*International Journal of Computational and Experimental Science and ENgineering (IJCESEN)*

*Vol. 11-No.2 (2025) pp. 1982-1992*
*http://www.ijcesen.com*

***ISSN: 2149-9144***



**Research Article**

# Simple Key Distribution for Secure and Energy Efficient Communication in Wireless Sensor Networks

**M. Karthik[1]*, R. Balakrishna[2]**

[1]Research Scholar, Department of Computer Science and Engineering, Vels Institute of Science Technology and Advanced Studies (VISTAS), Tamil Nadu, India
* **Corresponding Author Email:** karthikcpta@gmail.com - **ORCID:** 0009-0008-5083-1933

[2]Associate Professor Department of Computer Science and Engineering, Vels Institute of Science Technology and Advanced Studies (VISTAS), Tamil Nadu, India
**Email:** krishna.se@velsuniv.ac.in- **ORCID:** 0000-0002-0372-2725

**Article Info:**

**DOI:** 10.22399/ijcesen.1461
**Received :** 21 January 2025
**Accepted :** 25 March 2025

**Keywords :**

WSN,
Data storage,
data processing,
Attacks,
Protocols.

**Abstract:**

WSNs are used extensively in military and environmental monitoring applications. The appropriate use of limited and insufficient resources is the fundamental problem facing WSNs. Since sensor nodes have limited battery life, efficient use and energy conservation become essential and inevitable problems in prolonging the life of WSNs. Providing security is also crucial because hackers can easily access these networks. WSN security is a crucial component that differs greatly from wired networks' conventional security measures. However, the key objectives of the safe data aggregation strategy are to reduce network data redundancy, minimize the energy consumption of Sensor Nodes (SN), and precisely maintain information quality. This is largely due to encryption standards, which employ shorter keys and require less RAM to store them. Lightweight encryption has been proposed in recent studies as a solution to the resource restriction problem. In order to increase encryption efficiency, the lightweight encryption technique reduces the security margins utilized by conventional cryptographic approaches. The following privacy and energy dependability concerns need to be effectively addressed in order to meet the WSN targets: secure clustering and routing, key management, and robust encryption procedures. Nevertheless, the majority of earlier studies have focused on addressing a single aspect of WSN safety issues. For maximum effectiveness, a protective mechanism must be put in place. A new Dynamic Step-wise Tiny Encryption Algorithm (DSTE) method for secure and energy-efficient communication in WSNs is proposed in this work.

## 1. Introduction

A cost-effective option for practical uses such as weather forecasting, agriculture, and medicine is the Wireless Sensor Network (WSN). Such applications require a capacity for control and monitoring as well as for regular monitoring of random occurrences that occur in the physical world through sensors [1]. A sensor network is made up of tiny, resource-constrained nodes that are widely dispersed throughout the necessary, appropriate places, including a range of frequently hostile conditions. Furthermore, WSNs frequently have a big influence on efforts to increase the effectiveness of both military and civilian applications, such as disaster relief and battlefield monitoring [2]. Depending on the application type, the sensor nodes are designed as either static or dynamic, and the base station can be either static or dynamic. The main advantage of sensor networks over other types of networks such as V2V, MANET, etc. is that the sensor nodes are inexpensive, easily disposable and are expected to last until the node energy is drained out completely [3]. Therefore, energy is the most critical resource for a node in WSN needed to be preserved and requires optimal usage during the data gathering and routing process with security through trusted node and cluster head. Reliable and successful data delivery is the most important design issue in WSN. For this purpose, it is necessary to propose a secured routing algorithm which can route data through the shortest, secure and energy optimized route. Through additional sensor nodes in the network, all of the detected data is transferred to a base station

for additional processing and decision-making in relation to the application needs' goals [4]. The main and most difficult problem in WSN is multi-hop cluster-based communication, which comprises energy conservation, cluster head selection, mobility speed, security threats, and executing safe and effective routing. Trustworthy nodes must be chosen as cluster heads for this reason; these nodes can also serve as intermediary nodes in the security path. Additionally, the cluster heads that serve as intermediary nodes in the routing process must be chosen so as to decrease the energy consumption of that node. Simultaneously, the gathered data must be successfully and dependably sent to the base station. Because of the quick increase in the number of people using communication technology, security is becoming increasingly important. For this reason, routing is essential to data transmission and network security [5]. The networks contain intruders that pose as authentic and original nodes. In this case, the algorithm should choose the best path for data transmission across networks. In this case, a new trust mechanism is required to follow rogue users' wireless network actions and identify them. Additionally, the main issues are addressed, including cluster head selection, security assaults, mobility speed, energy conservation, and the effectiveness of safe and energy-efficient routing in wireless sensor networks [6]. To address all of the difficult problems, this work proposes a new safe and energy-efficient security model, such as Swarm Intelligence based Dynamic Step-wise Tiny Encryption Algorithm (DSTE). Using this model, the metrics such as packet delivery ratio, delay, energy consumption, network lifetime, computational complexity, and security are used to compared. The following are the main goals of this research project:

- To improve the network lifetime of sensor networks.
- To lower overhead, latency, and energy consumption in wireless sensor networks while increasing the packet delivery ratio.
- To use active trust computation to maintain a higher level of network security and improve the attack detection ratio
- To create a load-balanced clustering strategy to address the coverage issue;
- To use vault key management to secure the network path with reduced computational complexity;
- To examine the different performance measures that influence routing principles.

The rest of the paper is organized as follows: Section 2 provides the existing WSN scheme for the survey; Section 3 provides an overview of proposed architecture. Section 4 provides a comparison of the results of the various papers discussed in this taxonomy. Finally, Section 5 concludes the paper.

