

## Federated Learning with Blockchain Assisted Image Classification for Clustered UAV Networks

Ibrahim Abunadi<sup>1</sup>, Maha M. Althobaiti<sup>2</sup>, Fahd N. Al-Wesabi<sup>3,4</sup>, Anwer Mustafa Hilal<sup>5</sup>,  
Mohammad Medani<sup>6</sup>, Manar Ahmed Hamza<sup>5,\*</sup>, Mohammed Rizwanullah<sup>5</sup> and Abu Serwar Zamani<sup>5</sup>

<sup>1</sup>Department of Information Systems, Prince Sultan University, Rafha Street, Riyadh, 11586, Saudi Arabia

<sup>2</sup>Department of Computer Science, College of Computing and Information Technology, Taif University, Taif, 21944, Saudi Arabia

<sup>3</sup>Department of Computer Science, College of Science & Art at Mahayil, King Khalid University, Muhayel Aseer, 62529, Saudi Arabia

<sup>4</sup>Faculty of Computer and IT, Sana'a University, Sana'a, 61101, Yemen

<sup>5</sup>Department of Computer and Self Development, Prince Sattam bin Abdulaziz University, Al-Kharj, 16278, Saudi Arabia

<sup>6</sup>Department of Information Systems, College of Science & Art at Mahayil, King Khalid University, Muhayel Aseer, 62529, Saudi Arabia

\*Corresponding Author: Manar Ahmed Hamza. Email: ma.hamza@psau.edu.sa

Received: 25 November 2021; Accepted: 29 December 2021

**Abstract:** The evolving “Industry 4.0” domain encompasses a collection of future industrial developments with cyber-physical systems (CPS), Internet of things (IoT), big data, cloud computing, etc. Besides, the industrial Internet of things (IIoT) directs data from systems for monitoring and controlling the physical world to the data processing system. A major novelty of the IIoT is the unmanned aerial vehicles (UAVs), which are treated as an efficient remote sensing technique to gather data from large regions. UAVs are commonly employed in the industrial sector to solve several issues and help decision making. But the strict regulations leading to data privacy possibly hinder data sharing across autonomous UAVs. Federated learning (FL) becomes a recent advancement of machine learning (ML) which aims to protect user data. In this aspect, this study designs federated learning with blockchain assisted image classification model for clustered UAV networks (FLBIC-CUAV) on IIoT environment. The proposed FLBIC-CUAV technique involves three major processes namely clustering, blockchain enabled secure communication and FL based image classification. For UAV cluster construction process, beetle swarm optimization (BSO) algorithm with three input parameters is designed to cluster the UAVs for effective communication. In addition, blockchain enabled secure data transmission process take place to transmit the data from UAVs to cloud servers. Finally, the cloud server uses an FL with Residual Network model to carry out the image classification process. A wide range of simulation analyses takes place for ensuring the betterment of the FLBIC-CUAV approach. The experimental outcomes portrayed the betterment of the FLBIC-CUAV approach over the recent state of art methods.

**Keywords:** UAV networks; clustering; secure communication; blockchain; federated learning; image classification

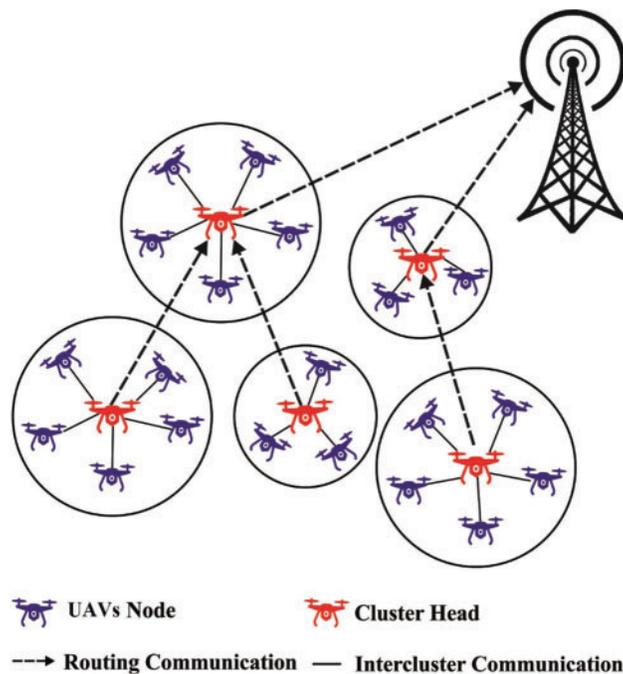


This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

## 1 Introduction

The Industrial Internet of Things (IIoT) relates to the billions of physical devices (like connected instruments, sensors, etc.) globally which is currently interconnected to the internet without needing human-to-computer interaction/human-to-human [1]. It is beneficial in extensive geographic coverage and low deployment cost and has determined various applications in different fields, comprising environment monitoring, transportation, pervasive healthcare, smart city, and so on. Most innovations of autonomous robots employed in industry 4.0 is the generalization of the usage of drones (unmanned aerial vehicle (UAV)) to perform data collection tasks and multitude of inspections. The study focuses on the construction companies as it is one of the sectors in which conventionally lesser state-of-the-art technologies were employed and hence applicable for using novel Technology of Industry 4.0 [2]. Construction industries are mainly employing UAVs to offer high definition (HD) videos and images for recognizing change and for realtime job site monitoring and preventing or solving numerous problems. Also, they are employed to the maintenance task and inspection which is dangerous, costly, or inaccessible from the ground [3].

Incorporating UAVs into the IoT characterizes interoperability challenges since each IoT system has its individual communication protocol. Furthermore, a slight delay/error over the tolerated limits can lead to a disaster for many applications, like aircraft monitoring and manufacture and UAV. Fig. 1 illustrates the overview of cluster UAV networks. When the (IoT) offers Internet access to any ‘thing’, UAV could be a portion of this interconnected thing and transmit its onboard data to the cloud [4]. Computational abilities could be prolonged to the cloud, using the offered service, and save the energy consumption and cost of an implanted UAV scheme. There is an increasing trend toward the 3 layers IIoT architectures using fog computing, through a convergence network of distributed and interconnected intelligent gateways.



