EasyChair Preprint

№ 15924

IoT Based Secure Data Sharing for Precision Agriculture with Optimal Clustering and Hybrid Encryption Algorithm

Nagendra Reddy Palugula and Savitri Bevinakoppa

March 19, 2025

IoT Based Secure Data Sharing for Precision Agriculture with Optimal Clustering and Hybrid Encryption Algorithm

Nagendra Reddy Palugula
School of IT and Engineering
Melbourne Institute of Technology
Victoria, Australia
MIT224504@stud.mit.edu.au

Savitri Bevinakoppa
School of IT and Engineering
Melbourne Institute of Technology
Victoria, Australia
sbevinakoppa@mit.edu.au

***Abstract*— Sensor nodes in precision agriculture may send secure data. The primary issues for this project are energy efficiency and data privacy. This system employs data clustering, which involves sensor nodes organizing into clusters under the supervision of a cluster head (CH). The CH oversees the other CHs and the cluster's data sharing. Several objective criteria, such as energy, delay, execution time, distance, and residual energy, are considered for determining the optimal CH. The proposed hybrid optimization models will be formed by hypothetically integrating both the conventional Pufferfish Optimization Algorithm (POA) and Reptile Search Algorithm (RSA). When more than one node meets the necessary requirements, this hybrid approach can be used to choose. This hybrid approach is helpful in choosing the best CH for communication when there are numerous nodes that meet the necessary requirements. After the best CH has been chosen, the data must be encrypted before being sent. A cutting-edge hybrid cryptographic technique that combines Blowfish symmetric key encryption with Elliptic Curve cryptography to secure data while maintaining trust and privacy. By choosing the best way, the path selection technique based on self-improved Bald Eagle Search optimization reduces interception and ensures the safe transmission of encrypted data. This thorough research, which focuses on data security and energy saving, gives farmers trustworthy and safe information to help them make more informed agricultural decisions.**

Keywords*— *Cluster head, Pufferfish Optimization Algorithm, Reptile Search Algorithm, Elliptic Curve cryptography, Cryptographic technique

I. INTRODUCTION

IoT devices provide a massive data stream by utilizing a variety of technologies, such as wireless communication, processing, and sensing. It improves quality of life and adds to global economic growth [1]. An application of the IoT-driven WSN platforms in precision agriculture has the potential to transform the agricultural data landscape and promote the highly liked machine-driven agriculture approach, which requires extensive knowledge of ecological conditions at the fundamental level and quick data transfer to a local or remote server where factors such as plant identity, identifying insects within the plants, burial or hyperbolic moisture, alternative generation, and plantation equipment are finished quickly (automatic propulsion apparatus, such as fog, sprinkler systems, and so on, are used for management of irrigation, fertilization, and pest control to offset the negative effects of agriculture) [2]. Nowadays, precision agriculture (PA) is thought to be a crucial technical advancement that will allow for a more effective use of agricultural resources. The main objectives of PA are to reduce input costs and minimize the detrimental effects of the farming environment, such as excessive pesticide and fertilizer use and ineffective irrigation, while also increasing farmers' profitability through improved harvest and/or quality yields [3].

Agriculture-related Internet of Things (IoT) technologies offer a novel approach to gathering agricultural data by recording data from the farming environment and realizing machine-to-machine and machine-to-person interactions using a variety of sensors, hardware and software systems, and communication network devices [4]. However, the biggest challenge is securing massive amounts of data on the cloud [5]. Data reduction, energy-aware routing, clustering, and other techniques are examples of energy-saving strategies. These strategies concentrate on reducing energy loss and extending device lifetimes. The cluster head is a single, non-overlapping node that gathers data and forwards it to the other nodes in the cluster. Because of this, the cluster head is the only node that perceives data while consuming the least amount of power. The IoT was developed to improve agricultural energy efficiency [6].

The obtained data is transferred to cloud servers (CSs) for processing complex agricultural issues such as yield prediction, water feed computation, and so on. This allows farmers and other stakeholders to make more informed decisions, increasing the amount and quality of agricultural [7]. There are three requirements to use IoT: Use Internet of Things (IoT) devices to: (i) collect direct data about plants, soil, or the environment and transmit it to the sink node; (ii) a gateway node that provides translation services to facilitate communication between various sensor variants; and (iii) transmit all aggregated data to a dispersed cloud-based storage unit known as a data center [8]. Using software tools like Arduino, Eclipse IoT, Kinoma, Node-RED, IoT System, or Common IoT is one way to gather sensor data [9].