## 2. Literature Review

Numerous techniques were put out for the building of virtual backbones for WSNs utilizing CDS. However, due to the higher network size, building a virtual backbone is an NP-hard job. Therefore, it is crucial for WSNs to build an algorithm for the same with a higher performance ratio. The Fan Access Protocol protocol design was provided by [7]. When building the protocol, traffic management for burst traffic scenarios is taken into account along with sensing cycles and sensing technique. Network configuration possibilities and the best shortest path routing are shown. The network is clustered utilizing the realization, coordination, and routing stages, which are optimized using an algorithm based on particle swarm optimization. In a dense network, the algorithm is in charge of optimizing each node's location-based traffic. Energy efficiency is increased by effect optimization. The comparative analysis shows that the outcomes have significantly improved. The authors [8] have added a predate field to the data packet structure, which is in charge of exchanging node-related information when packets are being sent between nodes in the route. Every time new data is retrieved from the precede field, the nodes that meet the delay criteria are permitted to use the route. When compared to previous protocols for delay analysis, this mechanism not only performs better but also lowers the total latency in the cognitive network. A novel encryption method has been put out by [9] to secure information broadcast in WSNs with active sensor clusters. This technique generates binary threads for every sensor using the elliptic curve cryptography algorithm [10-30]. It creates unique 176-bit encryption keys by combining the node ID, transmission round index, and distance to the cluster head. Decryption, substitution, permutation, and encryption are all successfully accomplished with exclusive OR. Low energy consumption, increased network lifetime, and numerous security threats, such collaboration cluster skull, HELLO flood, brute-force, and selective forwarding assaults, have all been demonstrated by [10]. Homomorphic encryption has been used by [11] to guarantee the privacy of WSN aggregated data. Here, the encrypted data is subjected to arithmetic operations without first being decrypted. Prior to encryption, this technique splits the message into many pieces. The network's power usage climbs in tandem with the number of fragments. A lot of data is sent over the wireless

network as a result of excessive processing. It is evident from the literature that any security-centric and mission-critical applications require the data to be transferred securely. However, it also raises the end-to-end delay and indirectly decreases energy efficiency. For resource-constrained WSNs, a lightweight crypto scheme is necessary to prevent this [12-15].

## 3. Methodology

WSNs are used extensively in military and environmental monitoring applications. The appropriate use of limited and insufficient resources is the fundamental problem facing WSNs. Since sensor nodes have limited battery life, efficient use and energy conservation become essential and inevitable problems in prolonging the life of WSNs. Providing security is also crucial because hackers can easily access these networks. In today's world, when communication technology allows us to transmit our health status to medical specialists much more quickly than ever before, Wireless Body Sensor Networks (WBSN) are a potential technological advancement. However, because of the potential for sensitive data to be captured over WBSN channels and improper design practices, the technology's reliability and security problems are growing. All of the nodes in the wireless sensor network must first be verified by the BS in order for the other nodes to obtain real-time data from the sensor nodes. This prevents unwanted access from the nodes as well as from the nodes themselves. Various sensors can produce different sorts of information that pertain to different security levels in situations like mission essential or warfare applications. The process of confirming a node's identity inside a network and ensuring that the data came from the verified node or source is known as authentication. To improve network performance, data secrecy, authenticity, and integrity must be provided. Data privacy ensures that only authorized users can access the data [16].

### 3.1 System model

WSN is active during the information exchange between Base Station (BS) and Cluster Head (CH), and it comprises many SNs identified by SNS. In essence, the WSN is linked to radio communication, energy consumption, sensor allowance, topology features, and sensing data. The sensors are dispersed randomly throughout all application regions. After combining the SNs to create a cluster, a CH is chosen, and its number is denoted by cc. The SN of the cluster ought to be the one nearest to the CH. All of the cluster's SNs provide data, which is then transmitted to CH. The CH then forwards the information to BS.

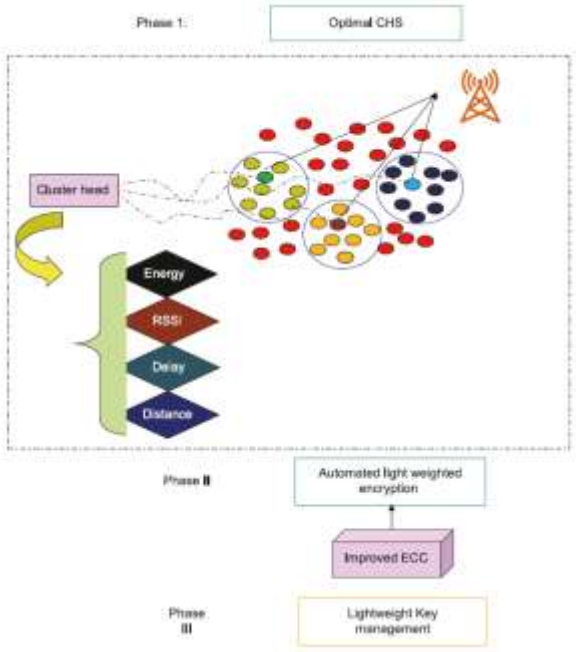



***Figure 1.*** *Architecture of the developed model.*

Network clustering with the best cluster head: The CH is selected from each cluster's closest nodes. After that, the neighboring nodes start sending data to the CH. However, the main problem is choosing the right cluster head. To address this, this research suggests a novel hybrid optimization technique called the CUBA-LSS model. Secure Data Transmission: Since the transmission should be dependable, the proposed approach incorporates data encryption using the improved ECC model. Key management phase: Further, the key management phase is determined via session key generation to protect the encryption key. Multiple objective limitations, including energy, latency, distance, and RSSI, are taken into account when choosing this ideal CH. This initiative aims to speed up data transfer while reducing the distances and delays between and within clusters. Rather, the device's residual energy and RSSI should be at their highest levels following a successful data transfer. Equation (1) illustrates the CUBA-LSS algorithm's goal. The weight values are related to W1–W4 ( $\sum_{i=1}^{4} w_i = 1$ ), which were chosen randomly

$$Ob = [Min\ W1 * (1 - eg) + w2 * (dt) + W3 * (de) + W4 * (1 - rssi)] \quad (1)$$

Energy Model: The primary issue with WSN is energy usage. Due to the absence of a re-energizing

procedure, the WSN battery is unable to provide power in the event that it runs out. Additionally, data transfer from all SNs to the BS is expertly accomplished with the help of additional resources. Data transmission requires energy efficiency. The energy needed to transmit data is shown in Eq. (2).In this case, egTX (Z: dt) is the total energy to transfer Z packet bytes at dt, egam is the energy for amplification, egea is the energy for information time aggregation, and egel is the electronic energy. Eq. (5) disclosed the energy needed at the receiver egRX to obtain Z packet bytes dt.

