Addressing the Vulnerability of Data Routing in IoT Network based on Optimization Techniques and Advanced Blow Fish Encryption

Omar Hisham Rasheed alsadoon[*]

[*] College of Islamic sciences, Al-Iraqia University, Baghdad, Iraq
Email:omaralsadoon345@yahoo.com
https://orcid.org/0009-0008-1768-8813

Abstract

This study focuses on evaluating the data routing protocol in the Internet of Things (IoT). The evaluation is conducted using the Whale Optimization Algorithm (WOA), enhanced by the advanced Blowfish encryption algorithm. In this study, Cipher Block Chaining (CBC) is employed to improve the typical Blowfish technique. Furthermore, several key factors, including the rate of energy consumption, trust, distance, and delay, are considered to ensure the effectiveness of data routing. To demonstrate the feasibility of the proposed approach, four other schemes are utilized in a comparative study. These schemes are particle swarm optimization (PSO), secure routing protocol (SARP),Genetic algorithm (GA), QoS-based Cross Multi-sink Routing protocol (QCM2R). The results clearly demonstrate the feasibility of the proposed approach when compared to the aforementioned schemes, with the lowest energy consumption, distance, and delay recorded as 0.44325 Joule, 0.43257 meters, and 1.35 x 10^{-9} seconds, respectively. Additionally, the trust level is the highest at 0.71255, and the throughput reaches its peak at 2.30 Megabytes/ms when the data size is 7 KB. In terms of security dimension, the proposed improved Blowfish encryption technique is compared with Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA) and typical Blow fish algorithm (BFA) encryption techniques to assess its security robustness against Chosen-Ciphertext Attack (CCA) and Chosen-Plaintext Attack (CPA) with varying the size of data bits from 5KB, 7 KB and 10KB. The obtained results show that the proposed improved blow fish approach outperforms three aforementioned schemes with the smallest similarity between unique text and hacked text under CCA and CPA. Furthermore, the least time of decryption occurs with the proposed approach compared to other three schemes.

Keywords- blow fish encryption, trust, throughput, Cipher Block Chaining, delay.

I. INTRODUCTION

Today, Internet of Things (IoT) has been acquiring a tremendous attractiveness in communication world particularly with the mounting evolution of smart networks [1-5]. An enormous number of sectors for instance the military, healthcare, intelligent buildings, farming have been witnessing detection and assembling various physical data [6-8]. In this regard, wireless sensor networks (WSNs) are considered the backbones of IoT expansion, and they are comprised of a countless number of intelligent sensors that interrelate with the IoT in order to observe and collect data [9-11].

However, many limitations obstruct sensors` performances including but not limited to energy resources, memory, and computation [12-14]. There are numerous studies have been conducted to address these limitations particularly energy efficiency in WSN based on IoT. Afsar *et al.* [15] introduced an adaptive competition-based clustering approach (ACCA) to decide the optimal path for data. The authors considered different factors such as residual energy and the centrality of the nodes. However, the shortcoming of the proposed approach is inappropriateness for large scale networks, due to the vulnerability of sensors data against malicious attacks.

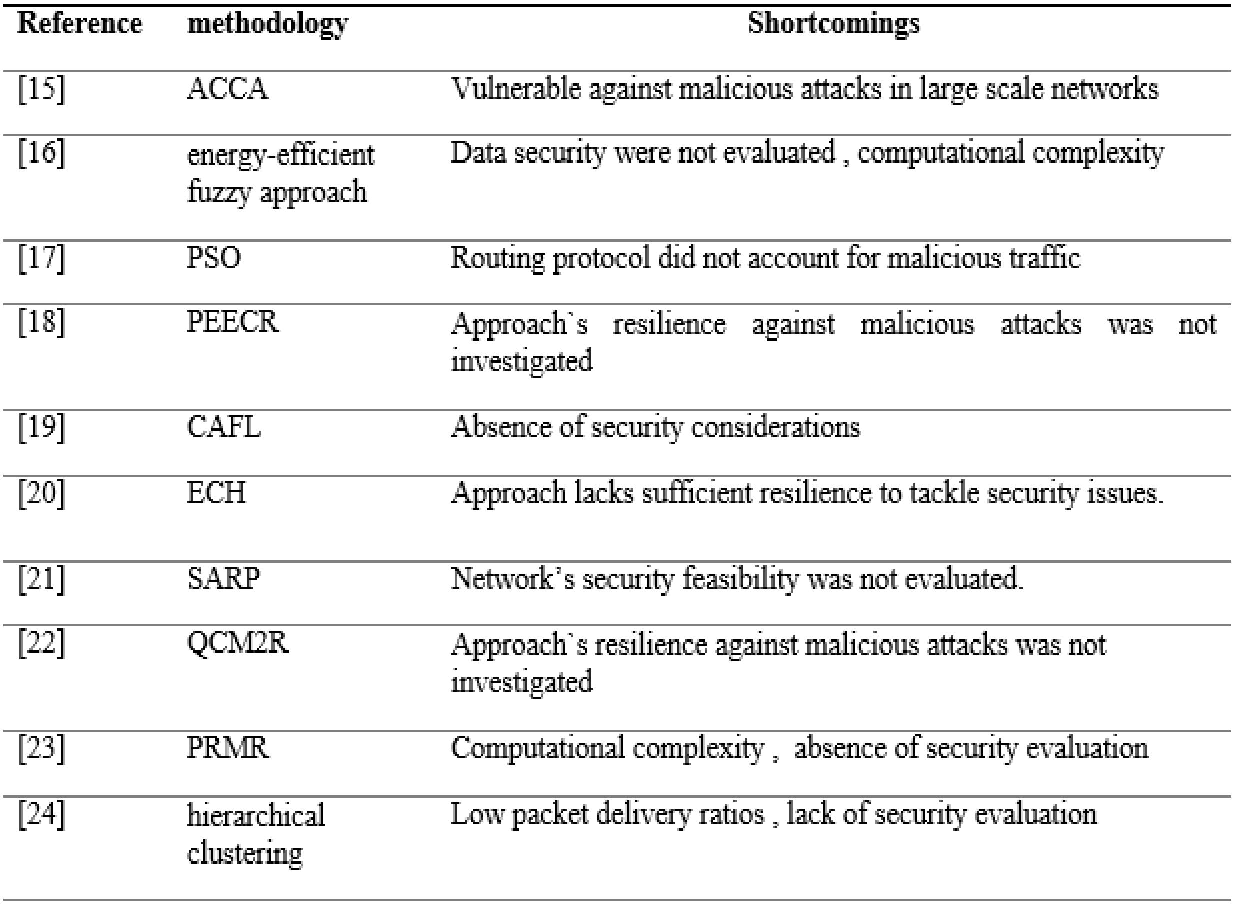
Hamzah *et al.* [16], proposed an energy-efficient fuzzy approach to optimize the routing protocol for WSN, the proposed solution demonstrated its feasibility in diverse aspects besides energy . Nevertheless, the achievability of this solution was not evaluated for data security and the computational complexity is another downside in this study. Edla *et al.* [17] determined an optimal routing protocol by using a particle swarm optimization (PSO). The attained results showed a significant reduction in energy consumption to prolong the lifetime of network. However, the malicious traffic was discounted in routing protocol. Zhang *et al.* [18] developed novel predictive efficient energy consumption reclaim PEECR-based clustering routing approach for data in WSN. The authors considered

http://doi.org/10.58564/IJSER.3.1.2024.142

various aspects such as energy consumption and distance between nodes, the proposed algorithm was based on swarm colony optimization. The results obtained proved the viability of the proposed approach, however the robustness of network against the malicious attacks was not investigated.
El *et al.* [19] presented an advanced fuzzy logic algorithm (CAFL) to advance the lifespan of WSN. The authors employed the fuzzy logic to optimize the cluster heads according to different factors. However the downside of the this approach is disregarding the security investigation. El Alami *et al.* [20] introduced an enhanced clustering hierarchy (ECH) approach to maximize the lifespan of WSN and energy efficiency. However, the proposed approach is not sufficiently resilient to confront the security problems. Mauro *et al.* [21] developed a secure routing protocol (SARP) for data transmission. The simulation results revealed a remarkable contribution of the proposed approach in addressing delay ration and energy consumption. However, the feasibility of network was not evaluated from the security perspective.

Waqas *et al.* [22] proposed QoS-based Cross Multi-sink Routing protocol (QCM2R). The proposed approach was sufficiently feasible in terms of throughput, delay and lifespan, however the robustness of network against the malicious attacks was not investigated. Zeheng *et al* [23] introduced a path reservation multipath routing (PRMR) protocol in IoT network, the simulation results showed the viability of the proposed solution in enhancing the packet delivery rate and reducing the deferment for data routing. However, the complexity of computation and discounting the security evaluation are the main shortcomings in this study. A hierarchical layer balanced clustering pattern to optimize the routing protocol in WSN was introduced by Prasad *et al.* [24]. The authors enriched the energy consumption and the lifespan of network. However, discounting the security evaluation is the key downside in this approach. Table 1 summarizes methodologies, and shortcomings of a number of recent previous studies that investigated the performance of WSN based on IoT.

