Hindawi
Security and Communication Networks
Volume 2023, Article ID 9840321, 1 page
https://doi.org/10.1155/2023/9840321

Retraction

Retracted: Enhanced Secure Technique for Detecting Cyber Attacks Using Artificial Intelligence and Optimal IoT

Security and Communication Networks

Received 10 October 2023; Accepted 10 October 2023; Published 11 October 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] A. Kumar, M. Rahmath, Y. Raju et al., "Enhanced Secure Technique for Detecting Cyber Attacks Using Artificial Intelligence and Optimal IoT," *Security and Communication Networks*, vol. 2022, Article ID 8024518, 13 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 8024518, 13 pages
https://doi.org/10.1155/2022/8024518

Research Article

Enhanced Secure Technique for Detecting Cyber Attacks Using Artificial Intelligence and Optimal IoT

Anand Kumar,[1] **Mohammed Rahmath**,[2] **Yeligeti Raju**,[3] **Sridhar Reddy Vulapula**,[4] **Boppuru Rudra Prathap**,[5] **Mohamed M. Hassan**,[6] **Mohamed A. Mohamed**,[7,8] **and Simon Atuah Asakipaam**[9]

[1]*Cambridge Institute of Technology, North Campus, Bangalore 562110, Karnataka, India*
[2]*Department of Computer Science, Prince Sattam Bin Abdulaziz University, Wadi Ad-Dawasir,KSA, Saudi Arabia*
[3]*Department of Computer Science and Engineering, Vignana Bharathi Institute of Technology, Hyderabad, Telangana, India*
[4]*Department of IT, Vignana Bharathi Institute of Technology, Hyderabad, India*
[5]*Department of Computer Science and Engineering, Christ University, Bangalore, India*
[6]*Department of Biology, College of Science, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*
[7]*Department of Medical Instruments Engineering Techniques, AI-Turath University, Baghdad 10021, Iraq*
[8]*Department of Medical Instruments Engineering Techniques, Al-Farahidi University, Baghdad 10021, Iraq*
[9]*Department of Electrical and Electronics Engineering, Tamale Technical University, Tamale, Ghana*

Correspondence should be addressed to Simon Atuah Asakipaam; simonasakipaam@gmail.com

Received 17 April 2022; Revised 31 May 2022; Accepted 9 June 2022; Published 20 July 2022

Academic Editor: Mukesh Soni

The Internet of Things (IoT) is a broad term that refers to the collection of information about all of the items that are linked to the Internet. It supervises and controls the functions from a distance, without the need for human interaction. It has the ability to react to the environment either immediately or via its previous experiences. In a similar vein, robots may learn from their experiences in the environment that is relevant to their applications and respond appropriately without the need for human interaction. A greater number of sensors are being distributed across the environment in order to collect and evaluate the essential information. They are gaining ground in a variety of industries, ranging from the industrial environment to the smart home. Sensors are assisting in the monitoring and collection of data from all of the real-time devices that are reliant on all of the different types of fundamental necessities to the most advanced settings available. This research study was primarily concerned with increasing the efficiency of the sensing and network layers of the Internet of Things to increase cyber security. Due to the fact that sensors are resource-constrained devices, it is vital to provide a method for reacting, analysing, and transmitting data collected from the sensors to the base station as efficient as possible. Resource requirements, such as energy, computational power, and storage, vary depending on the kind of sensing devices and communication technologies that are utilised to link real-world objects together. Sensor networks' physical and media access control layers, as well as their applications in diverse geographical and temporal domains, are distinct from one another. Transmission coverage range, energy consumption, and communication technologies differ depending on the application requirements, ranging from low constraints to high resource enrich gadgets. This has a direct impact on the performance of the massive Internet of Things environment, as well as the overall network lifetime of the environment. Identifying and communicating matching items in a massively dispersed Internet of Things environment is critical in terms of spatial identification and communication.

1. Introduction

The increased capacity for the computing powers of the IoT devices has increased the adaptability of these devices for agricultural purposes to a greater extent. The improvement in computing capacity is due to other enhancements in technology, such as edge or fog computing. The detailed survey carried out by Yu et al. [1] has clearly listed the

benefits of adopting edge-based computing for agricultural IoT solutions. Following similar directions, many other researchers have also demonstrated various use of IoT devices for agricultural purposes. The work by Pan and McElhannon [2] is one such example. Nonetheless, many parallel research attempts have listed many challenges for these adaptations. The work by Safara et al. [3] have clearly listed few challenges such as:

(i) Low capacity of the battery resulting in less sustainable application frameworks. This problem can be solved by deploying the IoT devices optimally to reduce the additional burden on the clusters and cluster heads.

(ii) Low coverage due to the lesser bandwidth for communication. Once again, the optimal placement of the devices can manage the challenge of coverage.

(iii) Finally, the remote manageability of such frameworks is highly challenging due to the additional cost of cloud-based storage and processing solutions. This problem demands a different approach and can be solved by deploying an additional layer for data management on the IoT network stack.

Hence, clearly these abovementioned factors are the recent research demand and must be addressed. This work proposed a framework for optimal IoT device placements and proposes a novel structure for effective data collection and management, to solve all these problems.

The rest of the work is organized such as in Section 2, the recent research attempts are analyzed critically to identify the research gaps. Section 3 is dedicated to understand the fundamental principles of device placements and manageability. Section 4 discussed the problem after the initial analysis carried out in the previous sections. The solution to the identified problems can be seen in Section 5. Based on the proposed solution, the deployable algorithms and the framework can be understood from Section 6. The obtained results as outcomes from the deployed framework can be seen in Section 7 with a comparative analysis in Section 8 and the conclusion of this research can be identified in Section 9.

2. Parallel Research Outcomes for Detecting Cyber Attacks Using Artificial Intelligence and Optimal IoT

Following the establishment of the background in the prior portion of this work, the subsequent research outputs from the parallel studies are reviewed more critically in this section.