**Figure 1:** Overview of clustered UAV networks

Using big data, lower cost computing, analytics, mobile, and cloud technologies, IIoT devices could collect and share data with minimum human interference. The data gathered by the IIoT device could be transferred to the central cloud server for storage [5]. The privacy and security problems could be simply resolved using data encryption; but, IIoT based system frequently faces privacy and security issue, particularly in analytic and data processing. Federated learning (FL) is deliberated a novel computational model which goals at training multiple local datasets/machine learning approaches in local mobile nodes without obviously interchanging data instances [6]. But, DL solution yet faces several novel privacy and security problems once it is needed to encounter the mobile IIoT model. In the conventional FL method, the centric server aggregate submodels are trained locally through the shared mobile nodes. The centric trained FL method would be distributed to each mobile node in the scheme. Furthermore, the FL frameworks participator could initiate membership inference attacks for judging either certain participators are included in the scheme for model training [7]. Additionally, the participators could initiate attacks on another participator past training data from the centric paradigm. In addition, few malicious participators could transmit fake submodels for damaging the centric paradigm, make the FL method fails.

In all rounds of FL, more than one user (for example organization, datacentres, mobile/IoT device) are elected for training modules locally to generate a global paradigm when the raw data is kept in client and not transferred/exchanged. Blockchains have been currently leveraged in IIoT FL for providing incentives and data integrity for attracting adequate user data and computational resources for training [8]. But, there was an insufficient holistic and systematic framework model for supporting efficient developments and effective approaches for addressing the challenges of data heterogeneity in device failure detection of IIoT. Even though FL has attained various advantageous in privacy preserving learning solutions for IoT systems, also it possesses major problems like robustness, resource management, incentive, and security mechanism [9]. Such problems will be difficult and more significant for handling in industrial IoT (IIoT), where high levels of safety, reliability, and security are needed. For enabling FL in IIoT applications, various studies have been conducted in recent years.

This study designs federated learning with blockchain assisted image classification model for clustered UAV networks (FLBIC-CUAV) on IIoT environment. The proposed FLBIC-CUAV technique involves three major processes namely clustering, blockchain enabled secure communication and FL based image classification. For UAV cluster construction process, beetle swarm optimization (BSO) algorithm with three input parameters is designed to cluster the UAVs for effective communication. In addition, blockchain enabled secure data transmission process take place to transmit the data from UAVs to cloud servers. Finally, the cloud server uses an FL with Residual Network model to carry out the image classification process. An extensive set of experiments are carried out to guarantee the supremacy of the FLBIC-CUAV technique.

## 2 Related Works

Wang et al. [10] presented the Fed-SCNN detection architecture. At first, a hybrid method is determined on the user side via DNN and SCNN that distinguishes the data of in-vehicle image and upload the encrypted parameter to the cloud. Next, the cloud servers perform FL on main parameter via DNN for building a global cloud module. Lastly, the DNNs are upgraded on the user side for additionally optimizing the hybrid method. The aforementioned 3 phases are cycled for continuously iterating the local hybrid method. The FedSCNN architecture is a dynamic learning procedure which tackles the 2 main problems of privacy protection and data isolation. Salhaoui et al. [11] present a smart IIoT control and monitoring method depending on a UAV which exploits CC service and uses

FC as the bridges among IIoTs layer. Its innovation lies in the UAVs are manually incorporated into an industrial control scheme via IoT gateways, whereas UAV images are instantly and systematically analyzed and computed in the cloud. Visual supervision of the plant using cloud services and drones are incorporated in realtime for controlling loops of the industrial control scheme.

In order to address the data heterogeneity problem in IIoT detection failure, Zhang et al. [12] proposed a new CDW FedAvg approach considering the distances among negative and positive classes of all user datasets. Additionally, to inspire users to take part in FL, smart contract based incentive mechanisms are developed based on the centroid distance and size of user data employed in local model training. Lim et al. [13] presented the adaption of an FL based method for enabling privacy preserving collaborative ML through a federation of independent DaaS providers for the growth of IoV application, for instance, car park occupancy management and traffic prediction.

Zhang et al. [14] considered image classification task in UAV supported exploration scenario, in which the co-ordinations of various UAVs are executed with a GFC located in a strategic, however unavailable locations, like a mountain top while refreshing the battery is uneconomic or might be impossible. On-board cameras are brought by all UAVs and next, FL is invoked to reduce the transmission costs among the GFC and UAVs, and the computation complexity enforced on the GFC. To additionally minimize the computation complexity enforced on the GFC through the UAVs, WZF-TPC is employed at all UAVs depending on realistic imperfect CSI.

Kim et al. [15] proposed blockchain based FL scenarios. Blockchain could effectively induce users to take part in learning and could split all contributing users as a 'node'. Furthermore, it could be pursued stability, integrity, etc. also they considered 2 kinds of weight for selecting the subsets of clients to update the global method. Firstly, deliberate the weight according to local learning precision of every user. Next, deliberate the weight according to the participation rate of every user. They select 2 essential performances indicator, standard deviation and learning speed, for comparing the efficiency of this presented method using present approach. Sharma et al. [16] proposed a dispersed computing defence architecture for sustainable society with the features of FL and blockchain technology. The presented method presents an approach for meeting the challenge of constrained training data for obtaining higher accuracy and prevent reasons specific method.

Rahman et al. [17] presented a lightweight hybrid FL architecture where blockchain smart contracts handle the authentication, edge training plan, and trust management of contributing federated nodes, the reputation of edge nodes, and their uploaded datasets/models the distributions of locally or global trained model. Also, the frameworks support the complete encryption of a model training, inferencing process, and the dataset. All federated edge nodes perform additive encryption, whereas the blockchain exploits multiplicative encryptions for aggregating the upgraded model's parameter. Pokhrel [18] developed a new method for a constellation of LEO satellites by making a Blockchain based architecture for continuous knowledge learning and sharing collaboratively. They ablated FL effective features as a foundation for ensuring higher accuracy of learning inference at timescale applicable to the channel dynamics and primary time varying space network.

Khan et al. [19] proposed enhancing the efficiency of UAVs with a decentralized ML architecture depending on blockchain. The presented model has the significance of considerably enhancing the storage and integrity of data for making smart decisions amongst various UAVs. They presented the usage of blockchain for achieving decentralized prediction analytics and architecture which could effectively share and apply ML methods in a decentralized way. Zhang et al. [20] bridge blockchain technology and FL via developing a blockchain based smart agent framework and apply it in FL.

The FL approach is a developing collaborative ML method which trains models through various servers/devices hold private data instances without interchanging their data.

### 3 The Proposed FLBIC-CUAV Technique

In this study, a new FLBIC-CUAV technique is derived to accomplish secure communication and classification in UAV networks. The proposed FLBIC-CUAV technique involves distinct major processes namely BSO based clustering, blockchain enabled secure communication and FL based image classification. The detailed working of these processes is provided in the succeeding sections.