Table 1. Summary of reviewing previous studies in routing of IoT Networks



Reference	methodology	Shortcomings
[15]	ACCA	Vulnerable against malicious attacks in large scale networks
[16]	energy-efficient fuzzy approach	Data security were not evaluated , computational complexity
[17]	PSO	Routing protocol did not account for malicious traffic
[18]	PEECR	Approach`s resilience against malicious attacks was not investigated
[19]	CAFL	Absence of security considerations
[20]	ECH	Approach lacks sufficient resilience to tackle security issues.
[21]	SARP	Network's security feasibility was not evaluated.
[22]	QCM2R	Approach`s resilience against malicious attacks was not investigated
[23]	PRMR	Computational complexity , absence of security evaluation
[24]	hierarchical clustering	Low packet delivery ratios , lack of security evaluation

Based on the above-mentioned literature, it can be obviously understood that the security challenge has not been paid an adequate attention in the previous studies which only focused on the optimal routing of data .Despite , the security is one of the key challenges for WSN in a vulnerable environment against malicious nodes. Furthermore, other crucial factors such as trust, distance and throughput still need further improvement to enhance the performance of the routing protocol. Moreover, some of the previous methodologies characterized by computational complexity , therefore, this research develops a recent methodology to determine the optimal routing based on whale optimization algorithm (WOA) which is one of the metaheuristic optimization algorithms that have occupied large attention in different applications, and the typical Blowfish encryption technique is improved in this research to address the secuirty challenge . Consequently, the contributions that characterize this study are as follows:

1. To develop a novel approach using whale optimization algorithm (WOA) to determine the optimal routing protocol considering the security evaluation
2. To develop an objective function that deliberates crucial aspects including trust, distance, and delay and energy consumption.
3. To address the vulnerability of IoT network by developing an advanced blowfish encryption approach to enhance the security of data routing against different attacks.

II. THE PROPOSED METHODOLOGY

1. Introduction

The proposed approach employs WOA to optimize the data routing protocol, energy consumption, delay, distance and trust are utilized to develop the objective function that is employs in a whale in the optimization algorithm. Primarily, the network is created and all nodes of IoT are arbitrarily distributed, over the sensing zone of 250 × 250 m. In the simulation stage, the total number of sensor nodes are varied 100, 200, and 300. To transfer IoT data the proposed approach utilized Thingsboard interface platform, it is a web-based open Application Programming Interface (API) maintains data of IoT and shows it in visual form on the web [25],[26]. Thingsboard collaborates with the receiver controller via an internet that represents a ‘‘data packet’’ carrier between the connected things such as laptops, mobiles, or medical sensors. The cloud of Thingsboard implements miscellaneous tasks such as observing and analysing data that is detected by a certain sensor. The methodology of the presented study can be summarized into three stages (1) the optimal routing path of data is optimized by employing WOA that considers crucial constraints including trust, distance, delay and energy consumption, (2) the security of data transmission is enhanced by an advanced Blowfish encryption algorithm. The entire methodology of the proposed solution is shown in Figure 1.

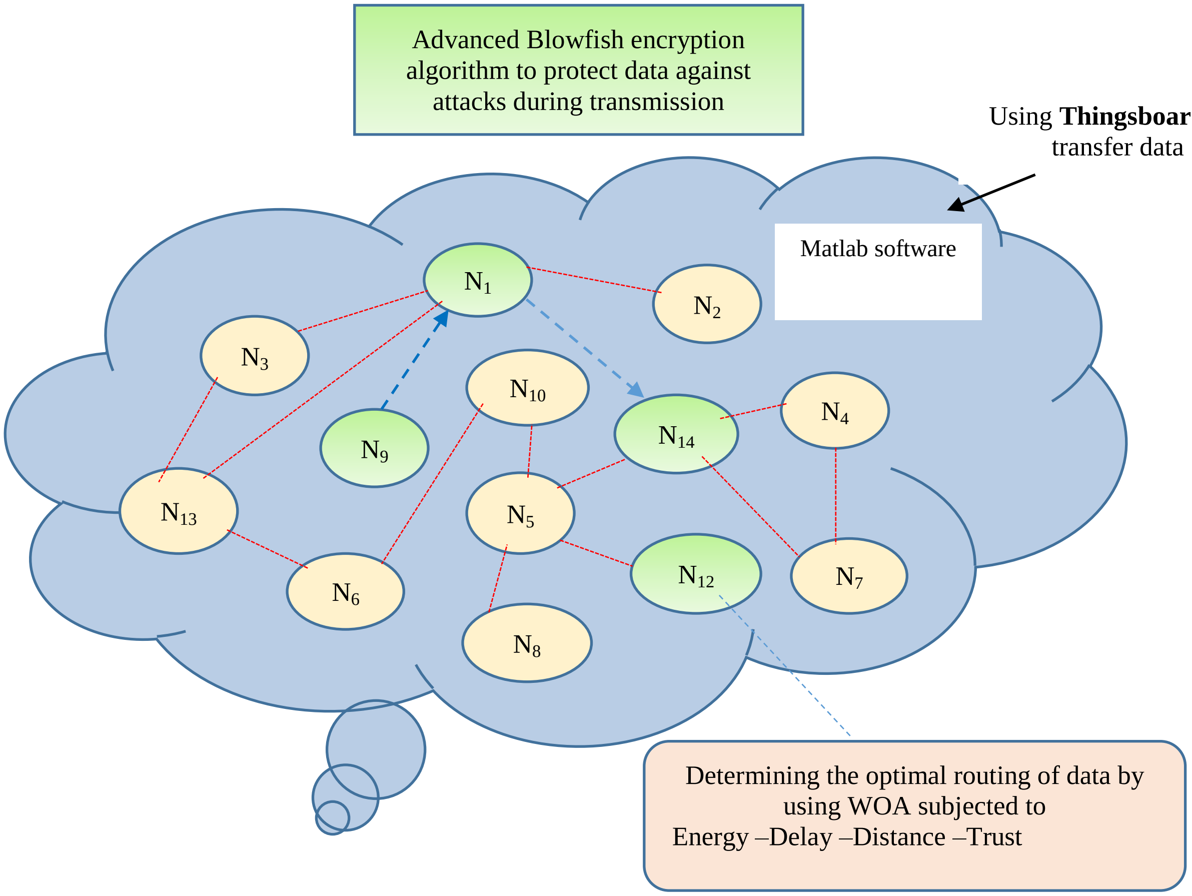

Advanced Blowfish encryption algorithm to protect data against attacks during transmission
Using **Thingsboard** to transfer data
Matlab software
N1
N2
N3
N10
N4
N14
N9
N13
N5
N6
N12
N7
N8
Determining the optimal routing of data by using WOA subjected to
Energy –Delay –Distance –Trust

Figure1. Entire methodology of the introduced solution

2. Objective Function Modelling

- The Energy

As explain earlier, the proposed approach developed an objective function takes account of energy, delay, distance and trust. Indeed, WSN based on IoT consumes a considerable amount of energy to accomplish different tasks including but not limited to transmission, reception and detecting. The proposed approach utilizes the mean of energy of nodes that convey data in the optimal route [27].

- Trust

The trust is an essential measure to assess the feasibility of the proposed scheme that aims to optimize the transmitting route of data in WSN. The priority of confidential node that has low energy is higher an untrustworthy node that has high energy [28].

- Distancing

Undoubtedly, the physical separation between nodes in WSN is a crucial factor significantly influences in determining the optimal routing path of data, hence the mean Euclidean distance between nodes is deliberated [29].

- Delay

The time delay is characterized as the time that is taken by the data packet to reach at the destination [29].The developed objective function can be expressed by:

$$obj = \text{Min}[\, w_1 \times (1 - E) + w_2 \times (Dl) + w_3 \times D + w_4 \times (1 - T)] \qquad (1)$$

It is worth to mention that very term in the above equation is weighted based on its impact Therefore, the objective function is constrained by:

$$w_1 + w_2 + w_3 + w_4 = 1 \qquad (2)$$

The developed objective function is minimized by the whale optimization algorithm to determine the optimal routing path of data in IoT network.

III. WHALE OPTIMIZATION ALGORITHM (WOA)

From the scientific persppective, whale can be described as the hugest creature universally, the length and weight of are reach 30 meter and 180 tons respectively .Naturally whales are sufficiently intelligent to think, choose, and expressively interact [30]. The hunting technique of whales inspired an outstanding metaheuristic optimization algorithm [31-32]. Whale swims 12 m into sea to produce a bubble mesh to encircle the quarry and move up as presented in Figure2.

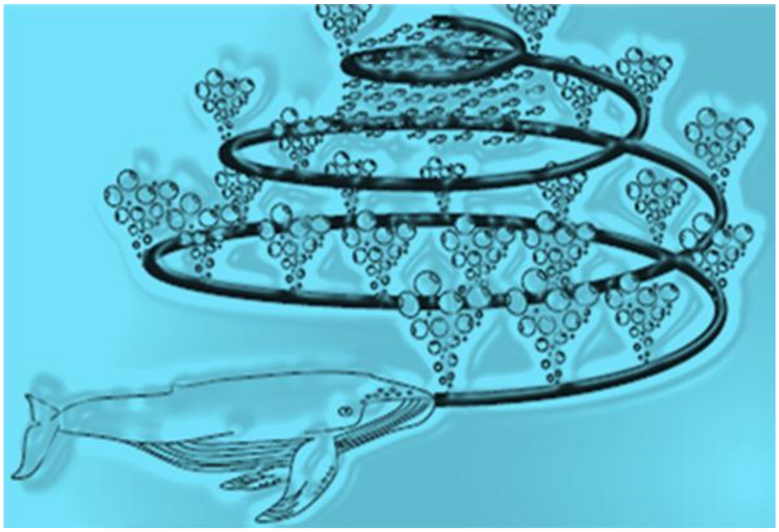


Figure 2. Bubble-mesh hunting of whales

Whale optimization algorithm (WOA)is one of Metaheuristics that have become more widespread in numerous engineering fields since they do not necessitate gradient information and evade the local optima. Metaheuristics are categorized into two kinds:individual-solution and multiple-solution. WOA is one of multiple-solution-based algorithms that achieves a number of solutions (population). In these algorrithms, the many solutions transfer the information between each other around the search space in order to evade local optimal solutions[31-33].

