Computers, Materials & Continua
DOI: 10.32604/cmc.2022.031909
Article

Tech Science Press

Intelligent Optimization-Based Clustering with Encryption Technique for Internet of Drones Environment

Dalia H. Elkamchouchi[1], Jaber S. Alzahrani[2], Hany Mahgoub[3,4], Amal S. Mehanna[5], Anwer Mustafa Hilal[6,*], Abdelwahed Motwakel[6], Abu Sarwar Zamani[6] and Ishfaq Yaseen[6]

[1]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[2]Department of Industrial Engineering, College of Engineering at Alqunfudah, Umm Al-Qura University, Saudi Arabia
[3]Department of Computer Science, College of Science & Art at Mahayil, King Khalid University, Saudi Arabia
[4]Faculty of Computers and Information, Computer Science Department, Menoufia University, Egypt
[5]Department of Digital Media, Faculty of Computers and Information Technology, Future University in Egypt, New Cairo 11845, Egypt
[6]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, AlKharj, Saudi Arabia
*Corresponding Author: Anwer Mustafa Hilal. Email: A.hilal@psau.edu.sa

Received: 29 April 2022; Accepted: 17 June 2022

Abstract: The recent technological developments have revolutionized the functioning of Wireless Sensor Network (WSN)-based industries with the development of Internet of Things (IoT). Internet of Drones (IoD) is a division under IoT and is utilized for communication amongst drones. While drones are naturally mobile, it undergoes frequent topological changes. Such alterations in the topology cause route election, stability, and scalability problems in IoD. Encryption is considered as an effective method to transmit the images in IoD environment. The current study introduces an Atom Search Optimization based Clustering with Encryption Technique for Secure Internet of Drones (ASOCE-SIoD) environment. The key objective of the presented ASOCE-SIoD technique is to group the drones into clusters and encrypt the images captured by drones. The presented ASOCE-SIoD technique follows ASO-based Cluster Head (CH) and cluster construction technique. In addition, signcryption technique is also applied to effectually encrypt the images captured by drones in IoD environment. This process enables the secure transmission of images to the ground station. In order to validate the efficiency of the proposed ASOCE-SIoD technique, several experimental analyses were conducted and the outcomes were inspected under different aspects. The comprehensive comparative analysis results established the superiority of the proposed ASOCE-SIoD model over recent approaches.

Keywords: Internet of drones; atom search algorithm; clustering; encryption; signcryption

1 Introduction

Internet of Drones (IoD) is defined as a platform that is created to provide users with accessibility and control upon drones through internet [1]. In general, drones can be quickly turned into easily-accessible devices. Every single user can perform distinct operations using multiple drones under controlled airspace. Even though technology helps in mass production of onboard elements of Unmanned Aerial Vehicles (UAVs) such as energy storage batteries, sensors, and processors, the execution boundaries of such components hinder and diminish the application of UAVs [2,3]. IoD is a concept of coupling the drones and vehicles together using cloud mobility operations in order to achieve distant drone control and access and smooth adaption of offloading with distant cloud storage abilities [4]. UAVs with fixed wings have a primary advantage over UAVs with rotating wings i.e., less maintenance, low-cost repair and simple structure. These characteristics allow the customer to have more operating duration at minimum cost [5].

In general, drones have insufficient battery sources and their computational energy is confined to a certain level. These drawbacks affect the entire transmission efficacy in IoD. Routing process is mandatory for effective transmission and communication of data amongst drones [6]. It is challenging to ensure effective transmission of data amongst drones due to quickly varying topology and the portability of drones from IoD. In this scenario, clustering, the hierarchal routing process is the only solution to overcome such issues. In a cluster, there exists both Cluster Members (CMs) and a Cluster Head (CH) which altogether form a network with sub groups [7]. The selection of CH assumes a significant role in clustering and every CM is eligible to be an applicant in the selection of CH. The increasing familiarity of the drones has in turn inclined the occurrence of cyber-attacks toward UAV systems in the past few decades. A cyber attacker tend to focus on radio associations of UAV system so as to delay the ability of systems in terms of interacting with user devices [8]. This inculcates the data required by the user's mobile devices which controls Global Positioning System (GPS) signals [9]. In general, image processing techniques are also linked with network atmospheres. Images are sensitive and intuitive in nature due to which the absence of appropriate protective measures may result in leakage of data like confidential information, security breach and loss of private information too [10]. So, there is a need exists to prevent the increasing number of cyber-attacks that severely attack the privacy and security of the data, especially image information. In this background, image information can be saved through encryption processes.

Bera et al. [11] presented a Blockchain (BC)-based access control method for IoD environment which permits secure communication amongst the drones and between drones and Ground Station Server (GSS). The data collected by GSS procedure and individual communications are converted securely into blocks. Block is added at last from the BC, while the cloud services are associated with GSS using Ripple Protocol Consensus Algorithm (RPCA) from a peer-to-peer cloud server network. Wazid et al. [12] presented a novel light-weight user authentication method in which a user from IoD environment who requires data access from a drone directly is provided such access to the data in drone. Aftab et al. [13] presented a CH selection method based on connectivity with Base Station (BS) with Fitness Function (FF) that contains Residual Energy (RE) and information about the place of drones. Besides, route election can present an optimum path election based upon RE and the place of drones for effectual communications. Saif et al. [14–17] concentrated on performance evaluation of clustering technique by identifying wireless coverage service through increasing energy efficacy. The performance was evaluated through realistic model from ground to air channel Line-of-Sight (LoS). The outcomes depict that the CH efficiently connects the UAV and CMs at less energy expenditure. Bera et al. [18] presented and analyzed a novel BC-based secure structure for data management amongst IoD transmission entities. The presented method is capable of resisting numerous potential attacks that are important from Internet of Things (IoT)-allowed IoD environments.

The current study introduces Atom Search Optimization based Clustering with Encryption Technique for Secure Internet of Drones (ASOCE-SIoD) environment. The presented ASOCE-SIoD technique follows ASO-based Cluster Head (CH) and cluster construction technique. The presented model derives a FF involving multiple parameters especially trust parameters for secure process. In addition, signcryption technique is also applied to effectually encrypt the images captured by drones in IoD environment which enables secure transmission of images to the ground station. In order to validate the increased efficiency of the proposed ASOCE-SIoD model, numerous experimental analyses were conducted and the outcomes were examined under different aspects.

2 Design of ASOCE-SIoD Model

In this study, a novel ASOCE-SIoD approach has been developed to group the drones into clusters and encrypt the images captured by drones. The presented ASOCE-SIoD technique follows ASO-based CH and cluster construction technique. The presented model derives a FF involving multiple parameters especially trust parameters for secure process. In addition, signcryption technique is also applied to effectually encrypt the images captured by drones in IoD environment. Fig. 1 illustrates the overall processes involved in ASOCE-SioD method.