II. BACKGROUND

Precision agriculture (PA) uses technologies like the IoT and WSNs to collect real-time data on various environmental factors that affect crop health and yield. However, securely transmitting sensitive data across resource-limited sensor networks is a significant challenge. Traditional security solutions frequently require significant processing power and memory, which exceeds the capabilities of sensor nodes. This raises concerns about data theft, unauthorised access, and potential influence during transmission.

The planning and creation of a secured system that can continuously measure a few parameters, such as temperature, agro-field temperature, soil moisture, and air humidity [10]. A cluster election approach based on fuzzy logic inference systems is adopted [11]. In 2022, Akhter and Sofi [12] have explored using data analytics and the Internet of Things to predict when the apple scab disease may spread among apple farms in Kashmir Valley. In 2022, Riaz et al., [13] have

discussed how to use adaptive security in Internet of Things-based smart farming, with a focus on cost, risk, and safety. In 2022, Rokade et al., [14] have shown how to apply a regression-based supervised machine learning approach to precisely manage sensor parameters in a smart greenhouse cropping system, such as CO2, soil moisture, humidity, and light intensity.

In 2023, Ravi et al., [15] have recommended an IoT network cluster-based reliable data aggregation (CRDA) strategy that ensures energy-efficient data gathering and aggregation as well as efficient data transport to a different end. In 2023, Fathy and Ali [16] have suggested to address the needs of IoT devices with limited resources, lightweight cryptography solutions should be incorporated into the IoT ecosystem for smart agriculture.

III. OBJECTIVES

Main objectives of this paper are:

- To create a hybrid optimization model for optimal cluster head selection in sensor networks by combining the Pufferfish Optimization Algorithm (POA) and the reptile Search Algorithm (RSA). This model takes multi-objective parameters into consideration and optimizes data management, energy consumption, and data transmission delays.
- To maintain data privacy and trust, a safe data transfer technique combining Elliptic Curve Cryptography (ECC) and Blowfish symmetric key encryption is required, especially in the sector of agriculture.
- Optimization strategy to decrease data interception and ensure maximal green path selection for records transmission by using a self-stepped forward Bald Eagle Search technique for steady facts transfer.

IV. FRAMEWORK

The sensor deployment in agricultural fields are to monitor parameters like moisture, temperature, and nutrient levels. Data is collected and transmitted to a central node within each cluster. Clustering and cluster head selection are carried out using a hybrid optimization model that incorporates the Pufferfish Optimization Algorithm (POA) and the Reptile Search Algorithm (RSA).

Elliptic Curve Cryptography (ECC) and Blowfish Symmetric Key Encryption are two components of the hybrid cryptography technique that ensures data security. The optimal path selection for data transmission is achieved through Self-Improved Bald Eagle Search (SIBES) optimization. The data is transmitted securely and efficiently, with real-time monitoring of network performance. Performance evaluation is conducted using metrics such as energy consumption, latency, network lifespan, and data delivery ratio. The methodology is implemented through simulations, field trials, and comparison with existing methods as shown in Fig. 1.

Clustering head selection: The cluster head was selected by using multi objective optimization technique. The cluster head portion uses a hybrid optimization technique that combines the reptile search algorithm with the puffer fish optimization algorithm (POA).

Hybrid optimization algorithm: The combination of the Pufferfish Optimization Algorithm (POA) and the Reptile Search Algorithm (RSA) offers a reliable hybrid optimization technique for precision agriculture. By addressing difficult multi-objective optimization issues like the best cluster head (CH) selection, this method seeks to provide effective data transmission and collection in wireless sensor networks (WSNs) that are connected to the Internet of Things (IoT).