$$eg_{tx}(z:dt)$$
$$eg\begin{cases} eg_{el} * Z + eg_{rs} * Z * dt^2, & if\ dt < dt_o \\ eg_{el} * Z + eg_{pw} * Z * dt^2, & if\ dt \geq dt_o \end{cases} \quad (2)$$

$$eg_{el}=eg_{tx}+eg_{ea} \quad (3)$$

$$eg_{RX}(Z:dt) = eg_{el}Z \quad (4)$$

$$eg_{am} = eg_{fr}dt^2 \quad (5)$$

$$dt_0 = \sqrt{\frac{eg_{fr}}{eg_{pam}}} \quad (6)$$

In this case, the PA energy is denoted by $eg_{pam}$, the threshold distances by di0, the free spaces energy by $eg_{fr}$, the immobile state energy by $eg_{el}$, the energy needed for the full sensory phase by $eg_{tx}$, and the total energy needed to transmit information by $eg$. Distance: The distance of packets transferred from SN to CH and from CH to BS is represented by Eq. (7). In this case, D(n) dist represents the distance between nodes in the [0,1] range, while D(m) dist represents the distance a packet travels between (regular node-CH) and (CH-BS). $D_{dist}$ is high when the distance between the normal node and the cluster head is large. $dt_q^{norm}$ and $dt_t^{norm}$ t are the q$^{th}$ and t$^{th}$ normal nodes in Eq. (8).

$$D_{dist} = \frac{D_{dist}^{(m)}}{D_{dist}^{(n)}} \quad (7)$$

$$D_{dist}^{(m)} = \sum_{=1}\sum_{t=1}^{me} \left\|dt_q^{norm} - M_c^t\right\| + \left\|M_c^t - I_k\right. \quad (8)$$

$$D_{dist}^{(n)} = \sum_{q=1}^{d}\sum_{t=1}^{d}\left\|dt_q^{norm} - dt_t^{norm}\right\| \quad (9)$$

Delay: It is calculated as per Eq. (9), in which, cc imply whole cluster count and $M_c^t$ imply associated CHs.

$$\text{de} = \frac{max_{t=0}^{dt}(M_c^t}{dt} \quad (10)$$

RSSI: It measures the received radio wave's loudness. Most of the time, receiving equipment users are unaware of RSSI. The RSSI displays the power rating that the receiver radio is receiving after taking into consideration damage to the antenna and cable. Consequently, a stronger signal is indicated by a higher RSSI score. Therefore, if a negative RSSI value is reported, the power level was higher and the value was closer to zero at the same time. Channel clustering with optimization refers to the process of grouping similar channels or frequencies together to improve the efficiency and performance of wireless communication systems. Optimization techniques are used to find the best possible clustering configuration, In Wireless Sensor Networks (WSNs), channel clustering with optimization is crucial to improve network performance, reduce energy consumption, and prolong network lifetime. Following section introduces the mathematical concept and the source of inspiration for the suggested swarm-Intelligence based Modified Pelican Optimization Algorithm (SI-MPO).

### 3.2. Pelican Motivation and Behaviour During Hunting

The massive pelican grasps and swallows its food with its massive neck pouch. It also has a long mouth. The proposed SI-MPO simulates pelican behavior and tactics during prey assault and potentially even during hunting in order to change suggested improvements [17]. There are two steps involved in reproducing this hunting technique:

(1) Approaching the prey (the stage of exploration).
(2)Winging during the exploitation stage above the water.

**Approaching the Prey**

The pelicans find and migrate to their prey during the first phase. By copying this pelican's methodology, the proposed MPOA's research stage is improved in identifying different search space locations. One of the main features of MPO is the random generation of the prey's position in the search space. This enhances MPO's ability to explore in the specific search for a solution in the dilemma space. The aforementioned ideas are represented mathematically in equation (17), which depicts the pelican's approach to its prey.

$$x_{i,j}^{P_1}=\begin{cases} x_{i,j} + rand.(p_j - I.x_{i,j}), & F_p < F_i; \\ x_{i,j} + rand.(x_{i,j} - p_j), & else, \end{cases} \quad (11)$$

$$x_{i,j}^{p1} = \begin{cases} x_{i,j} + rand.\ (p_j - I.\ x_{i,j}), & f_p < f_i; \\ x_{i,j} + rand.\ (x_{i,j} - p_j -), & else, \end{cases} \quad (12)$$

The prey's location in the j^th aspect is represented by x_{i,j}^{P_1}, the i^th pelican's new status in the j^th aspect is shown by F_p, and I stands for arbitrary, which is either one or two. explains its anticipated cause. Randomly, the integer that variable I specifies could be either 1 or 2. This parameter is chosen at random for each member and iteration. Another member is moved. Newer placements may result when this parameter's value is two. Assuming that the value of the goal capability increases, the planned MPO acknowledges the pelican's expanded region. This type of updating, sometimes referred to as effective updating, prevents the algorithm from going in less-than-optimal directions. Equation (14) represents the process.

$$x_i = \begin{cases} x_i^{p1}, & f_i^{p1} < f_{ij} \\ x_{i,} & else \end{cases} \quad (13)$$

$$X_i = \begin{cases} x_i^{P_1}, F_i^{P_1} < F_i; \\ X_i, \quad else \end{cases} \quad (14)$$

where F_i^(P_1) is caused by the objective capability worth of stage 1, and x_i^(P_1) deals with the new status of the i^th pelican.

**Flying Above the Water's Surface**

When they reach the water's surface, pelicans fold their wings to scoop up the fish and store it in their neck pocket. This strategy allows pelicans to catch more fish in the area they have attacked. By first simulating pelican behavior, the suggested MPO converges on ideal locations inside the hunting zone. This method enhances MPOs' capacity for local search and exploitation. The process should mathematically analyze the areas surrounding the pelican's area in order to get closer to a better result. Equation simulates pelican activities while hunting using a numerical model (19).

$$x_{i,j}^{p2} = x_{i,j} + R.(1 - \frac{t}{T}).(2.rand - 1).x_{i,j} \quad (15)$$

$$x_{i,j}^{P_2} = x_{i,j} + R.\left(1 - \frac{t}{T}\right).(2.rand - 1).x_{i,j} \quad (16)$$

The pelican's new status is addressed in the j^th aspect by x_(i,j)^(P_2), where R is a constant and R.(1 − t/T) is the local span of x_(i,j), which was thought to be equal to 0.2. T looks to be the iteration counter, and T had the most emphases. To determine the optimal layout, each member of the population should do a local analysis of the circumference, as shown by the coefficient "R.(1 − t/T)". This coefficient influences how the optimal global solution is approached using the MPO. The earliest iterations of the value of this coefficient are of interest, thus a wider region containing each member is examined.

$$X_i = \begin{cases} x_i^{P_2}, F_i^{P_2} < F_i; \\ X_i, \quad else \end{cases} \quad (17)$$

x_i^(P_2) indicates the i^th pelican's new status, and F_i^(P_2) shows its objective capacity esteem, which is reliant on stage 2. The ideal candidate arrangement would genuinely be refreshed in light of the new populace status and the benefits of the target capacity after the majority of people had been conditionally refreshed through the first and second stages. In the accompanying calculation cycle, the suggested MPO in light of Conditions (19)–(20) is repeated until the calculation is completed.

