.-N.; Mungur, A.; Armoogum, S.; Pudaruth, S. Resource Allocation in 4G and 5G Networks: A Review. *Int. J. Commun. Netw. Inf. Secur. IJCNIS* **2021**, *13*, 401–408. [CrossRef]
31. Arumugam, S.; Shandilya, S.K.; Bacanin, N. Federated Learning-Based Privacy Preservation with Blockchain Assistance in IoT 5G Heterogeneous Networks. *J. Web Eng.* **2022**, *21*, 1323–1346. [CrossRef]
32. Ramanan, M.; Singh, L.; Suresh Kumar, A.; Suresh, A.; Sampathkumar, A.; Jain, V.; Bacanin, N. Secure blockchain enabled Cyber- Physical health systems using ensemble convolution neural network classification. *Comput. Electr. Eng.* **2022**, *101*, 108058. [CrossRef]
33. Sampathkumar, A.; Murugan, S.; Elngar, A.A.; Garg, L.; Kanmani, R.; Malar, A.C.J. A Novel Scheme for an IoT-Based Weather Monitoring System Using a Wireless Sensor Network. In *Integration of WSN and IoT for Smart Cities. EAI/Springer Innovations in Communication and Computing*; Rani, S., Maheswar, R., Kanagachidambaresan, G., Jayarajan, P., Eds.; Springer: Cham, Switzerland, 2020. [CrossRef]
34. Ugochukwu, N.A.; Goyal, S.B.; Arumugam, S. Blockchain-Based IoT-Enabled System for Secure and Efficient Logistics Management in the Era of IR 4.0. *J. Nanomater.* **2022**, *2022*, 7295395. [CrossRef]
35. Bedi, P.; Goyal, S.B.; Rajawat, A.S.; Shaw, R.N.; Ghosh, A. Application of AI/IoT for Smart Renewable Energy Management in Smart Cities. In *AI and IoT for Smart City Applications. Studies in Computational Intelligence*; Piuri, V., Shaw, R.N., Ghosh, A., Islam, R., Eds.; Springer: Singapore, 2022; Volume 1002. [CrossRef]
36. Sharma, S.; Rani, M.; Goyal, S.B. Energy Efficient Data Dissemination with ATIM Window and Dynamic Sink in Wireless Sensor Networks. In Proceedings of the 2009 International Conference on Advances in Recent Technologies in Communication and Computing, Kottayam, India, 27–28 October 2009; pp. 559–564. [CrossRef]
37. Raikwar, M.; Gligoroski, D.; Kralevska, K. SoK of Used Cryptography in Blockchain. *IEEE Access* **2019**, *7*, 148550–148575. [CrossRef]
38. Esmaeily, A.; Kralevska, K. Small-Scale 5G Testbeds for Network Slicing Deployment: A Systematic Review. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 6655216. [CrossRef]