#### 3.1 Design of BSO Based Clustering Technique

Initially, the BSO algorithm is designed to select the proper set of UAV CHs and organize clusters in the network. According to the SI behaviours of beetle, the BSO approach was proposed [21]. Now, all individual beetles define a potential solution to the optimization issue, and all refer to a fitness value calculated by the FF. Similar PSO approach, the beetle distributes data. But, the direction and distance of the beetles are calculated by the speed and data intensity to be recognized by the longer antenna. Arithmetically, the beetles population of  $n$  beetle is represented as  $X = (X_1, X_2, \dots, X_n)$  in an  $S$  dimension search area, in which the  $i$  th beetles indicate  $S$  dimensional vector  $X_i = (x_{i1}, x_{i2}, \dots, x_{iS})^T$ , illustrates the location of  $i$  th beetles in the  $S$  dimensional search area and implies the potential solution to problem. The rate of  $i$  th beetles could be determined as  $V_i = (V_{i1}, V_{i2}, \dots, V_{iS})^T$ . The certain limit of the beetles could be specified as  $P_i = (P_{i1}, P_{i2}, \dots, P_{iS})^T$ , and the group extreme value of population could be indicated as  $P_g = (P_{g1}, P_{g2}, \dots, P_{gS})^T$ . These behaviours could be arithmetically modelled as:

$$X_{is}^{k+1} = X_{is}^k + \lambda V_{is}^k + (1 - \lambda)\xi_{is}^k \tag{1}$$

Whereas  $s = 1, 2, \dots, S$ ;  $i = 1, 2, \dots, n$ ;  $k$  represents the current iteration.  $V_{is}$  denote the beetled speed, and  $\xi_{is}$  describes the increase in beetle's location motion.  $\lambda$  denotes a positive constant. Then, the speed could be defined in the following equation [22]:

$$V_{is}^{k+1} = c\omega V_{is}^k + c_1r_1(P_{is}^k - X_{is}^k) + c_2r_2(P_{gs}^k - X_{is}^k) \tag{2}$$

Let  $c_1$  &  $c_2$  represents 2 positive constant variables, and  $r_1$  &  $r_2$  indicates 2 random functions in the range of zero and one.  $\omega$  signifies the inertia weight.

In this instance, the method of decreasing inertia weights are defined in Eq. (3):

$$\omega = \omega_{\max} - \frac{\omega_{\max} - \omega_{\min}}{K} * k \tag{3}$$

In which  $\omega_{\min}$  &  $\omega_{\max}$  are the minimum and maximum values of  $\omega$ .  $k$  and  $K$  represent the present and maximum iteration. Now, the extrema values of  $\omega$  are set to be 0.9, and the lowest values are predetermined as 0.4, therefore the method searches the highest range at the primary phase of the evolutions and rapidly recognizes the best solution. As the value of  $\omega$  gets reduced iteratively, the speed of beetles is decreased and enters the local search. The  $\xi$  function characterizes the increment function that could be defined in Eq. (4):

$$\xi_{is}^{k+1} = \delta^k * V_{is}^k * sign(f(X_{rs}^k) - f(X_{rs}^k)) \tag{4}$$

Let  $\delta$  represent the step size. The searching behaviors of left and right antenna could be determined as follows:

$$X_{rs}^{k+1} = X_{rs}^k + V_{is}^k * d/2$$

$$X_{ls}^{k+1} = X_{ls}^k - V_{is}^k * d/2 \quad (5)$$

The trajectory paths of the swarm of beetle in two and three dimensional areas respectively. For the depiction of the searching paths in an extremely visual manner, smaller population size is applied and showed the location modification procedure of ten rounds in three dimensional areas. Because the factors such as inertia weight coefficient and step length get reduced continually, the BSO approach doesn't convergence to the target quickly and avoids the local optimal problems.

In BSO technique, a random set of solutions are initialized. Then, in all rounds, the searching agents would upgrade the position based on the individual searching approach and the optimal solution which occurs now. The incorporation of these 2 area speeds on the runtime also decreases the probability of trapping to local optimal. Hence, it is established to be reliable in dealing with higher dimension challenges. Hypothetically, the BSO approach consists of the capabilities of exploration and exploitation. Furthermore, the linear incorporation of speed and beetles searching procedure enhances the accuracy and rapidness of population optimization and makes the approach highly consistent. The BSO algorithm derives a fitness function for CH selection involving the following three parameters.

### 3.1.1 Residual Energy in UAV

The RE of UAV (x) but interactive  $k$  bits to target UAV (y) on distance  $d$ , is determined as:

$$RE = E - (E_T(k, d) + E_{R(k)}) \quad (6)$$

where  $E$  refers the present energy of UAV and  $E_T$  implies the energy utilized to sense information.

$$E_T(k, d) = kE_e + KE_a d^2 \quad (7)$$

where  $E_e$  represents the energy of electrons and  $E_a$  has been needed amplified energy,  $E_{R(k)}$  is the energy dissipated for receiving data, and is determined as:

$$E_{R(k)} = kE_e \quad (8)$$

### 3.1.2 Average Distance to Nearby UAVs

The most 3 parameter for CH election is the average distance (AvgD) for neighboring UAVs. The AvgD represents the average of distance values to UAVs for their single hob adjacent UAV which is demonstrated as:

$$AvgNBDist_i = \frac{\sum_{j=1}^{NB_i} dist(i, nb_j)}{NB_i} \quad (9)$$

where  $dist(i, nb_j)$  stands for distance in UAV to the adjacent  $j^{th}$  UAV their neighbor  $nb_j$

### 3.1.3 UAV Degree

In order to time instance  $t$ , the degree of UAV represents the amount of neighboring nodes which exist from the UAV. It is determined as:

$$Deg_x = |N(x)| \quad (10)$$

where  $N(x) = \{n_y / \text{dist}(x, y) < \text{trans}_{\text{range}}\} x \neq y$ , and  $\text{dist}(x, y)$  signifies the distance amongst 2 UAVs  $n_x$  and  $n_y$ ,  $\text{trans}_{\text{range}}$  refers the broadcast range of UAVs.