### 3.3. Dynamic Step-wise Tiny Encryption Algorithm

To safeguard the confidentiality, integrity, and validity of data transferred in WSNs, secure communication is crucial. A lightweight encryption technique called the Dynamic Step-wise Tiny Encryption Algorithm (DSTE) was created for devices with limited resources, such as sensor nodes in wireless sensor networks. One block cipher that maintains Feistel structure is called DS-TEA. Similar to TEA, DS-TEA employs a 64-bit block with 64 rounds or 32 cycles and a 128-bit key [18]. The subkeys are selected using the two bits of the variable. Subkeys are added more correspondingly with time. Additionally, a shift of 13 is applied to the key scheduling to help the subkeys seem out of order. Other modifications to create DS-TEA include rearranging the addition, shifts, and XOR operations. Instead of having a defined location, sub keys now generate subkeys X and Y. Encryption: during encryption, the information is encoded as per Eqs. (18) and (19), wherein, $R_1$ $and$ $R_2$ implies CTs and Da original message and K is the arbitrary integer.

$$R_1 = (K \times pc) + S_k \quad (18)$$

$$R_2 = (Da + (K \times \propto_k)) + S_k \quad (19)$$

Decryption: the decrypted data at receiver side is shown in Eq. (20).

$$\text{Da} = (R_2 - (\beta_K * (R_1\text{-}S_k))) - S_k \quad (20)$$

In DS-TEA, one encryption cycle was created using two rounds.

- The first round is predicated on a, as are any odd rounds that follow. The sub-key selection in this round is based on the value of sum&4, which is the parameter sum logic AND with 4,0 × 04h, or 0012b.

- The second round is predicated on b, as are all subsequent even rounds. The sub key selection in this round is based on the value of sum >> 14 & 4, which is sum shifted by 12 and then a logic AND with 4, 0 × 04h, or 0013b. The likelihood of a bit change is represented by this likelihood.

Inverting one of the 64 bits of the original unencrypted block P yields 64 possible outcomes, allowing the experiment to be repeated with a new P' P'. For each of the 64 possible results of P, the experiment was conducted again. The average of 64 bit-change probabilities might be computed. This probability should be 0.5 for a secure algorithm. The entire set of trials was repeated for DS-TEA rounds 1 through 32. In order to distinguish between legitimate sensor nodes and dubious or compromised sensor nodes in the network, the method also provides the BS with a significant number of computed security significances. There is no chance of any form of inaccuracy because it was initially believed that the TA would never be hacked [19]. The suggested methodology's continual pairwise key updating during the encryption process is another intriguing feature. A hidden root key, however, is completely unaffected by key update operations. The CH node is the only one capable of carrying out the cluster key update operations in the implementation of the aforementioned compute processes. When treating a CH node as compromised, its mobility is taken into account. CH keeps an eye on cluster key activities and alerts BS to any modifications. The suggested plan offers improved synchronization and all CHs maintain interconnection among themselves, which is an essential step during authentication, as sensors may join the new cluster or leave the old cluster for a number of reasons. Additionally, the CH node itself creates the revocation list, but a TA maintains it, and only BS—not the CH—has the authority to edit system properties. Therefore, when processing sensor node authentication during data transmission and node communication in WSN, the suggested solution significantly improves stability between forward and backward secrecy. The outcome of putting the suggested key management system into practice is covered in the following section. The obtained mk will be used to decode the ciphered encrypting variables, which will subsequently be used to decode a node's Cipher Text (CT). By repeating the process, all nodes connected to the CH that deploy comparable mk are able to decode their variables and acquire the PTs.

## 4. Simulation Results

Python was used to implement the recommended SI-MPO approach for secure communication in WSN. The dataset is derived from UCI Machine Learning Repository - WSN Dataset and Intel Lab Data for simulations based on encryption. With respect to cost, latency, energy, distance, and other factors, the following algorithms were compared with existing simulation model. The transmission simulation configuration for 100 and 200 nodes is shown in Figure 2. Figure 3 presents the convergence analysis of the proposed SI-MPO technique across 100 and 200 nodes over GA, LP, DES, IP, AES, and SA. Figure 3 shows that while the convergence rate is strong at prime iterations, the cost values for both SI-MPO and other GA, LP, DES, IP, AES, and SA methods for 100 and 200 nodes decrease as the number of iterations increases.

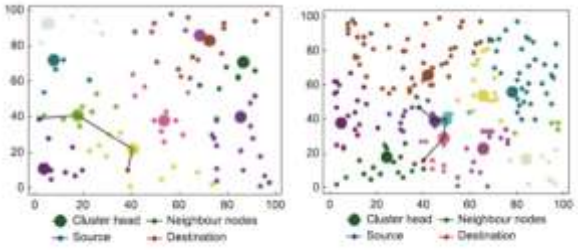
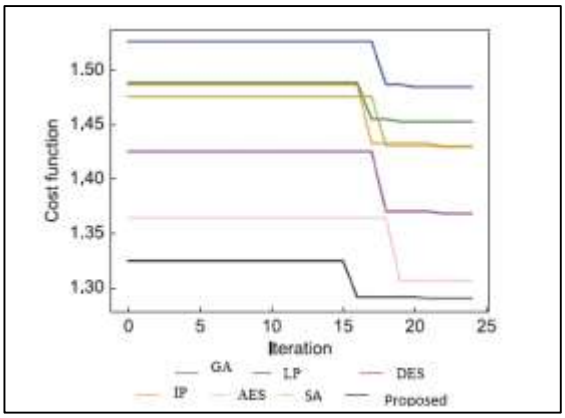