The majority of the findings of parallel research have revealed just one single solution point to make deployments more sustainable. This solution point involves adopting the edge or fog computing architecture in conjunction with the IoT framework. The work of Yu et al. [4] has stated this possibility numerous times with considerable arguments and evidence of this notion. It is one of the most notable results in this approach. In spite of this, while working on the design of the concept framework that was proposed, the crucial bottleneck of this implementation emerged as the trade-off between the optimization of costs and the sustainability of the deployment. In order to make a deployment sustainable, the costs cannot be increased, as was demonstrated in the research work that was discussed in parallel.

The bulk of the outputs of the parallel research have focused on a single problem that needs to be addressed, as shown by the information that is included in the abstract of this study. Through the use of fibre optics as the link, the research that was carried out by Al Ridhawi et al. [5]. They had the goal of overcoming challenges that were related to both the connection and the range of the signal. The number of persons who agree with this work and those who disagree with it is, for all intents and purposes, the same. On the one hand, the effectiveness of the solution has gained a huge popularity for adaptation, as can be seen in the report by Sarkar et al. [6], and on the other hand, the nations that are primarily dependent on agriculture for per capita income are unable to deploy such expensive networking backbones for such purposes because of their limited financial resources. It is difficult to use this response as a standard for anything else because of the reasons stated above.

The enormous amount of data is an aspect of this investigation that cannot be disregarded since it is tied to this inquiry. It is anticipated that the Internet of Things sensors that have been installed would capture a massive amount of data, which will, at some point in time, need migration to a centralised storage, preprocessing, analysis, and visualisation. The challenges that are associated with this task have been outlined in the work that was done by Kaur and Singh [7]. Additionally, the effect of these difficulties is outlined in a distinct body of work by the same author, Feng et al. along with other researchers [8]. The answer to this issue is also provided in the framework that has been offered, which includes an extra layer for data management. There is a possibility that this offered solution is not particularly original in terms of the thinking process, given that Guo et al. [9] have presented an application that is quite similar to this one. The implementation tactics have been supported and enhanced as a result of the work done by Yousefpour et al. [10]. However, the solution that was proposed by this parallel research attempt took into consideration the use of a virtualized layer of communication in order to accomplish this objective, and the proposed framework relies heavily on the protocol stack of the IoT network in order to accomplish this improvement.

The IoT stack-oriented solutions can also be seen in parallel research works as showcased by Tomar and Shukla [11]. Nevertheless, these works showcasing similar approaches can be highly critical in terms of power management and building sustainable solutions or deployments. The work by Kaur et al. [12] have strongly criticised such approaches. Few researchers have claimed to achieve the optimal distribution of the power utilization. One such example can be observed in the work by Al-Salim et al. [13]. Nonetheless, this work criticises such claims due to the fact that, the optimal power distribution cannot really be achieved without a proper placement of the IoT devices. In another work by Al-Salim et al. [14], this critical direction

can be found, which is a significant proof for continuing the research in this direction.

In the similar direction, yet another work by Al-Quzweeni et al. [15] have demonstrated a periodic activation of the IoT devices to improve the duty cycle for increasing the sustainability. However, the work by Janarthanan et al. [16] claimed that the improvement over the routing algorithms can improve the sustainability by selectively deploying the cluster heads for the framework. These outcomes are the extension of the guidelines formulated by Al-Azez et al. [17]. Nonetheless, these solutions are primarily software driven solutions and without any improvement on the hardware devices. These solutions highly depend on other form of computing such as cloud, fog, or edge computing, which can increase the trade between cost and sustainability. Hence, this work directs the research towards more IoT driven solutions.

Henceforth, with the knowledge of the parallel research outcomes, the fundamental strategy for IoT device placements for optimal coverage is presented in the next section of this work [18].

3. Fundamentals of Device Placements for Optimal Coverage

After the understanding of the parallel research outcomes, in this section of the work, the fundamental strategy for node placement is understood using mathematical models.

The traditional method completely relies on the image processing for understanding the boundaries of the given area and further maps the available IoT devices to the edge conditions.

Assuming that, the total information about the agricultural field is captured in form of an image, and the image information can be presented as I, which is a collection of pixel information, $PX[][]$. The pixel collection contains all individual information about the pixels and every pixel can be represented as $PX[i][j]$.

This fundamental assumption can be presented as follows:

$$I = PX[\,]. \tag{1}$$

And, rightfully, for an $n \times m$ image,

$$PX[\,][\,] = PX[0][0], PX[1][1], \ldots PX[n-1][m-1]. \tag{2}$$

In order to calculate the boundaries, this process must take few steps as elaborated here.

Step 1. Firstly, the mean intensity, MI, of the pixels must be calculated as follows:

$$MI = \frac{\sum_{i=0}^{n} \sum_{j=0}^{m} PX[i][j]}{n.m}. \tag{3}$$

The mean intensity of the image will contribute towards the categorization of the image pixels into multiple groups.

Step 2. Assuming that, there will three categories of the pixels as pixels higher than the MI, lower than MI, and equal to the MI. Thus, this categorization can be formulated as follows:

$$K[0.2] \leftarrow \begin{cases} PX[i][j] > \text{MI} \\ PX[i][j] < \text{MI} \\ PX[i][j] = \text{MI} \end{cases}. \tag{4}$$

Also, the categorization is as per the formulation $K[0]$ for pixel with higher intensity, $K[1]$ with lower intensity, and $K[2]$ with equal intensity.

Step 3. It is conclusive to mention that the pixels in $K[0]$ primarily denotes the inner pixels of the image, $K[1]$ denotes the outer pixels, and $K[2]$ denotes the centroid pixels. Thus, the pixels from $K[1]$ collection can be identified as edge, $E[]$, pixels, which can be formulated as follows:

$$E[\,] \leftarrow K[1]. \tag{5}$$

Step 4. Finally, the edge pixels can be converted to equal distance points, R. The traditional method of calculating the number of equidistance points is to find the total number, η, of pixel elements in the edge, $E[]$, collection as follows:

$$\eta \leftarrow f(E[\,]). \tag{6}$$

Furthermore,

$$R = If f \begin{cases} \eta \% R = 0 \\ R \longrightarrow 1 \end{cases}. \tag{7}$$

Then, R will be considered as a set of equidistance points and at these points, the IoT devices will be deployed. Regardless, to mention that the placement is generic and has no consideration of the coverage. Furthermore, the problems with the existing method are furnished in the next section of this work.