### 3.2 Blockchain Enabled Data Transmission

The BC is employed for secure data transmission among CHs and cloud servers. BC is a significantly advantageous ledger to ensure data quality. BC produces controlling operations for various decentralized industrial device. It provides authority and amenability for all independent schemes when solving security problems. In industrial sector, private BC could be applied for achieving security. It finds beneficial in various areas like supply chain, healthcare, large scale, and transportation IoT data. It aids to attain decentralization, privacy, and trust. The BC allows simple connections to various devices. The device could be supercomputer/end node that computes data. The node could broadcast the secure data to other peer nodes so that no attackers could implement attack. It can transfer data to a decentralized device/centre place connected to another device. The hash values in the BC are the private fingerprint of every data in the chain. The pair of hash values are iteratively hashed in a block for obtaining a single hash value. Fig. 2 describes the basic architecture of BC.

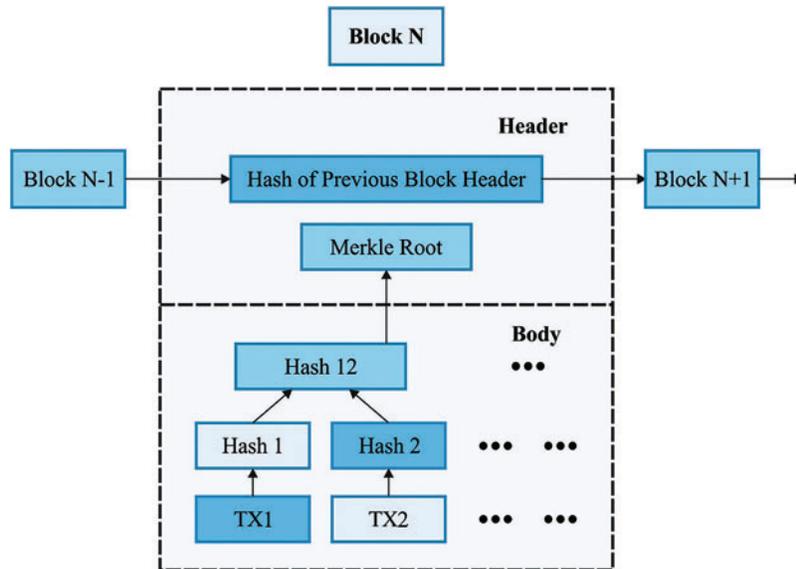


Figure 2: Architecture of blockchain

The client/server computer could be a node that starts the transaction. The transaction is integrated to generate a block; but, these blocks get added to the chain afterward authenticating from the endorse node. The transactions get initiated by the submission of the proposal from the client. It gets started from the data transmission through the user SDK. The transaction process utilizes 2 varying types of peer i.e., committer peer and endorser peer. The last one validates the transaction result previous to writing a block of transaction to the dispersed ledger. For the initialization of novel transactions, the client applications transmit the transaction proposal to peer for updating/reading the ledger. The endorser peer gets the virtual results as a certain read and writes data. The response from endorser peers includes write and read datasets. When the validation and reply of the transactions are obtained, the user transmits it to the ordered that commands the transaction to a block and passes the block to each committer peer. It could authenticate and read the endorsement policy. When it is guaranteed, it carry out writing operations. Finally, the committer peers create an asynchronous

announcement associated with the transaction state. The ordered peer notifies another node when the transactions are inefficient or not. Once the blocks save the transaction, it couldn't have interfered.

### 3.3 FL Based Classification

FL approach is a developing technique of ML that are initially developed by Google in 2016. The main concept is to secure user data at the time of processes [23]. Since a dispersed ML approach, it supports model training on huge amount of dispersed data. The training procedure is for fitting the global optimum statistical method via the integration of training parameters is given as follows:

$\min F(w)$ ,

whereas

$$F(w) = \sum_{k=1}^m p_k F_k(w) \quad (11)$$

Let  $m$  represents the overall number of devices,  $p_k \geq 0$ , and the amount of  $p_k$  is 1;  $F_k(\cdot)$  indicates the objective function of the  $k$ th device. With the emergence of FL model, several researches depend on FL have developed, for example, personalized FL, privacy preserving ML, and multitask FL. The scene contains 2 data owners (for example enterprises A & B) for introducing the FL framework. The certain framework principles are given in Fig. 3. Simultaneously, it could exploit big data to efficiently resolve the problems of Data Island that assures that FL methods are better compared to isolated model in machine detection. Based on the distribution of user data dimension, it can be separated FL approach into 2 classes: HFL, VFL, and FTL. Fed SCNN belongs to FTL class. It is the initial type tailored for distracted driving.

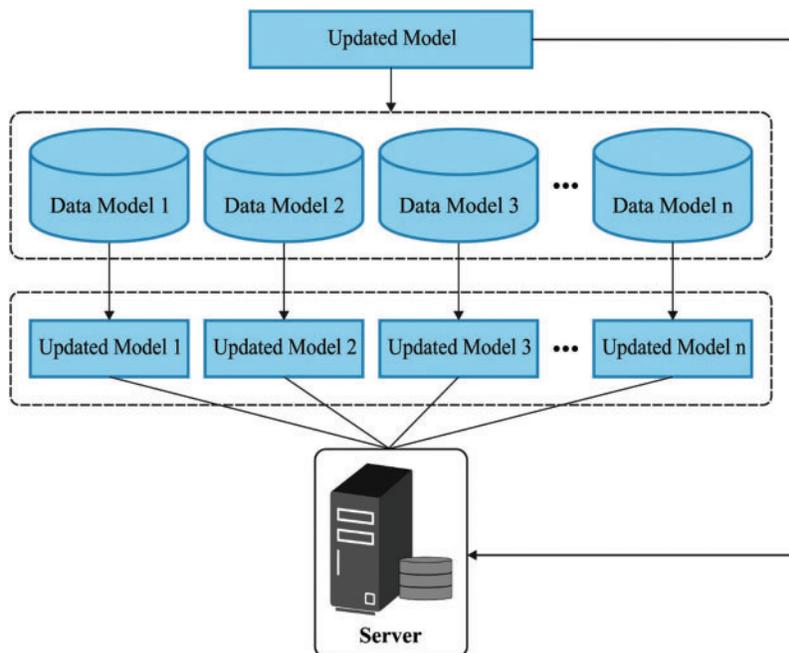


Figure 3: Overview of FL

The fundamental parameters are separated to the cloud and a huge amount of user side. Basic parameters data could be transferred among the user and cloud in encrypted model. In this study, ResNet model is utilized for learning user-side and cloud methods. Consider the features of FL, this study makes substantial developments to local ResNet network, i.e., the main parameter beforehand the final hidden layer is distributed, and the parameters among the final hidden and output layers aren't distributed. The complete reasons are described as follows.