***Figure 2.*** *Simulation setup for different transmission. (a) 100 nodes. (b) 200 nodes. Convergence analysis*



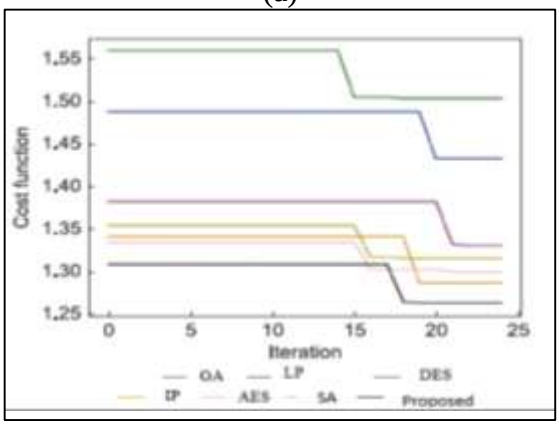
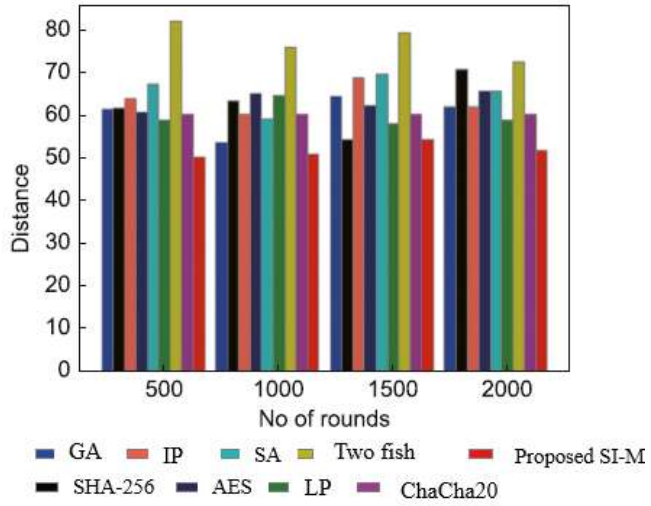




***Figure 3.*** *Convergence analysis of the suggested and conventional algorithms for different nodes. (a) 100 nodes. (b) 200 nodes.*

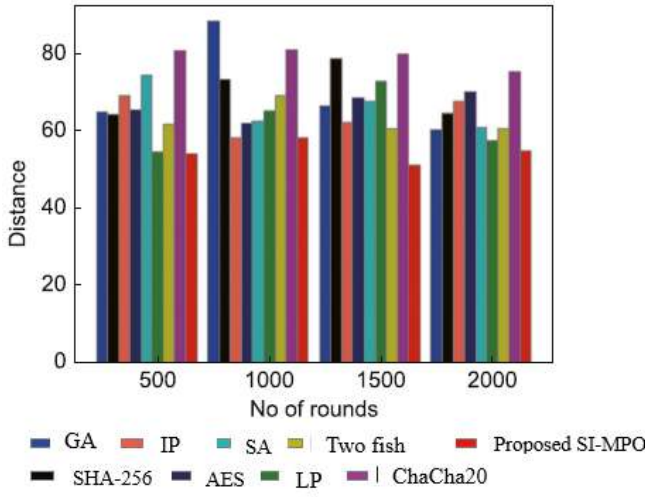
Both the current approach and the proposed SI-MPO approach have decreased in value at the 25th iteration. However, compared to the current schemes, our SI-MPO plan showed lower costs. SI-MPO achieves a lower cost of 1.25 for 100 nodes at the 25th iteration. This investigation demonstrates how well the suggested algorithm performs in choosing the best CH in the shortest amount of time. It therefore demonstrates the rapid rate of convergence.

**Analysis on distance and energy**

For 100 and 200 nodes, the energy and distance studies are conducted for SI-MPO over alternative options. The analysis of distance is shown in Figure 4, and the analysis of energy is shown in Figure 5. A variety of rounds, including 500, 1000, 1500, and 2000, are evaluated. A good system should have a small distance and a higher amount of energy left over.



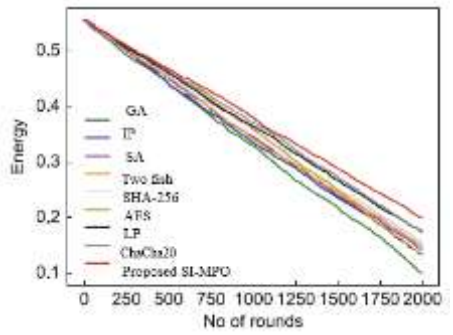

(a)



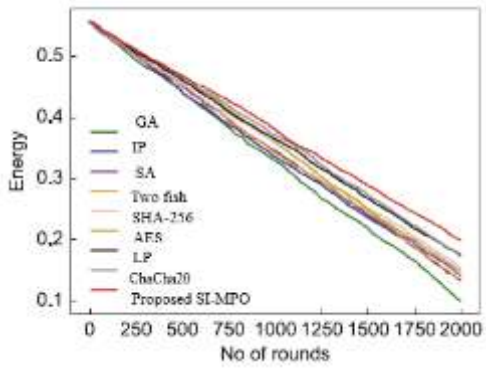

(b)

***Figure** 4. Distance analysis of the suggested and conventional algorithms for different nodes. (a) 100 nodes. (b) 200 nodes.*

Comparing SI-MPO to other schemes such as GA, IP, SA, Twofish, SHA-256, AES, LP and chacha 20, the distance obtained is negligible in Figure 4(a). In the case of 500 rounds, a minimum distance is specifically noted. With a high distance, the LP technique performs the worst across all rounds.




(a)




(b)

***Figure** 5. Energy analysis of the suggested and conventional algorithms for different nodes. (a) 100 nodes. (b) 200 nodes.*

This improvement is the result of DSTEs improvisations with the best CHS. With regard to energy in Figure 5, we can observe that as the number of rounds increases, the amount of energy left decreases. Our SI-MPO model, however, achieved high remaining energy above GA, IP, SA, Two fish, SHA-256, AES, LP and chacha 20 for all rounds. For both 100 and 200 nodes, GA achieves less energy left over at the end of each round. This improvement is the result of DSTE's improvisations and ideal CHS.

**Network lifetime analysis**

Table 1 shows the results of the network lifespan analysis conducted with the proposed SI-MPO approach over the GA, IP, SA, two fish, SHA-256, AES, LP and chacha 20 models. In this case, 100 and 200 nodes are analysed. For both sets of nodes, Table 1 shows that the SI-MPO approach has a higher network lifetime than alternative approaches. SI-MPO achieved a network lifespan of 2859 at an anode count of 100, and a network lifetime of 3394 when the node count was 200. The improved

network lifetime is the result of DSTE improvisations and optimized CHS.