1.Mathematical Modelling

a. Encircling prey stage:

Whale can discriminate the location of prey and enclose it. Mathematically, this behavior is expressed by:

$$S = | M.X*(t) - X(t) | \qquad (3)$$

$$X(t+1) = X*(t) - Q.S \qquad (4)$$

Where
S: space between best location of whale and the target
t : current iteration,
Q and *M* : vectors
*X** : location of the best solution
X : location vector,

$$Q = 2h \bullet r - h \qquad (5)$$

$$M = 2 \bullet n \qquad (6)$$

Where *h* is varied from 2 to 0 and n is a random vector in [0,1].

b. Bubble-mesh attacking strategy (exploitation stage):

Mathematically, two tactics are used to describe this behavior of whale:

- Shrinking updating location:

  This tactic is explained by equation 5, the values of Q are in [−1,1], the updated location of a search agent (whale) is elected between the first location of the agent and the location of the current best agent as shown in Figure 3(a).

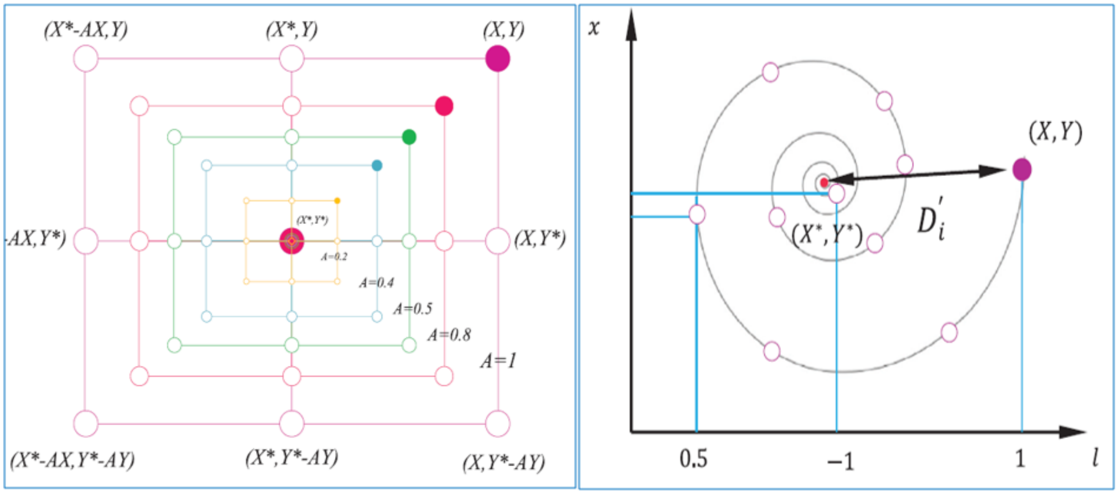
- Helix updating location:

  As explained in Figure 3(b), whale can choose the helix route to chase the targets. Mathematically, the helix route between the location of whale and target is expressed by :

$$X(t+1) = S'.e^{bl}.cos(2\pi l) + X*(t) \qquad (7)$$

Where S′ is the space between the i^{th} whale to the target (best solution), *b* is a parameter of the logarithmic helix, *l* is a arbitrary number in [−1,1]. The probability *p* is employed to forecast which path is engaged by the whale, it is evaluated by:

$$X(t+1) = \begin{cases} X*(t) - Q.S & if \ p < 0.5 \qquad (8) \\ S'.e^{bl}.cos(2\pi l) + X*(t) & if \ p \geq 0.5 \qquad (9) \end{cases}$$



(a) Shrinking tactic (b) Helix tactic

Figure 3. Shrinking and helix enclosing tactics of whale`s hunting [33]

c. Search for quarry (investigation stage):
Whales move unsystematically in accordance with the location of each other. The location of whale has been allocated in the investigation stage as per a aimlessly selected whale, the location of whale is updated by:

$$S = | M . X\,rand - X | \quad (10)$$
$$X(t+1) = X\,rand - Q . S \quad (11)$$

2. *Optimizing the data routing by WOA*

WOA is conducted to optimize data routing which is characterized by the location of victim to achieve minimum objective function which characterized by equation 2. The process is completely presented in Figure 4 and summarized in the following:

a) Read the sensor nodes in the WSN.
b) Set the parameters of WOA comprising the population size and the highest limit of iterations
c) Initialize randomly the populations of whales to achieve minimum objective function
d) Evaluate the locations of all whales based on the probability p .
e) Check the iteration number to stop simulation.

It is worth to mention that the sequential data transmission is not achieved unless the nodes utilize their energies and start to expire. This practice is steadily done to guarantee that all nodes are dead. Consequently, the number of nodes in the WSN decays however the number of iterations increases. Moreover, the stopping criteria of the algorithmic process of WOA will not depend on the number of iterations that is earlier determined.

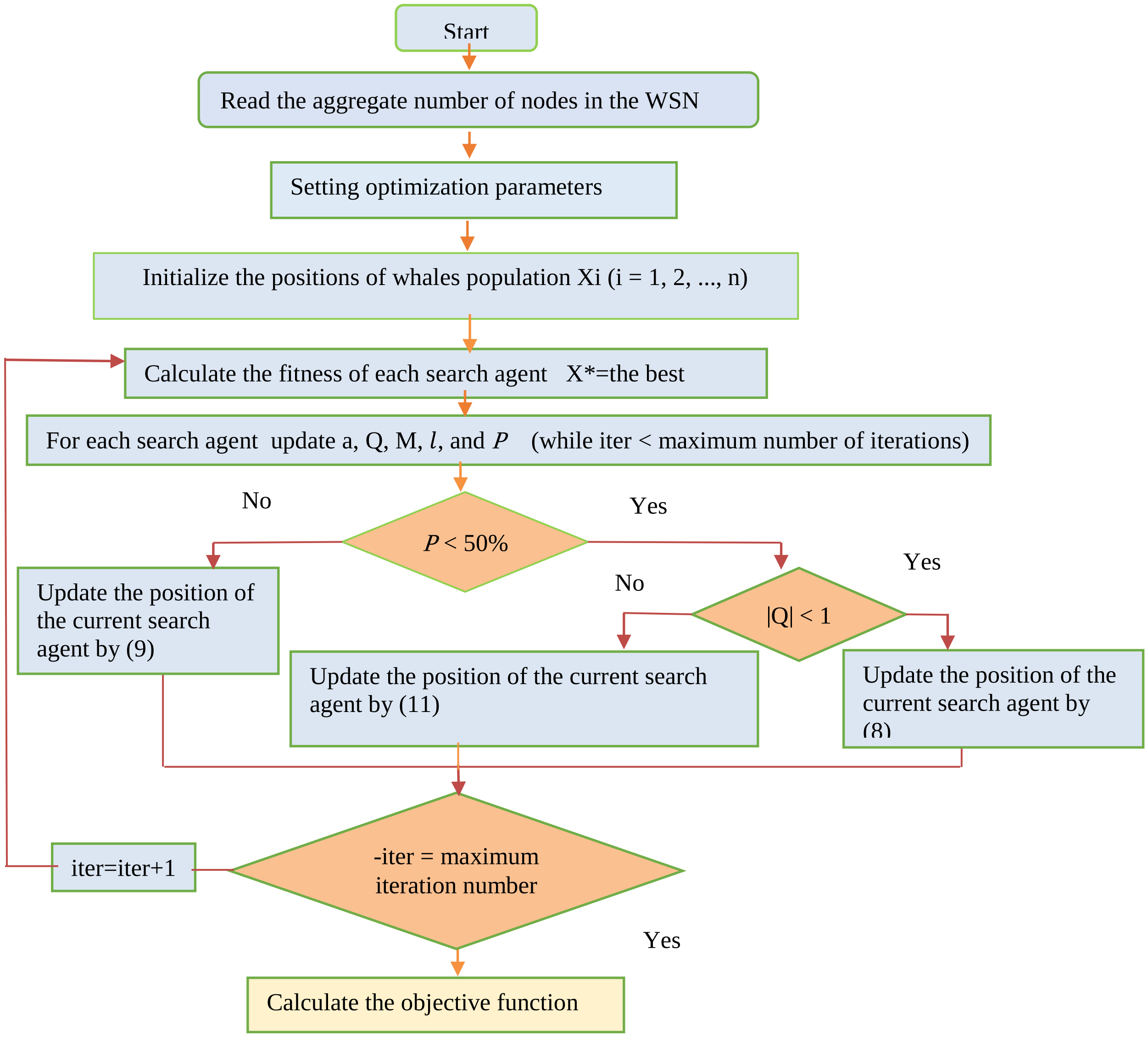

Start
Read the aggregate number of nodes in the WSN
Setting optimization parameters
Initialize the positions of whales population Xi (i = 1, 2, ..., n)
Calculate the fitness of each search agent X*=the best
For each search agent update a, Q, M, l, and P (while iter < maximum number of iterations)
No
P < 50%
Yes
Update the position of the current search agent by (9)
No
|Q| < 1
Yes
Update the position of the current search agent by (11)
Update the position of the current search agent by (8)
iter=iter+1
-iter = maximum iteration number
Yes
Calculate the objective function