The cloud server exploits public data and the parameter set by the user for establishing a global cloud method  $f_s$ . The objective optimization procedure in training could be given in the following equation

$$\arg \min_{\Theta} L = \sum_{i=1}^n l(y_i, f_s(x_i)) \quad (12)$$

Whereas  $l(\cdot, \cdot)$  represents the loss function of training method, for example, cross entropy loss function.  $\{x_i, y_i\}$  denotes instance  $x_i$ , and the respective labels  $y_i$ ,  $n$ , denote the instance size of public data.  $\Theta$  denotes the variable matrix which must be learned, comprising the bias and weight of the hidden layer. Afterward, the cloud models are determined, the variable  $\Theta$  is shared with every user.

The user constructs a local ResNet model such as cloud module. The training procedure remains unchanged, excepting the instance data is comparatively smaller and belongs to personal privacy data [24]. For each user  $u$ , the local ResNet model is stated as  $f_u$ , and the objective function could be given in the following equation

$$\arg \min_{\Theta^u} L = \sum_{i=1}^n l(y_i^u, f_u(x_i^u)) \quad (13)$$

Since the significant variable of local ResNet model,  $\Theta^u$  is uploaded to the cloud in the encrypted model. The cloud trains the variable sets  $\{\Theta^1, \Theta^2, \dots, \Theta^n\}$ , for updating the global cloud method and the variable  $\Theta$ , and distribute the upgraded variable  $\Theta$  to each user. Based on actual requirements, local parameters could be upgraded frequently, like regularly upgraded at night.

During this case, it can be current residual learning for beating this issue and made DL structure for classifying the image. During the residual network, stacked layer carries out residual mapping by creating shortcuts influences which perform identity mapping ( $x$ ). An output is contained in the output of stacked layer residual function  $F(x)$ . During this trained deep network with backpropagation (BP), the gradient of error is propagating as well as calculating to the shallow layers. In deep layer, these errors develop small still it finally reduces. It can be named the gradient decreasing issue of deep network. This issue is resolved by residual learning. This analysis utilizes ResNet-34 approach. The last layer of the ResNet-34 model includes a softmax layer for classification process, which allocates the data instances to  $k$  class labels.

#### 4 Performance Validation

This section investigates the performance of the FLBIC-CUAV technique under different aspects. The FLBIC-CUAV technique is inspected against UC Merced Land Use Dataset with 21 class labels. Each class includes a total of 100 images with the size of  $256 * 256$  pixels. Fig. 4 illustrates few sample images. The FLBIC-CUAV technique is examined under two different scenarios, namely scenario 1 (comprising 25 UAV images) and scenario 2 (comprising 50 UAV images).



**Figure 4:** Sample images

The results analysis of the FLBIC-CUAV technique with existing techniques on scenario 1 is provided in [Tab. 1](#). On examining the results in terms of ECM, the FLBIC-CUAV technique has gained enhanced outcome with the reduced ECM under distinct rounds of operation. For instance, with 1000 rounds, the FLBIC-CUAV technique has offered a lower ECM of 27 mJ whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C methods have obtained a higher ECM of 32, 36, 39, and 42 mJ respectively. Moreover, with 3000 rounds, the FLBIC-CUAV technique has provided a minimum ECM of 66 mJ whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C approaches have attained a maximum ECM of 71, 81, 87, and 92 mJ respectively. Furthermore, with 5000 rounds, the FLBIC-CUAV technique has accomplished a decreased ECM of 95 mJ whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C manners have achieved an increased ECM of 102, 118, 126, and 135 mJ respectively.

**Table 1:** Results of existing with proposed FLBIC-CUAV method in terms of various parameters on scenario 1

No. of rounds	Energy consumption (ECM) (mJ)				
	FLBIC-CUAV	T2FL-C	KHA-C	MPSO-C	T1FL-C
1000	27	32	36	39	42
2000	50	54	61	64	68
3000	66	71	81	87	92
4000	74	79	95	103	110
5000	95	102	118	126	135

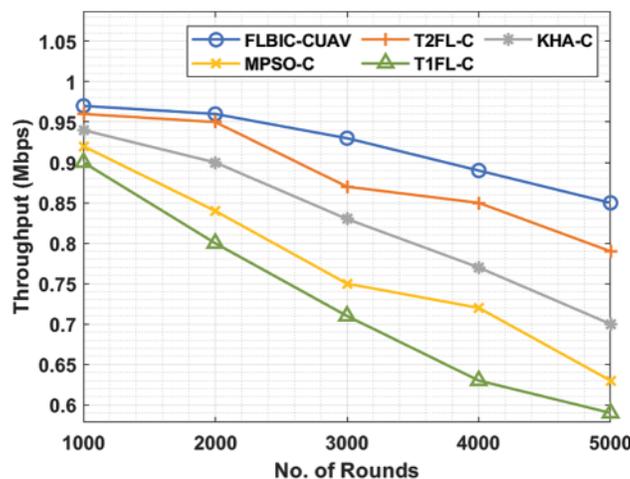
No. of rounds	End to end delay (sec)				
	FLBIC-CUAV	T2FL-C	KHA-C	MPSO-C	T1FL-C
1000	1.95	2.03	2.12	2.18	2.27
2000	2.47	2.56	2.65	2.98	3.79
3000	2.52	2.67	3.37	3.66	4.87
4000	3.19	3.34	4.28	4.89	5.89
5000	4.89	5.06	5.83	6.32	6.45

No. of rounds	Throughput (Mbps)				
	FLBIC-CUAV	T2FL-C	KHA-C	MPSO-C	T1FL-C
1000	0.97	0.96	0.94	0.92	0.90
2000	0.96	0.95	0.90	0.84	0.80
3000	0.93	0.87	0.83	0.75	0.71
4000	0.89	0.85	0.77	0.72	0.63
5000	0.85	0.79	0.70	0.63	0.59

On investigating the results with respect to ETED, the FLBIC-CUAV approach has attained improved results with the decreased ETED under distinct rounds of operation. For instance, with 1000 rounds, the FLBIC-CUAV approach has obtainable a lesser ETED of 1.95 s whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C methods have attained an increased ETED of 2.03, 2.12, 2.18, and 2.27 s correspondingly. Also, with 3000 rounds, the FLBIC-CUAV manner has provided a minimal ETED of 2.52 s whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C methods have attained a maximum ETED of 2.67, 3.37, 3.66, and 4.87 s respectively. However, with 5000 rounds, the FLBIC-CUAV technique has accomplished a decreased ETED of 4.89 s whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C algorithms have gained a maximum ETED of 5.06, 5.83, 6.32, and 6.45 s correspondingly.