***Table 1.*** *Network lifetime analysis*

| Methods | Nodes = 100 | Nodes = 200 |
|---|---|---|
| GA | 2770 | 3370 |
| IP | 2803 | 3376 |
| SA | 2805 | 3311 |
| Two fish | 2706 | 3299 |
| SHA-256 | 2644 | 3262 |
| AES | 2750 | 3279 |
| LP | 2736 | 3352 |
| ChaCha20 | 2683 | 3266 |
| Proposed | 2864 | 3398 |

**Analysis on attacks**

The attack analysis derived from the SI-MPO approach over optimization schemes such as GA, IP, SA, Two fish, SHA-256, AES, LP and chacha 20 is displayed in Table 2. The attack analysis obtained utilizing the SI-MPO technique across a variety of encryption schemes, is displayed in Table 3.

The following attacks are taken into consideration: brute force, man-in-the-middle, chosen-plaintext attack, and known-plaintext attack (KPA). We have implemented an enhanced DSTE that guarantees greater system security in order to reduce the threats. Here, we might determine the system's improvement by examining the effects of attacks from the tables below. According to Table 1, SI-MPO has a lower KPA attack (0.001084) than GA, IP, SA, Twofish, SHA-256, AES, LP and chacha 20, which have higher KPA attack values.

***Table 2.*** *Evaluation on attacks for different optimization techniques*

| | | | | | | |
|---|---|---|---|---|---|---|
| GA | 0.031347 | 0.031297 | 5.287427 | 13.09493 | GA | 0.031349 |
| IP | 0.031347 | 0.031297 | 5.287427 | 13.09493 | IP | 0.031349 |
| SA | 0.021099 | 0.020616 | 5.28244 | 13.9308 | SA | 0.021099 |
| Two fish | 0.004532 | 0.002955 | 5.683367 | 14.40559 | Two fish | 0.0045233 |
| SHA-256 | 0.043506 | 0.046292 | 5.634798 | 11.40411 | SHA-256 | 0.043507 |
| AES | 0.018451 | 0.019648 | 5.199104 | 12.20842 | AES | 0.018451 |
| LP | 0.040822 | 0.042131 | 5.699182 | 11.15148 | LP | 0.040823 |
| ChaCha20 | 0.002511 | 0.028972 | 5.375271 | 13.12285 | ChaCha20 | 0.002510 |
| Proposed | 0.001090 | 0.007925 | 6.379069 | 14.74804 | Proposed | 0.001091 |

***Table 3.*** *Evaluation on attacks for different encryption techniques.*

| Methods | KPA | CPA | Man in middle | Brute force |
|---|---|---|---|---|
| AES | 0.01319 | 0.0129 | 5.63468 | 12.5346 |
| ECC | 0.00349 | 0.01077 | 5.64011 | 13.3935 |
| RSA | 0.05798 | 0.12359 | 5.41633 | 11.2544 |
| Blowfish | 0.17318 | 0.21863 | 5.62228 | 11.6704 |
| Improved ECC | 0.00114 | 0.00797 | 6.37912 | 14.755 |

***Table 4.*** *Statistical analysis on delay.*

| Schemes | Min ($\times 10^{-07}$) | Max ($\times 10^{-07}$) | Mean ($\times 10^{-07}$) | Median ($\times 10^{-07}$) | Std ($\times 10^{-08}$) |
|---|---|---|---|---|---|
| GA | 3.20 | 4.80 | 4.13 | 4.08 | 4.93 |
| IP | 3.28 | 4.00 | 4.10 | 4.03 | 2.62 |
| SA | 3.24 | 4.55 | 4.00 | 3.97 | 4.43 |
| Two fish | 2.96 | 4.83 | 4.00 | 3.99 | 3.54 |
| SHA-256 | 3.14 | 4.67 | 4.05 | 4.05 | 4.60 |
| AES | 3.05 | 4.41 | 3.96 | 3.94 | 4.66 |
| LP | 4.19 | 4.39 | 4.73 | 4.73 | 3.22 |
| ChaCha20 | 3.86 | 3.66 | 3.86 | 3.86 | 4.99 |
| Proposed | 2.71 | 2.86 | 3.45 | 3.46 | 3.14 |
| GA | 3.19 | 4.90 | 4.28 | 4.25 | 4.87 |
| IP | 3.40 | 4.98 | 4.12 | 4.12 | 3.55 |
| SA | 3.21 | 4.32 | 4.15 | 4.13 | 4.41 |
| Two fish | 3.44 | 4.95 | 4.14 | 4.41 | 3.22 |
| SHA-256 | 3.16 | 4.57 | 4.29 | 4.27 | 4.80 |
| AES | 2.20 | 4.60 | 4.12 | 4.09 | 4.32 |
| LP | 3.23 | 4.75 | 3.00 | 3.99 | 3.35 |
| ChaCha20 | 4.06 | 4.95 | 4.73 | 4.72 | 3.37 |
| Proposed | 2.83 | 4.19 | 3.20 | 3.85 | 3.05 |

***Table 5.*** *Statistical analysis on RSSI*

| Schemes | Min | Max | Mean | Median | Std |
|---|---|---|---|---|---|
| GA | −220.063 | −186.932 | −201.642 | −201.257 | 5.478 |
| IP | −211.223 | −187.815 | −199.62 | −199.576 | 3.976 |
| SA | −216.533 | −185.375 | −199.951 | −199.991 | 5.015 |
| Two fish | −211.598 | −182.461 | −199.28 | −199.245 | 3.856 |
| SHA-256 | −217.899 | −185.62 | −200.841 | −200.812 | 4.989 |
| AES | −215.916 | −185.399 | −199.272 | −199.072 | 4.930 |
| LP | −217.183 | −203.351 | −210.361 | −210.379 | 2.552 |
| ChaCha20 | −209.54 | −198.039 | −198.089 | −198.034 | 0.591 |
| **SI-MPO** | **−198.028** | **−177.822** | **−190.744** | **−190.891** | **3.672** |
| GA | −219.985 | −186.65 | −203.592 | −203.740 | 5.386 |
| IP | −213.407 | −189.716 | −200.98 | −200.949 | 3.858 |
| SA | −218.596 | −187.392 | −202.091 | −202.25 | 5.070 |
| Two fish | −211.598 | −188.513 | −201.968 | −202.081 | 3.380 |
| SHA-256 | −219.092 | −187.130 | −204.234 | −204.351 | 5.352 |
| AES | −217.451 | −184.974 | −201.458 | −201.042 | 5.024 |
| LP | −211.42 | −187.815 | −199.231 | −198.845 | 4.241 |
| ChaCha20 | −218.336 | −198.94 | −209.799 | −209.890 | 2.928 |
| **SI-MPO** | **−200.387** | **−175.920** | **−191.998** | **−192.273** | **3.283** |

Additionally, Table 3 shows that the enhanced ECC has less of an effect on brute force attacks. Similarly, SI-MPO has a lower impact than other attacks for all attacks. As a result, the use of the suggested SI-MPO algorithm and enhanced DSTE is verified.