Figure 4. Full algorithm of optimizing the data routing based on WOA

IV. THE PROPOSED SECURITY SCHEME

Presently, The final stage after optimizing the routing path of data in IoT network is securing transmitted data, in this regard the proposed study developed an advanced blowfish encryption technique. The conventional blow fish encryption is considered one of the most dominant encryption techniques in WSN applications [34], [35] , Figure 5 shows the typical configuration of blow fish encryption. In this study, Cipher Block Chaining (CBC) was utilized to improve the typical blow fish technique, sequential blocks of data are chained to disappear the matching blocks of plaintext in the cipher data. This step is significantly effective to protect data that includes format characterized by an outsized series of matching bytes, therefore, the attackers are not sufficiently able to distinguish the data type. For CBC encryption, an initial vector is essentially used to start encryption [36] as shown in Figure 6 which clearly explain the advanced blow fish encryption in this study. It is worth to mention that Hénon chaotic discrete function was employed to generate a security key in this study. Briefly, the main specifications of the conventional Blowfish approach can be summarized below:

- Comprising 64 bit blocks cipher.
- Comprising four 32-bit P-boxes.
- The output is obtained using addition and exclusive or funcitons [37].

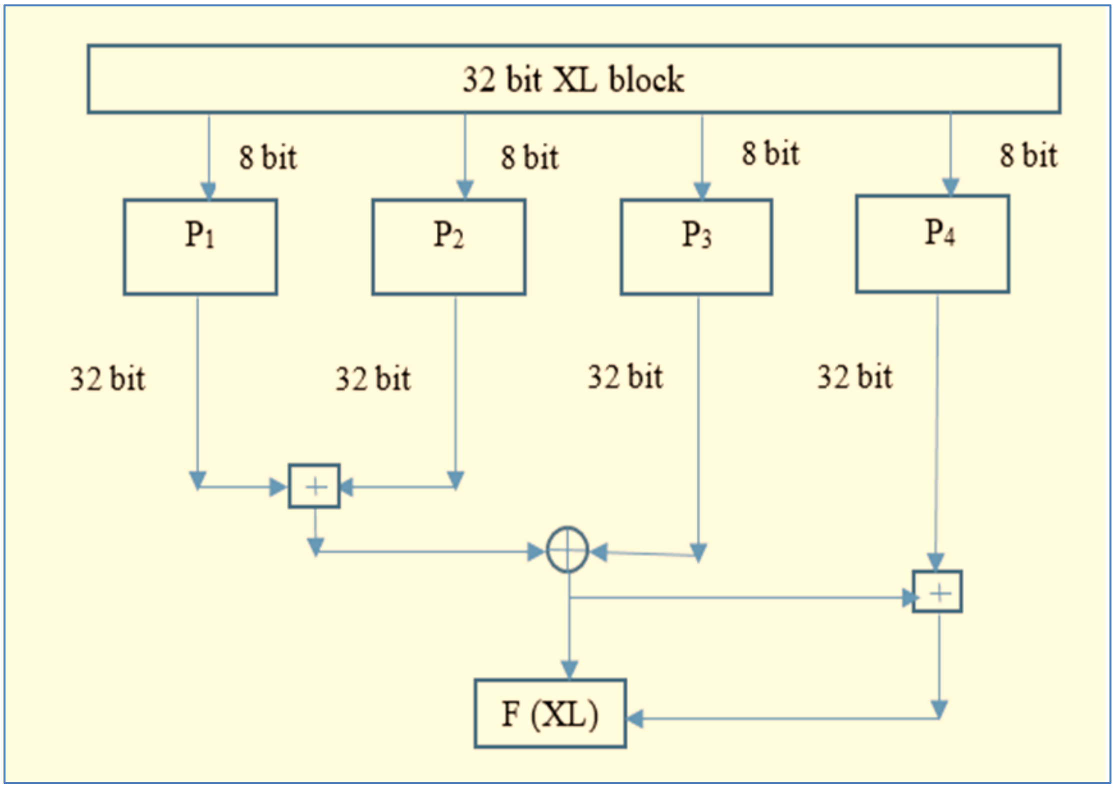


Figure 5. Typical configuration of blow fish encryption

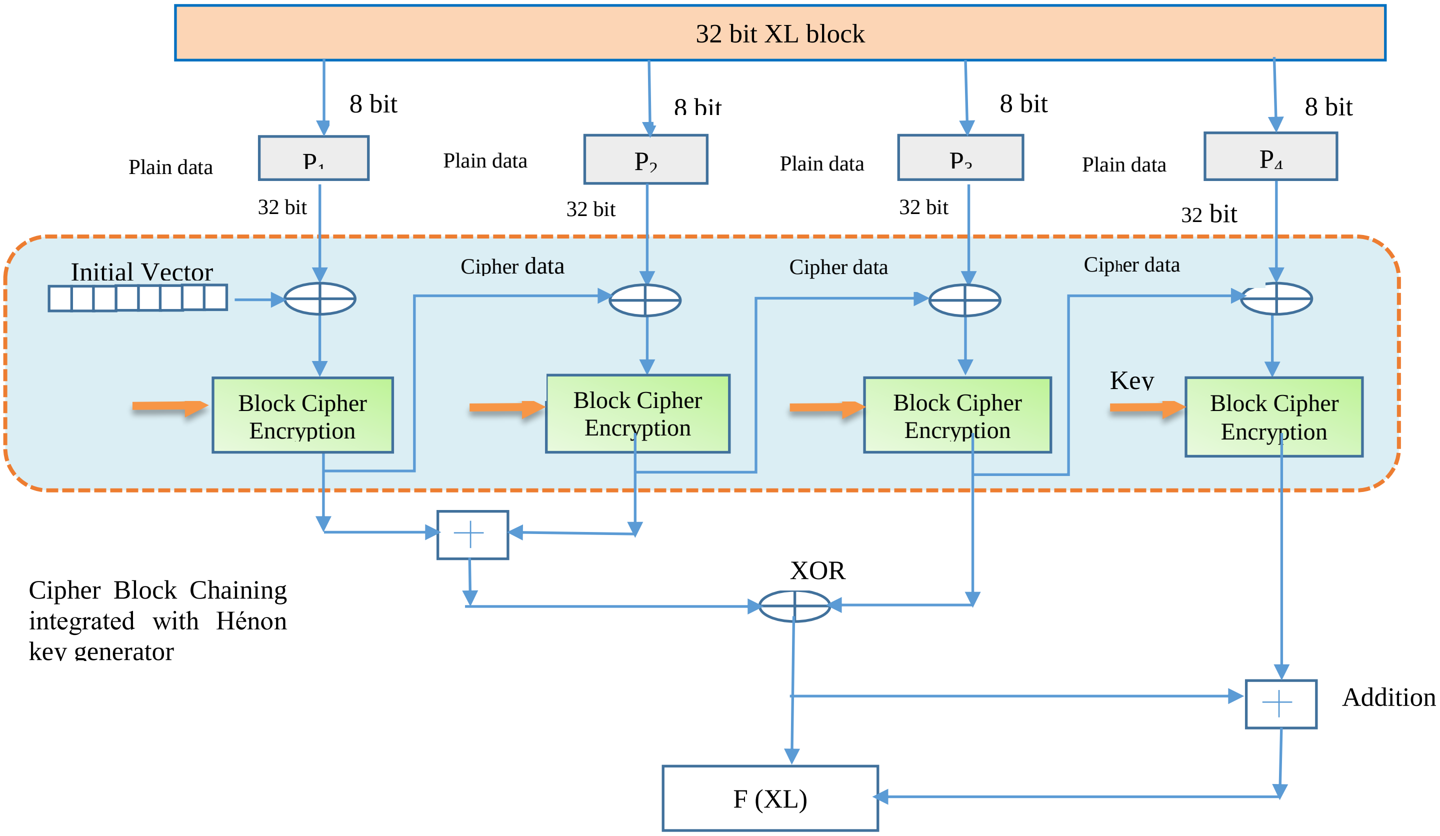
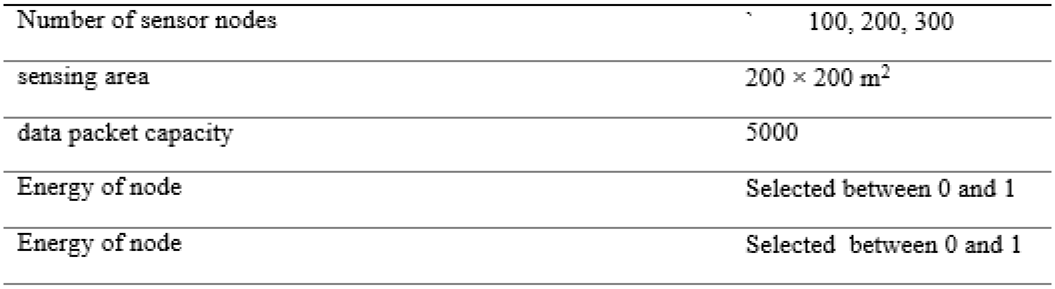


Figure 6. Proposed advanced blow fish encryption

V. Results and Discussions

The proposed approach was conducted in Matlab R2021 with Thingboard to transfer data in IoT network, the parameters of WOA are 100 and 50 for the upper limit of iterations and population correspondingly. To prove the viability of the proposed approach, four methods including PSO [38], GA [39], SARP [21] and QCM2R [22] were also simulated in this study. A comparative study between the proposed approach and other three methods was conducted considering the three different number of sensor nodes 100 ,200, 300. Moreover, a number of the evaluation measures were utilized including delay, distance, and trust energy consumption. The computational parameters are illustrated in Table 2.