4. Problem Formulation

After analysing the fundamental principle of IoT device placements in the previous section of this work, this section is dedicated to analysing the problems of the existing basic principles.

The challenges identified in the existing systems are as follows:

(i) Firstly, the existing method is completely focused on the image-based analysis. Thus, the time complexity is significantly higher.

Assuming that, the size of the captured image is $n \times m$. Hence, the time complexity to analyse the complete data, $T1$, can be formulated as follows:

$$T1 = n.m. \tag{8}$$

Furthermore, categorization for the image pixels into k number of categories will demand analysing each pixel $(n \times m)$ for k number of times. Thus, the

additional time complexity can be formulated as follows:

$$T1 = n.m + k.n.m. \tag{9}$$

Or, as k is a constant and $n \approx m$,

$$T1 = n.n. \tag{10}$$

Furthermore,

$$T1 = O\left(n^2\right). \tag{11}$$

Henceforth, it is conclusive to mention that the time complexity of this process is significantly higher.

(ii) Secondly the image acquisition and preprocessing are time-consuming, so image capturing is difficult using drones. It is evident that, during the capturing process, only one image will not be captured to increase the success rate. Assuming that, S number of images are captured and the images are stored in the $IS[]$ image collections. Thus,

$$f(IS[\,]) \longrightarrow S. \tag{12}$$

Furthermore, in order to understand the best captured image, it is often observed that, the histogram method is utilised. Considering the image size for each iVmage is $n \times m$, the time complexity, $T2$, for generating the histogram for a single image can be formulated as follows:

$$T2 = n^m. \tag{13}$$

However, the collected number of images are S. Thus, the final time complexity shall be as follows:

$$T2 = S.n^m. \tag{14}$$

Assuming that, S is a constant and $n \approx m$, the time complexity can be rewritten as follows:

$$T2 = O\left(n^n\right). \tag{15}$$

Thus, up to this point in time, the total complexity, $T1$ and $T2$, can be formulated as follows:

$$T1 + T2 = O\left(n^2\right) + O\left(n^n\right). \tag{16}$$

Finally, due to image-based analysis of the existing methods, the additional challenge is to further map the edge pixels to the actual coordinates. Hence, in a two-dimensional space, (X, Y) the time complexity, $T3$, of mapping R attributes can be formulated as follows:

$$T3 = R^{X,Y}. \tag{17}$$

Converting 7 in terms of n and m,

$$T3 = n^{n.m}. \tag{18}$$

Again, the time complexity can be rewritten as follows:

$$T3 = O\left(n^{n^2}\right). \tag{19}$$

Henceforth, the final time complexity of this process, $T1$, $T2$, and $T3$, can be formulated as follows:

$$T1 + T2 + T3 = O\left(n^2\right) + O\left(n^n\right) + O\left(n^{n^2}\right). \tag{20}$$

Furthermore, based on the principle of function maximization,

$$T1 + T2 + T3 \approx O\left(n^{n^2}\right). \tag{21}$$

Finally, the proposed solutions are formulated in the next section of this work.

5. Proposed Solutions for Detecting Cyber Attacks Using Artificial Intelligence and Optimal IoT

After analysing the parallel research outcomes in terms of enhancements to the basic principle and the basic principle for IoT node placements, this section of the work, formulate the proposed solutions. This work aims to solve the identified problems in three segments.

5.1. Selection of the Edge Coordinates. The first phase of the proposed solutions is to start considering the complete field in terms of a graph, F, where each and every point or coordinate is considered as vertices, $V[]$, and the connection between the coordinates are the edges, $E[]$. Hence, this relation can be formulated as follows:

$$F \Rightarrow \{V[\,], E[\,]\}. \tag{22}$$

Furthermore, each and every vertex is a collection of two factors as the coordinate (X, Y) and the directional vector, $\vec{d}$. Thus, for any vertex $V[i]$, this can be formulated as follows:

$$V[i] = \{(X, Y), d\}. \tag{23}$$

At this point in time, the first factor, that is the coordinates are considered for analysis.

The primary objective of this first phase of the solution is to identify the extreme coordinates of the field. This outcome from this phase, will contribute to the start of the next phase of the solution to decide the start and end point of the analysis.

Thus, the collection of the extreme vertices, $VE[]$, can be formulated as follows:

$$VE[\,] = \left\{ \prod_{X->\min, Y->\min} V[\,], \prod_{X->\max, Y->\min} V[\,], \prod_{X->\min, Y->\max} V[\,], \prod_{X->\max, Y->\max} V[\,] \right\}. \tag{24}$$

Here, the element of the $VE[]$ collection will contain the left uppermost vertex, rightmost uppermost vertex, left

Algorithm - I : Maxima-Minima Based Extreme Coordinates Identification (**MMECI**) Algorithm

Objective: Identification of the outmost four coordinates

Input:

V[] as collection of all coordinates for the field

E[] as collection of the connecting edges between V[]

Output:

VE[] as the extreme coordinates

Strategy:

Step - 1. Load all the coordinates of the field as V[]

Step - 2. Extract the coordinate information as (X,Y)[]

Step - 3. For each element in V[] as V[i] with (X,Y)[i]

a. If (X)[i]<(X)[i+1] && (Y)[i]<(Y)[i+1]
   i. Then, VE[0] = V[i]
b. Else If (X)[i]>(X)[i+1] && (Y)[i]<(Y)[i+1]
   i. Then, VE[1] = V[i]
c. Else If (X)[i]<(X)[i+1] && (Y)[i]>(Y)[i+1]
   i. Then, VE[2] = V[i]
d. Else If (X)[i]>(X)[i+1] && (Y)[i]>(Y)[i+1]
   i. Then, VE[3] = V[i]
e. Else,
   i. Continue

Step - 4. For each element in the E[] as E[j]

a. If VE[0].E[j] -> VE[1].E[j]
b. Confirm VE[0]
c. If VE[1].E[j] -> VE[3].E[j]
d. Confirm VE[1]
e. If VE[2].E[j] -> VE[1].E[j] || VE[2].E[j] -> VE[3].E[j]
f. Confirm VE[2]
g. If VE[3].E[j] -> VE[1].E[j] || VE[3].E[j] -> VE[2].E[j]
h. Confirm VE[3]

Step - 5. Return VE[]

Figure 1: Maxima-minima based extreme coordinates identification (MMECI) algorithm.

bottom most vertex, and right bottom most vertex, respectively.