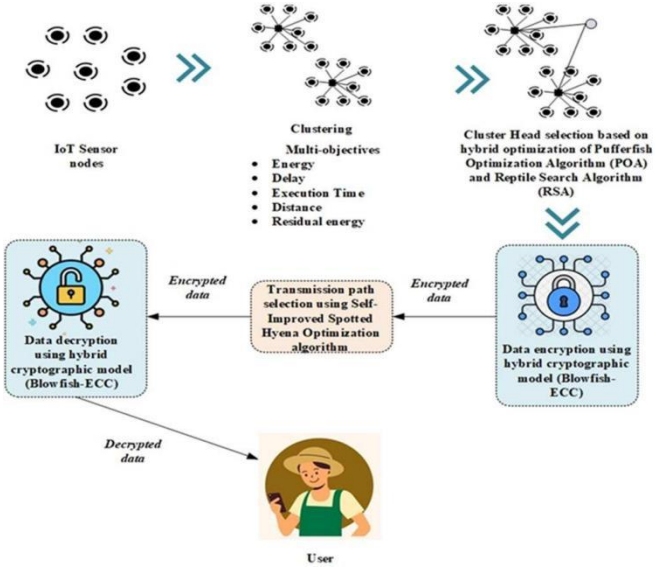

Fig. 1. Implementation Framework

A. Puffer fish optimization algorithm (POA)

Pufferfish belong to the Tetraodontidae family and Tetraodontiformes order of fish, and they are mostly found in estuaries and the ocean. This fish resembles porcupinefish, which have enormous spines, in terms of form. Pufferfish have tiny to medium-sized bodies and can reach a maximum length of 50 cm. One of the most characteristic characteristics of pufferfish is its quartet of teeth, which resembles beaks.

Algorithm initialization: Through a generation-based technique, the population-primarily based approach known as POA leverages its population search strength in the problem-solving space to provide effective solutions to optimization problems. Each member of the POA sets values for the annoyance's decision variables based on how the hassle behaves inside the search space. As a result, every member of the POA stands for a possible resolution to the problem, which may be mathematically described by using a vector, each of whose components is associated with a selection variable. Collectively, POA members shape the algorithm's population. From a mathematical perspective, Equation (1) can be used to model the community of these vectors using a matrix. Equation (2) is used to initialize each POA member's primary location at the start of the algorithm.

$$j = \begin{bmatrix} X_1 \\ j^{2} \\ \vdots \\ X_N \end{bmatrix}_{N\times m} \quad (1)$$

$$x_{i,d} = lb_d + r.(ub_d - lb_d) \quad (2)$$

The Ţth POA member (possible solution) is represented by $j_Ţ$ the POA population matrix is represented by j, and the

search space's dth dimension is represented by $ub_{j,y}$. The population consists of $\ddot{\upsilon}$ members, there are m decision variables, r is a random number in the interval [0, 1], and $\tilde{r}_y$ and xr_y are the lower and upper bounds of the dth decision variable, respectively.

It is possible to assess the problem's objective function by considering each POA member as a potential solution. Equation (3) can be used to express the set of evaluated values for the problem's objective function as a vector.

$$\ddot{\upsilon} = \begin{bmatrix} F_1 \\ \vdots \\ \ddot{\upsilon}_{\tilde{F}} \\ \vdots \\ F_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} F(X)_1 \\ \vdots \\ \ddot{\upsilon}(j)_{\tilde{F}} \\ \vdots \\ F(X)_N \end{bmatrix}_{N\times 1} \quad (3)$$

Where, the evaluated objective function in this case is based on the ith POA member, and its vector is denoted by $\ddot{\upsilon}_{\tilde{F}}$.

The evaluated values of the objective function provide suitable standards by which to evaluate the quality of possible solutions proposed by each POA member. The greatest evaluated value for the objective function denotes the ideal candidate solution, or best member, whereas the lowest evaluated value for the objective function denotes the lowest candidate solution, or worst member. The POA members' locations in the problem-solving space are updated with each iteration, therefore the best member should also be altered based on a comparison of freshly evaluated values for the objective function.

Mathematical Modelling of POA: Based on a modelling of pufferfish and their predators' natural behaviors, the suggested POA approach takes into account the function of population contributors inside the trouble-fixing region. In this natural process, the predator's main prey is the pufferfish. The pufferfish then employs its defense mechanism to change into a ball of sharp spines, endangering the predator and allowing the fish to flee. As a result, the locations of POA population members are altered with each release, first in the stage of exploration (which simulates a predator attacking a pufferfish) and then in the stage of exploitation (which simulates a pufferfish deploying its defense mechanism against a predator).

Phase 1: Exploration Phase: During the initial phase of POA, the population's current location is determined just by simulating the predator's attack strategy on the pufferfish. Pufferfish move slowly, making them easy pickings for ravenous hunters. To substitute the POA members' position in the trouble-fixing space, the predator's alternate position at a certain point in the attack in the direction of the pufferfish is simulated. The role of the POA participants is drastically altered when the predator's movement toward the pufferfish is modelled, which ultimately strengthens the set of rules for global search's exploratory potential.