The throughput analysis showcased that the FLBIC-CUAV technique has gained effective results with the supreme throughput under all iterations, as shown in Fig. 5. For instance, with 1000 iterations, the FLBIC-CUAV technique has demonstrated improved outcomes with the increased throughput of 0.97 Mbps whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C algorithms have resulted in a reduced throughput of 0.96, 0.94, 0.92, and 0.90 Mbps respectively. Concurrently, with 3000 iterations, the FLBIC-CUAV approach has showcased increased results with maximum throughput of 0.93 Mbps whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C manners have resulted in a decreased throughput of 0.87, 0.83, 0.75, and 0.71 Mbps correspondingly. Meanwhile, with 5000 iterations, the FLBIC-CUAV algorithm has exhibited higher outcomes with the superior throughput of 0.85 Mbps whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C methodologies have resulted in a lesser throughput of 0.79, 0.70, 0.63, and 0.59 Mbps correspondingly.



**Figure 5:** Throughput analysis of FLBIC-CUAV technique on scenario 1

The results analysis of the FLBIC-CUAV method with existing algorithms on scenario 2 is given in Tab. 2. On inspecting the outcomes with respect to ECM, the FLBIC-CUAV technique has attained results with the minimum ECM under varying rounds of operation. For instance, with 1000 rounds, the FLBIC-CUAV approach has existed at least ECM of 30 mJ whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C methods have obtained a higher ECM of 36, 39, 41, and 45 mJ respectively. Besides, with 3000 rounds, the FLBIC-CUAV approach has offered a lesser ECM of 68 mJ whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C algorithms have reached a maximal ECM of 75, 84, 89, and 97 mJ correspondingly. Followed by, with 5000 rounds, the FLBIC-CUAV methodology has accomplished a reduced ECM of 98 mJ whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C manners have attained an improved ECM of 107, 123, 128, and 137 mJ correspondingly.

**Table 2:** Results of existing with proposed FLBIC-CUAV method in terms of various parameters on scenario 2

No. of rounds	Energy consumption (mJ)				
	FLBIC-CUAV	T2FL-C	KHA-C	MPSO-C	T1FL-C
1000	30	36	39	41	45
2000	52	58	65	69	71
3000	68	75	84	89	97
4000	79	84	100	106	115
5000	98	107	123	128	137

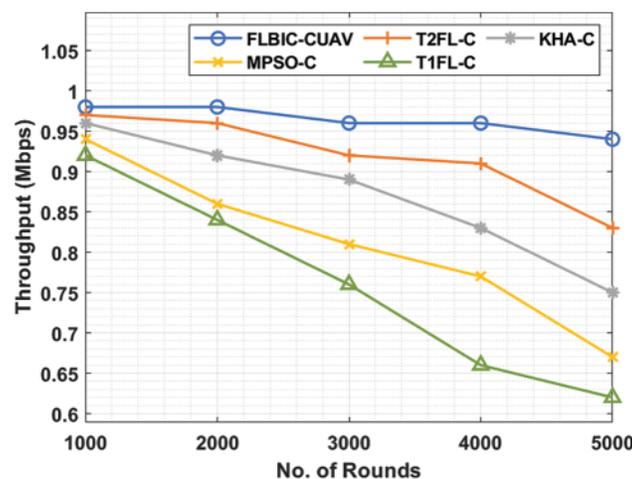
No. of rounds	End to end delay (sec)				
	FLBIC-CUAV	T2FL-C	KHA-C	MPSO-C	T1FL-C
1000	1.97	2.08	2.14	2.23	2.32
2000	2.52	2.59	2.69	3.03	3.84
3000	2.57	2.69	3.41	3.72	4.89
4000	3.25	3.38	4.30	4.94	5.93
5000	4.93	5.11	5.87	6.38	6.50

No. of rounds	Throughput (Mbps)				
	FLBIC-CUAV	T2FL-C	KHA-C	MPSO-C	T1FL-C
1000	0.98	0.97	0.96	0.94	0.92
2000	0.98	0.96	0.92	0.86	0.84
3000	0.96	0.92	0.89	0.81	0.76
4000	0.96	0.91	0.83	0.77	0.66
5000	0.94	0.83	0.75	0.67	0.62

Then, on investigating the results interms of ETED, the FLBIC-CUAV manner has obtained improved outcomes with the least ETED under different rounds of operation. For sample, with 1000 rounds, the FLBIC-CUAV method has offered a minimal ETED of 1.97 s whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C systems have gained a superior ETED of 2.08, 2.14, 2.23, and 2.32 s respectively. Moreover, with 3000 rounds, the FLBIC-CUAV manner has provided a minimal ETED of 2.57 s whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C algorithms have attained a maximum ETED of 2.69, 3.41, 3.72, and 4.89 s respectively. Likewise, with 5000 rounds, the FLBIC-CUAV method has accomplished a minimum ETED of 4.93 s whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C methodologies have achieved an increased ETED of 5.11, 5.87, 6.38, and 6.50 s respectively.

The throughput analysis demonstrated that the FLBIC-CUAV manner has attained effective results with the supreme throughput under all iterations, as shown in Fig. 6. For sample, with 1000 iterations, the FLBIC-CUAV approach has outperformed increased outcome with the maximal throughput of 0.98 Mbps whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C methodologies have resulted in a lesser throughput of 0.97, 0.96, 0.94, and 0.92 Mbps correspondingly. Simultaneously, with 3000 iterations, the FLBIC-CUAV algorithm has depicted improved outcomes with the higher throughput of 0.96 Mbps whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C manners have resulted in a reduced throughput of 0.92, 0.89, 0.81, and 0.76 Mbps correspondingly. In the meantime, with 5000 iterations, the FLBIC-CUAV technique has portrayed enhanced outcomes with the increased throughput of 0.94 Mbps whereas the T2FL-C, KHA-C, MPSO-C, and T1FL-C methods have resulted in a reduced throughput of 0.83, 0.75, 0.67, and 0.62 Mbps correspondingly.



**Figure 6:** Throughput analysis of FLBIC-CUAV technique on scenario 2

Fig. 7 showcases the comparative ECM and ETE delay analysis of the FLBIC-CUAV technique with existing techniques under two different scenarios. The results showcased that the FLBIC-CUAV technique has gained effective performance with minimal ECM and ETE delay over the other existing techniques.

A comprehensive comparison study of the FLBIC-CUAV technique with existing techniques takes place in terms of accuracy in Tab. 3 and Fig. 8 [25].