Nonetheless, these identified vertices in $VE[]$ must ensure a connectivity using the edge collection, $E[]$, as follows:

$$VE[i] \longrightarrow VE[i+1] \Rightarrow \exists \left(\sum_{i=0}^{m} E_i \right). \tag{25}$$

Furthermore, with the $VE[]$ collection as extreme points as terminating conditions to the next phase of the solution, phase two is formulated.

5.2. Edge Identification Using the Curve Fitting Method. The second most important challenge of the existing method is to identify the edge locations for the irregular geometric shape.

Continuing from equation (23), the directional vector can be reformulated as follows:

$$\vec{d} = \left\{ \vec{a}, \vec{b}, \vec{c}, \vec{d} \right\} \tag{26}$$

Here, these four components of the directional vector define four directional individual vectors on a two-dimensional space.

It is natural to realize that, for any two vertices, if any of the directional vectors, out of four, matches, then these two vertices are falling on the same line. This logic can be formulated as follows:

$$\begin{aligned} \{f'(V[i]) = f'(V[i+1])\} \\ \Rightarrow V[i], V[i+1]. \end{aligned} \tag{27}$$

Algorithm - II: Edge Identification using Curve Fitting Method (**EICF**) Algorithm

Objective: Identification of the edge of the field for an irregular shape

Input:

V[] as collection of all coordinates for the field

VE[] as the extreme coordinates

Output:

P[] as connected set of points on the edge

Strategy:

Step - 1. Load all the coordinates of the field as V[]

Step - 2. Extract the directional vector information as D[]

Step - 3. For each element in V[] as V[i] with D[i]

a. If V[i] belongs to VE[]

i. Then, If D[i] -> D[i+1]

1. Then, V[i],V[i+1] -> P[]

Step - 4. Return P[]

Figure 2: Edge Identification using curve fitting method (EICF) algorithm.

Algorithm - III: Optimal IoT device Placements using Range Analysis (**O-IoT-RA**) Algorithm

Objective: Optimal Placements of the IoT devices on the field

Input:

IT[] as IoT Device sets

P[] as connected set of points on the edge

Output:

P1[] as coordinate positions for the IoT devices

Strategy:

Step - 1. Load the P[] collection

Step - 2. Load the IT[] collection

Step - 3. For each element in P[] as P[i]

a. If IT[j] U IT[j+1]

i. Then, P[i]=>P1[] & P[i+1]=>P1[]

b. Else,

i. Then, P[i]=>P1[]

Step - 4. Return P1[]

Figure 3: Optimal IoT device placements using range analysis (O-IoT-RA) algorithm.

Here, $V[i]$ and $V[i+1]$ are conclusively connected vertices.

However, the starting position and the terminating positions must be guided by the extreme vertices as follows:

$$P[\,] = \prod_{f'(V[i+1])}^{VE[\,]} V[i], \tag{28}$$

where $P[\,]$ is the identified and connected set of vertices on which the IoT devices can be placed.

Now, the next challenge is to utilize this collection $P[]$ for formulating the optimal placements of the IoT devices.

5.3. Optimal IoT Device Placements. The most challenging problem of this research is to identify the optimal placements of the IoT devices. Assuming that each IoT device, IT, is a collection of various components as battery level, B, range of communication, R, processing capacity, C, transmission power, T, and mobility factor, M, then this can be represented for any IoT device, IT_i, as follows:

$$IT_i = \{B_i, R_i, C_i, T_i, M_i\} \tag{29}$$

Furthermore, assuming that two IoT devices have the overlapping range and within that range two edge vertices are situated, then these two edge points can be considered as optimal placements of the IoT devices as follows:

$$R_i \cap R_{i+1} \Rightarrow P[i] \cup P[i+1] \tag{30}$$

Here, $P[i]$ and $P[i+1]$ locations are identified as optimal IoT device placements points.

Finally, the developed algorithms based on these proposed mathematical models are furnished in the next section of this work.

6. Proposed Algorithms and Framework for Data Collection in Detecting Cyber Attacks Using Artificial Intelligence and Optimal IoT

In the previous section of this work, the proposed solutions are formulated using the mathematical models. The mathematical models are helpful in realizing the facts and principles of the proposed solutions. Nonetheless, the

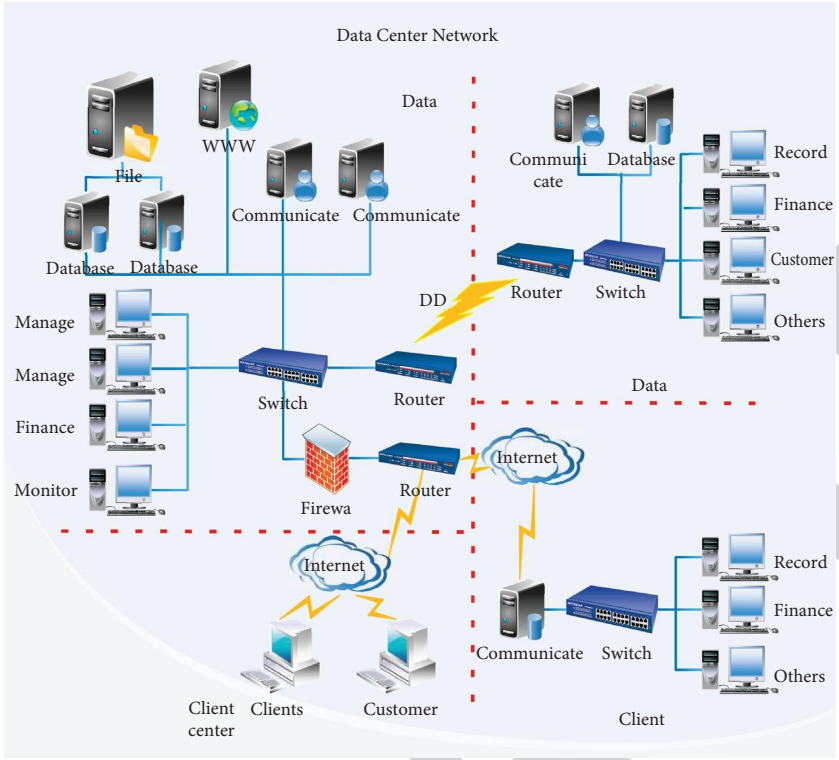

Figure 4: The proposed data management and IoT node placement automation framework.

