Received: January 1, 2024. Revised: February 24, 2024.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Eco-friendly and Secure Data Center to Detection Compromised Devices Utilizing Swarm Approach

Halah Hasan Mahmoud[1] Marwan Kadhim Mohammed Al-Shammari[1]* Ibtihaal M. Hameed[2] Israa Ibraheem Al_Barazanchi[3]* Ravi Sekhar[4] Pritesh Shah[4] Nitin Solke[4]

[1]*University of Baghdad, Computer Center, 6751, Baghdad, Iraq*
[2]*University of Baghdad, Ibn Sina Center for E-Learning, 6751, Baghdad, Iraq*
[3]*Computer Technology Engineering Department, College of Information Technology, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq*
[4]*Symbiosis Institute of Technology (SIT) Pune Campus, Symbiosis International (Deemed University) (SIU), Pune, 412115, Maharashtra, India*
* Corresponding author's Email: israa.albarazanchi2023@gmail.com

Abstract: Modern civilization increasingly relies on sustainable and eco-friendly data centers as the core hubs of intelligent computing. However, these data centers, while vital, also face heightened vulnerability to hacking due to their role as the convergence points of numerous network connection nodes. Recognizing and addressing this vulnerability, particularly within the confines of green data centers, is a pressing concern. This paper proposes a novel approach to mitigate this threat by leveraging swarm intelligence techniques to detect prospective and hidden compromised devices within the data center environment. The core objective is to ensure sustainable intelligent computing through a colony strategy. The research primarily focusses on the applying sigmoid fish swarm optimization (SiFSO) for early compromised device detection and subsequently alerting other network nodes. Additionally, our data center implements an innovative ant skyscape architecture (ASA) cooling mechanism, departing from traditional, unsustainable cooling strategies that harm the environment. To validate the effectiveness of these approaches, extensive simulations were conducted. The evaluations primarily revolved around the fish colony's ability to detect compromised devices, focusing on source tracing, realistic modelling, and an impressive 98% detection accuracy rate under ASA cooling solution with 0.16 ºC within 1,300 second. Compromised devices pose a substantial risk to green data centers, as attackers could manipulate and disrupt network equipment. Therefore, incorporating cyber enhancements into the green data center concept is imperative to foster more adaptable and efficient smart networks.

Keywords: Eco-friendly data center, Compromised devices, ASA, SiFSO, Cybersecurity.

1. Introduction

The advancement of data center computing has resulted in an increase the need to the green computing and sustainability in a variety of academic and industry societies. Intelligent computing platforms made it possible to connect disparate infrastructures, leading in the technologies such as the Internet-of-Things and the computing everywhere. The sustainable green intelligent computing is becoming increasingly important for practitioners executing long-term objectives [1, 2]. Providing secure execution environments across data centers is one of the important characteristics for attaining full sustainability in computing. Balancing expenses for security, energy, performance, and sustainability is a significant difficulty in creating high-performance secure green intelligent computing. Because computer resources are distributed, network systems are vulnerable to assaults because every device may be targeted and exploited. Furthermore, resource limits and inefficiency concerns in sustainable and green computing might result in systems with limited

memory and processing capability [3, 4]. The limits of wireless communications in the green data center make ensuring security problematic. The sustainable green smart computing platforms connected to the network are more exposed to security attacks than standard computing [5-8]. Regardless of how many security controls are in place, there will always be issues such as software flaws and vulnerabilities that hackers can exploit [9, 10]. The security community emphasizes the need of developing secure software applications, while the number of new vulnerabilities is rising, and long-studied flaws remain [10]. The vulnerabilities in software are break points in the decision-making processes of engineers because they are frequently omitted out of the heuristics that developers apply throughout programming activities [11] Although the software security has developed, there is always opportunity for advancement. Because there are an infinite number of zero-day vulnerabilities and formidable state-sponsored attackers, system and data protection are vital. Software security flaws are frequently caused by minor low-level mistakes, although models, architectures, and tools may assist prevent risks. Software security is sometimes disregarded, although it is critical for any company or organization. An effective approach to addressing sustainability and providing adaptable and scalable services in networked platforms is urgent research in green data center computing applications [12]. However, full monitoring of every device in these platforms is generally not possible in the real world [13]. This limitation is particularly evident in large-scale network platforms [14]. Short-range communications and transmission in these platforms occur in a multi-hop manner, making it difficult to detect and prevent cyber threats from spreading [15]. While current implementations of green intelligent computing platforms rely on observing a few devices and detecting cyberattacks through the data center, full surveillance of all devices would be more efficient [16]. However, achieving full monitoring is challenging due to resource constraints and cost-efficiency issues. By precisely analysing the security condition of monitored devices, system designers and administrators may safeguard them against intrusions in a timely way. Unmonitored devices, on the other hand, provide a concern since their hacked condition may go unnoticed, allowing cyberattacks to propagate across networked systems. This can have serious repercussions [17]. To solve this issue, suitable protocols and frameworks must be in place to protect connected devices from cyberattacks [18], [19]. Device attestation is a promising method that provides dependable assurances for networked devices [20]. Additionally, keeping up-to-date firmware on security equipment is crucial for prevention, but it may be tough without automation or the intervention of a service provider [21]. Scientific communities have tried to participate in finding solutions to the problem of hardware hacking. One of the most prominent of these solutions is the use of the colony approach. For instance, utilize sigmoid-based fish swarm optimization approach to merge comparable communities and discover compromised nodes in the community more accurately. The SiFSO technique may be used in a variety of domains, including biology, chemistry, linguistics, and social sciences, where rapid community recognition in complicated networks is required. The SiFSO technique may be used to identify efficient network communities in complicated networks. The SiFSO technique may be used to improve movement and community detection in complicated networks by applying the sigmoid function for different fish movements in a swarm. The SiFSO method outperformed state-of-the-art particle swarm optimization (PSO) techniques in terms of Q-modularity and normalized mutual information (NMI) [22]. The proposed paper is about solved the difficulties mentioned above. Where the research facing the follows challenges:

1) comprehend how cyber risks (such as malware, viruses, or bugs) move to unmonitored devices on networked platforms.

2) assessing the status of security for unmonitored devices in an eco-friendly data center based on the condition of monitored devices.

The purpose of this study is to secure networked devices in an intelligent eco-friendly data center from cyberattacks in real time, even if the majority of them are not being monitored. We offer a sigmoid fish swarm optimization (SiFSO) based classifier to evaluate the security of unattended devices based-on information acquired from monitored devices, as well as an eco-friendly cooling system employing ant skyscape architecture (ASA).

To detection compromised device, two new technologies have been created.

1) determine the source of cyberattacks by delivering reverse copies of threats originating from hacked monitoring equipment.

2) provide a computational formula of anti-malware propagation in open ports. Which distinguishes between hacked devices.

We mimic the propagation of cyber threats in networks and then collect data from the monitored devices for analysis. We compare SiFSO to three state-of-the-art algorithms and ASA to four.