The results depicted that PlacesNet and VGG-VD19 techniques have accomplished poor outcomes with the accuracy of 91.44% and 93.15%. Followed by, all the other techniques except DL-MOPSO, C-PTRN, and FLBIC-CUAV techniques have showcased moderately closer accuracy values. Simultaneously, the DL-MOPSO technique has tried to obtain reasonable performance with an accuracy of 95.32%. Concurrently, the C-PTRN technique has resulted in a near-optimal performance with an accuracy of 98.67%. However, the FLBIC-CUAV technique has gained maximum performance over the other techniques with a maximum accuracy of 99.15%.

From these result analyses, it can be concluded that the FLBIC-CUAV technique can be employed as an effective approach for secure UAV communication in IIoT environment.

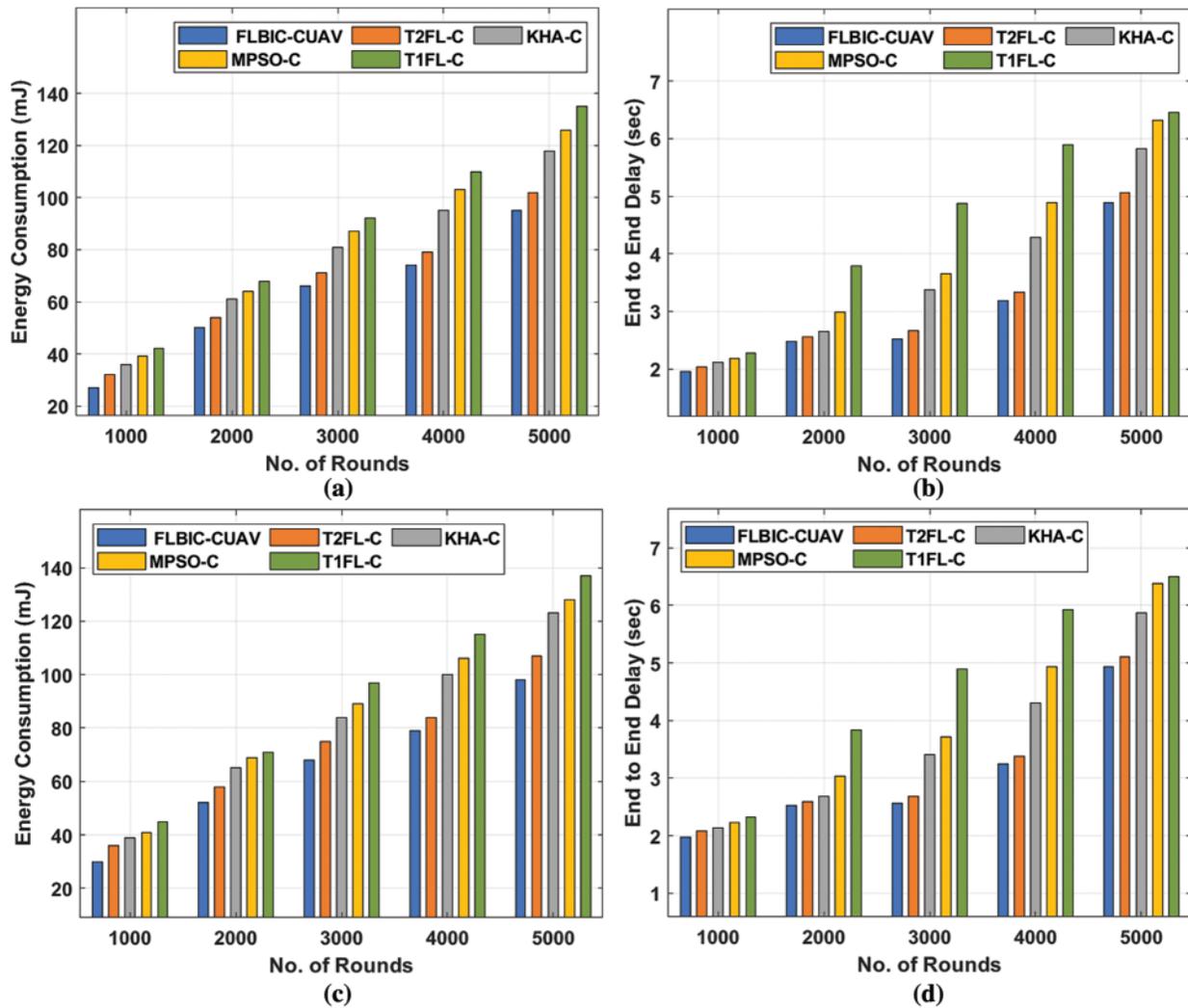


Figure 7: Comparative energy consumption and ETE delay analysis (a, b) Scenario 1; (c, d) Scenario 2

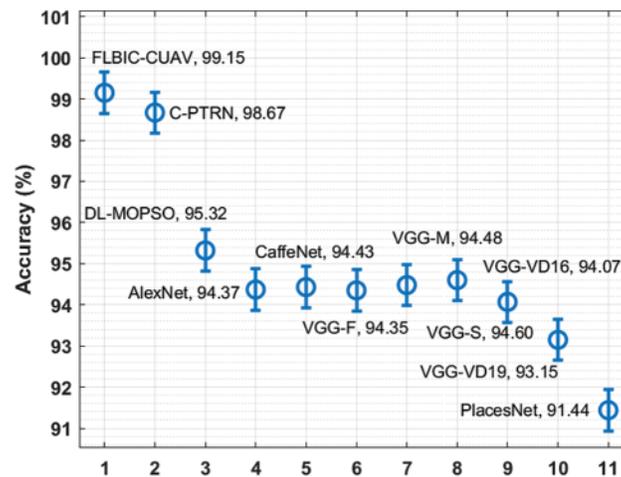
Table 3: Accuracy analysis of FLBIC-CUAV with various CNN models

Methods	Accuracy
FLBIC-CUAV	99.15
C-PTRN	98.67
DL-MOPSO	95.32
AlexNet	94.37
CaffeNet	94.43
VGG-F	94.35

(Continued)

**Table 3:** Continued

Methods	Accuracy
VGG-M	94.48
VGG-S	94.60
VGG-VD16	94.07
VGG-VD19	93.15
PlacesNet	91.44

**Figure 8:** Accuracy analysis of FLBIC-CUAV model with recent approaches

## 5 Conclusion

In this study, a new FLBIC-CUAV technique is derived to accomplish secure communication and classification in UAV networks. The proposed FLBIC-CUAV technique involves distinct major processes namely BSO based clustering, blockchain enabled secure communication and FL based image classification. The BSO algorithm derives a fitness function involving three input parameters related to UAV for effective choice of CHs. Besides, the use of FL based image classification technique involves the concepts of ResNet and softmax functions. An extensive set of experimentations are carried out to guarantee the supremacy of the FLBIC-CUAV technique. The simulation results demonstrated the betterment of the FLBIC-CUAV technique over the recent state of art methods. In future, the energy efficiency of the UAV network can be boosted by data aggregation and context aware route planning approaches.