2.1 Overview of ASO Algorithm

ASO is one of the recently-developed, physics-inspired, population-based heuristic approach that stimulates the atomic motion under control of constraint and interaction forces to project a better searching method for global optimization problems [19]. The overall interaction forces to act upon *i-th* atom in *d* dimensional vector, i.e., the amount of repulsions and the attraction applied in vigorous modification of neighbor atom on *i-th* atom is as follows.

$$F_i^d(t) = \sum_{j \in Kbest} rand_j F_{ij}^d(t) \tag{1}$$

In Eq. (1), the random numbers with 0 and 1 are denoted via $rand_j$ and *Kbest* which indicate a set of atom populations that comprises of initial K atoms and an optimal FF. Thus, the values of K need to be reduced in a linear fashion at iteration, using the following equation,

$$K(t) = N - (N-2) \times \sqrt{\frac{t}{T}} \tag{2}$$

In Eq. (2), the overall number of atoms in the atomic system is denoted via N, t indicates the existing iteration and T denotes the maximal amount of iterations. F_{ij}^d in (1) indicates the interaction force that *j-th* optimal atom exerted on *i-th* atom in *d* dimensional vector.

$$F_{ij}^d = -\eta(t)\left[2\left(h_{ij}(t)\right)^{-13} - \left(h_{ij}(t)\right)^{-7}\right]\frac{\vec{r}_{ij}}{r_{ij}} \tag{3}$$

In Eq. (3), $\eta(t)$ indicates the depth function for adjusting attractive or repulsion areas whereas $h_{ij}(t) = r_{ij}/\sigma(t)$ indicates the ratio of distance between two atoms to the scaling length that is named as scaling distance between two atoms. $\vec{r} = \vec{x} - \vec{x}$ denotes the location variance vector in which $\vec{x} = \left(x_{j1}, x_{j2}, x_{j3}\right)$ indicates the location vector of *j-th* atom and $\vec{x} = (x_{i1}, x_{i2}, x_{i3})$ signifies the location vector of *i-th* atom. Therefore, r_{ij} implies the Euclidian distance between *i-th* and *j-th* atoms

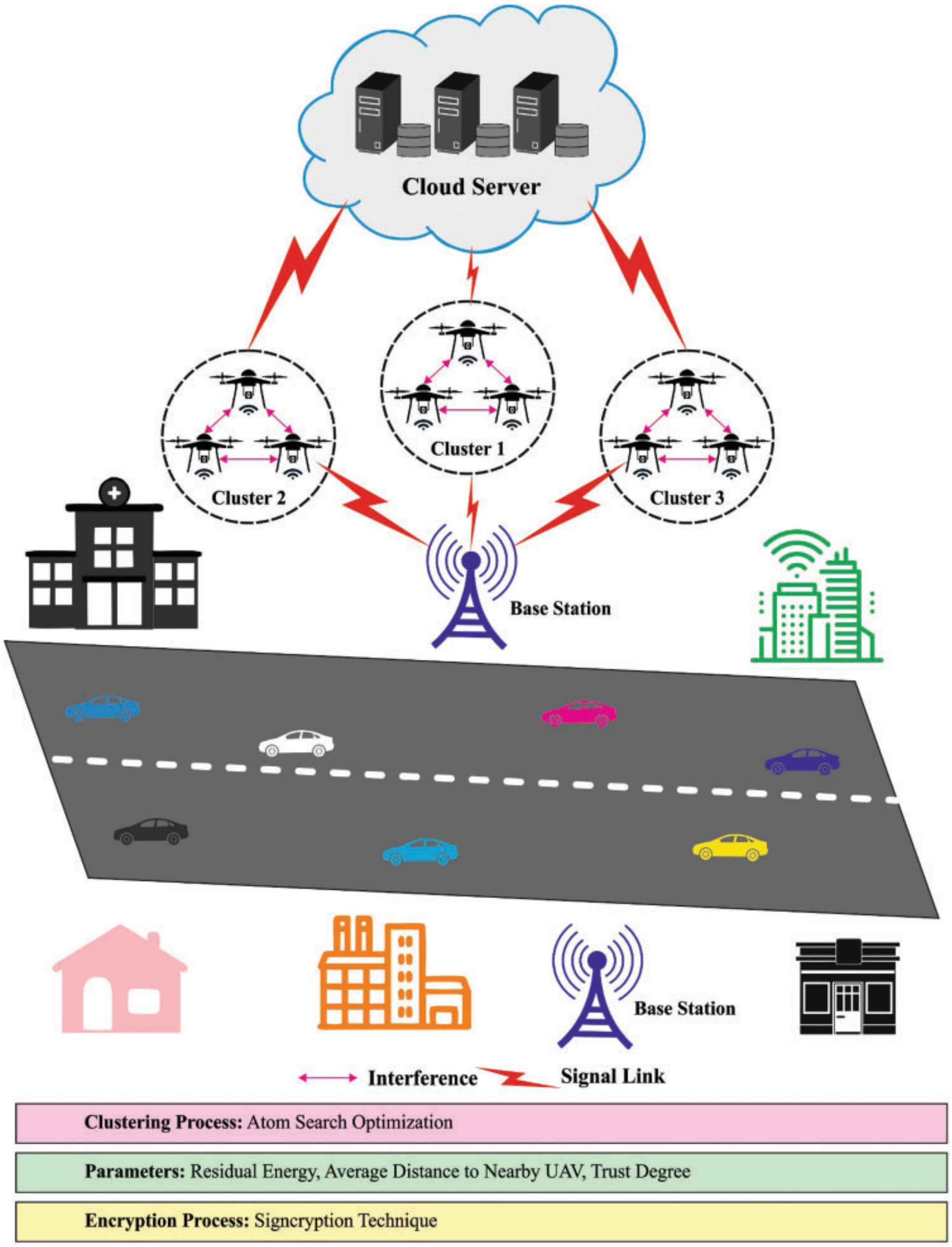
Cloud Server
Cluster 1
Cluster 2
Cluster 3
Base Station
Base Station
Interference
Signal Link
Clustering Process: Atom Search Optimization
Parameters: Residual Energy, Average Distance to Nearby UAV, Trust Degree
Encryption Process: Signcryption Technique

Figure 1: Overall processes of the proposed method

$$r_{ij} = \|\vec{x}_{\mathrm{j}} - \vec{x}_{\mathrm{i}}\| = \sqrt{(x_{j1} - x_{i1})^2 + (x_{j2} - x_{i2})^2 + (x_{j3} - x_{i3})^2} \tag{4}$$

In (3), the depth function is described as follows.

$$\eta\left(t\right)=\alpha\left(1-\frac{t-1}{T}\right)^{3}e^{-\frac{20t}{T}} \tag{5}$$

Here α indicates the depth weight and is equivalent to 50. The scaling distance between two atoms is shown below.