To detect the hacked device, we propose a unique

Table 1. A notation list for variables in proposed equations

Variables	Description
A	the maximum value of curve
z	the real number in between -ꝏ and + ꝏ
F(t)	time and current position for each fish
t	current position period time
t+1	next move of position
e	the natural algorithm
F_{center}	swarm central position
F_n	number of swarm nodes
s	the total no. of edges connected to cluster of s
η_{ijk} (t)	pheromone intensity of k-type ASA
τ_{ijk} (t)	heuristic value of k-type ASA
P_{ijk} (t)	probability
$Suit_{ijk}$	suitability of cooling for cell(i, j)
Suitxk	suitability of all cells belonging to study area
G	total number of cells in study area
γ, θ	parameters were adjusted to 0.75 and 1.25, respectively, to determine the relative impact of pheromone density vs heuristic information.
α, β	weights for suitability and LST
F_{center}	swarm central position
F_n	number of swarm nodes
l_s	total number of connected devices in the cluster of s vertices linked to the green datacenter.
S	vertices
ds	summation of all node degrees in “s”.
M	the total number of connected devices in the chosen network.
T_s	temperature of the radiating surface (in Kelvin)
T_b	the temperature of the dark body (in Kelvin)
λ	wavelength of radiance emitted
a	“h c /k” where “h” stands for Planck’s constant, “c” stands for the velocity of light, and “k” stands for Boltzmann’s constant
ε	surface emissivity

source-based categorization, and. Extensive trials have demonstrated the usefulness and strength of our method.

The following is the paper’s structure. Section 2 describes past research, whereas Section 3 evaluates performance and justifies approach. Section 4 contains an analysis and discussion of the findings. Finally, section 5 concludes the paper. Table 1 shows the variables in equations.

2. Prior studies

The literature proposes an eco-friendly and protected data center that uses a swarm technique to identify compromised devices. The system uses swarm authentication, as another type of attestation, to check the cybersecurity states of several devices in a vast network simultaneously [23, 24]. The suggested approach tries to decrease duplication while also addressing issues such as verify the Denial of Service (DoS), and malware [25]. A learning-based autonomous swarm attestation protocol is also being developed to identify suspicious mobiles utilize a neural network architecture. The system also uses feature selection techniques and ensemble classifiers to improve attacks in an Internet - of - things Cyber-Physical System [26]. Furthermore, secure aggregation employing blockchain technologies and completely homomorphic encryption are used to safeguard data privacy in cooperative training settings. These methods have demonstrated encouraging results of accuracy rate, privacy preservation, and resilience to different assaults. Some studies Identified infected mobiles devices utilizing graph inference, which follows the Guilt-by-Association concept [27]. Another research, focused on achieving security against fraud attacks in wireless sensor networks (WSN), uses a swarm intelligence algorithm to adapt to network topology and ant transmission based on random selection [28]. Other authors implemented the accurate grading normalization (GN) approach to a swarm-based deep learning (DL) classifier to create a smart intrusion detection system for various clouds. It is an opposite-inspired enhancement of opposition-based learning (OBL-RIO) for feature selection [29]. The Sailfish Optimization Algorithm (SOA) has been suggested as a method to identify malicious data injection attacks in various another research [30]. Some studies employed semantic analysis for event correlations, extracting features and building feature vectors, to evaluate the security of IoT devices in smart cities [31]. Data transmission in data centers can be dramatically impacted by spoofing and jamming attacks. In the face of jamming, packet size and

redundancy are adjusted to facilitate datagram recovery with minimal resending throughout the network [32]. Furthermore, in some communication tasks, the Ahlswede/Dueck identification approach has been shown to be better efficient than Shannon's transmission strategy, particularly when jamming assaults are present [33]. The Ahlswede and Dueck identification hypothesis boosts channel capacity by modifying the recipient's aim, resulting in benefits in secure data transfer [34]. Furthermore, in a wireless network system, a technique for transmitting/receiving data comprises waiting for an acknowledgement signal from the reception node through a different channel, which can assist limit the impact of spoofing and jamming assaults [32]. Overall, previous research emphasizes the need of considering the recipient's goals and creating robust and secure data centers to prevent the effects of spoofing and jamming attacks on data transmission in data centers.

Green cloud computing tries to address data center's excessive energy use and environmental impact. [35]. Integrating energy-efficient cooling, processing, storage, and transport systems inside the data center environment is required. Several approaches to achieve this goal have been proposed. One approach is to develop energy-efficient scheduling models for data centers and train them with deep neural networks based on artificial intelligence [36]. Another strategy focuses on balancing service quality and energy savings by measuring service quality and estimating the computing resources required based on workload changes [37]. Furthermore, green energy sources, such as renewable energy, have been examined for directly powering servers or virtual machines in data centers [38]. These methods aim to minimize energy consumption, save money, and provide proper resource control in cloud computing centers.

Cloud computing has become more sustainable and intelligent as low-power resources and intelligent devices are used in networks to prevent negative transmission and distribution repercussions. Furthermore, combining Mobile cloud computing (MCC) with the Green Smart Grid (GSG) provides trustworthy energy management as well as cost-effective data sharing between end-users and service providers [39]. Furthermore, the use of cloud computing technologies such as HDFS, MapReduce, and H-base in a smart distribution network cloud platform enables for the rapid storage and processing of power data while also ensuring data security and integrity [40]. These advancements in cloud computing contribute to the overall sustainability and efficiency of the electrical grid.

However, there are still obstacles to be solved. When a data center become smart, it may become more vulnerable to cyber-attacks. Among the issues is the necessity to combine, the sustainability and security requirements. Identifying propagation sources when threats emerge in green data centers is critical from both a practical and technological standpoint. In terms of malicious applications spreading, for instance, recognizing malicious applications sources can correctly penalize hackers. Locating the origins of a mobile devices vulnerable is helpful in identifying network vulnerabilities.

There are several state-of-the-art algorithms are compared with the suggested SiFSO technique to detect compromised devices. There are studies used adaptive particle swarm optimization (APSO) to improve exploration and exploitation capabilities [41], mult-objective genetics algorithm (MOGA) that achieved accuracy with minimum redundancy [42], and graph base optimization method (GOM) which can deal with a huge amount of nodes [43]. From the other side there are also state-of-the-art algorithms compared with the suggested Ants Skyscape Architecture (ASA) to cooling green data center. Some of these algorithms are, partial swarm optimization (PSO) [44], firefly colony optimization (FCO) [45], bee colony optimization (BCO) [46], and cuckoo swarm optimization (CSO) [47].

Compared with our suggestion, certain types of assaults in wireless sensor networks are difficult to safeguard, including verifier-impersonation DoS attacks, dynamic networks, malware, and TOCTOU attacks. Aside from the issues posed by the broadcast nature of wireless communication and the weak links between hacked devices and their apps. Difficulty in automatically downloading and installing programs without user interaction. In addition, noisy data for instance for example, user activity, might have an impact on the approaches' performance. In addition, noisy data might cause false detection alerts.