Because of the candidate pufferfish's position in an assault, other population contributors with a greater price for the objective function are placed differently in POA designs for each member of the population acting as a predator. Equation (4) is used to identify each population member's group of pufferfish.

$$CP_i = \{X_k : F_k < F_i \text{ and } k \neq i\} \quad \text{where } \tilde{F} = 1,2,\ldots\ldots,\ddot{\upsilon}\} \quad (4)$$

The collection of potential pufferfish locations for the $\tilde{F}$th predator is denoted by $\ddot{\upsilon}\lambda_{\tilde{F}}$, the population member with a higher objective function fee than the $\tilde{F}$ th predator is represented by j_k, and its objective feature cost is represented by $\ddot{\upsilon}_k$.

The POA arrangement predicts that the predator would select a pufferfish at random to be regarded as the chosen pufferfish (SP) from among the multiple candidate pufferfish identified in the CP set. Using the concept of the predator's migration closer to the pufferfish, equation (5) is applied to each member of the POA to create a new function in the problem-fixing area. Then, if the goal feature value is raised in the new role, this new position takes the place of the corresponding member's previous role in line with Equation (6).

$$x^{P1}_{\tilde{F},j} = x_{i,i} + r_{i,i}.\,(SP_{i,i} - I_{i,i}, x_{i,i}) \quad (5)$$

$$j_{\tilde{F}} = \begin{cases} X^{P1}_{\tilde{F}}, & F^{P1}_{\tilde{F}} \leq F_i; \\ j_{\tilde{F}}, & \text{otherwise}, \end{cases} \quad (6)$$

Here, $j^{\lambda 1}_{\tilde{F}}$ is the new position calculated for the $\tilde{F}$ th predator based entirely on the first section of the proposed POA, $j^{\lambda 1}_{\tilde{F},j}$ is its jth size, $\ddot{\upsilon}^{\lambda 1}_{\tilde{F}}$ is its objective feature cost, $\tilde{r}_{F,j}$ are random numbers from the interval [0, 1], and $\ddot{\upsilon}_{F,j}$ are numbers that are randomly selected as 1 or 2. $U\lambda_{\tilde{F}}$ is the chosen pufferfish for the ith predator, chosen randomly from the $\ddot{\upsilon}\lambda_{\tilde{F}}$ set (i.e., $U\lambda_{\tilde{F}}$ is a detail of the $\ddot{\upsilon}\lambda_{\tilde{F}}$ set).

Phase 2: Défense Mechanism of Pufferfish against Predators (Exploitation Phase) The research mimics the defense system of pufferfish against predator assaults. When the pufferfish fills its elastic stomach with water, it turns into a ball of sharp spines that deters predators from approaching the pufferfish. This leads to minor modifications in the Point of Affect (POA) members' functions, improving the algorithm's performance for local searches. For every POA member, a new function is computed based on the predator's position trade as it moves away from the pufferfish. Since the purpose of the POA design is to enhance the algorithm, the new location replaces the previous member if it increases the target feature value. If the new role is appropriate and the matching member stays in the old role, the new function is effective.

$$F^{P2}_{\tilde{F},j} = F_{\tilde{F},j} + (1 - 2r_{\tilde{F},j}).\frac{ub_j - lb_j}{t}, \quad (7)$$

$$j_{\tilde{F}} = \begin{cases} X^{p2}_{\tilde{F}}, & F^{p2}_{\tilde{F}} \leq F_i: \\ j_{\tilde{F}}, & \text{otherwise}, \end{cases} \quad (8)$$

Where, F_i^P2 is the goal function value, r_(i,j) are random values from the C language [0,1], t is the generation counter, and X_i^P2 is the new location determined for the ith predator based on the second one segment of the suggested POA.

B. Reptile Search Algorithm (RSA)

The Reptile Search Algorithm (RSA) is an optimization approach inspired by the hunting and exploration behaviors of reptiles, such as lizards and snakes. These animals' keen senses, agility, and adaptability allow them to efficiently

navigate their environments to capture prey, which RSA emulates to explore search spaces and find optimal solutions to complex problems. RSA is particularly effective in scenarios with few dimensions, non-linear relationships, and dynamic changes. It leverages advanced sensing capabilities to detect subtle signals and process information from the environment, enabling it to make informed decisions and adjust its search strategy. Additionally, RSA employs strategic mobility, focusing on promising regions of the search space, which enhances its ability to converge toward optimal solutions.

Encircling Phase (Exploration): This section contains the RSA's exploratory behaviour (encircling). In accordance with their encircling behaviour, crocodiles engage in two behaviours when they walk: high walks and stomach walks. The RSA divides the number of iterations into four elements and the overall broad variety of iterations into four portions in order to move between the exploration and exploitation seek levels. The RSA exploration mechanisms use principal search strategies as their primary basis for examining the hunt regions and finding a higher answer.