$$h_{ij}\left(t\right)=\begin{cases}h_{\min} & \frac{r_{ij}(t)}{\sigma(t)}<\mathrm{h}_{\min}\\ \dfrac{r_{ij}\left(t\right)}{\sigma\left(t\right)} & \mathrm{h}_{\min}\leq\dfrac{r_{ij}\left(t\right)}{\sigma\left(t\right)}\leq h_{\max}\\ h_{max} & \dfrac{r_{ij}\left(t\right)}{\sigma\left(t\right)}>h_{\max}\end{cases} \tag{6}$$

Here $h_{\min}$ and $h_{\max}$ indicate the lower and upper limits of the scaling distance (h), correspondingly which are determined as follows.

$$\begin{cases}h_{\min}=g_0+g\left(t\right)\\ h_{\max}=u\end{cases} \tag{7}$$

In Eq. (7), g_0 indicates the lowermost bound fixed at 1.1 and u signifies the uppermost bound fixed at 1.24, and $g\left(t\right)$ denotes the drift factor to ensure a proficient drift in the process from exploration to exploitation as given below.

$$g\left(t\right)=0.1\times\sin\left(\frac{\pi}{2}\times\frac{t}{T}\right) \tag{8}$$

In Eq. (6), the scaling length $\sigma\left(t\right)$ symbolizes the collision diameter.

$$\sigma\left(t\right)=\|x_{ij}\left(t\right),\frac{\sum_{j\in Kbest}x_{ij}\left(t\right)}{K\left(t\right)}\|_2 \tag{9}$$

When all the atoms in ASO have a covalent bond with optimal atoms, the resultant geometric restriction force i.e., weighted location variance between the optimal atoms is shown below.

$$G_i^d\left(t\right)=\lambda\left(t\right)\left(x_{best}^d\left(t\right)-x_i^d\left(t\right)\right) \tag{10}$$

Here $x_{best}^d\left(t\right)$ denotes the location of optimal atom in *d-th* dimensional vector and $\lambda\left(t\right)$ indicates the Lagrangian multiplier that is determined as given herewith.

$$\lambda\left(t\right)=\beta e^{-\frac{20t}{T}} \tag{11}$$

Fig. 2 depicts the flowchart of ASO technique. Now, β indicates the multiplier weight and is equivalent to 0.2 [20]. Both constraint and interaction forces are yielded from bond-length and L-J potential correspondingly. The acceleration of *i-th* atom in d dimensional vector in t iteration is estimated as given herewith.

$$a_i^d(t) = \frac{F_i^d(t)}{m_i^d(t)} + \frac{G_i^d(t)}{m_i^d(t)}$$
$$= -\alpha\left(1 - \frac{t-1}{T}\right)^3 e^{-\frac{20t}{T}} \times \sum_{j\in Kbest} \frac{rand_j[2(h_{ij}(t))^{-13} - \left(h_{ij}(t))^{-7}\right]}{m_i(t)} \cdot \frac{\left(x_j^d(t) - x_i^d(t)\right)}{\|\vec{x}_{\mathrm{i}}(t), \vec{x}_{\mathrm{j}}(t)\|_2}$$
$$+ \beta e^{-\frac{20t}{T}} \frac{\left(x_{best}^d(t) - x_i^d(t)\right)}{m_i(t)} \tag{12}$$

Here $m_i^d(t)$ signifies the mass of *i-th* atom in *d* dimensional vector during *t* iteration, and is estimated using the FF.

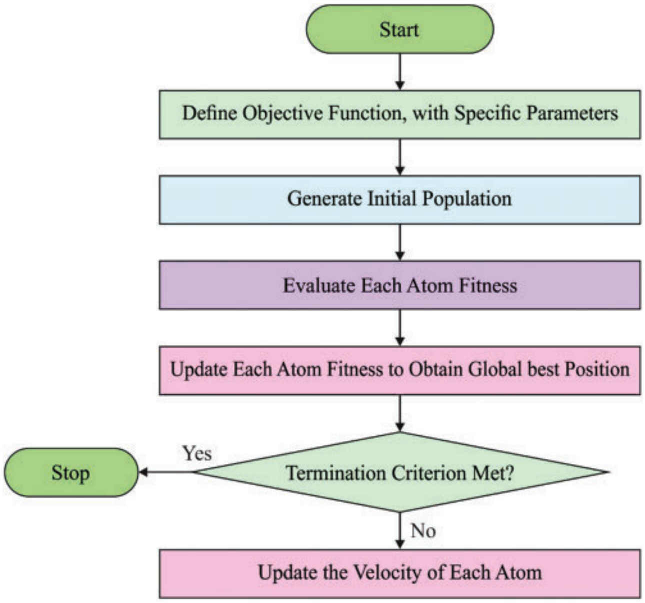
Start
Define Objective Function, with Specific Parameters
Generate Initial Population
Evaluate Each Atom Fitness
Update Each Atom Fitness to Obtain Global best Position
Termination Criterion Met?
Yes
Stop
No
Update the Velocity of Each Atom

Figure 2: Flowchart of ASO technique

$$M_i(t) = e^{-\frac{Fit_i(t) - Fit_{best}(t)}{Fit_{worst}(t) - Fit_{best}(t)}} \tag{13}$$

$$m_i(t) = \frac{M_i(t)}{\sum_{j=1}^{N} M_j(t)} \tag{14}$$

Now $Fit_i(t)$ indicates the FF of *i-th* atom in t iteration, $Fit_{best}(t)$ and $Fit_{worst}(t)$ denote the fitness values of optimal and the worst atoms during t iteration, correspondingly

$$Fit_{best}(t) = \min_{i\,\epsilon\{1,2,\ldots N\}} Fit_i(t) \tag{15}$$

$$Fit_{worst}(t) = \max_{i\,\epsilon\{1,2,\ldots N\}} Fit_i(t) \tag{16}$$

At last, the position and velocity of *i-th* atom are updated during $(t+1)$ iteration and is described as follows.

$$v_i^d\,(t+1) = rand_i^d \cdot v_i^d\,(t) + a_i^d\,(t) \tag{17}$$

$$x_i^d\,(t+1) = x_i^d\,(t) + v_i^d\,(t+1) \tag{18}$$

2.2 Processes Involved in ASO-Based Clustering Technique

The presented ASO model derives a FF that involves multiple parameters especially trust parameters for secure process. The RE of UAV (x), when transferring k bits to the terminus UAV (y), on distance d, is determined as follows.

$$RE = E - \left(E_T\,(k,d) + E_{R(k)}\right) \tag{19}$$

In Eq. (19), E indicates the present energy of UAV and E_T denotes the energy expended for sensing the information.

$$E_T\,(k,d) = kE_e + KE_a d^2 \tag{20}$$

In Eq. (20), E_e represents the energy of electrons and E_a denotes the amplified energy, $E_{R(k)}$ signifies the energy dissipated to obtain information as given below.

$$E_{R(k)} = kE_e \tag{21}$$

Three variables are used to select the CH and calculate the average distance (AvgD) for neighboring UAVs. Here, AvgD symbolizes the average distance value to the UAV and its individual neighbouring UAV as given below.

$$AvgNBDist_i = \frac{\sum_{j=1}^{NB_i} dist\left(i, nb_j\right)}{NB_i}, \tag{22}$$

In Eq. (22), $dist\left(i, nb_j\right)$ denotes the distance from UAV to the neighbouring *jth* UAV.