Table 1: Coverage analysis.

Node id	Received packets	Dumped packets	Lost packets
1	0	0	0
2	5	0	0
3	2	0	0
4	3	0	0
5	4	0	0
6	5	0	0
7	4	0	0
8	4	0	0
9	3	0	0
10	5	0	0
11	4	0	0
12	3	0	0
13	3	0	0
14	4	0	0
15	4	0	0
16	4	0	0
17	5	0	0
18	4	0	0
19	3	0	0
20	3	0	0
21	4	0	0
22	4	0	0
23	5	0	0
24	5	0	0
25	4	0	0

practical implementations of the proposed strategies demand an implementable outline in the form of an algorithm. Hence, this section of the work is dedicated to furnishing the proposed algorithms.

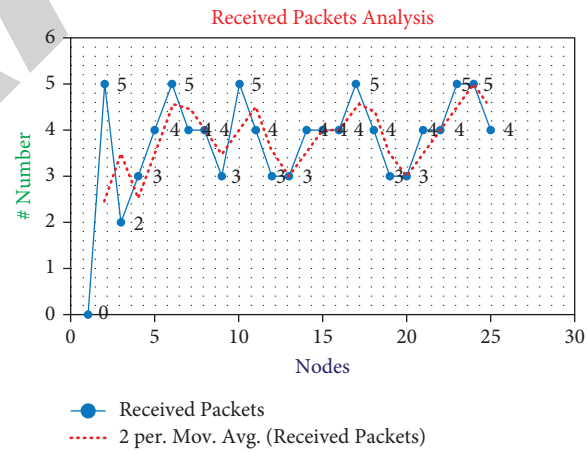

Figure 5: Coverage analysis.

The first proposed algorithm is intended to solve the extreme points identification and is furnished as shown in Figure 1:

The benefit of this proposed algorithm is furnished in the previous section of this work [19].

The second proposed algorithm is intended to solve the connected edge point identification problem and is furnished as shown in Figure 2:

The benefit of this proposed algorithm is furnished in the previous section of this work. [20].

The third and final algorithms is designed to solve the problem of optimal placement on the agricultural field and is furnished as shown in Figure 3:

Table 2: Connectivity analysis.

Node id	Number of hops	Extra time (ms)
1	0	0.0
2	1	1.0
3	1	1.1
4	2	1.0
5	3	1.3
6	2	1.5
7	2	1.0
8	2	4.8
9	3	1.2
10	2	1.0
11	4	1.0
12	5	1.1
13	3	1.1
14	4	1.0
15	3	1.2
16	4	1.1
17	3	1.5
18	4	1.1
19	5	1.2
20	4	1.9
21	5	1.2
22	6	0.6
23	5	0.8
24	5	1.4
25	6	4.8

Table 3: Responsiveness analysis.

Node id	Response time
1	0.0
2	8.2
3	8.5
4	16.0
5	56.0
6	19.6
7	17.3
8	76.3
9	26.7
10	16.6
11	34.5
12	46.0
13	26.0
14	69.5
15	26.3
16	34.5
17	27.6
18	35.8
19	43.7
20	47.0
21	53.3
22	280.5
23	187.4
24	71.6
25	87.8

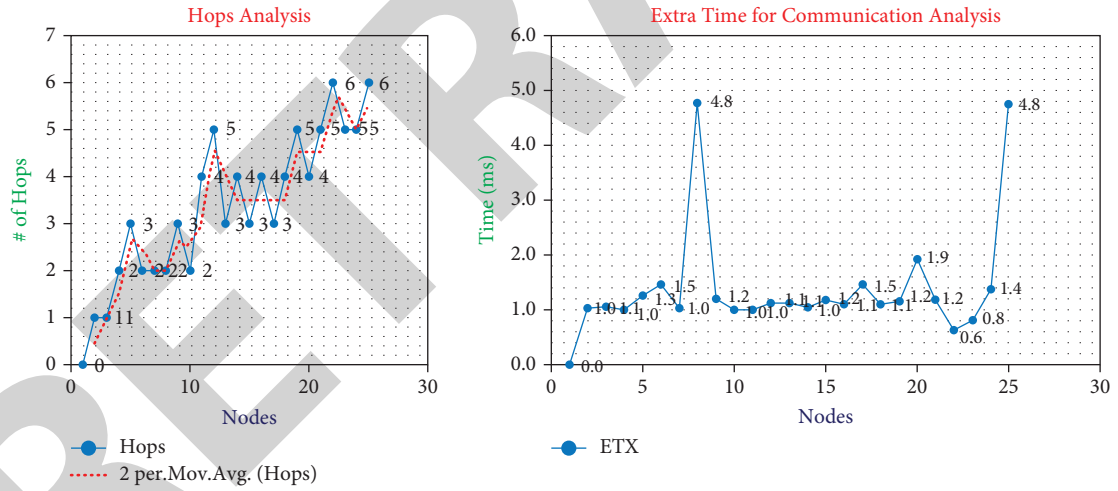

Figure 6: Connectivity analysis.

The benefit of this proposed algorithm is furnished in the previous section of this work. [21].

Furthermore, the proposed framework is furnished and discussed with the proposed algorithms, as shown in Figure 4.

The proposed framework is designed to initially accept the field information in terms of graph-based structure. Furthermore, the first algorithm MMECI must be deployed to identify the most extreme cornered coordinates, so that the edge coordinates can be detected within finite time. Furthermore, the O-IoT-RA algorithm must be deployed to identify the optimal coordinates to place the IoT devices. [22].