For the duration of this search phase, one requirement must be satisfied. The belly walking search method is applied in accordance with t>2 T/4 and t>T/4, whereas the high walking search method is applied in accordance with t⩽T/4. Equation presents the process of updating a position. The position-updating process is presented in Equation (9)

$$x_{(i,j)}(t+1) = \begin{cases} Best_j(t) \times \eta_{(i,j)}(t) \times \beta - R_{(i,j)}(t) \times rand & t \le \frac{T}{4} \\ Best_j(t) \times x_{(i,j)} \times ES(t) \times rand & t \le 2\frac{T}{4} \text{ and } t > \frac{T}{4} \end{cases} \quad (9)$$

where rand is a random number, t is the current iteration, T is the maximum number of iterations, and $Best_j(t)$ is the best-received solution. Equation (2) is used to determine the searching parameter, $\eta_{(i,j)}$. The parameter β is set to 0.1. Equation (3) determines the lessen function $R_{(i,j)}$. N is the used solutions, $R_1 - r_4$ are random values, and $x_{(r_1,j)}$ is a random position. Equation (4) is used to compute the probability parameter known as Evolutionary Sense (ES).

$$\eta_{(i,j)} = Best_j(t) \times P_{(i,j)} \quad (10)$$

$$\text{Ð}_{(i,j)} = \frac{\text{Best}_j(t) \times x_{(i,j)}}{\text{ES}(t) + } \quad (11)$$

$$ES(t) = 2 \times r_3 \times \left(1 - \frac{1}{T}\right) \quad (12)$$

Where, ɔ is a tiny number. Equation (13) yields the difference parameter $\text{Ø}_{(i,j)}$.

$$\text{Ø}_{(i,j)} = \alpha + \frac{x_{(i,j)} - M(x_j)}{Best_j(t) \times (UB_{(j)} - LB_{(j)}) + e} \quad (13)$$

Where, the average positions as calculated by Equation (14) are denoted by ÐÆ. Upper and lower bounds are denoted by Æ and $\text{ÐÐ}_{(j)}$. is a constant parameter set at 0.1.

$$M(x_i) = \frac{1}{\varepsilon} \sum_{j=1}^{n} \text{Æ}_{(i,j)} \quad (14)$$

Hunting Phase (Exploitation): Based on their hunting habits, crocodiles employ two different hunting strategies: cooperation and coordination. This phase of the search (hunting coordination) is carried out and determined based on t ≤ 3 T 4 and t > 2 T 4; if t ≤ T and t > 3 T 4 are not met, the hunting cooperation is carried out. Equation (15) displays the position-updating procedures.

$$x_{(i,j)}(t+1) = \begin{cases} \text{Best}_j(t) \times P_{(i,j)} \times \text{rand}, t \le 3\frac{T}{4} \text{ and } t > 2\frac{T}{4} \\ \text{Best}_j(t) - \eta_{(i,j)}(t) \times \epsilon - R_{(i,j)}(t) \times \text{rand}, t \le T \text{ and } t > 3\frac{T}{4} \end{cases} \quad (15)$$

Where, $_{(i,j)}$ is the hunting parameter found by Equation (10) and $\text{ÐÐ}()$ is the best solution achieved. Equation (13) yields the difference parameter $\text{Ø}_{(i,j)}$. Equation (10) determines the hunting parameter, $_{(i,j)}$. Equation (11) determines $\text{Ð}_{(i,j)}$.

V. Performance Analysis

The suggested model's network lifetime analysis is compared to current optimization methodologies, taking into account varying node counts (50, 100, 150, 200, and 250).