Here, energy trust is measured if the node has sufficient RE for completing novel transmissions and data processing tasks. The present research case made use of direct trust between the nodes, A as well as B of all the clusters, and their mathematical model is signified as follows.

At this point, Tr_{ij}^{dir} and TR_{ij}^{indir} represent the direct as well as indirect trust values of one node to another node correspondingly.

2.3 Signcryption Process

In this work, signcryption technique is applied to effectually encrypt the images captured by drones in IoD environment which enables secure transmission of the images to ground station [21]. Here, public key encryption system is used as a security approach in which digital signature is used and it optimizes integrity, authenticity, confidentiality, availability, and nonrepudiation. Encryption can be done instead of modest encryption. Further, single session keys are also reprocessed for some encryption to obtain remarkable outcome than signcryption system. Essentially, signcryption methodology has the following processes namely, designcryption stage, key generation, and signcryption process. Meanwhile, encryption offers security and signature provides authenticity. In parallel, signcryption implements both encryption and signature functions from the logical stage itself. However, the overhead values of communication and calculation are less than the series of signatures. In signcryption process, there exists different stages such as key generation, initialization of parameters, designcryption, and signcryption. Initially, signature-based security analysis allows the variables namely huge prime values for sender and receiver keys, key generation, and hash values.

In this method, the keys are produced with the help of cryptographic technique; the function of the elliptical curve-based shape is to generate the prime numbers and influence the numbers created. The initializing parameters are Sr_1, Su_1, Rr_2, and Ru_1. In order to maximize the secure communication, the key is utilized.

i) Encryption technique transfers the dataset to receiver after analyzing the security; both hash and one-keyed hash values are taken into account based on the encrypted data as well as motion vector. This transformation of plain dataset into ciphered dataset can be defined in subsequent phases. At first, the sender transmits the data with a suitable value, A from $[\,1, \ldots, PF—1]$.

ii) The hash values of the sender are evaluated using Ru_2 receiver and A denotes the output O_H_o of hash values i.e., 128bits. The mathematical expression of the equation is given below.

$$O\_H_o = HASH\left(Ru_2^A * mod\ PN\right). \tag{23}$$

iii) The output values of 128bits are partitioned into 64 pieces with each piece containing two bits such as O_H_o1 and O_H_o2.

iv) The sender encrypts the data for E encryption as well as O_H_o1. It is defined as follows.

$$C_i = EO\_H_o1\ (info). \tag{24}$$

v) Next, the O_H_o2 values are efficiently employed from one-way keyed hash function K_H_o to hash the data that results in 128bits hash which is characterized as follows.

$$F = K\_H_o2\ (info). \tag{25}$$

vi) At last, the signcryption of the data is estimated. Then, the cipher dataset is characterized as follows.

$$S = A/_{(F+A_{O\_H_O}1)} mod\ PF \tag{26}$$

vii) From the estimation, three different values, F, and C_i are transferred to the receiver and sender.

3 Experimental Validation

The current section validates the clustering and encryption performance of the proposed ASOCE-SIoD model under diverse number of drones and grid sizes. A comparison study was conducted with existing models such as Ant Colony Optimization (ACO), Grey Wolf Optimizer (GWO), and blockchain with clustering in IoD (BICIoD).

Tab. 1 provides a detailed overview on Cluster Building Time (CBT) analysis results achieved by ASOCE-SIoD model and other existing models on grids sized such as (1000 × 1000 m) and (2000 × 2000 m). Fig. 3 exhibits the results of comparative CBT analysis accomplished by ASOCE-SIoD model and other existing models under the grid sized at 1000 × 1000 m and distinct number of drones. The figure indicates that the proposed ASOCE-SIoD model required less CBT over existing techniques. For instance, with 15 drones, the proposed ASOCE-SIoD model required the least CBT of 1.73 s, whereas ACO, GWO, and BICIoD techniques demanded high CBT such as 6.04, 4.75, and 2.81 s respectively.

Along with that, with 35 drones, the proposed ASOCE-SIoD approach required a minimal CBT of 3.24 s, whereas ACO, GWO, and BICIoD methods obtained the maximal CBT of 23.52, 14.03, and 4.75 s correspondingly.

Table 1: CBT analysis results of ASOCE-SIoD technique under distinct grid sizes and count of drones

Cluster building time (sec)				
No. of drones	ACO	GWO	BICIoD	ASOCE-SIoD
Grid size (1000 × 1000 m^2)				
15	6.04	4.75	2.81	1.73
20	9.06	6.26	3.35	1.84
25	11.87	8.09	4.64	2.81
30	19.64	9.93	4.64	2.48
35	23.52	14.03	4.75	3.24
Grid size (2000 × 2000 m^2)				
15	8.19	6.62	4.57	2.05
20	10.87	8.51	5.28	3.39
25	15.59	10.55	6.93	4.10
30	23.23	13.31	7.40	3.94
35	27.56	13.54	8.58	5.20

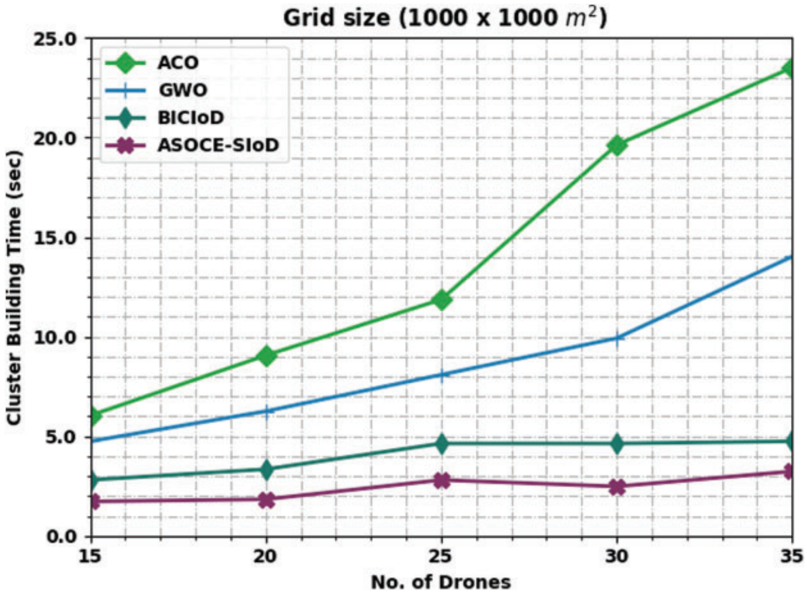

Figure 3: CBT analysis results of ASOCE-SIoD technique under grid size, 1000 × 1000 m