Once the IoT devices are placed, the data collection agents from the framework will start collecting the data and build the customizable dashboard.

After the detailed analysis and discussion on the proposed algorithms, the obtained results are discussed on the next section of this work.

7. Results and Discussions

The obtained results from the proposed algorithms and the framework are highly satisfactory and are furnished here.

The analysis of the proposed framework is carried out on various situations with 1000 nodes. However, for presentation purposes, only 25 node information has been furnished.

The outcomes are discussed in five sections.

7.1. Coverage Analysis. The initial phase of the outcomes from the proposed framework is to test the coverage of the deployed IoT frameworks. The observed outcomes are discussed in Table 1.

The results are visualized graphically in Figure 5.

From the obtained data about the coverage of the deployed IoT devices, it is conclusive to mention that the placement of the devices is highly optimized as the packet-based communications are absolutely matched with the average trend of the network [3].

7.2. Connectivity Analysis. The connectivity analysis for any IoT network will ensure the device distributions over any area, which are placed.

The connectivity analysis is carried out in Table 2.

The results are visualized graphically in Figure 6.

After the detailed analysis of the number of hops, it is highly evident that, the number of hops between any two nodes are similar to the average of the hops for the entire network. Thus, this also ensures and confirms the optimal placements of the IoT devices. Also, due to various factors, some of the instances are demonstrating lower bandwidth on few challenges. However, this cannot be considered as benchmark as the extra-time requirement is appearing only in few cases [23].

7.3. Responsiveness Analysis. Apart from the connectivity and coverage, the responsiveness is also one of the most important parameter for analysing the performance of any deployed network. Hence the response time analysis is performed in Table 3.

The results are visualized graphically in Figure 7.

After the analysis of the results for this section, it is noteworthy to focus on the fact that, the response time is fairly moderate and few of the instance is highly responsive. In few of the situations, it is evident that sudden increase for response time can be observed, which is due to the natural causes such as low light or low wind, which causes higher time for data capturing.

7.4. Repositioning Analysis. Once the network is deployed, the framework need not to reposition or redeploy itself. The analysis parameters such as number of churns and number of reboots will demonstrate the stability of the network. The result is furnished in Table 4.

The results are visualized graphically in Figure 8.

The lower churn rates, almost zero reboots, and higher beacon frequency are highly evident of a very stable deployment of the network.

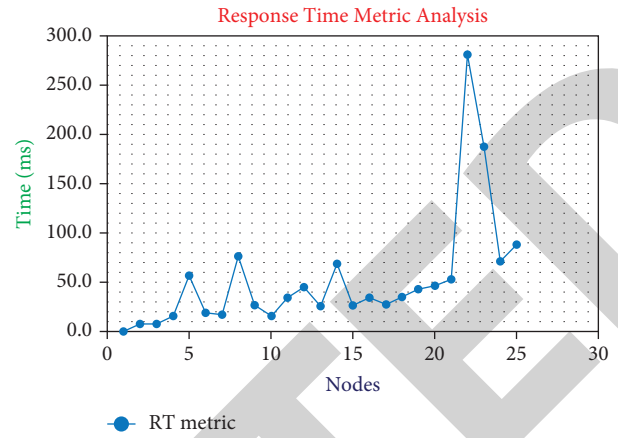

Figure 7: Responsiveness analysis.

Table 4: Repositioning analysis.

Node id	Number of churns	Beacon interval (ms)	Number of reboots
1	0	0	0
2	0	102400	0
3	0	96000	0
4	0	138666	0
5	2	28000	0
6	0	92800	0
7	0	96000	0
8	0	82000	0
9	0	69333	0
10	0	140800	0
11	0	74000	0
12	1	64000	0
13	0	69333	0
14	0	58000	0
15	0	80000	0
16	0	96000	0
17	0	83200	0
18	0	84000	0
19	0	149333	0
20	0	64000	0
21	0	88000	0
22	1	88000	0
23	1	96000	0
24	0	108800	0
25	0	73000	0

7.5. Power Awareness Analysis. The final claim of this work is to justify the sustainability of the deployed framework. Thus, the power consumption analysis is carried out in Table 5.

The results are visualized graphically in Figure 9.

Furthermore, the comparative analysis is carried out in the next section of this work.

8. Comparative Analysis

After the detailed analysis of the obtained outcomes from the proposed framework, in this section, is compared with the parallel research outcomes, as shown in Table 6.

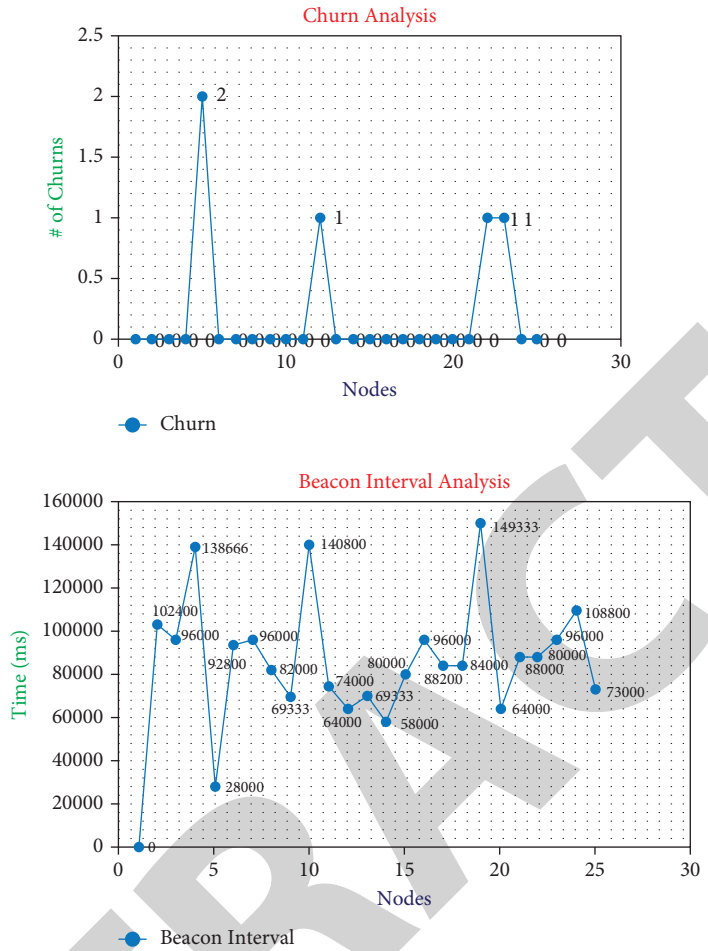

Figure 8: Repositioning analysis.