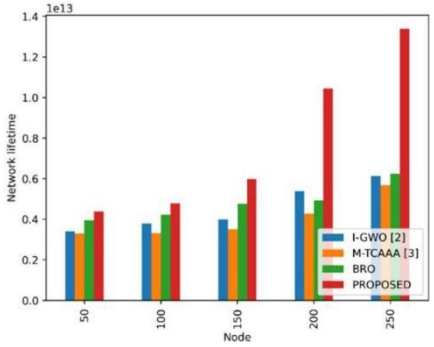

Fig. 2: Performance Analysis for Network Lifetime

Fig. 2 shows a comparison between the lifetime and the number of nodes for both the proposed and existing strategies. The proposed lifetimes of BRO, M-TCAAA, and I-GWO, starting at node 50, are 4.37994E+12, 3.95313E+12, 3.30159E+12, and 3.41565E+12. Proposed BRO, M-TCAAA, and I-GWO lifetimes are 4.78274E+12, 4.21794E+12, 3.31793E+12, and 3.78274E+12 if the node is 100. For node 150, the suggested lifetimes are 5.97701E+12, 4.76607E+12, 3.50448E+12, and 3.99172E+12. These are the BRO, M-TCAAA, and I-GWO estimates. If the node counts 200, the suggested lifetimes for BRO, M-TCAAA, and I-GWO are 1.04368E+13, 4.93324E+12, 4.27646E+12, and 5.39229E+12. And finally, in node 250, the proposed, BRO, M-TCAAA, and I-GWO lifetime are 1.33881E+13, 6.23552E+12, 5.68063E+12, and 6.13324E+12. Compared to other techniques the proposed one has the highest lifetime. Thus, the proposed one outperforms the other existing approaches

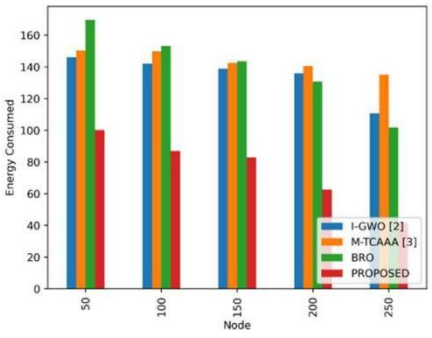

Fig. 3. Performance Analysis for Energy Consumption

Analyzing the differences in energy consumption between the newly developed optimization technique and the established optimization strategies in the context of various node counts, including 50, 100, 150, 200, and 250. In Fig. 3, the number of nodes and the energy usage for the suggested and existing methods are compared. For node 50, the estimated BRO, M-TCAAA, and I-GWO energy consumption are 100.27, 169.65, 150.32, and 146.15, respectively. Similarly, Fig. 3 shows for nodes 100, 150, 200 and 250. When compared to existing procedures, the proposed method uses less energy. Hence it is an efficient system. As a result, the proposed method outperforms the other current methods.

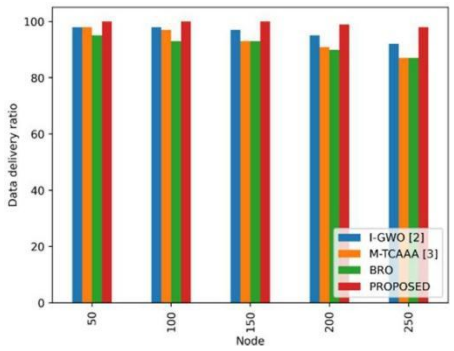

Fig. 4. Performance Analysis for Data Delivery Ratio

The examination of packet delivery between the suggested model and the current optimization methods while taking into account varying node counts (50, 100, 150, 200, and 250). Fig. 4 compares the number of nodes with the delivery ratio for the various numbers of nodes for the current and planned approaches. For node 50, the suggested delivery ratios for BRO, M-TCAAA, and I-GWO are 100, 95, 98, and 98. Fig. 4 shows for nodes 100, 150, 200 and 250. The proposed method has a high delivery ratio in comparison to current strategies. Consequently, the suggested approach performs better than the current ones.

An analysis of the energy efficiency between the newly designed optimization approach and the existing optimization techniques in the proposed energy model with varying numbers of nodes (50, 100, 150, 200, and 250) is shown. Fig. 5 compares the energy efficiency of the proposed and existing approaches with the number of nodes. For node 50, the suggested energy efficiency values are 3.26, 2.21, 2.80, and 2.92 for BRO, M-TCAAA, and I-GWO. Fig. 5 shows for nodes 100, 150, 200 and 250. When compared to existing procedures, the proposed method uses high energy. Hence it is an efficient system. As a result, the proposed method outperforms the other current methods.

The comparison of latency between the suggested model and the current optimization methods, taking into account varying node counts (50, 100, 150, 200, and 250). Fig. 6 shows the number of nodes compared to the latency for the various numbers of nodes for the current and suggested techniques. For node 50, the suggested latency values are 12.45866053, 19.86997883, 17.84845647, and 16.86997883 for BRO, M-TCAAA, and I-GWO. Fig. 6 shows for nodes 100, 150, 200 and 250. When compared to existing strategies, the proposed method's latency is low. As a result, the proposed strategy outperforms the other ones already in use.