**Acknowledgement:** We deeply acknowledge Taif University for supporting this research through Taif University Researchers Supporting Project Number (TURSP-2020/328), Taif University, Taif, Saudi Arabia. The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

**Funding Statement:** The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work under grant number (RGP.2/209/42). [www.kku.edu.sa](http://www.kku.edu.sa)

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

## References

- [1] M. Aazam, S. Zeadally and K. A. Harras, “Deploying fog computing in industrial Internet of Things and industry 4.0,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4674–4682, 2018.
- [2] H. Shakhathreh, A. H. Sawalmeh, A. A. Fuqaha, Z. Dou, E. Almaita *et al.*, “Unmanned aerial vehicles: A survey on civil applications and key research challenges,” *IEEE Access*, vol. 7, pp. 48572–48634, 2019.
- [3] T. Lagkas, V. Argyriou, S. Bibi and P. Sarigiannidis, “UAV IoT framework views and challenges: Towards protecting drones as ‘Things’,” *Sensors*, vol. 18, no. 11, pp. 4015, 2018.
- [4] M. Itkin, M. Kim and Y. Park, “Development of cloud-based UAV monitoring and management system,” *Sensors*, vol. 16, no. 11, pp. 1913, 2016.
- [5] F. Tang, Z. M. Fadlullah, N. Kato, F. Ono and R. Miura, “AC-POCA: Anticoordination game based partially overlapping channels assignment in combined UAV and D2D-based networks,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 2, pp. 1672–1683, 2018.
- [6] J. Konecny, H. B. McMahan, F. X. Yu, P. Richtarik, A. T. Suresh *et al.*, “Federated learning: Strategies for improving communication efficiency,” arXiv preprint arXiv: 1610.05492, 2016.
- [7] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya *et al.*, “Adaptive federated learning in resource constrained edge computing systems,” *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 6, pp. 1205–1221, 2019.
- [8] H. Kim, J. Park, M. Bennis and S. Kim, “Blockchained on-device federated learning,” *IEEE Communications Letters*, vol. 24, no. 6, pp. 1279–1283, 2020.
- [9] U. Majeed and C. S. Hong, “FLchain: Federated learning via MEC-enabled blockchain network,” in *2019 20th Asia-Pacific Network Operations and Management Symp. (APNOMS)*, Matsue, Japan, pp. 1–4, 2019.
- [10] Y. Wang, X. Cui, Z. Gao and B. Gan, “Fed-SCNN: A federated shallow-cnn recognition framework for distracted driving,” *Security and Communication Networks*, vol. 2020, pp. 1–10, 2020.
- [11] M. Salhaoui, A. G. González, M. Arioua, F. J. Ortiz, A. E. Oualkadi *et al.*, “Smart industrial IoT monitoring and control system based on UAV and cloud computing applied to a concrete plant,” *Sensors*, vol. 19, no. 15, pp. 3316, 2019.
- [12] W. Zhang, Q. Lu, Q. Yu, Z. Li, Y. Liu *et al.*, “Blockchain-based federated learning for device failure detection in industrial IoT,” *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5926–5937, 2021.
- [13] W. Y. B. Lim, J. Huang, Z. Xiong, J. Kang, D. Niyato *et al.*, “Towards federated learning in uav-enabled internet of vehicles: A multi-dimensional contract-matching approach,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5140–5154, 2021.
- [14] H. Zhang and L. Hanzo, “Federated learning assisted multi-UAV networks,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 14104–14109, 2020.
- [15] Y. J. Kim and C. S. Hong, “Blockchain-based node-aware dynamic weighting methods for improving federated learning performance,” in *2019 20th Asia-Pacific Network Operations and Management Symp. (APNOMS)*, Matsue, Japan, pp. 1–4, 2019.
- [16] P. K. Sharma, J. H. Park and K. Cho, “Blockchain and federated learning-based distributed computing defence framework for sustainable society,” *Sustainable Cities and Society*, vol. 59, pp. 102220, 2020.
- [17] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh and G. Muhammad, “Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach,” *IEEE Access*, vol. 8, pp. 205071–205087, 2020.
- [18] S. R. Pokhrel, “Blockchain brings trust to collaborative drones and LEO satellites: An intelligent decentralized learning in the space,” *IEEE Sensors Journal*, vol. 21, no. 22, pp. 25331–25339, 2021.
- [19] A. A. Khan, M. M. Khan, K. M. Khan, J. Arshad and F. Ahmad, “A Blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs,” *Computer Networks*, vol. 196, pp. 108217, 2021.

- [20] Z. Zhang, T. Yang and Y. Liu, "SABlockFL: A blockchain-based smart agent system architecture and its application in federated learning," *International Journal of Crowd Science*, vol. 4, no. 2, pp. 133–147, 2020.
- [21] T. Wang, L. Yang and Q. Liu, "Beetle swarm optimization algorithm: Theory and application," *Filomat*, vol. 34, no. 15, pp. 5121–5137, 2020.
- [22] Y. Mu, B. Li, D. An and Y. Wei, "Three-dimensional route planning based on the beetle swarm optimization algorithm," *IEEE Access*, vol. 7, pp. 117804–117813, 2019.
- [23] W. Sun, H. Ma, W. Li, Y. Pan, F. Hao *et al.*, "Multi branches dilated CNN federated learning for transmission line fault diagnosis," in *Int. Conf. on Mechanical Engineering, Measurement Control, and Instrumentation*, Guangzhou, China, pp. 146, 2021.
- [24] S. Wan, Y. Liang and Y. Zhang, "Deep convolutional neural networks for diabetic retinopathy detection by image classification," *Computers & Electrical Engineering*, vol. 72, pp. 274–282, 2018.
- [25] I. V. Pustokhina, D. A. Pustokhin, P. K. Pareek, D. Gupta, A. Khanna *et al.*, "Energy-efficient cluster-based unmanned aerial vehicle networks with deep learning-based scene classification model," *International Journal of Communication Systems*, vol. 34, no. 8, 2021.