Table 5: Power aware analysis.

Node id	CPU power	LPM power	Listen power	Transmit power
1	0.39	0.15	0.44	0.21
2	0.44	0.15	0.74	0.18
3	0.41	0.15	0.61	0.19
4	0.38	0.15	0.51	0.16
5	0.38	0.15	0.45	0.18
6	0.37	0.15	0.44	0.12
7	0.42	0.15	0.66	0.19
8	0.41	0.15	0.52	0.28
9	0.38	0.15	0.47	0.20
10	0.39	0.15	0.61	0.12
11	0.43	0.15	0.53	0.23
12	0.37	0.15	0.46	0.18
13	0.38	0.15	0.46	0.17
14	0.42	0.15	0.66	0.25
15	0.45	0.15	0.74	0.25
16	0.37	0.15	0.41	0.13
17	0.42	0.15	0.60	0.28
18	0.37	0.15	0.44	0.14
19	0.36	0.15	0.50	0.12
20	0.40	0.15	0.60	0.20
21	0.39	0.15	0.44	0.21
22	0.40	0.15	0.44	0.52
23	0.38	0.15	0.40	0.18
24	0.37	0.15	0.42	0.12
25	0.38	0.15	0.45	0.21

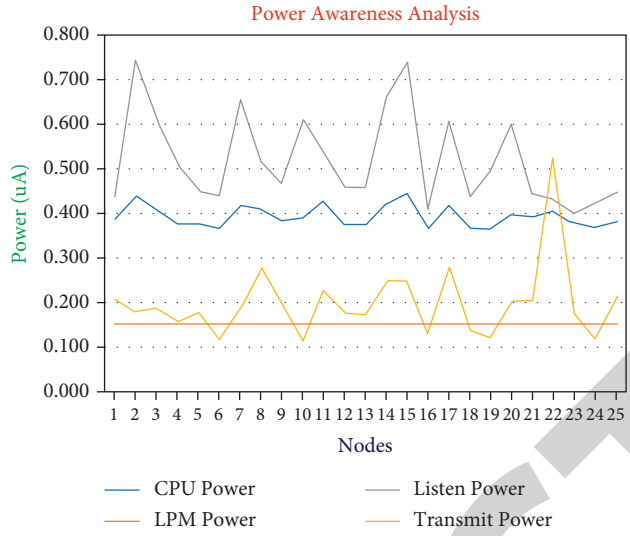

Figure 9: Power awareness analysis.

Table 6: Comparative analysis.

Author, year	Proposed model	Average response time (ms)	Average churn	Model complexity
Yousefpour et al., 2019 [10]	Framework for energy optimization	200.50	7	$O(n^{n^2})$
Tomar and Shukla, 2019 [11]	Service based optimization	172.31	6	$O(n^{n^2})$
Al-Salim et al., 2018 [13]	Service distribution	387.62	6	$O(n^{n^2})$
Janarthanan et al., 2021 [16]	Priority routing	257.76	7	$O(n^{n^2})$
Proposed framework, 2021	Extreme coordinates identification, edge identification and optimal IoT device placements	52.70	1	$O(n)$

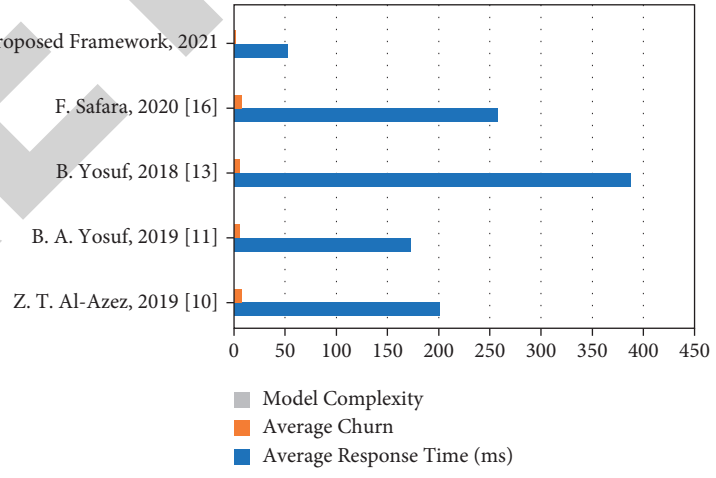

Figure 10: Comparison from existing works.

Henceforth, it is natural to observe that, the proposed framework has outperformed the parallel research outcomes. The proposed framework has improved response time by 15% and the average churn rates by nearly 20% compared to the parallel research outcomes. Finally, the calculated model complexity is $O(n)$, which is again much lesser than that of the other parallel works.

Figure 10 represents the comparison of existing work with proposed work which concludes that the proposed work have less error rate.

9. Conclusion

The effective support from technology to improve the agricultural situation is evident, and this work also contributes towards the same improvement objectives. This proposed framework is a combination of a wide variant of benefits, such as complete automation in IoT device placement optimization, data management framework, and improved power consumptions, and all these benefits are obtained using low model complexity. This work formulates the algorithms for identification of extreme boundary conditions to reduce multiple iterations for edge detection and indirectly reduces the time complexity. Furthermore, the second algorithm ensures that the detected edges have connectivity in terms of physical reachability in order to optimize the range finding process for the IoT devices. Finally, the IoT devices are placed with the optimal process based on range analysis, which is again automated by another proposed algorithm. Finally, this work demonstrates good improvements over the parallel research outcomes and must be considered as one of the benchmarked application in this domain of research.