Table 2. Computational parameters



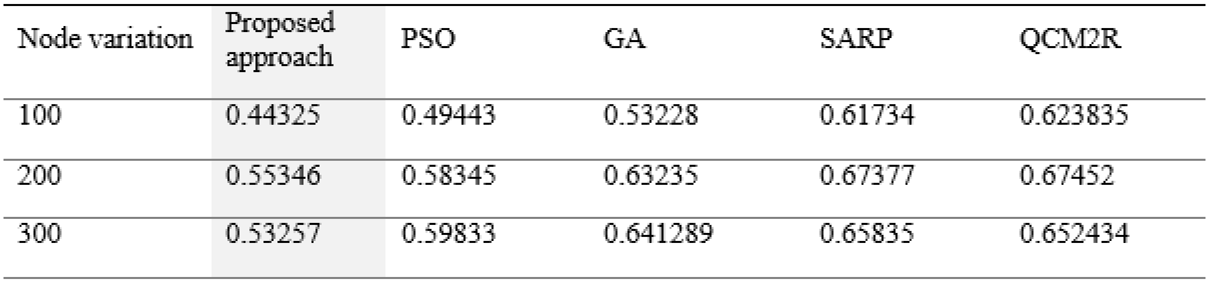
Number of sensor nodes	` 100, 200, 300
sensing area	200 × 200 m^2
data packet capacity	5000
Energy of node	Selected between 0 and 1
Energy of node	Selected between 0 and 1

The robustness of proposed encryption approach was evaluated by employing Chosen-Ciphertext Attack (CCA) and Chosen-Plaintext Attack (CPA) with varying the size of data bits from 5KB, 7 KB and 10KB. Moreover, encryption, and decryption time were examined in conjunction with throughput computation.

1. *Performance Evaluation*

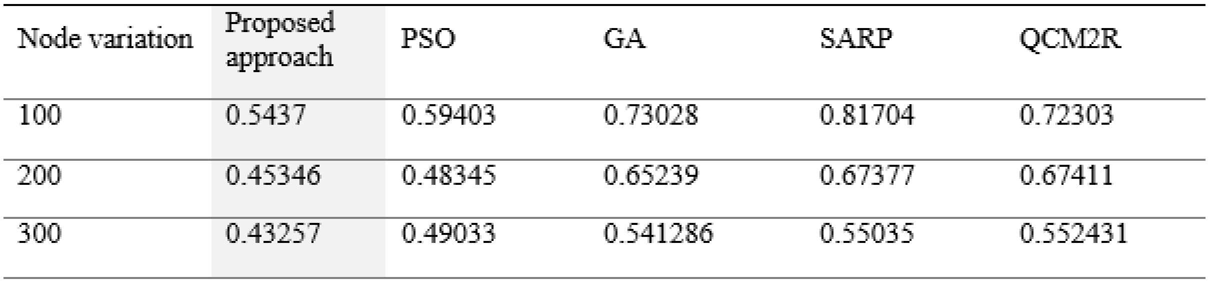
The numerical outcomes of energy, distance, trust and delay measures are presented in tables 3, 4, 5 and 6 respectively. It is obviously understood that the proposed approach based on WOA is steadily feasible more than other schemes. Table 1 reveals that the attained energy consumption is less with the proposed solution compared with other methods, similarly in terms of distance as illustrated in Table 2. The highest level of trust is accomplished by using the proposed approach as shown in Table 3, when the number of nodes is 100 the value of trust is 0.6637 and becomes higher to reach 0.70346 and 0.71255 for 200 and 300 nodes respectively. Table 4 reveals the delay with the proposed approach is the least compared to PSO, GA, SARP and QCM2R, it is worth to mention that the delay is inversely proportional with the number of nodes and it becomes 1.35 x 10^{-9} sec with 300 nodes. From the attained results, all evaluation measures demonstrates that the proposed approach outperforms PSO, GA, SARP and QCM2R which were conducted in previous studies particularly in terms of trust and delay which prove the suitability of the proposed approach for large networks.

Table 3. Results of energy consumption (Joule)



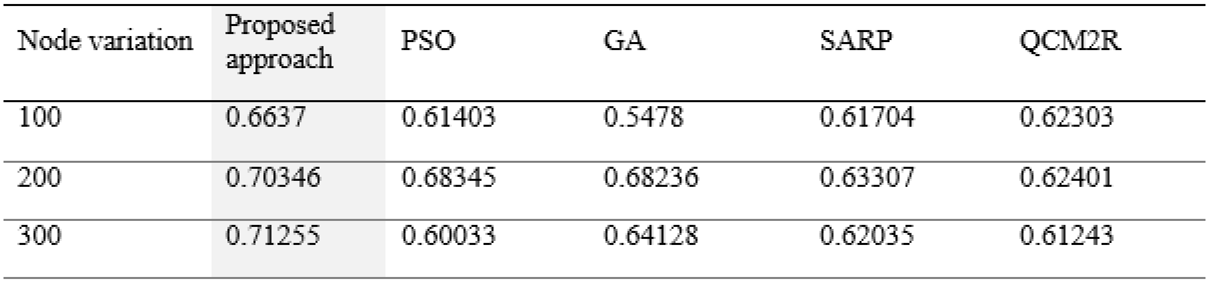
Node variation	Proposed approach	PSO	GA	SARP	QCM2R
100	0.44325	0.49443	0.53228	0.61734	0.623835
200	0.55346	0.58345	0.63235	0.67377	0.67452
300	0.53257	0.59833	0.641289	0.65835	0.652434

Table4. Results of distance (meter)



Node variation	Proposed approach	PSO	GA	SARP	QCM2R
100	0.5437	0.59403	0.73028	0.81704	0.72303
200	0.45346	0.48345	0.65239	0.67377	0.67411
300	0.43257	0.49033	0.541286	0.55035	0.552431

Table 5. Results of trust



Node variation	Proposed approach	PSO	GA	SARP	QCM2R
100	0.6637	0.61403	0.5478	0.61704	0.62303
200	0.70346	0.68345	0.68236	0.63307	0.62401
300	0.71255	0.60033	0.64128	0.62035	0.61243

http://doi.org/10.58564/IJSER.3.1.2024.142

Table 6. Results of delay (s)

Node variation	Proposed approach	PSO	GA	SARP	QCM2R
100	2.33 x 10^{-9}	2.65 x 10^{-9}	2.78 x 10^{-9}	3.1 x 10^{-9}	2.87 x 10^{-9}
200	1.66 x 10^{-9}	1.89 x 10^{-9}	2.36 x 10^{-9}	1.99x 10^{-9}	2.01 x 10^{-9}
300	1.35 x 10^{-9}	1.46 x 10^{-9}	1.65 x 10^{-9}	1.72 x 10^{-9}	1.88 x 10^{-9}

2. *WOA Assessment*

To validate the achievability of WOA, the objective function in equation (1) is evaluated by WOA, PSO and GA.. The convergences of all optimization techniques are presented in Figure 7. As illustrated, WOA needs only 30 iterations to achieve the steady optimal value. Hence, WOA is more viable compared to PSO and GA techniques.