3. Preliminary

3.1 Proposed system

The essential components of an Eco-Friendly and Secure Green Data Center are depicted in Fig. 1:

- Eco-friendly cooling systems: These systems use ASA to cool the data center using natural resources, which can help to reduce energy use and environmental impact.
- Renewable energy sources, such as solar cells, can help to further minimize the data center's reliance on fossil fuels and its carbon impact.
- Sustainable building materials: These materials

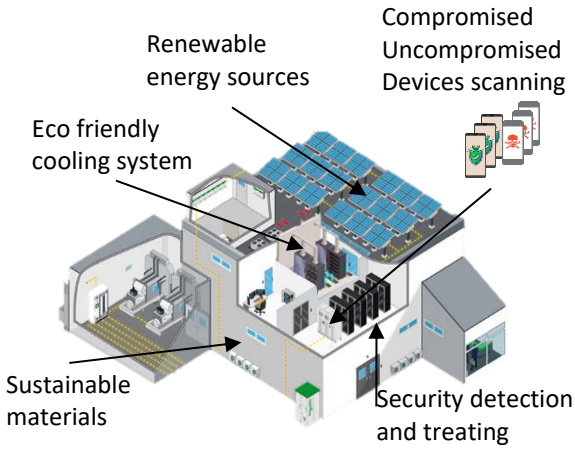

Figure. 1 Eco-Friendly and Secure Green Data Center proposed system

are made from recycled or renewable materials and help to reduce the data center's environmental impact.

- Security detection and treating: SiFSO-based security mechanisms protect the data center from hacked devices.

The suggested solution illustrates how these components work together to produce a secured and long-lasting data center environment. The adoption of sustainable building materials helps to reduce the data center's environmental impact. Furthermore, the security procedures help to protect the data center against compromised equipment.

3.1.1 Proposed network scheme

The proposed algorithm to detect compromised packet traffic caused by mobile devices malwares utilizing SWARM algorithms is the Sigmoid Fish Swarm Optimization (SiFSO). Meanwhile SAS approach used to achieve the eco-friendly cooling approach. The suggested green data center block diagram, as shown in Fig. 2, is a "Permit or Deny mobile devices" that is meant to regulate access to a resource depending on criteria or permissions. The diagram has three major layers:

1. Network layer: Which indicated the mobile devices that were connected to the green data center that requires access control and protect.
2. Eco-friendly data center layer: the layer responsible to achieve sustainable and eco-friendly data center.
3. SiFSO detect compromised devices layer: which is responsible to managing permissions and implementing access control policies. It accepts requests for resource access and decides whether to permit or deny access based on the SiFSO policy. Access control policy specifies the rules and criteria for permitting or denying resource access. It states who has access to the resource and under what conditions the SiFSO approach applies.

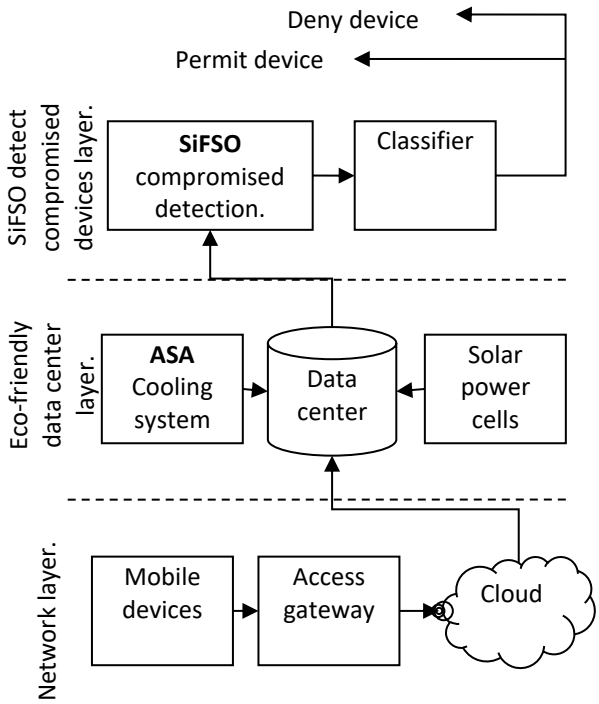

Figure. 2 Eco-Friendly and Secure Data Center to Detection Compromised Devices architecture

The diagram also depicts the information flow between the components, with access requests being given to the permit manager, who then checks the access control policy to make a decision.

3.1.2 SiFSO for efficient compromised device detection

The study employed Sigmoid Fish Swarm Optimization (SiFSO) as the best method for detecting compromised devices in a green database center. SiFSO's goal is to enhance fish movement patterns (represented by mobile devices in this article) in order to provide more accurate network community detection. The approach consists of two phases: initialization and fish movement, with a linear time complexity of O (n×m), where n is the network population size, and m are the number of repetitions. The sigmoid function is defined as a nonlinear mathematical technique for smoothing turns in fish movement patterns, with the goal of ultimately improving cluster quality within the network [48]. The method mathematical procedure is as follows:

1. Sigmoid function mathematically can represent in Eq. (1).
2. Density. The number of mobile devices within the visual range is represented by density. (The

density value ranges from 0 to 1, with 1 denotes high density while 0 denotes low density. Eq. (2) describes the density numerically.

3. When fish reach a point where they can no longer locate food, they migrate aimlessly in any direction. Meanwhile, when the fish approaches the nearby boundary in the SiFSO method for optimizing the swarm of fake fish represented by mobile devices searching for compromised devices via centralized datacenter, it takes any estimated route using the sigmoid function. Mathematical formula can be calculated by Eq. (3).
4. The next movement of colony elements is depending on the search for the compromised device. Each device initially che
5. cks its own coverage space and then relies on neighbouring devices within the network. The compromised device is determined based on packet density data, as shown in Eqs. (4) and (5).
6. One of the characteristics of the proposed theory is to move in groups as a coherent swarm where it helps the swarm to reach the compromised devices quickly and accurately. Eq. (6) shows a concentrated calculation, while Eq. (7) shows the search for compromised devices.
7. When a datacenter detects compromised activity during the movement of a swarm of mobile devices, it directs attention to the compromised activity. In this case, some neighbouring devices get more information about accurately locating the compromised device. This process is called the movement tracking process, where the datacenter continues to check all devices in the area covered for better identification of the location of the security breach, as shown in Eq. (8).