Data Availability

The data that support the findings of this study are available on request from the corresponding author.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

The authors extend their appreciation to Taif University for supporting the current work by Taif University Researchers Supporting Project number (TURSP-2020/59), Taif University, Taif, Saudi Arabia.

References

[1] W. Yu, F. Liang, X. He et al., "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2018.

[2] J. Pan and J. McElhannon, "Future edge cloud and edge computing for Internet of Things applications," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 439–449, Feb. 2018.

[3] F. Safara, A. Souri, T. Baker, I. Al Ridhawi, and M. Aloqaily, "PriNergy: a priority-based energy-efficient routing method for IoT systems," *The Journal of Supercomputing*, vol. 76, no. 11, pp. 8609–8626, Jan. 2020.

[4] K. Yu, L. Tan, C. Yang et al., "A blockchain-based shamir's threshold cryptography scheme for data protection in industrial Internet of Things settings," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8154–8167, 2022.

[5] I. Al Ridhawi, Y. Kotb, M. Aloqaily, Y. Jararweh, and T. Baker, "A profitable and energy-efficient cooperative fog solution for IoT services," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3578–3586.

[6] S. Sarkar, S. Chatterjee, and S. Misra, "Assessment of the suitability of fog computing in the context of Internet of Things," *IEEE Trans. Cloud Comput.*vol. 6, no. 1, pp. 46–59, Jan. 2018.

[7] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 281–301, 2021.

[8] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K.-K. R. Choo, "Blockchain-based cross-domain authentication for intelligent 5G-enabled Internet of drones," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6224–6238, 2022.

[9] H. Guo, J. Liu, and H. Qin, "Collaborative mobile edge computation offloading for IoT over fiber-wireless networks," *IEEE Network*, vol. 32, no. 1, pp. 66–71, 2018.

[10] A. Yousefpour, C. Fung, T. Nguyen et al., "All one needs to know about fog computing and related edge computing paradigms: a complete survey," *Journal of Systems Architecture*, vol. 98, pp. 289–330, 2019.

[11] M. S. Tomar and P. K. Shukla, "Energy efficient gravitational search algorithm and fuzzy based clustering with hop count based routing for wireless sensor network," *Multimedia Tools and Applications*, vol. 78, no. 19, pp. 27849–27870, 2019.

[12] M. Kaur, D. Singh, V. Kumar, B. B. Gupta, and A. A. Abd El-Latif, "Secure and energy efficient-based E-health care framework for green Internet of Things," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1223–1231, Sept, 2021.

[13] A. M. Al-Salim, A. Q. Lawey, T. E. H. El-Gorashi, and J. M. H. Elmirghani, "Energy efficient big data networks: impact of volume and variety," *IEEE Transactions on Network and Service Management*, vol. 15, no. 1, pp. 458–474, 2018.

[14] A. M. Al-Salim, T. E. H. El-Gorashi, A. Q. Lawey, and J. M. H. Elmirghani, "Greening big data networks: velocity impact," *IET Optoelectronics*, vol. 12, no. 3, pp. 126–135, 2018.

[15] A. N. Al-Quzweeni, A. Q. Lawey, T. E. H. Elgorashi, and J. M. H. Elmirghani, "Optimized energy aware 5G network function virtualization," *IEEE Access*, vol. 7, pp. 44939–44958, 2019.

[16] R. Janarthanan, R. U. Maheshwari, P. K. Shukla, P. K. Shukla, S. Mirjalili, and M. Kumar, "Intelligent detection of the PV faults based on artificial neural network and type 2 fuzzy systems," *Energies*, vol. 14, no. 20, p. 6584, 2021.

[17] Z. T. Al-Azez, A. Q. Lawey, T. E. H. El-Gorashi, and J. M. H. Elmirghani, "Energy efficient IoT virtualization framework with peer to peer networking and processing," *IEEE Access*, vol. 7, pp. 50697–50709, 2019.

[18] B. A. Yosuf, M. Musa, T. Elgorashi, and J. M. H. Elmirghani, "Impact of distributed processing on power consumption for IoT based surveillance applications," *Proc. 21st Int. Conf. Transparent Opt. Netw. (ICTON)*, vol. 12, pp. 1–5, 2019.

[19] N. Koli and U. Mamodiya, "Review paper on automation of robotics in spatial with life forms" international," *Journal of Engineering Science Invention Research & Development*, vol. 5, no. Issue 11, pp. 349–353, 2018.

[20] C. Sridhar, P. K. Pareek, R. Kalidoss, S. S. Jamal, P. K. Shukla, and S. J Nuagah, "Optimal medical image size reduction model creation using recurrent neural network and Gen-PSOWVQ," *Journal of Healthcare Engineering*, vol. 2022, pp. 1–8, Article ID 2354866, 2022.

[21] B. Yosuf, M. Musa, T. Elgorashi, A. Q. Lawey, and J. M. H. Elmirghani, "Energy efficient service distribution in Internet of Things," *Proc. 20th Int. Conf. Transparent Opt. Netw. (ICTON)*, vol. 16, pp. 1–4, 2018.

[22] B. A. Yosuf, *Energy Efficient Distributed Processing for IoT*Univ. Leeds, Leeds, U.K, 2019.

[23] J. M. H. Elmirghani, T. Klein, K. Hinton et al., "GreenTouch GreenMeter core network energy-efficiency improvement measures and optimization," *Journal of Optical Communications and Networking*, vol. 10, no. 2, p. A250, Feb. 2018.

[24] A. A. Alnuaim, M. Zakariah, C. Shashidhar et al., "Speaker gender recognition based on deep neural networks and ResNet50," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–13, Article ID 4444388, 2022.

[25] M. Gupta, K. K. Gupta, and P. K. Shukla, "Session key based fast, secure and lightweight image encryption algorithm," *Multimedia Tools and Applications*, vol. 80, no. 7, pp. 10391–10416, 2021.

[26] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, "Systematic review of security vulnerabilities in ethereum blockchain smart contract," *IEEE Access*, vol. 10, pp. 6605–6621, 2022.