**Statistical analysis**

Tables 4 and 5 provide the statistical analysis of latency and RSSI for SI-MPO over GA, IP, SA, Twofish, SHA-256, AES, LP and chacha 20. For better data transmission in WSN, there must be minimal delay and a high RSSI. Since we have implemented the best CHS idea with clear goals, DSTE has proven this statement over GA, IP, SA, Twofish, SHA-256, AES, LP and chacha 20 schemes.

**Analysis on encryption and decryption time**

Tables 6 and 7 present the encryption and decryption time analysis for the various encryption models and optimization strategies. According to Table 6, the suggested SI-MPO method has an encryption time of 0.0036 and outperforms the current GA, IP, SA, Twofish, SHA-256, AES, LP and chacha 20 schemes by 75.19%, 75%, 75.57%, 75.02%, 75.5%, 75%, and 98.88%.

***Table 6.*** *Encryption and decryption time analysis for varied optimization schemes.*

| Methods | Encryption time | Decryption time |
|---|---|---|
| AOA | 0.01455 | 0.013791 |
| ARCHOA | 0.0149 | 0.01377 |
| BES | 0.014742 | 0.018 |
| BOA | 0.014416 | 0.013698 |
| CA | 0.014695 | 0.013959 |
| DHO | 0.014408 | 0.013690 |
| ECDSA [15] | 0.320733 | 0.304697 |
| **SI-MPO** | **0.0036** | **0.00348** |

The suggested algorithm value is 0.00342, which is less than the current ones when taking the decryption time into account. According to Table 7, the enhanced DSTE encrypting and decryption times are 0.0036 and 0.00342, respectively.

***Table 7.*** *Encryption and decryption time analysis for varied encryption modes.*

| Methods | Encryption time | Decryption time |
|---|---|---|
| SA | 0.006363 | 0.006045 |
| LP | 0.162974 | 0.154824 |
| RSA | 0.01479 | 0.014227 |
| Blowfish | 0.61775 | 0.586775 |
| **DSTE** | **0.0047** | **0.00350** |

The suggested approach outperforms the traditional SA, LP, RSA, and blowfish encryption models in terms of encryption time by 43.32%, 97.79%, 75.95%, and 99.42%, respectively. As a result, the suggested encryption model and algorithm's effectiveness for safe data transfer are confirmed.

**Analysis on computing time**

The computing time accomplished by the SI-MPO model over others is shown in Table 8. Table 8 shows the computing time for both 100 and 200 nodes. From Table 8, the presented SI-MPO model shows less computing time for 100 and 200 nodes. For 200 nodes, the computing time is slightly higher than that for 100 nodes. In our everyday lives, WSNs are employed for a variety of purposes. The effective utilization of these resources, particularly the energy resource, is crucial for maintaining the lifespan of the WSNs because the sensor nodes have limited resources. WSNs must have an effective routing protocol design in order to extend the network lifetime because communication uses more energy.

***Table 8.*** *Computing time analysis.*

| Methods | Nodes = 100 | Nodes = 200 |
|---|---|---|
| SA | 0.030077 | 0.036559 |
| LP | 0.030289 | 0.026451 |
| RSA | 0.094648 | 0.073981 |
| Blowfish | 0.022499 | 0.025495 |
| IP | 0.031658 | 0.033058 |
| AES | 0.039094 | 0.04849 |
| **DSTE** | **0.017573** | **0.019733** |

## 5. Conclusion

The most crucial design concern in WSN is the successful and dependable conveyance of data. To achieve this, a secure routing algorithm that can route data via the most efficient, safe, and energy-efficient path must be proposed. This can be accomplished by sending the collected data via trusted nodes, which can serve as the cluster head and send the data in a more secure and dependable manner. One significant problem associated with the network layer of the network protocol stack in a WSN is routing. This research project presents an energy-efficient hierarchical cluster-based algorithm for Wireless Sensor Networks (WSNs). The proposed algorithm is SI-MPO and DSTE. These new algorithms offer improved performance in terms of energy efficiency, making them suitable for WSN applications. The enhancement of the tiny encryption method, incorporating a novel clustering technique that considers the distance from the Base Station (BS) and residual energy of nodes. The algorithm also integrates an energy-efficient method to enhance sink mobility, further improving energy efficiency. Simulation results demonstrate the effectiveness of the proposed algorithm, outperforming DSTE and its variant with node mobility in terms of energy efficiency.

## Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

## References

[1]Khan, S. U., Khan, Z. U., Alkhowaiter, M., Khan, J., & Ullah, S. (2024). Energy-efficient routing protocols for UWSNs: A comprehensive review of taxonomy, challenges, opportunities, future research directions, and machine learning perspectives. *Journal of King Saud University-Computer and Information Sciences*, 102128.

[2]Shwetha, G. R., & Murthy, V. N. (2024). Hybrid Compressed Sensing and Secure Fault Tolerant Data Aggregation in Wireless Sensor Networks. *International Journal of Communication Networks and Information Security*, 16(1), 211-227.

[3]Devi, V. A., & Sampradeepraj, T. (2024). End-to-End Self-organizing Intelligent Security Model for Wireless Sensor Network based on a Hybrid (AES–RSA) Cryptography. *Wireless Personal Communications*, 136(3), 1675-1703.

[4]AlMajed, H. N., & AlMogren, A. S. (2019). Simple and effective secure group communications in dynamic wireless sensor networks. *Sensors*, 19(8), 1909.

[5]Al-Hejri, I., Azzedin, F., Almuhammadi, S., & Syed, N. F. (2024). Enabling Efficient Data Transmission in Wireless Sensor Networks-Based IoT Applications. *Computers, Materials & Continua*, 79(3).

[6]Alsumayt, A., Alshammari, M., Alfawaer, Z. M., Al-Wesabi, F. N., El-Haggar, N., Aljameel, S. S., ... & Aldossary, N. (2024). Efficient security level in wireless sensor networks (WSNs) using four-factors authentication over the Internet of Things (IoT). *PeerJ Computer Science*, 10, e2091.