The suggested SiFSO algorithm movements to detect compromised devices is shown in Algorithm 1 and Fig. 3.

$$Sigmoid(z) = \frac{A}{1+ e^{-z}} \quad (1)$$

$$Density = \frac{mobile\ devices\ in\ visual\ range}{total\ number\ of\ mobile\ devices} \quad (2)$$

$$F(t+1) = F(t) + step \times sigmoid(-1,1) \quad (3)$$

$$F_i = F_i + visual \times rand\ (-1,1) \quad (4)$$

$$F_i\,(t+1) = F_i\,(t) + \left[\frac{F_j - F_i(t)}{distance(i,j)}\right] \times step \times sigmoid \quad (5)$$

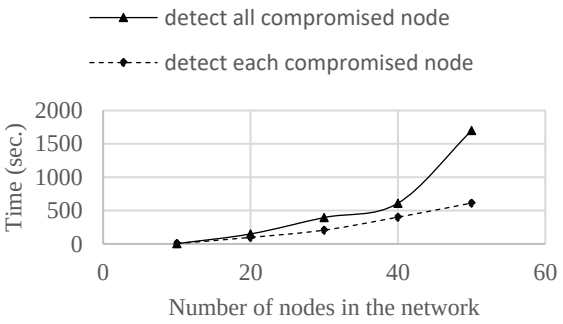

Figure. 3 Average time to Detection Compromised nodes

$$F_{center} = \frac{1}{N}\sum_{i=0}^{N} F_i \quad (6)$$

$$F_i\,(t+1) = F_i\,(t) + \frac{F_{center} - F_i(t)}{distance(i,center)} \times step \times sigmoid(0,1) \quad (7)$$

$$F_i\,(t+1) = F_i\,(t) + \frac{F_n - F_i(t)}{distance(i,n)} \times step \times sigmoid(0,1) \quad (8)$$

Algorithm 1. SiFSO algorithm to detect compromised activity

Mobile device movement:
Method: Sigmoid Fish Swarm Optimization (SiFSO)
Input: Mobile device coordinates, Try number, Factor, Step, Step decrease, Minimum step, Pixels Iteration number, Visual range, Minimum visual range, visual decrease
Output: Each solution represents a network division.
1. Start the algorithm.
2. The normalization of minimum and maximum.
3. Initialization of label propagation.
4. For iteration no. ← 1 iteration do.
5. For device no. ← 1 device do.
6. Current device neighbour ←0.
7. Device neighbour ←device in coverage area.
8. If neighbour == Zero
9. Move to the next ← the first sigmoid.
movement.
10. Break and go to the step - 1.
11. Else loop
12. If density > compromised activity.

13. Move to next ← the prey sigmoid. movement.
14. Else loop
15. Move to the next ← the random swarm movement.
16. End if condition.
17. End for loop.
18. End for loop.
19. The Final result → apply modularity.
20. End algorithm.

3.1.3 SiFSO green datacenter implementation

The suggested SiFSO method is applied and simulated in OMNET++ Ver. 2022 on an Intel-Corei7 CPU with speed of clock equal 2.67 GHz and RAM with 8GB size. To execute preprocessing processes such as data normalization, C++ and NED have been used. Table 2 displays the Simulation Parameters. The suggested algorithm's performance is assessed using two fitness functions: normalized mutual information (NMI), and Q-modularity. The suggested SiFSO technique is compared to multi-objective genetic algorithm (MOGA), and graph base optimization method (GOM), adaptive particle swarm optimization (APSO), which all represents state-of-art algorithms. Both fitness activities evaluate the accuracy and efficiency of clusters generated by complicated network community identification approaches. The accuracy of cherished discovered communities is evaluated by Q-modularity. Modularity may be calculated by subtracting the expected or estimated nodes from the fraction of edge nodes in the cluster or community. In contrast, nodes near the network's edges move at random, independent of group structure. The modularity Q is defined by Eq. (9). The (s) indicates all network nodes, while the (m) indicates the total number of network edges. The proposed method computes the similarities issue between the real network and the discovered network by the proposed strategy using normalized mutual information (NMI). The same network is divided into two halves, (A) and (B), identified using two different approaches. Partition (A) include (R) communities and partition (B) contain (D) communities. The entry (C_{ij}) indicates the number of nodes in both communities, the confusion matrix (C) is defined. The normalized mutual information between (A) and (B) is defined mathematically as in Eq. (10).

$$Q = \sum_{s=1}^{k}\left[\frac{ls}{m} - \left(\frac{ds}{2m}\right)^2\right] \quad (9)$$

Table 2. The experimental parameters and setup for the proposed system

Input	Values
Coverage area range	1000 pixels
Decrease value	10 pixels
Minimum range	50.0
Pixel's iteration number	60.0
Step per Node	20 pixels
Step decrease	0.5 pixels
The minimum steps number	3 pixels
The number of trying per behaviour	3 trying
The factor of crowd for swarm	0.8 cons.
Mobile device coordinates	x, and y
The Iterations number	60 iterations
The number of mobile devices	200

$$NMI(A,B) = \frac{-2\sum_{i=1}^{R}\sum_{j=1}^{D} C_{ij}\log(C_{ij}N/C_iC_j)}{\sum_{i=1}^{R} C_i\log(C_i/N) + \sum_{j=1}^{D} C_j\log(C_j/N)} \quad (10)$$

$$\eta_{ijk} = \frac{Suit_{ijk}}{\sum_x Suit_{ijk}} \quad (11)$$

$$\tau_{ijk}(t=0) = \frac{1}{G} \quad (12)$$

$$P_{ijk}(t) = \frac{[\tau_{ijk}(t)]^{\gamma}[\eta_{ijk}(t)]^{\theta}}{\sum_{type\epsilon k}[\tau_{ijk}(t)]^{\gamma}[\eta_{ijk}(t)]^{\theta}} \quad (13)$$

$$cv(t) = \alpha \times \left(std_{suit}(t) - std_{suit}(t-1)\right) + \beta \times \left(std_{suit}(t) - std_{suit}(t-1)\right) \quad (14)$$

$$\tau_{ijk}(t+1) = \tau_{ijk}(t)(1-\rho) + \Delta\tau_{ijk}(t) \quad (15)$$

$$\Delta\tau_{ijk}(t) = r.\tau_{ijk}(0) = \frac{\tau}{G} \quad (16)$$

$$Q = \sum_{s=1}^{k}\left[\frac{ls}{m} - \left(\frac{ds}{2m}\right)^2\right] \quad (17)$$

$$NMI(A,B) = \frac{-2\sum_{i=1}^{R}\sum_{j=1}^{D} C_{ij}\log\left(\frac{C_{ij}N}{C_iC_j}\right)}{\sum_{i=1}^{R} C_i\log\left(\frac{C_i}{N}\right) + \sum_{j=1}^{R} C_j\log\left(\frac{C_j}{N}\right)} \quad (18)$$

3.1.4 ASA

Python 3.9 has been used to implement and process the ASA technique to control on the temperature of green data center as a sustainable approach. Algorithm 2 illustrate the ASA procedure to achieve a sustainable green data center temperature cooling solution.