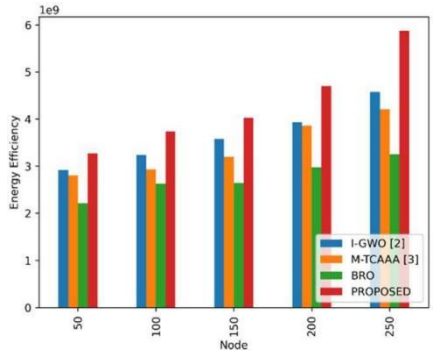

Fig. 5. Performance Analysis for Energy Efficiency

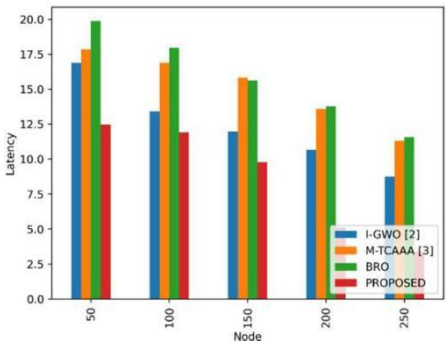

Fig. 6. Performance Analysis for Latency

Security Analysis based on Proposed and Other Existing method

The security analysis is based on the proposed and other existing methods such as AES Encryption and RSA Encryption. These encryption and decryption analysis are provided in the graphical representation.

Fig 7 The comparison of encryption timings across increasing nodes for AES, RSA, and a proposed technique reveals that AES generally has shorter encryption times, though it gradually increases with more nodes. RSA shows a sharper rise in encryption time as node count grows. The proposed technique consistently demonstrates the lowest encryption times across all node counts, indicating superior efficiency.

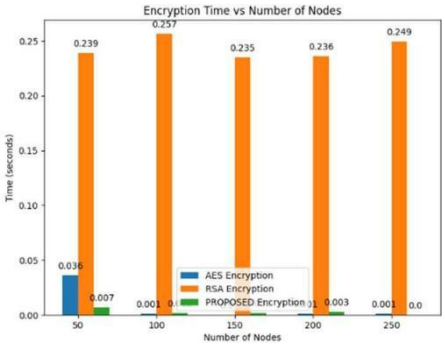

Fig. 7. Performance Analysis for Encryption time graph

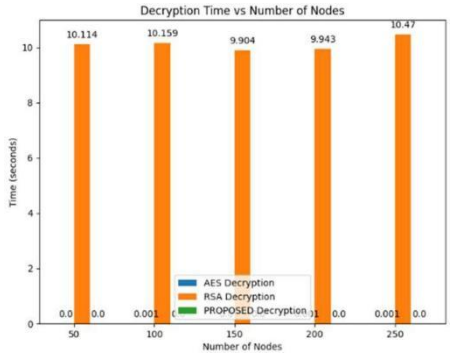

Fig. 8. Performance Analysis for Decryption Time Graph

Fig. 8 shows how the number of nodes in a system relates to the amount of time needed to decrypt data using three distinct encryption algorithms: RSA, AES, and a suggested technique. This Fig. 's x-axis displays the number of nodes in the system, while the y-axis displays the decryption time in seconds. The performance of various decryption techniques is shown by the graph bar. In general, AES decryption scales well with the number of nodes and has shorter decryption times. However, when the number of nodes increases, RSA decryption shows a steeper increase and much longer decryption times than AES. As a result, the Proposed Decryption shows the quickest decryption timings across all node counts, indicating possible gains in efficiency. As a result, when the AES decryption time gradually increases, the number of nodes in a system grows. The decoding time of RSA grows quickly. Even when a lot of nodes are involved, the suggested decryption technique keeps the lowest decryption time.

VI. Conclusion, Limitation and Future Scope

In this research paper, we have developed an extensive framework for transmitting stable statistics over sensor nodes in the field of precision agriculture. Our framework addresses the crucial concerns of privacy and power efficiency. To achieve this, we propose a method that clusters sensor nodes under the control of carefully selected cluster heads (CHs) based on various parameters such as residual power, strength, delay, execution time, and distance. The most suitable CH for dataset communication is determined using a hybrid optimization approach that combines the reptile search algorithm (RSA) and the buffer fish optimization algorithm (POA).

To ensure the security of data during transmission while maintaining trust and privacy, we have devised a novel hybrid encryption method. This method combines symmetric Blowfish encryption with elliptic curve cryptography. Additionally, we have employed the exclusive Bald Eagle Search optimization technique for route selection. This technique minimizes the risk of interception and guarantees the secure transfer of encrypted data.