[7]Dudeja, D., Hera, S. Y., Doohan, N. V., Dubey, N., Mahaveerakannan, R., Ahanger, T. A., ... & Hinga, S. K. (2022). Energy efficient and secure information dissemination in heterogeneous wireless sensor networks using machine learning techniques. *Wireless Communications and Mobile Computing*, 2022, 2206530.

[8]Chmielowiec, A., Klich, L., & Woś, W. (2024). Energy efficient ECC authenticated key exchange protocol for wireless sensor networks with star topology. *Journal of Telecommunications and Information Technology*.

[9]Urooj, S., Lata, S., Ahmad, S., Mehfuz, S., & Kalathil, S. (2023). Cryptographic data security for reliable wireless sensor network. *Alexandria Engineering Journal*, 72, 37-50.

[10]Gupta, S. K., & Singh, S. (2022). Survey on energy efficient dynamic sink optimum routing for wireless sensor network and communication technologies. *International Journal of Communication Systems*, 35(11), e5194.

[11]Yilmaz, S., & Dener, M. (2024). Security with Wireless Sensor Networks in Smart Grids: A Review. *Symmetry*, 16(10), 1295.

[12]Tharani, B., & Devi, B. P. (2024). Optimizing Energy Efficiency and Security in Wireless Sensor Networks with a Hybrid HF-ECC. *In 2024 10th International Conference on Advanced Computing and Communication Systems* (ICACCS).

[13]Cheng, Y., Liu, Y., Zhang, Z., & Li, Y. (2023). An Asymmetric Encryption-Based Key Distribution Method for Wireless Sensor Networks. *Sensors*, 23(14), 6460.

[14]Shah, S., Munir, A., Waheed, A., Alabrah, A., Mukred, M., Amin, F., ... & Salam, A. (2023). Enhancing security and efficiency in underwater wireless sensor networks: a lightweight key management framework. *Symmetry*, 15(8), 1484.

[15]Oztoprak, A., Hassanpour, R., Ozkan, A. G., & Oztoprak, K. (2024). A Comparative Study on Key Generation in Wireless Sensor Networks. *In 2024 IEEE International Conference on Big Data* (BigData).

[16]Hussein, S. M., López Ramos, J. A., & Ashir, A. M. (2022). A secure and efficient method to protect communications and energy consumption in IoT wireless sensor networks. *Electronics*, 11(17), 2721..

[17]Aqeel, I. (2024). Enhancing Security and Energy Efficiency in Wireless Sensor Networks for IoT Applications. *Journal of Electrical Systems*, 20(3s), 807-816..

[18]Khashan, O. A., Ahmad, R., & Khafajah, N. M. (2021). An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. *Ad Hoc Networks*, 115, 102448..

[19]Alghamdi, A., Al Shahrani, A. M., AlYami, S. S., Khan, I. R., Sri, P. A., Dutta, P., ... & Venkatareddy, P. (2024). Security and energy efficient cyber-physical systems using predictive modeling approaches in wireless sensor network. *Wireless Networks*, 30(6), 5851-5866..

[20]Alshammari, M. R., & Elleithy, K. M. (2018). Efficient and secure key distribution protocol for wireless sensor networks. *Sensors*, 18(10), 3569.

[21]V. Thamilarasi, P. K. Naik, I. Sharma, V. Porkodi, M. Sivaram and M. Lawanyashri, (2024). Quantum Computing - Navigating the Frontier with Shor's Algorithm and Quantum Cryptography, *2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies, Pune, India*, 2024, pp. 1-5, doi: 10.1109/TQCEBT59414.2024.10545283.

[22]Ganta, S. R., & Naga Malleswara Rao Nallamothu. (2025). A dynamic integrity and data confidentiality based wireless N2N data communication and security protocol on large networks. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.720

[23]Udayakumar, P., & R. Anandan. (2025). Comparative Study of Lightweight Encryption Algorithms Leveraging Neural Processing Unit for Artificial Internet of Medical Things. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.1259

[24]Thammuluri, R., Gottala Surendra Kumar, Bellamgubba Anoch, Ramesh Babu Mallela, Anuj Rapaka, & Veera V. Rama Rao M. (2025). Enhanced Hybrid Adaptive DNA Compression: Accelerating Genomic Data Compression through Parallel Processing. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.943

[25]C. Kiruthiga, & K. Dharmarajan. (2025). Data-Driven Insights: A Critical Analysis of Farmer Call Centre Data Using Machine Learning Techniques. *International Journal of Computational and Experimental Science and Engineering*, 11(2). https://doi.org/10.22399/ijcesen.1348

[26]Mohammed F Ibrahim Alsarraj, Aliza Binti Abdul Latif, & Rohaini Binti Ramli. (2025). Human Activity-Based Machine Learning and Deep Learning Techniques. *International Journal of Computational and Experimental Science and Engineering*, 11(2). https://doi.org/10.22399/ijcesen.1368

[27]J Jeysudha, K. Deiwakumari, C.A. Arun, R. Pushpavalli, Ponmurugan Panneer Selvam, & S.D. Govardhan. (2024). Hybrid Computational Intelligence Models for Robust Pattern Recognition and Data Analysis. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.624

[28]K. Tamilselvan, , M. N. S., A. Saranya, D. Abdul Jaleel, Er. Tatiraju V. Rajani Kanth, & S.D. Govardhan. (2025). Optimizing data processing in big data systems using hybrid machine learning techniques. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.936

[29]Olola, T. M., & Olatunde, T. I. (2025). Artificial Intelligence in Financial and Supply Chain Optimization: Predictive Analytics for Business Growth and Market Stability in The USA. *International Journal of Applied Sciences and Radiation Research*, 2(1). https://doi.org/10.22399/ijasrar.18

[30]Ibeh, C. V., & Adegbola, A. (2025). AI and Machine Learning for Sustainable Energy: Predictive Modelling, Optimization and Socioeconomic Impact In The USA. *International Journal of Applied Sciences and Radiation Research*, 2(1). https://doi.org/10.22399/ijasrar.19

[30]Fowowe, O. O., & Agboluaje, R. (2025). Leveraging Predictive Analytics for Customer Churn: A Cross-Industry Approach in the US Market. *International Journal of Applied Sciences and Radiation Research*, 2(1). https://doi.org/10.22399/ijasrar.20