Fig. 4 demonstrates the comparative CBT examination results achieved by the proposed ASOCE-SIoD methodology and other techniques under grid size 2000 × 2000 m and distinct number of drones. The figure expose that the proposed ASOCE-SIoD system required less CBT over existing approaches. For sample, with 15 drones, the proposed ASOCE-SIoD algorithm required the least CBT of 2.05 s, whereas ACO, GWO, and BICIoD systems demanded the maximum CBT such as 8.19, 6.62, and 4.57 s correspondingly. Likewise, with 35 drones, ASOCE-SIoD system required the least CBT of 5.20 s, whereas ACO, GWO, and BICIoD techniques demanded high CBT such as 27.56, 13.54, and 8.58 s correspondingly. Tab. 2 provides a detailed overview on Energy Consumption (ECM) analysis results accomplished by the proposed ASOCE-SIoD methodology and other approaches on grids sized at (1000 × 1000 m) and (2000 × 2000 m).

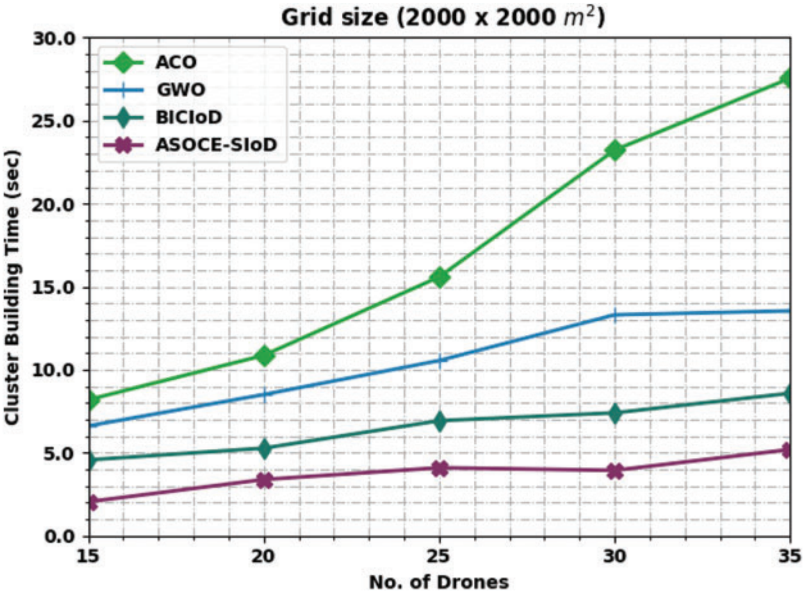

Figure 4: CBT analysis results of ASOCE-SIoD technique under grid size, 2000 × 2000 m

Table 2: ECM analysis results of ASOCE-SIoD technique with distinct grid sizes and count of drones

Energy consumption (J)				
No. of drones	ACO	GWO	BICIoD	ASOCE-SIoD
Grid size (1000 × 1000 m^2)				
15	1.73	1.94	1.24	0.56
20	2.52	2.79	1.64	1.09
25	3.25	3.96	2.08	1.48
30	3.78	4.64	2.61	1.81
35	4.40	5.13	3.20	2.25

(Continued)

Table 2: Continued

Energy consumption (J)				
No. of drones	ACO	GWO	BICIoD	ASOCE-SIoD
Grid size (2000 × 2000 m^2)				
15	2.19	2.52	1.52	0.92
20	2.98	3.33	2.32	1.79
25	3.80	4.15	2.61	2.25
30	4.31	4.64	3.33	2.71
35	4.71	5.26	4.13	2.98

Fig. 5 showcases the comparative Energy Consumption (ECM) analysis results accomplished by the proposed ASOCE-SIoD methodology and other existing approaches under grid size of 1000 × 1000 m and distinct number of drones. The figure shows the superior performance of ASOCE-SIoD system with low ECM over existing approaches. For sample, with 15 drones, the proposed ASOCE-SIoD methodology obtained the ECM of 0.56 J, whereas ACO, GWO, and BICIoD techniques obtained high ECM values such as 1.73, 1.94, and 1.24 J respectively. Eventually, with 35 drones, the proposed ASOCE-SIoD technique obtained the least ECM of 2.25 J, whereas ACO, GWO, and BICIoD algorithms obtained high ECM values such as 4.40, 5.13, and 3.20 J correspondingly.

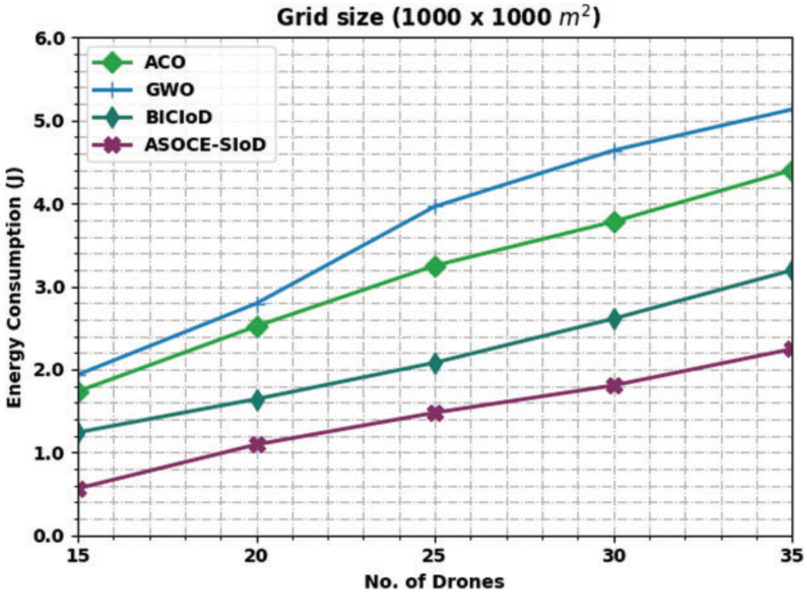

Figure 5: ECM analysis results of ASOCE-SIoD algorithm under grid size, 100 × 1000 m

Fig. 6 portrays the comparative ECM inspection results achieved by the proposed ASOCE-SIoD model and other existing methods under grid size of 2000 × 2000 m and distinct number of drones. The figure expose that the proposed ASOCE-SIoD system achieved a low ECM over existing techniques. For instance, with 15 drones, ASOCE-SIoD model offered the least ECM of 0.92 J, whereas ACO, GWO, and BICIoD techniques obtained high ECM values such as 2.19, 2.52, and 1.52 J correspondingly. In addition, with 35 drones, the proposed ASOCE-SIoD approach achieved the least ECM of 2.98 J, whereas ACO, GWO, and BICIoD systems gained enhanced ECM values such as 4.71, 5.26, and 4.13 J correspondingly.