Algorithm 2. ASA procedure to achieve a sustainable green data center temperature cooling system

Green data center cooling:
Method: Ants Skyscape Architecture (ASA)
Input: Random pixel (i, j) cooling region
Output: the suitable structure using pixel (i, j), *n* pheromone intensities
1. Start the algorithm.
2. By using Eqs. (11) and (12), calculate the initial heuristic values and pheromone intensities.
3. By using Eq. (13), calculate the selection probabilities.
4. Determine the suitable *k* at pixel (i, j).
5. Determine whether selected *k* at pixel (i, j) is suitable, by using Eq. (14).
6. Enhance the intensity of the pheromone using Eqs. (15) and (16).
7. Update and synchronous the remaining of pheromone at pixel (i, j).
8. End algorithm.

3.2 Benchmark

3.2.1 SiFSO benchmark

The suggested algorithm's performance can be evaluated using two fitness functions: normalized mutual information (NMI) and Q-modularity. The suggested SiFSO technique is compared to state-of-art algorithms such as adaptive particle swarm optimization (APSO), mult-objective genetics algorithm (MOGA), and graph base optimization method (GOM). Both fitness functions evaluate the efficiency and accuracy of clusters generated by complicated network community identification approaches. The accuracy of discovered compromised communities is evaluated by Q-modularity. Modularity may be defined quantitatively as the fraction of devices that belong to a cluster or community minus the expected or estimated value of the compromised devices. In contrast, the devices of a network move at random, regardless of the group structure. Eq. (17) shows how to define modularity Q. The proposed approach evaluates the similarities between the participating nodes and the observed compromised devices using normalized mutual information (NMI). Examining two different partitions (A, and B), with same network identified using two different techniques. Partition A should have R communities, whereas partition B should contain D communities. The confusion matrix C is defined when the item Cij denotes the number of nodes in both communities. The normalized mutual information between A, and B is determined mathematically as illustrated in Eq. (18) [48].

3.2.2 ASA benchmark

The usage of ant skyscrapers to manage temperature and thermal radiation will cause changes in the green database's emission. At the same time, the computation of Surface Temperature (ST) for the green data center is primarily connected to a, λ, ε, and b factors, and the emission of the data center's surface is computed directly using Eq. (19) which conducted to calculate ST [49].

$$T_s = \frac{T_b}{1+(\frac{\lambda \times T_b}{a})ln\varepsilon} \quad (19)$$

4. Results and discussion

4.1 Compromised devices detection

Mobile devices are vulnerable in two different ways: directly and indirectly. When devices are hacked during the logistics activities or by insiders, the direct approach is used to directly alter the configuration of the devices or the programs that run on them. In this situation, the attackers target the devices directly, without the use of any intermediate devices. However, indirect procedures are more commonly used and frequently need immediate access to the computing software that runs the network's devices. Once the attacker gains access to those mobile devices, he or she has the ability to modify the settings and behavior of the edge devices. If a device has a vulnerability is a weakness installed on it, we consider it compromised. A malfunctioning hardware or software element might be to blame for the dangerous function. Furthermore, it is expected that the malicious code would modify the device's essential operation. In general, this feature can be added before, during, or after the device's manufacturing process. List1 depicts realistic cases of a hacked device caused by code injection. The malicious functions in this example seek to:

1. diminish the device's resources.
2. Save vital information in a file that will be transmitted to attackers later.

List 1. The outcome of malicious codes being injected into a vulnerable device

```
Void mem()
{
    rand(time())
    long size = rand()%21474
    malloc(size)
}
```

```
Void save_then_send(GoSubscriber subscriber)
{
    File *f = fopen("/root/data.dat",'a')
    Fprintf(f,'%' PRlu64 '\n',
    GoSubscriber_getCriticalValue(subscriber))
}
```

Normal device	Compromised device
1. Path_read_detach	**1.** Path_read_detach
2. Malloc	**2.** Malloc
3. Malloc	**3.** Malloc
4. Free	**4.** Malloc
5. Free	**5.** Malloc
6. Signal	**6.** Open
7. Malloc	**7.** Fre
8. Malloc	**8.** Free
9. Free	**9.** Signal
10. Free	**10.** Malloc
11...	**11.** Malloc
12...	**12.** Malloc
13...	**13.** Malloc
14...	**14.** Open
15...	**15.** Free
16...	**16.** Free

4.1.1 Compromised nodes simulation and analysis

In the simulations, the number of nodes in the network was increased but the proportion of identifying compromised nodes that penetrated the network remained constant. Fig. 3 depicts the time required to detect the hacked nodes as well as the average time required to detect each compromised node in the network. When a node becomes compromised, the time it takes the green data center to notify the remaining nodes of its existence is recorded and averaged for each set of simulated runs. Fig. 3 depicts the average time required to locate all infected nodes after their introduction into the network. All compromised nodes are inserted at the same time throughout these simulations. The average time elapsed for each simulation from the first compromised node to the last compromised node is indicated. The sample mean's 95% percent confidence interval was determined, and a difference was detected for each network size. The biggest intervals were seen for the 50 node networks in terms of the time it took to discover each compromised node, which was 612 +/-98, and for all compromised nodes, which was 1700 +/- 150. By increasing the number of runs for each network size from 20 to 40, the gap around the mean becomes narrower. This is accurate for all of the statistics shown in figure below.

When looking at this data, it is important to remember that 13% of the network's nodes were hacked. This indicates that the (10) nodes network will have one compromised node, but the (50) node network would have five. Because the green data center must handle all ALERT signals, the time required to detect the new nodes is longer in bigger networks. This is due to the increased number of packets propagating over the network, which results in a higher number of lost packets. The green data center's alert message buffer helps to reduce the amount of ALERT notifications that are ignored. A green data center with superior computational capacity would have reduced the time required to discover the affected nodes. Also, keep in mind that each network size has only one green data center. In a bigger wireless sensor network, it is likely to take longer to discover hacked nodes.

4.1.2 The comparison of proposed secure scheme

Efficient compromised device identification in a complex network is a fascinating problem due to its numerous applicability in various security fields. There are numerous techniques available for detecting network infected devices. We presented the sigmoid fish swarm optimization (SiFSO) method in this study to detect infected devices. In terms of two fitness factors, Q-modularity and normalized mutual information, the proposed SiFSO method outperforms other well-known swarm optimization algorithms, MOGA, APSO, and GOM (NMI). It has been observed that the performance of SiFSO has improved as a result of the addition of a sigmoid function to determine fish movement, where fish represents a mobile device or node. This section summarizes the findings of the performance assessment trials we did use SiFSO, as well as their comparison to the performance of other optimization algorithms. We experimented with a network of 10-50 nodes connected by a green data center. Fig. 4 depicts the existing nodes in this network. The findings reveal that the network built using SiFSO outperforms the other techniques in considerations of performance parameters and detecting compromised nodes. The mutual information value normalized

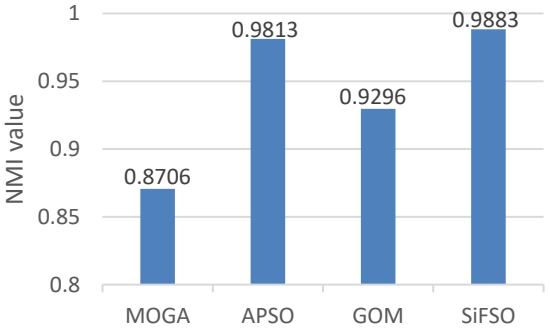

Figure. 4 Normalized mutual information (NMI) for selected optimization algorithms