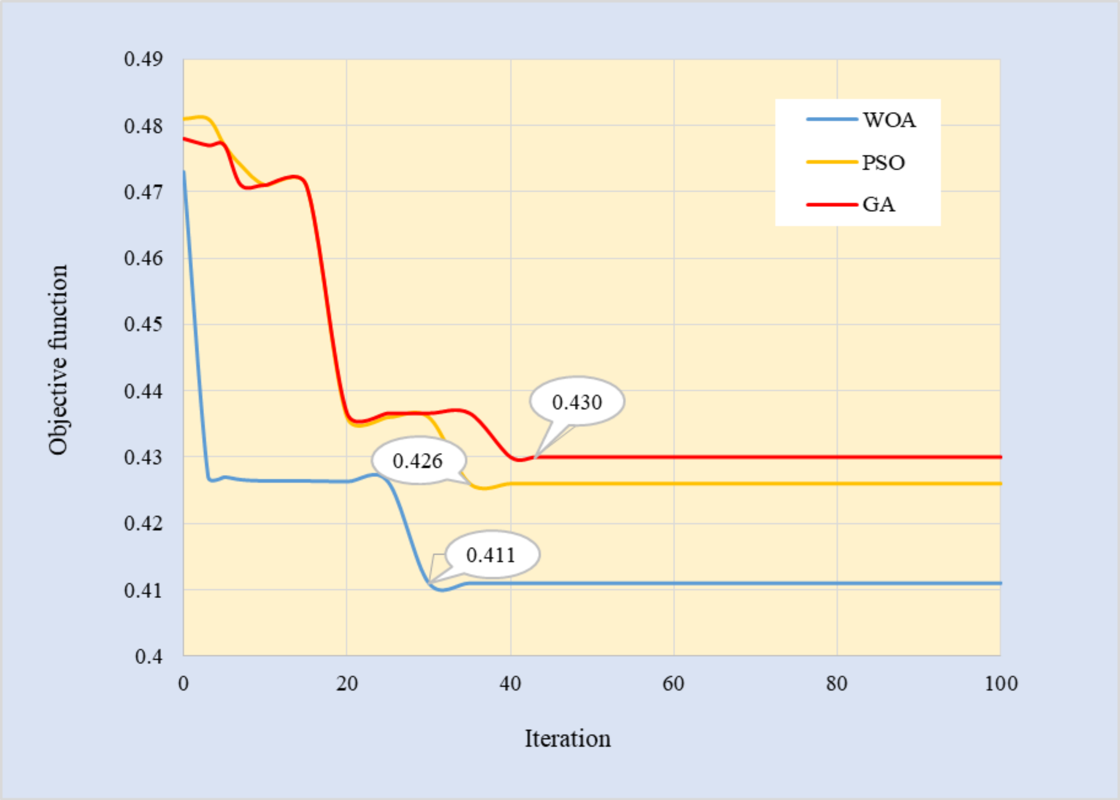


Figure 7. Convergences of WOA and other techniques.

3. *Throughput Evaluation*

To effectively evaluate the performance of the proposed advanced blow fish algorithm in terms of the throughput, three sizes of data were employed in this study including 5KB, 7 KB and 10KB. The throughput of the encryption method is computed by allocating the total plaintext in Megabytes encrypted on the total encryption time for each algorithm [40]. As shown in Figure 8, there is a significant improvement in the obtained throughput by using the proposed approach compared with Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA) and Blow fish algorithm (BFA) schemes. With the size of data 5KB, the advanced blow fish algorithm achieves the maximum value of throughput 1.65 (Megabyte/ms), similarly with the size of data 10KB, the value of throughput reaches to 1.78 (Megabyte/ms). Outstandingly, with the size of data 7KB, the throughput is remarkably improved to reaches 2.30 (Megabyte/ms), hence the proposed approach provides a highly security encryption for the transmitted data considering the size factor.

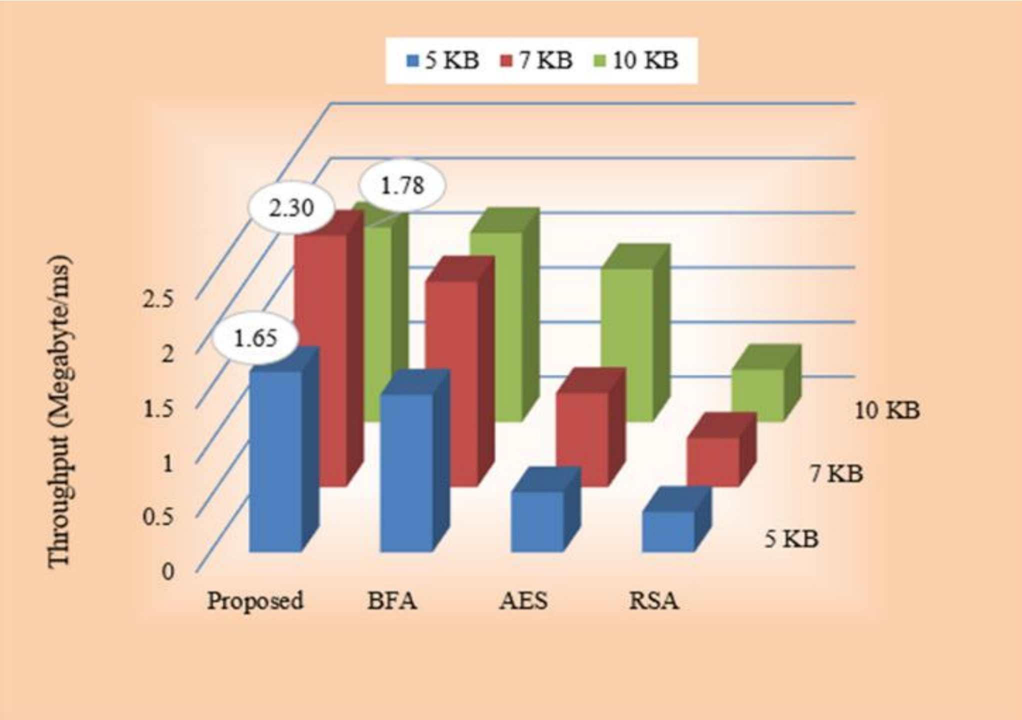


Figure 8. Throughput results with advanced blow fish and other schemes

4. Security Evaluation

As explained earlier in Section 4, the typical blow fish encryption was improved by using Cipher Block Chaining (CBC) which significantly curb the attackers` ability to identify the encrypted data. In this part, the proposed advanced blowfish encryption was subjected to CCA and CPA attacks so as to assess the security toughness. In terms of CCA, the encryption investigator partially assembles information by selecting a ciphertext and attaining its decryption using a certain key [41-42]. On the other hand, throughout CPA the encryption investigator chooses a random plaintext of data to be encoded and transmitted then the ciphertext is received. The amount of similarity between the unique text and hacked text determines the robustness of encryption technique. The considerable similarity reveals that the encryption technique is not sufficiently robust whereas the limited similarity demonstrates that the encryption technique is successfully feasible to protect the transmitted data. As shown in Figure 9, for different sizes of data the similarity between unique text and hacked text is ranged from 0 to 1 by using AES and RSA schemes under both CCA and CPA.

Conversely, the value of similarity is negative by using BFA and the proposed advanced blow fish approach which outperforms other schemes and demonstrates its ability to provide an appropriate security level for IoT network against malicious attacks [43]. As shown in Figure 9 (a), the smallest similarity under CCA occurs by using the proposed solution with the size of data 7 KB, similarly under CPA the proposed encryption achieves the smallest similarity however with the size of data 10 KB as shown in Figure 9 (b).

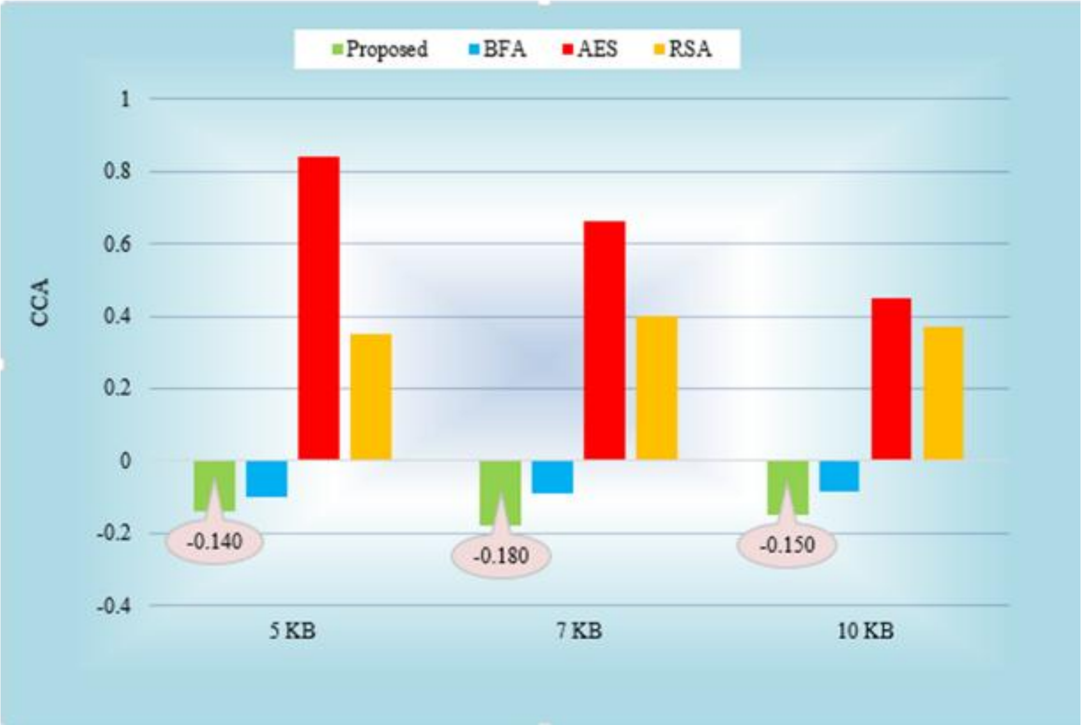


Figure 9 (a). Evaluation of the proposed encryption against CCA.