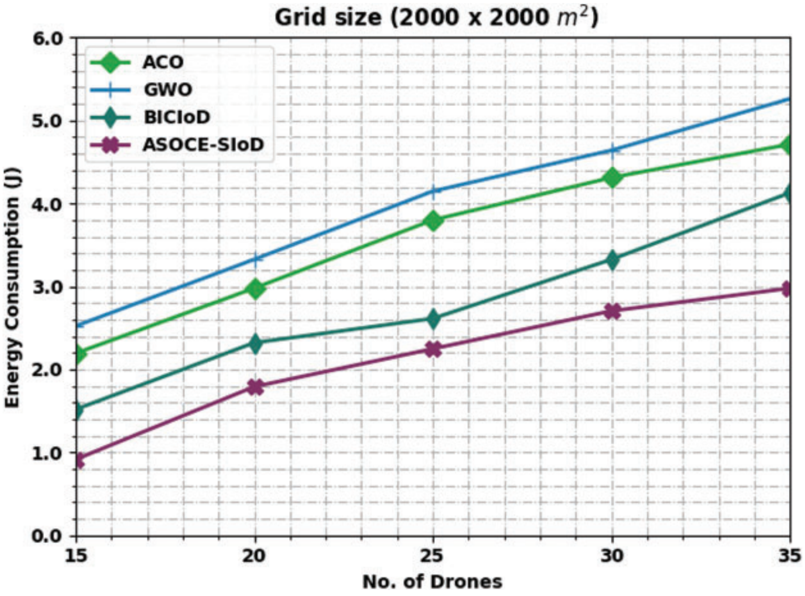

Figure 6: ECM analysis results of ASOCE-SIoD algorithm under grid size 2000 × 2000 m

A detailed Cluster Lifetime (CLT) analysis was conducted between ASOCE-SIoD model and other existing approaches and the results are shown in Tab. 3 under distinct sizes of grids and drones.

Table 3: CLT analysis results of ASOCE-SIoD algorithm under distinct grid sizes and count of drones

Cluster life time (sec)				
No. of drones	ACO	GWO	BICIoD	ASOCE-SIoD
Grid size (1000 × 1000 m^2)				
15	42.48	36.29	48.49	52.62
20	37.49	33.54	44.54	50.38
25	34.74	30.27	41.27	48.15
30	32.33	24.43	39.38	43.68
35	30.62	22.88	35.43	40.93

(Continued)

Table 3: Continued

Cluster life time (sec)				
No. of drones	ACO	GWO	BICIoD	ASOCE-SIoD
Grid size (2000 × 2000 $\boldsymbol{m}^2$)				
15	47.37	41.90	52.84	55.58
20	41.73	37.96	48.74	54.04
25	37.62	35.74	43.95	50.62
30	33.86	29.07	41.55	47.03
35	32.15	27.02	37.79	44.12

Fig. 7 exhibits the comparative CLT results accomplished by the proposed ASOCE-SIoD system and other existing models on grid size of 1000 × 1000 m. The figure implies that the proposed ASOCE-SIoD approach demonstrated effectual outcomes with increased CLT values under all the cases. For instance, with 15 drones, ASOCE-SIoD model attained a high CLT of 52.62 s, whereas ACO, GWO, and BICIoD techniques reached the least CLT values such as 42.48, 36.29, and 48.49 s respectively. Also, with 35 drones, the proposed ASOCE-SIoD system obtained a superior CLT of 40.93 s, whereas ACO, GWO, and BICIoD techniques attained minimal CLT values such as 30.62, 22.88, and 35.43 s correspondingly.

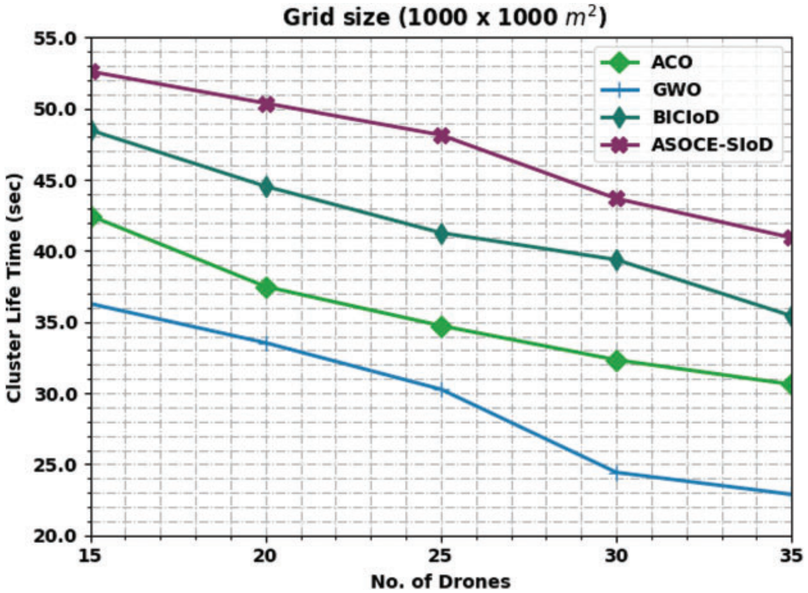

Figure 7: CLT analysis results of ASOCE-SIoD technique under grid size of 1000 × 1000 m

Fig. 8 shows the comparative CLT results attained by the proposed ASOCE-SIoD model with other existing approaches on grid size of 2000 × 2000 m. The figure infers that the proposed ASOCE-SIoD system depicted effectual outcomes with high CLT values under all the cases. For instance, with 15 drones, the proposed ASOCE-SIoD model obtained the maximum CLT of 55.58 s, whereas ACO, GWO, and BICIoD techniques reached low CLT values such as 47.37, 41.90, and 52.84 s correspondingly. Furthermore, with 35 drones, ASOCE-SIoD algorithm attained a high CLT of 44.12 s, whereas ACO, GWO, and BICIoD systems reached low CLT values such as 32.15, 27.02, and 37.79 s correspondingly.