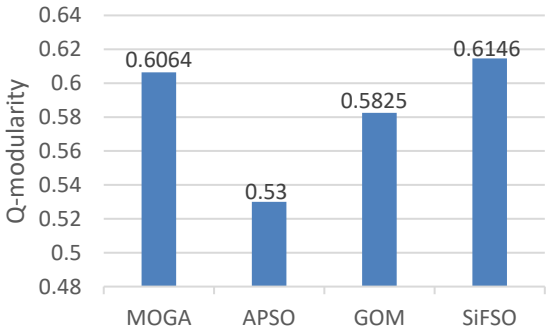

Figure. 5 Q-modularity for selected optimization algorithms

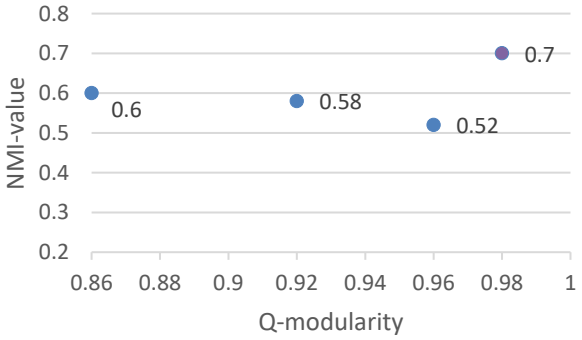

Figure. 6 Q-modularity and MNI for selected optimization algorithms

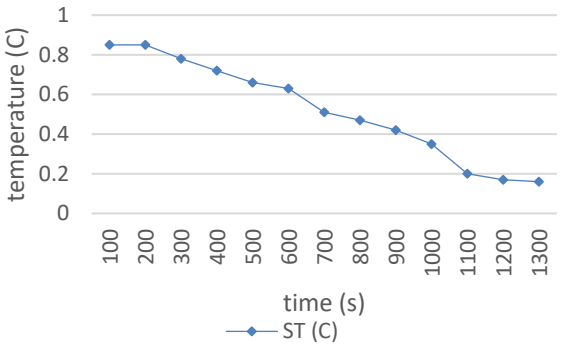

Figure. 7 Temperature per time ASA optimization results for green data center

attained by MOGA, APSO, and GOM on a particular green data center is 0.8706, 0.9813, and 0.9296, respectively, based on the fitness function findings. In comparison, the compromised nodes discovered by the proposed SiFSO technique had a mutual information value normalized of 0.9883. Despite the fact that the NMI value recommended by SiFSO optimization approaches is near to the APSO, it is still the highest NMI value produced by SiFSO optimization techniques. Fig. 4 depicts the NMI value findings of the chosen methods. Similarly, the Q-modularity attained by MOGA, APSO, and GOM on a particular green data center is 0.6064, 0.53, and 0.5825, respectively, based on the outcomes of the specified fitness functions. The compromised nodes discovered by the recommended SiFSO approach, on the other hand, achieved the highest Q-modularity of all available optimization strategies, as shown in Fig. 5. Fig. 6 depicts NMI and Q-modularity data in a 2D scattered plot. Similarly, with one exception, the compromised nodes detected by the proposed SiFSO approach are quite near to the original values. In contrast, compromised nodes recognized by other optimization techniques have an excessive number of mismatch nodes in each cluster.

4.2 ASA optimization technique applicability

The influence of ASA optimization may be seen in the ability to develop an optimum solution that meets the sustainability standards for temperature management in green data centers. Fig. 7 depicts the outcomes after 50 iterations of ASA tuning. As each category was randomly dispersed at the start of the iteration, the suitable and stable ST for green data center arrived after “1300 seconds” to be steady state condition at temperature “0.16 ºC” The eco-friendly has been chosen and designed in order to reduce the appropriateness disparity. The discrepancy between the modified temperature and the optimum temperature is likely to grow as a result of the excessive cooling, breaking the ASA optimization condition.

4.2.1 The comparison of proposed cooling scheme

To contrast the techniques of Ants Skyscape Architecture (ASA), partial swarm optimization (PSO), firefly colony optimization (FCO), bee colony optimization (BCO), and cuckoo swarm optimization (CSO). Swarm algorithms are utilized to design an eco-friendly cooling system in order to prevent temperature consumption. Table 3 compares the cooling performance and computing time of several optimization strategies for an environmentally friendly cooling system. ASA had the best cooling performance, with a result of 0.16 ºC and a computation time of 1,300 seconds. FCO had the highest cooling result (0.65 ºC), but also the longest

Table 3. Comparison of proposed ASA optimization method cooling results with other similar state-of-art methods

Algorithm	Cooling(ºC)	Time(s)
ASA	0.16	1,300
PSO	0.55	1,526
FCO	0.65	13,025
BCO	0.38	10,023
CSO	0.25	12,021

computing time (13,025 s), suggesting inferior speed efficiency. According to the comparison, ASA and CSO are more efficient in achieving cooling with appropriate computing durations, but FCO, although delivering greater cooling, takes a longer computational time. The algorithm chosen may be determined by the cooling system's unique requirements, considering both cooling efficacy and computing efficiency.

5. Conclusions

Efficient compromised device identification in a green data center is a fascinating topic due to its numerous applicability in many current fields. There are numerous techniques available for detecting network compromise. In the suggested study, we introduced the sigmoid fish swarm optimization (SiFSO) approach for detecting compromised devices and ant skyscape architecture (ASA) as an eco-friendly cooling solution. Under the banner of sustainability, we added the simulation and evident for improved compromised device identification in both algorithms. The proposed SiFSO approach is assessed and compared to three well-known swarm optimization methods, MOGA, APSO, and GOM, in terms of two fitness factors, namely, Q-modularity and normalized mutual information (NMI). Where SiFSO algorithm shows the highest detection for compromised devices with Q-modularity 61.4% and NMI 98.8% in the network content from 10 to 50 connected nodes. In contrast, the performance of the ant skyscape architecture (ASA) approach in terms of temperature and cooling time is explored and compared to that of other well-known swarm optimization methods, FSO, PSO, BSO, and CSO. Where the temperature stabilized on 16% After 1300 seconds in 50 connected nodes under a sustainable environment which is good value compared with other theories. The findings demonstrated that the suggested SiFSO algorithm outperformed the other methods Both in terms of NMI and Q-modularity. Furthermore, the suggested ASA algorithm is extremely near to the original cooling system temperature with the added benefit of sustainability.

Funding Statement

The authors received no funding for the proposed study.

Availability of Data and Materials

The data used to support the conclusions of this investigation are accessible upon request from the corresponding author.

Conflicts of Interest

The authors declare no conflicts of interest.