By prioritizing energy conservation and information protection, our studies provide farmers with accurate and timely information, thereby enhancing the reliability and security of information transmission in precision agriculture. The integration of better optimization strategies and robust cryptography approaches opens up possibilities for safer and more informed decision-making in agricultural practices. To further improve information security and energy efficiency in precision agriculture, future research should focus on investigating the integration of device awareness algorithms with the hybrid optimization and cryptography framework.

References

[1] P. Rajak, A. Ganguly, S. Adhikary, and S. Bhattacharya, "Internet of Things and smart sensors in agriculture: Scopes and challenges," *Journal of Agriculture and Food Research*, vol. 14, p. 100776, Dec. 2023.

[2] B. Alhasnawi, B. Jasim, and B. Issa, "Internet of Things (IoT) for smart precision agriculture," *Iraqi Journal for Electrical and Electronic Engineering*, vol. 16, no. 1, pp. 1–11, Apr. 2020

[3] M. T. Linaza *et al.*, "Data-Driven Artificial Intelligence applications for sustainable precision agriculture," *Agronomy*, vol. 11, no. 6, p. 1227, Jun. 2021.

[4] Y. Zhao, Q. Li, W. Yi, and H. Xiong, "Agricultural IoT data storage optimization and information Security method based on blockchain," *Agriculture*, vol. 13, no. 2, p. 274, Jan. 2023.

[5] M. N. Ramachandra, M. S. Rao, W. C. Lai, B. D. Parameshachari, J. A. Babu, and K. L. Hemalatha, "An efficient and secure big data storage in cloud environment by using triple data encryption standard," *Big Data and Cognitive Computing*, vol. 6, no. 4, p. 101, Sep. 2022.

[6] B. H. D. D. Priyanka, P. Udayaraju, C. S. Koppireddy, and A. Neethika, "Developing a region-based energy-efficient IoT agriculture network using region- based clustering and shortest path routing for making sustainable agriculture environment," *Measurement. Sensors*, vol. 27, p. 100734, Jun. 2023.

[7] R. Kumar, P. Kumar, A. Aljuhani, A. K. M. N. Islam, A. Jolfaei, and S. Garg, "Deep learning and smart Contract-Assisted secure data sharing for IoT-Based intelligent agriculture," *IEEE Intelligent Systems*, vol. 38, no. 4, pp. 42–51, Jul. 2023.

[8] G. S. Nagaraja, K. Vanishree, and F. Azam, "Novel Framework for Secure Data Aggregation in Precision Agriculture with Extensive Energy Efficiency," *Journal of Computer Networks and Communications*, vol. 2023, pp. 1–11, Feb. 2023.

[9] G. Manogaran, M. Alazab, K. Muhammad, and V. H. C. De Albuquerque, "Smart sensing based functional control for reducing uncertainties in agricultural farm data analysis," *IEEE Sensors Journal*, vol. 21, no. 16, pp. 17469–17478, Aug. 2021.

[10] S. V. Gaikwad, A. D. Vibhute, K. V. Kale, and S. C. Mehrotra, "An innovative IoT based system for precision farming," *Computers and Electronics in Agriculture*, vol. 187, p. 106291, Aug. 2021.

[11] E. Kristen, R. Kloibhofer, V. H. Díaz, and P. Castillejo, "Security Assessment of Agriculture IoT (AIOT) Applications," *Applied Sciences*, vol. 11, no. 13, p. 5841, Jun. 2021.

[12] M. Gheisari *et al.*, "An efficient cluster head selection for wireless sensor network-based smart agriculture systems," *Computers and Electronics in Agriculture*, vol. 198, p. 107105, Jul. 2022.

[13] R. Akhter and S. A. Sofi, "Precision agriculture using IoT data analytics and machine learning," *Journal of King Saud University. Computer and Information Sciences*, vol. 34, no. 8, pp. 5602–5618, Sep. 2022.

[14] A. R. Riaz, S. M. M. Gilani, S. Naseer, S. Alshmrany, M. Shafiq, and J.-G. Choi, "Applying adaptive security techniques for risk analysis of internet of things (IoT)-Based smart agriculture," *Sustainability*, vol. 14, no. 17, p. 10964, Sep. 2022.

[15] A. Rokade, M. Singh, P. K. Malik, R. Singh, and T. Alsuwian, "Intelligent Data Analytics framework for precision farming using IoT and regressor machine learning algorithms," *Applied Sciences*, vol. 12, no. 19, p. 9992, Oct. 2022.

[16] G. Ravi, M. S. Das, and K. Karmakonda, "Reliable cluster based data aggregation scheme for IoT network using hybrid deep learning techniques," *Measurement. Sensors*, vol. 27, p. 100744, Jun. 2023.