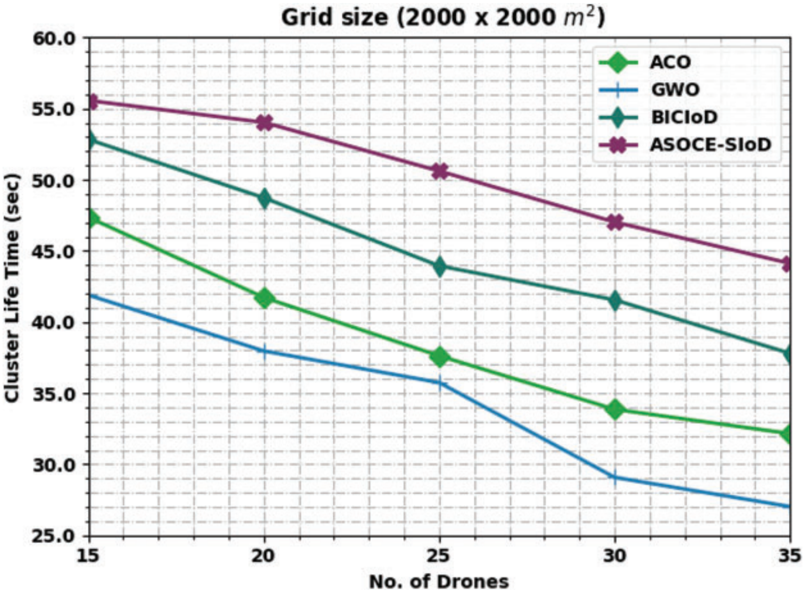

Figure 8: CLT analysis results of ASOCE-SIoD technique under grid size of 2000 × 2000 m

Tab. 4 reports the overall analysis results achieved by the proposed ASOCE-SIoD model under different measures such as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), and Correlation Coefficient (CC). The results indicate that the proposed ASOCE-SIoD model offered low MSE values and high PSNR values and CC on all the images. For instance, with image 1, the proposed ASOCE-SIoD model provided an MSE of 0.071, PSNR of 59.618 dB, and a CC of 99.52. Also, with image 3, ASOCE-SIoD method yielded an MSE of 0.085, PSNR of 58.837 dB, and a CC of 99.49. At the same time, with image 5, the proposed ASOCE-SIoD algorithm offered an MSE of 0.126, PSNR of 57.127 dB, and a CC of 99.77.

Table 4: Results of the analysis of ASOCE-SIoD technique under different measures and images

Test images	MSE	PSNR	CC
Image 1	0.071	59.618	99.52
Image 2	0.102	58.045	99.71
Image 3	0.085	58.837	99.49
Image 4	0.141	56.639	99.72
Image 5	0.126	57.127	99.77

Tab. 5 provides the comparative MSE and PSNR analysis results yielded by the proposed ASOCE-SIoD model. Fig. 9 briefly illustrates the MSE inspection results attained by ASOCE-SIoD model with other models. The results imply that ASOCE-SIoD model achieved less MSE values for all the images. For image 1, ASOCE-SIoD approach resulted in less MSE of 0.071, whereas Share Creation

(SC) scheme with Social Spider Optimization (SSO)-based Optimal Elliptic Curve Cryptography (ECC) called SC-SSOECC, HMOA-ECC, and Particle Swarm Optimization-based ECC (PSO-ECC) approaches gained high MSE values such as 0.094, 0.175, and 0.287 correspondingly. Besides, for image5, ASOCE-SIoD model provided the least MSE of 0.126, whereas SC-SSOECC, HMOA-ECC, and PSO-ECC approaches achieved high MSE values such as 0.177, 0.184, and 0.232 correspondingly.

Table 5: Comparative analysis results of ASOCE-SIoD technique and other existing algorithms with respect to MSE and PSNR

Test images	ASOCE-SIoD		SC-SSOECC		HMOA-ECC		PSO-ECC	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Image 1	0.071	59.618	0.094	58.400	0.175	55.700	0.287	53.552
Image 2	0.102	58.045	0.131	56.958	0.170	55.826	0.225	54.609
Image 3	0.085	58.837	0.095	58.354	0.198	55.164	0.235	54.420
Image 4	0.141	56.639	0.198	55.164	0.204	55.035	0.261	53.964
Image 5	0.126	57.127	0.177	55.651	0.184	55.483	0.232	54.476

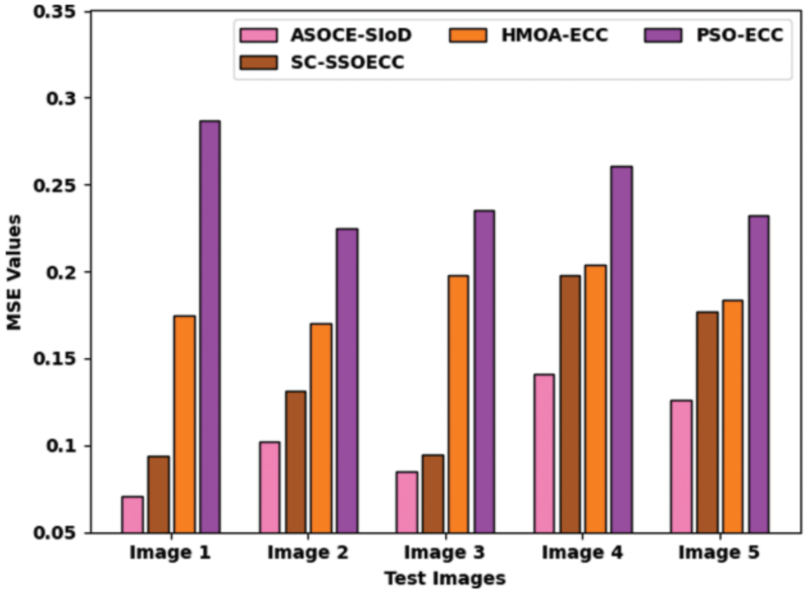

Figure 9: MSE analysis results of ASOCE-SIoD algorithm with recent methodologies

A detailed PSNR analysis was conducted between the proposed ASOCE-SIoD technique and other existing algorithms on distinct images and the results are shown in Fig. 10. The outcomes expose that the proposed ASOCE-SIoD system demonstrated high PSNR values. For image1, ASOCE-SIoD approach gained the maximum PSNR value of 59.618 dB, while SC-SSOECC, HMOA-ECC, and PSO-ECC algorithms reached minimal PSNR values such as 58.400, 55.700, and 53.552 dB respectively. Along with that, for image5, the proposed ASOCE-SIoD approach obtained the maximum PSNR of 57.127 dB, whereas SC-SSOECC, HMOA-ECC, and PSO-ECC algorithms gained the least PSNR values such as 55.651, 55.483, and 54.476 dB correspondingly. Based on the results and discussion made above, it is evident that the proposed ASOCE-SIoD model is superior to ther techniques.