Author Contributions

Conceptualization by Marwan Kadhim Mohammed Al-Shammari, Halah Hasan Mahmoud and Btihaal M. Hameed, methodology by Btihaal M. Hameed, Ravi Sekhar, Pritesh Shah, and Nitin Solke; software and validation by Halah Hasan Mahmoud; formal analysis by Marwan Kadhim Mohammed Al-Shammari; investigation by Israa Ibraheem Al Barazanchi; resources and data curation by Btihaal M. Hameed Ravi Sekhar, Pritesh Shah, and Nitin Solke.

References

[1] S. Obaid, N. Bawany, H. binte Tariq, A. Tahir, and N. Komal, "Recent Trends in Green Computing", In: Proc. of *Innovations in Smart Cities Applications Volume 4: The Proceedings of the 5th International Conference on Smart City Applications*, Springer, pp. 1071-1083, 2021.

[2] X. Zhang, G. Liu, M. Qiu, W. Xiang, and T. Huang, "Cloud Computing, Smart Grid, and Innovative Frontiers", In: *Proc. of Telecommunications: 9th EAI International Conference, CloudComp 2019, and 4th EAI International Conference*, SmartGIFT 2019, Beijing, China, December 4-5, 2019, and December 21-22, 2019, Springer Nature, Vol. 322. 2020.

[3] A. K. Jones, "Green computing: new challenges and opportunities", In: *Proc. of the on Great Lakes Symposium on VLSI 2017*, pp. 3-3, 2017.

[4] B. Herzog, T. Hönig, W. Schröder-Preikschat, M. Plauth, S. Köhler, and A. Polze, "Bridging the gap: Energy-efficient execution of software workloads on heterogeneous hardware components", In: *Proc. of the Tenth ACM International Conference on Future Energy Systems*, pp. 428-430, 2019.

[5] B. B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols", *Concurrency and Computation: Practice and Experience*, Vol. 32, No. 21, pp. e4946, 2020.

[6] N. N. Thilakarathne, M. K. Kagita, and W. M. Priyashan, "Green Internet of Things for a better world", *arXiv preprint arXiv:2012.01325*, 2020.

[7] T. Nazir and M. T. Banday, "Green Internet of Things: A survey of enabling techniques", In: *Proc. of 2018 International Conference on Automation and Computational Engineering (ICACE)*, pp. 197-202, 2018.

[8] S. Sen, J. Koo, and S. Bagchi, "TRIFECTA: security, energy efficiency, and communication capacity comparison for wireless IoT devices", *IEEE Internet Computing*, Vol. 22, No. 1, pp. 74-81, 2018.

[9] S. A. Shawkat, B. A. Tuama, and I. Al Barazanchi, "Proposed system for data security in distributed computing in using triple data encryption standard and Rivest Shamir Adlemen", *Int. J. Electr. Comput. Eng.*, Vol. 12, No. 6, pp. 6496–6505, 2022, doi: 10.11591/ijece.v12i6.pp6496-6505.

[10] M. Abadi, "Software Security: A Formal Perspective: (Notes for a Talk)", In: *Proc. of International Symposium on Formal Methods*, pp. 1-5, 2012.

[11] J. Sametinger, "Software Security", In: *Proc. of 2013 20th IEEE International Conference and Workshops on Engineering of Computer Based Systems (ECBS)*, pp. 216-216, 2013.

[12] S. El Kafhali, I. El Mir, and M. Hanini, "Security threats, defense mechanisms, challenges, and future directions in cloud computing", *Archives of Computational Methods in Engineering*, Vol. 29, No. 1, pp. 223-246, 2022.

[13] A. I. Tahirkheli, M. Shiraz, B. Hayat, M. Idrees, A. Sajid, U. Rahat, A. Nasir, K. Ki-Il, "A survey on modern cloud computing security over smart city networks: Threats, vulnerabilities, consequences, countermeasures, and challenges", *Electronics*, Vol. 10, No. 15, pp. 1811, 2021.

[14] D. Wang, T. Wu, S. Wen, X. Chen, Y. Xiang, and W. Zhou, "STC: exposing hidden compromised devices in networked sustainable green smart computing platforms by partial observation", *IEEE Transactions on Sustainable Computing*, Vol. 4, No. 2, pp. 178-190, 2017.

[15] A. Gadre, "PhD Forum Abstract: Low-Power Wide-Area Networks: Connect, Sense and Secure", In: *Proc. of 2020 19th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, IEEE, pp. 377-378, 2020.

[16] Y. Chen, H. Hu, and G. Cheng, "Design and implementation of a novel enterprise network defense system bymaneuveringmulti-dimensional network properties", *Frontiers of Information Technology and Electronic Engineering*, Vol. 20, No. 2, pp. 238-252, 2019.

[17] S. Manson and D. Anderson, "Cybersecurity for protection and control systems: An overview of proven design solutions", *IEEE Industry Applications Magazine*, Vol. 25, No. 4, pp. 14-23, 2019.

[18] C. Ye, P. P. Indra, and D. Aspinall, "Retrofitting security and privacy measures to smart home devices", In: Proc. of *2019 sixth international conference on internet of things: systems, management and security (IOTSMS)*, pp. 283-290, 2019.

[19] J. S. Grewal, "Responding to and Preventing Threats to Cybersecurity When Utilizing the Internet of Things", *International Journal of Computer (IJC)*, Vol. 30, No. 1, pp. 70-77, 2018.

[20] O. Arias, F. Rahman, M. Tehranipoor, and Y. Jin, "Device attestation: Past, present, and future", In: *Proc. of 2018 Design, Automation and Test in Europe Conference and Exhibition (DATE)*, IEEE, pp. 473-478, 2018.

[21] S. Van Till, "All security is now cybersecurity", *The Five Technological Forces Disrupting Security*, pp. 97-106, 2018.

[22] D. Selvaraj and R. Murugasamy, "Evaluation of Community Detection by Improving Influence Nodes in Complex Networks Using InfoMap with Sigmoid Fish Swarm Optimization Algorithm", *Acta Informatica Pragensia*, Vol. 2022, No. 3, pp. 380-395, 2022.

[23] B. Kuang, A. Fu, Y. Gao, Y. Zhang, J. Zhou, and R. H. Deng, "FeSA: Automatic Federated Swarm Attestation on Dynamic Large-Scale IoT Devices", *IEEE Transactions on Dependable and Secure Computing*, 2022, Accessed: Jan. 19, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9837456/

[24] M. A. Alohali, M. Elsadig, F. N. Al-Wesabi, M. Al Duhayyim, A. M. Hilal, and A. Motwakel, "Swarm intelligence for IoT attack detection in fog-enabled cyber-physical system", *Computers and Electrical Engineering*, Vol. 108, p. 108676, 2023.

[25] H. A. Madni, R. M. Umer, and G. L. Foresti, "Swarm-FHE: Fully Homomorphic Encryption-based Swarm Learning for Malicious Clients", *Int. J. Neur. Syst.*, Vol. 33, No. 08, pp. 2350033, 2023.