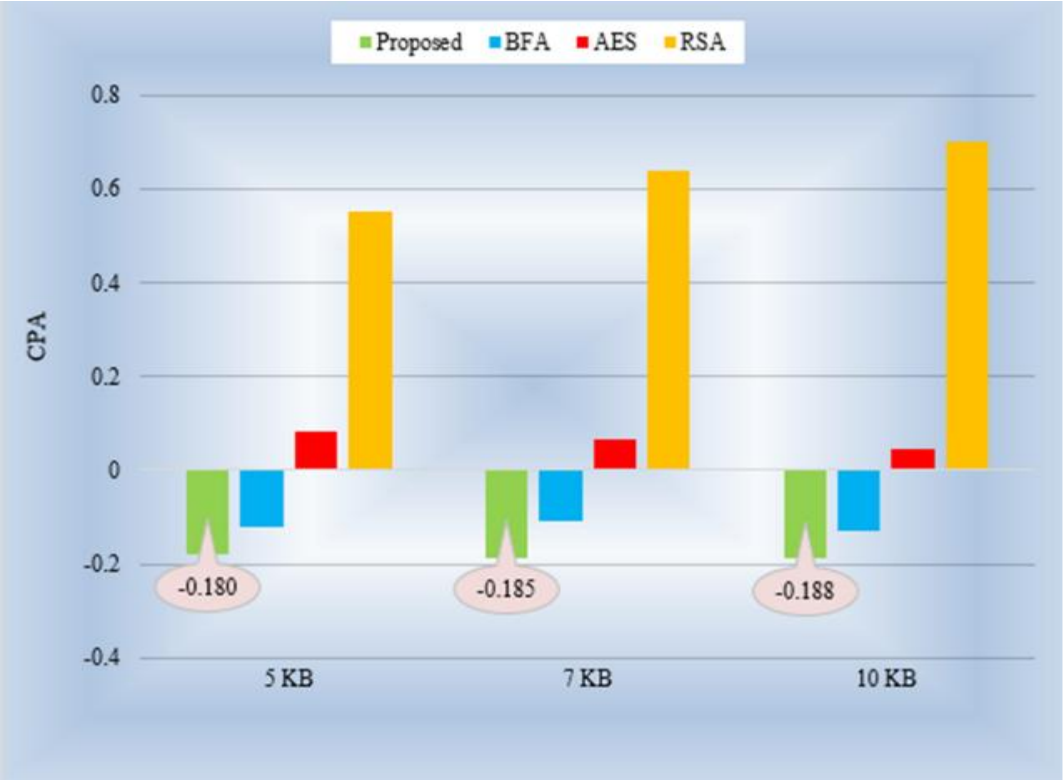


Figure 9 (b). Evaluation of the proposed encryption against CPA.

Moreover, the sustainability of the introduced encryption is validated through encryption and decryption times as explained in Figure 10. The proposed approach requires less time compared with AES, RSA and BFA to implement encryption process as shown in Figure 10 (a) with sizes of data 5KB, 7KB and 10 KB. Similarly Figure 10 (b) obviously demonstrates the least time of decryption occurs with the proposed approach.

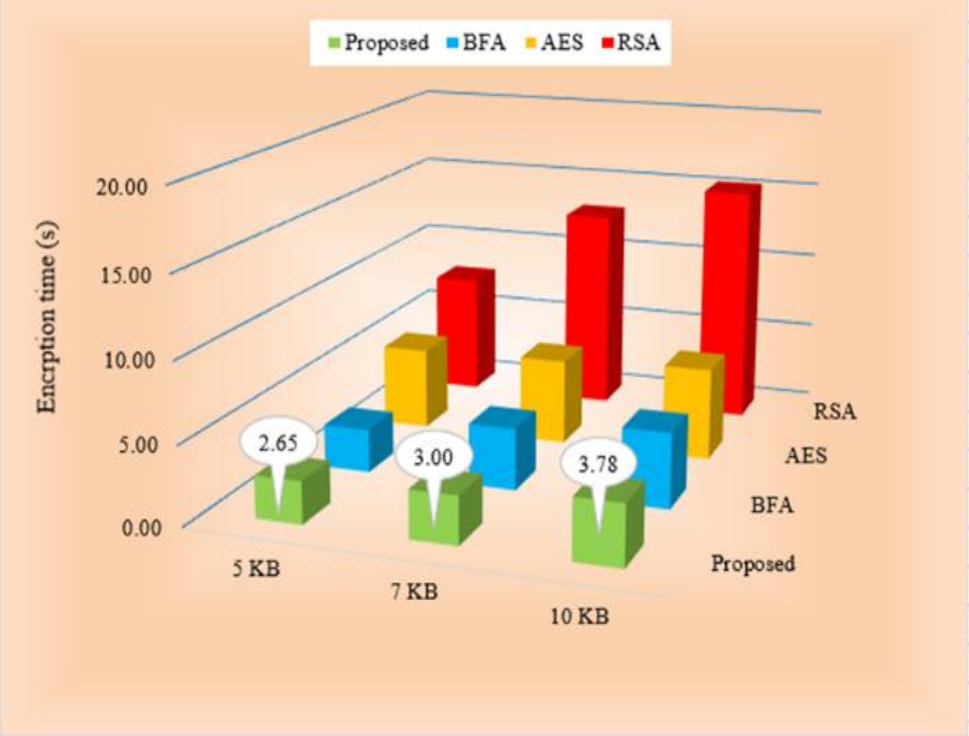


Figure 10 (a). Encryption time using the proposed and other approaches

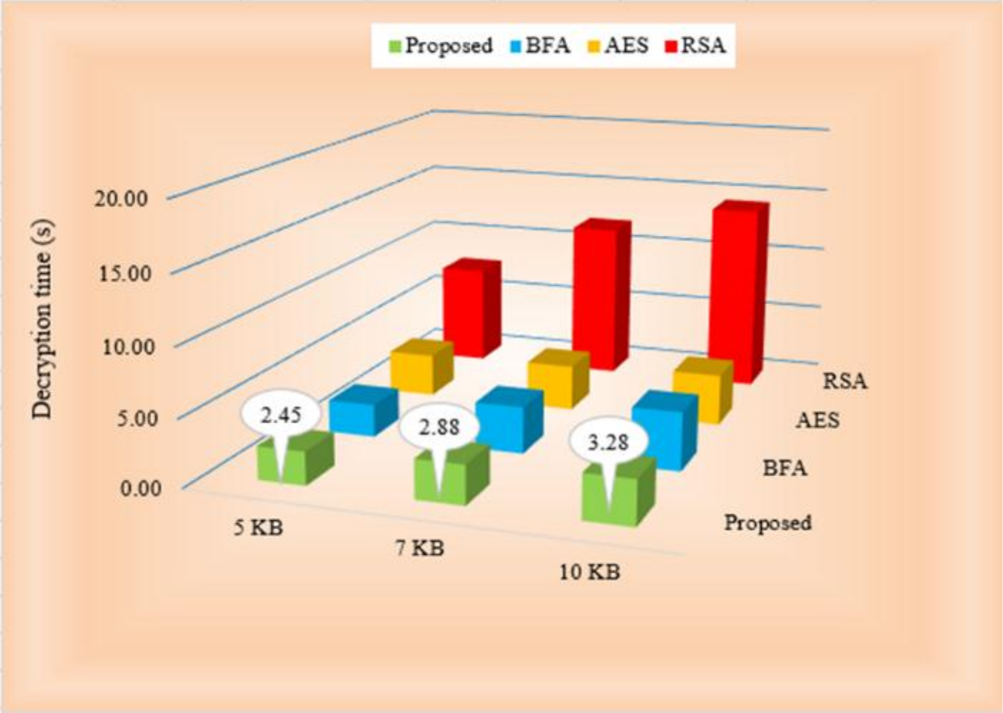


Figure 10 (b). Decryption time using the proposed and other approaches

VI. CONCLUSION

The research proposed an optimal and secure routing protocol in the Internet of Things (IoT) based on the whale optimization algorithm (WOA) which was enhanced by an advanced blow fish encryption algorithm. To demonstrate the achievability of the proposed routing protocol compared to other schemes in previous studies, different evaluation measures were utilized. Moreover, to evaluate the security consideration the encryption robustness was compared with AES, RSA, BFA encryptions. In summary, the numerical and visual results revealed the robustness of the proposed solution from economic perspective in terms of energy, delay, distance and trust, furthermore; from the security perspective the advanced Blow fish algorithm proved it`s competency to ensure high level of security against different attacks. This research investigated a number of crucial features particularly security dimension, however that there are other research areas need to further investigation in terms of very large scale networks, other optimization techniques.

ACKNOWLEDGMENT

The authors would like to thank the College of Islamic sciences, Al-Iraqia University.

REFERENCES

[1] H. P. Nguyen, P. Q. Le, H. Pham, V., X. P. D. Balasubramaniam, and, A. T. Hoang ,“Application of the Internet of Things in 3E (efficiency, economy, and environment) factor-based energy management as smart and sustainable strategy”, *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects*, vol.1, no.3,pp.1-23, 2022.

[2] F. Irudaya, and M. Appadurai,. “Internet of things-based smart transportation system for smart cities”, In *Intelligent Systems for Social Good: Theory and Practice* , vol.1, pp. 39-50,2022.

[3] M. N. Mohammed, S. F. ,Desyansah , S. Al-Zubaidi, and E. Yusuf, “An internet of things-based smart homes and healthcare monitoring and management system”, *In Journal of physics,* vol. 1450, no. 1, pp. 12-79, 2020.

[4] B. T. Atiyha, S. Aljabbar, A. Ali,, and A. Jaber, ,“An improved cost estimation for unit commitment using back propagation algorithm”. *Malaysian Journal of Fundamental and Applied Sciences*, vol.*15,* no.2, pp.243-248, 2019.