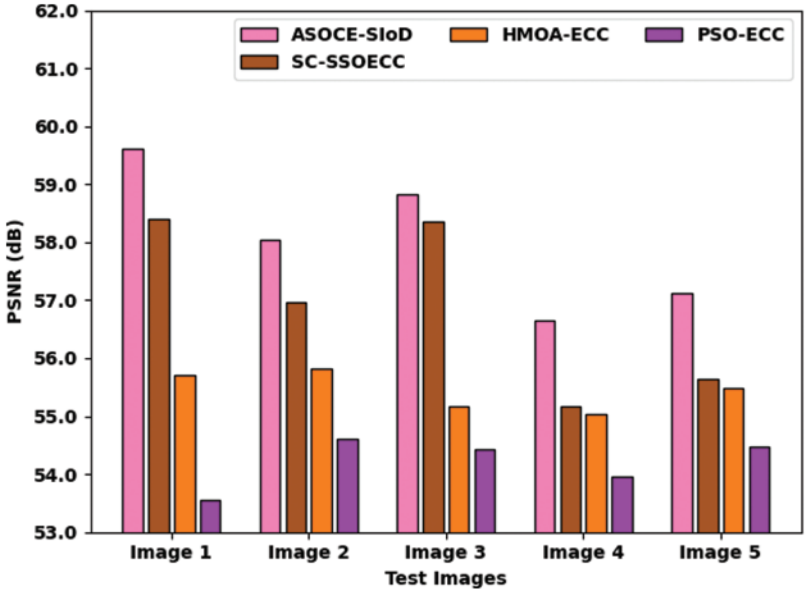

Figure 10: PSNR analysis results of ASOCE-SIoD algorithm with existing algorithms

4 Conclusion

In this study, a novel ASOCE-SIoD approach has been developed to group the drones into clusters and encrypt the images captured by drones. The presented ASOCE-SIoD technique follows ASO-based CH and cluster construction technique. The presented model derives an FF involving multiple parameters especially trust parameters for secure process. In addition, signcryption technique is also applied to effectually encrypt the images captured by drones in IoD environment which enables the secure transmission of images to ground station. In order to validate the better performance of the proposed ASOCE-SIoD model, different experimental analyses were conducted and the outcomes were examined under different aspects. A comprehensive comparison study was conducted and the results highlighted the betterment of ASOCE-SIoD model over recent approaches. In future, lightweight cryptographic solutions can be derived to increase the security levels in IoD environment.

Funding Statement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through Large Groups Project Under Grant Number (46/43). Princess Nourah bint Abdulrahman University Researchers Supporting Project Number (PNURSP2022R238), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: 22UQU4340237DSR25.

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

References

[1] L. Abualigah, A. Diabat, P. Sumari and A. H. Gandomi, "Applications, deployments, and integration of internet of drones (iod): A review," *IEEE Sensors Journal*, vol. 21, no. 22, pp. 25532–25546, 2021.

[2] M. Yahuza, M. Y. I. Idris, I. B. Ahmedy, A. W. A. Wahab, T. Nandy *et al.,* "Internet of drones security and privacy issues: Taxonomy and open challenges," *IEEE Access*, vol. 9, pp. 57243–57270, 2021.

[3] Y. Zhang, D. He, L. Li and B. Chen, "A lightweight authentication and key agreement scheme for internet of drones," *Computer Communications*, vol. 154, pp. 455–464, 2020.

[4] C. Lin, D. He, N. Kumar, K. K. R. Choo, A. Vinel *et al.,* "Security and privacy for the internet of drones: Challenges and solutions," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 64–69, 2018.

[5] Y. Tian, J. Yuan and H. Song, "Efficient privacy-preserving authentication framework for edge-assisted internet of drones," *Journal of Information Security and Applications*, vol. 48, pp. 102354, 2019.

[6] G. Choudhary, V. Sharma, T. Gupta, J. Kim and I. You, "Internet of drones (IoD): Threats, vulnerability, and security perspectives," arXiv preprint arXiv:1808.00203, 2018.

[7] S. A. Chaudhry, K. Yahya, M. Karuppiah, R. Kharel, A. K. Bashir *et al.,* "GCACS-IoD: A certificate based generic access control scheme for internet of drones," *Computer Networks*, vol. 191, pp. 107999, 2021.

[8] F. Aftab, A. Khan and Z. Zhang, "Hybrid self-organized clustering scheme for drone based cognitive internet of things," *IEEE Access*, vol. 7, pp. 56217–56227, 2019.

[9] M. N. A. Mhiqani, R. Ahmad, Z. Z. Abidin, K. H. Abdulkareem, M. A. Mohammed *et al.,* "A new intelligent multilayer framework for insider threat detection," *Computers & Electrical Engineering*, vol. 97, pp. 107597, 2022.

[10] O. A. Alzubi, J. A. Alzubi, K. Shankar and D. Gupta, "Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in internet of things," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 12, 2021.

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

[12] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment," *IEEE Internet Things Journal*, vol. 6, no. 2, pp. 3572–3584, 2019.

[13] F. Aftab, A. Khan and Z. Zhang, "Bio-inspired clustering scheme for internet of drones application in industrial wireless sensor network," *International Journal of Distributed Sensor Networks*, vol. 15, no. 11, pp. 155014771988990, 2019.

[14] A. Saif, K. Dimyati, K. A. Noordin, N. S. M. Shah, S. H. Alsamhi *et al.,* "Distributed clustering for user devices under uav coverage area during disaster recovery," in *2021 IEEE Int. Conf. in Power Engineering Application (ICPEA)*, Malaysia, pp. 143–148, 2021.

[15] F. Alrowais, A. S. Almasoud, R. Marzouk, F. N. Al-Wesabi, A. M. Hilal *et al.,* "Artificial intelligence-based data offloading technique for secure MEC systems," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 2783–2795, 2022.

[16] A. M. Hilal, J. S. Alzahrani, I. Abunadi, N. Nemri, F. N. Al-Wesabi *et al.,* "Intelligent deep learning model for privacy preserving IIoT on 6g environment," *Computers, Materials & Continua*, vol. 72, no. 1, pp. 333–348, 2022.

[17] I. Abunadi, M. M. Althobaiti, F. N. Al-Wesabi, A. M. Hilal, M. Medani *et al.,* "Federated learning with blockchain assisted image classification for clustered uav networks," *Computers, Materials & Continua*, vol. 72, no. 1, pp. 1195–1212, 2022.

[18] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz *et al.,* "Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9097–9111, 2020.

[19] B. Hekimoglu, "Optimal tuning of fractional order pid controller for dc motor speed control via chaotic atom search optimization algorithm," *IEEE Access*, vol. 7, pp. 38100–38114, 2019.

[20] W. Zhao, L. Wang and Z. Zhang, "Atom search optimization and its application to solve a hydrogeologic parameter estimation problem," *Knowledge-Based Systems*, vol. 163, pp. 283–304, 2019.

[21] M. Elhoseny and K. Shankar, "Reliable data transmission model for mobile ad hoc network using signcryption technique," *IEEE Transactions on Reliability*, vol. 69, no. 3, pp. 1077–1086, 2020.