[26] A. A. Alrababah, A. Alshahrani, and B. Al-Kasasbeh, "Efficiency Model of Information Systems as an Implementation of Key Performance Indicators", *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, Vol. 16, No. 12, pp. 139–143, 2016, [Online]. Available: http://paper.ijcsns.org/07_book/201612/20161219.pdf.

[27] E. Choo, M. Nabeel, M. Alsabah, I. Khalil, T. Yu, and W. Wang, "DeviceWatch: A Data-Driven Network Analysis Approach to Identifying Compromised Mobile Devices with Graph-

Inference", *ACM Trans. Priv. Secur.*, Vol. 26, No. 1, pp. 1-32, 2023.

[28] I. Sudha M.A. Mustafa, R. Suguna, S. Karupusamy, V. Ammisetty, S.N. Shavkatovich, M. Ramalingam, P. Kanani, "Pulse jamming attack detection using swarm intelligence in wireless sensor networks", *Optik*, Vol. 272, pp. 170251, 2023.

[29] Y. K. Salih, O. H. See, S. Yussof, A. Iqbal, and S. Q. Mohammad Salih, "A proactive fuzzy-guided link labeling algorithm based on MIH framework in heterogeneous wireless networks", *Wirel. Pers. Commun.*, Vol. 75, No. 4, pp. 2495–2511, 2014, doi: 10.1007/s11277-013-1479-z.

[30] N. S. Divya and R. Vatambeti, "Detecting false data injection attacks in industrial Internet of Things using an optimized bidirectional gated recurrent unit-swarm optimization algorithm model", *Acadlore Trans. Mach. Learn*, Vol. 2, No. 2, pp. 75-83, 2023.

[31] K. Li, Z. Li, Z. Gu, J. Guo, Z. Wang, and L. Sun, "Compromised IoT Devices Detection in Smart Home via Semantic Information", In: *Proc. of ICC 2022-IEEE International Conference on Communications*, pp. 4986-4992, 2022, Accessed: Jan. 19, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9838793/

[32] H. Boche and C. Deppe, "Secure identification under jamming attacks", In: *Proc. of 2017 IEEE Workshop on Information Forensics and Security (WIFS)*, IEEE, pp. 1-6, 2017.

[33] A. A. Al-rababah and M. A. Al-rababah, "Functional Activity Based Comparison Study for Neural Network Application", *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, Vol. 7, No. 1, pp. 153–158, 2007.

[34] M. K. Hanawal, D. N. Nguyen, and M. Krunz, "Jamming attack on in-band full-duplex communications: Detection and countermeasures", In: *Proc. of IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*, pp. 1-9, 2016.

[35] Z. Xie, Y. Yang, and Y. Ma, "Development of Data Center based on Cloud Computing Technology", In: *Proc. of 2022 International Conference on Edge Computing and Applications (ICECAA)*, pp. 27-30, 2022.

[36] M.-J. Yang, "Energy-efficient cloud data center with fair service level agreement for green computing", *Cluster Computing*, Vol. 24, No. 4, pp. 3337-3349, 2021.

[37] J. A. Jeba, S. Roy, M. O. Rashid, S. T. Atik, and M. Whaiduzzaman, "Towards green cloud computing an algorithmic approach for energy minimization in cloud data centers", In: *Proc. of Research Anthology on Architectures, Frameworks, and Integration Strategies for Distributed and Cloud Computing, IGI Global*, pp. 846-872, 2021.

[38] A. Montazerolghaem, M. H. Yaghmaee, and A. Leon-Garcia, "Green cloud multimedia networking: NFV/SDN based energy-efficient resource allocation", *IEEE Transactions on Green Communications and Networking*, Vol. 4, No. 3, pp. 873-889, 2020.

[39] A. Ibrahim, I. Al Sayed, M. Sameer Jabbar, and R. Sekhar, "Evaluating the Impact of Emotions and Awareness on User Experience in Virtual Learning Environments for Sustainable Development Education", *Ingénierie des systèmes d Inf.*, Vol. 29, No. 1, pp. 65–73, 2024, doi: 10.18280/isi.290108.

[40] A. Biswas, P. Jakovits, and D. G. Roy, "Sustainable Energy Management System Using Green Smart Grid in Mobile Cloud Computing Environment", In: *Proc. of Green Mobile Cloud Computing*, pp. 153-169, 2022.

[41] H. Liu, J. Zhang, and M. Zhou, "Adaptive Particle Swarm Optimizer Combining Hierarchical Learning with Variable Population", *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 53, No. 3, pp. 1397-1407, 2022.

[42] E.M. Novoa-del-Toro, E. Mezura-Montes, M. Vignes, M. Térézol, F. Magdinier, L. Tichit and A. Baudot, "A multi-objective genetic algorithm to find active modules in multiplex biological networks", *PLoS computational biology*, Vol. 17, No. 8, pp. e1009263, 2021.

[43] C. Liu, J. Wang, Y. Cao, M. Liu, and W. Shen, "GON: End-to-end optimization framework for constraint graph optimization problems", *Knowledge-Based Systems*, Vol. 254, pp. 109697, 2022.

[44] C. Pan, Z. Jia, J. Huang, Z. Chen, and J. Wang, "Optimization of Cooling Strategy for Lithium Battery Pack Based on Orthogonal Test and Particle Swarm Algorithm", *J. Energy Eng.*, Vol. 149, No. 5, pp. 04023026, Oct. 2023.

[45] X. Wang, H. Li, L. He, Z. Li, and Z. Wang, "Estimated temperature-dependent interfacial heat transfer coefficient during gas cooling based on firefly algorithm and finite element method", *Heat Mass Transfer*, Vol. 55, No. 9, pp. 2545-2558, Sep. 2019.

[46] A. M. Ali, M. A. Ngadi, R. Sham, and I. I. Al Barazanchi, "Enhanced QoS Routing Protocol for an Unmanned Ground Vehicle, Based on the

ACO Approach", *Sensors (Basel).*, Vol. 23, No. 3, 2023, doi: 10.3390/s23031431.

[47] M. H. Sulaiman, M. I. Mohd Rashid, M. R. Mohamed, O. Aliman, and H. Daniyal, "An application of cuckoo search algorithm for solving optimal chiller loading problem for energy conservation", *Applied Mechanics and Materials*, Vol. 793, pp. 500-504, 2015.

[48] Y. Ahmad, M. Ullah, R. Khan, B. Shafi, A. Khan, M. Zareei, A. Aldosary and E.M. Mohamed, "SiFSO: Fish Swarm Optimization-Based Technique for Efficient Community Detection in Complex Networks", *Complexity*, Vol. 2020, pp. e6695032, 2020.

[49] Y. Zhang, X. Chen, D. Lv, and Y. Zhang, "Optimization of urban heat effect mitigation based on multi-type ant colony algorithm", *Applied Soft Computing*, Vol. 112, pp. 107758, 2021.