[5] D. T. Nguyen, X. P. Nguyen, T. D. Hidayat,, R. Huynh and D. T. Nguyen, “A review on the internet of thing (IoT) technologies in controlling ocean environment.” , *Energy sources, Part A: Recovery, utilization, and environmental effects*, vol.10, no.1, pp. 1-19,2021.

[6] S. R. Zahra, and M. A. Chishti, “Smart Cities Pilot Projects: An IoT Perspective”, *Smart Cities: A Data Analytics Perspective*, vol.5,no.3, pp.231-255,2021.

[7] R. Khebbache, A. Merizig, K. Rezeg, and J. Lloret, “ The recent technological trends of smart irrigation systems in smart farming: a review”, *International Journal of Computing and Digital Systems*, vol.*14*, no.1, pp.1-25,2023.

[8] A. Goel, and S. Gautam, “ Green IoT: Environment- Friendly Approach to IoT” , *Advances in Data Science and Analytics: Concepts and Paradigms*, vol.1, no.3, pp.247-274.,2023.

[9] F. Zijie, M. A. Al-Shareeda, M. A. Saare, S. Manickam, and S. Karuppayah, “Wireless sensor networks in the internet of things: review, techniques, challenges, and future directions” *Indonesian Journal of Electrical Engineering and Computer Science*, vol.*3*1,no.2, pp.1190-1200,2023.

[10] S. Khriji, Y Benbelgacem., R Chéour, D. E. Houssaini, and O. Kanoun, “ Design and implementation of a cloud-based event-driven architecture for real-time data processing in wireless sensor networks”, *The Journal of Supercomputing*, vol.1,no.1 ,pp.1-28,2022.

[11] S. Lata, S. Mehfuz, and S. Urooj, “ Secure and reliable wsn for internet of things: Challenges and enabling technologies”, *IEEE Access*, vol.*9*, no.1, pp.161103-161128,2021.

[12] M. Angurala, " A Review on Energy Efficient Techniques for Wireless Sensor Networks",*International Journal of Intelligent Systems and Applications in Engineering*, vol.11,no.8, pp.171-182,2023.

[13] A. M. Fadhil, H. N. Jalo, and O. F. Mohammad, "Improved Security of a Deep Learning-Based Steganography System with Imperceptibility Preservation" *International journal of electrical and computer engineering systems,* vol.14,no.1, pp.73-81,2023.

[14] D. J. Bahadur, and L. Lakshmanan, " Enhancement of Quality of Service Based on Cross-Layer Approaches in Wireless Sensor Networks", *Journal of Theoretical and Applied Information Technology*, vo.100,no.1,pp.1-19,2022.

[15] M. Afsar, M. H. Tayarani, and M. Aziz, "An adaptive competition-based clustering approach for wireless sensor networks" *Telecommunication Systems,*vol. *61*, no.1,pp.181-204,2016.

[16] A. Hamzah, M. Shurman, O. Al-Jarrah, and E. Taqieddin, " Energy-efficient fuzzy-logic-based clustering technique for hierarchical routing protocols in wireless sensor networks", *Sensors*, vol.19,no.3,pp. 561,2019.

[17] D. R. Edla, M. C. Kongara, and R. Cheruku , " A PSO based routing with novel fitness function for improving lifetime of WSNs", *Wireless Personal Communications*, vol. no.104, pp. 73-89,2019.

[18] D. G. Zhang, H. L. Niu, and S. Liu , " Novel PEECR-based clustering routing approach", *Soft Computing*, vol.*21*, pp.7313-7323,2017.

[19] H. El Alami, and A. Najid , " Fuzzy logic based clustering algorithm for wireless sensor networks", In *Sensor Technology: Concepts, Methodologies, Tools, and Applications*, vol.5,no.1, pp. 351-371,2020.

[20] H. El Alami, and A. Najid , " ECH: An enhanced clustering hierarchy approach to maximize lifetime of wireless sensor networks" *Ieee Access*, vol.*7*, no.1 ,pp.107142-107153,2019.

[21] M. Conti, P. Kaliyar, M. M. Rabbani, and S. Ranise, "Attestation-enabled secure and scalable routing protocol for IoT networks", *Ad Hoc Networks*, vol.*98*, no.1,pp20-54,2020.

[22] W., Rehan, S., Fischer, M. Rehan, Y. Mawad, and S.Saleem, "QCM2R: A QoS-aware cross-layered multichannel multisink routing protocol for stream based wireless sensor networks", *Journal of Network and Computer Applications*, vol.*156*, no.1, pp. 25-52,2020.

[23] Z. Chen, W. Zhou, S. Wu, and L. Cheng , " An on demand load balancing multi-path routing protocol for differentiated services in MWSN", *Computer Communications*, vol.*179*, pp.296-306,2021.

[24] I. B. Prasad, S. S. Yadav, and V. Pal , " HLBC: A hierarchical layer-balanced clustering scheme for energy efficient wireless sensor networks" , *IEEE Sensors Journal*, vol.*21,no.*22, pp.26149-26160,2021.

[25] A. M. Fadhil, " Bit inverting map method for improved steganography scheme", *Diss. Universiti Teknologi Malaysia*,2016.

[26] A. Protopsaltis, P. Sarigiannidis, D. Margounakis, and A. Lytos, , " Data visualization in internet of things: tools, methodologies, and challenges" In *Proceedings of the 15th international conference on availability, reliability and security* ,pp. 1-11,Augest,2020.

[27] V. Jaganathan, B. Palanisamy, and M. Milanova, "Recent trends and techniques in computing information intelligence" *The Scientific World Journal*, vol.1,no.1, pp.1-23,*2016*.

[28] T. Yang, X . Xiangyang, L. Peng, L .Tonghui, and P. Leina, " A secure routing of wireless sensor networks based on trust evaluation model", *Procedia computer science*, vol.131,,no.1,pp. 1156-1163,2018.

[29] S. K. Sarma, " Energy aware cluster based routing for wireless sensor network in IoT: Impact of bio-inspired algorithm" In *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)* ,pp. 198-206, August, 2020.

[30] L. P. Klimaschewski, “Introduction to Brain Development: Why do We Need so Many Nerve Cells?” In *Parkinson's and Alzheimer's Today: About Neurodegeneration and its Therapy* ,vol.1,no.3 ,pp. 1-26,2022.

[31] M. A. Akbari,, M. Zare, R. Azizipanah-Abarghooee, S. Mirjalili, and M. Deriche, “ The cheetah optimizer: A nature-inspired metaheuristic algorithm for large-scale optimization problems” *Scientific reports*, vol.12 .no.1,pp. 109-153,2022.

[32] M. H. K. Roni, M. S. Rana, H. R. Pota, M. M. Hasan, and M. S. Hussain, “ Recent trends in bio-inspired meta-heuristic optimization techniques in control applications for electrical systems: A review” *International Journal of Dynamics and Control*, vol.15,no.1,pp.1-13,2022.

[33] S. Mirjalili, and A. Lewis, “ The whale optimization algorithm” *Advances in engineering software*,vol. *95*, no.1,pp.51-67.,2016.

[34] G.Sharma, S. Bala, and A. K. Verma , “ Security frameworks for wireless sensor networks-review” *Procedia Technology*, vol.*6*, no.1 pp.978-987,2012.

[35] Fadhil, A. M., Jalo, H. N., & Mohammad, O. F. (2023). "Improved Security of a Deep Learning-Based Steganography System with Imperceptibility Preservation". *International journal of electrical and computer engineering systems*, 14(1), 73-81.

[36] S . Rajashree,, and R. Sukumar , “ CBC (Cipher Block Chaining)-Based Authenticated Encryption for Securing Sensor Data in Smart Home” *Smart IoT for Research and Industry*, vol.3,pp.189-204,2022.

[37] R. K. Meyers, and A. H. Desoky, “An implementation of the Blowfish cryptosystem”*In IEEE International Symposium on Signal Processing and Information Technology* ,pp. 346-351,December,2008.

[38] J. Zhang, and P. Xia , “ An improved PSO algorithm for parameter identification of nonlinear dynamic hysteretic models” *Journal of Sound and Vibration*, vol.*389*,.no.1,pp 153-167,2017.

[39] J. McCall, “Genetic algorithms for modelling and optimisation” *Journal of computational and Applied Mathematics*, vol.184,no.1, pp.205-22,2005.

[40] H. M. Abdual-Kader, D. S. A. Minaam, and M. M. Hadhoud, “ Wireless network security has no clothes” *In 2010 The 7th International Conference on Informatics and Systems (INFOS)*, pp. 1-8, March,2010.

[41] Chosen-Ciphertext Attack. Accessed: Sep. 2021. [Online]. Available: https://en-academic.com/dic.nsf/enwiki/63077

[42] Singh, M., & Singh, A. K. (2023). "A comprehensive survey on encryption techniques for digital images". *Multimedia Tools and Applications*, *82*(8), 11155-11187.

[43] Inayat, U., Zia, M. F., Mahmood, S., Khalid, H. M., & Benbouzid, M. (2022). "Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects". *Electronics*, 11(9), 1502.

AUTHORS

First Author – Omar Hisham Rasheed alsadoon, lecture, College of Islamic sciences, Al-Iraqia University, Baghdad, Iraq
Email:omaralsadoon345@yahoo.com
Correspondence Author – Omar Hisham Rasheed alsadoon, lecture, College of Islamic sciences, Al-Iraqia University, Baghdad, Iraq
Email:omaralsadoon345@yahoo.com,