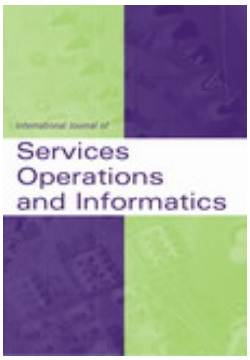


International Journal of Services Operations and Informatics

ISSN online: 1741-5403 - ISSN print: 1741-539X
https://www.inderscience.com/ijsoi

Blockchain-IoT based secure data sharing for precision agriculture with optimal clustering and a hybrid encryption algorithm

T. Senthil Murugan

DOI: 10.1504/IJSOI.2023.10058727

Article History:

Received:	23 May 2023
Last revised:	27 May 2023
Accepted:	04 July 2023
Published online:	19 March 2024

Blockchain-IoT based secure data sharing for precision agriculture with optimal clustering and a hybrid encryption algorithm

T. Senthil Murugan

Department of Information Technology,
Kakatiya Institute of Technology and Science,
Warangal, 506015, Telangana, India
Email: senthilmuruganme@gmail.com

Abstract: Precision agriculture is a farming management technique that uses technology such as Internet of Things (IoT), remote sensing, and information technology to improve crop yields and efficiency. To effectively utilise the resources in precision agriculture, a novel deterministic Blockchain-IoT based secure data sharing model is introduced. The system would use optimal clustering and a hybrid encryption algorithm to ensure the privacy and security of the data being shared. The new optimisation algorithm referred to as SSA-RFO, which combines the concepts of Salp swarm algorithm (SSA) and red fox optimisation algorithm (RFO) is utilised for optimal cluster head selection. Moreover, the hybrid encryption algorithm would use a combination of symmetric and asymmetric encryption to protect the data from unauthorised access. The proposed model has been validated over the existing works in terms of accuracy, specificity, sensitivity, and precision as well.

Keywords: precision agriculture; clustering; AES; advanced encryption standard; DES; data encryption standard; SSA; Salp swarm algorithm; RFO; red fox optimisation algorithm.

Reference to this paper should be made as follows: Senthil Murugan, T. (2023) 'Blockchain-IoT based secure data sharing for precision agriculture with optimal clustering and a hybrid encryption algorithm', *Int. J. Services Operations and Informatics*, Vol. 12, No. 4, pp.285–306.

Biographical notes: T. Senthil Murugan acquired his BE and ME degrees in Computer Science and Engineering (CSE) from Anna University, Chennai, Tamilnadu. His academic journey culminated in 2014 when he achieved his PhD in Computer Engineering from Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamilnadu. Presently, he holds the position of an Associate Professor within the Department of Information Technology at Kakatiya Institute of Technology and Science, situated in Warangal, Telangana. With a distinguished teaching career spanning over 15 years, he expertise is highly regarded. His contributions extend beyond the classroom, with a portfolio boasting more than 30 research articles published across various esteemed journals.

1 Introduction

Agriculture is the practise of preparing the soil for the growth of plants and animals. It entails putting plant and animal products into markets and preparing them for human use (Eyo, 2019; Vougioukas, 2019). One of the most major sectors of the economy that contributes significantly is the agriculture sector, which generates jobs and makes up a sizeable amount of GDP (Odhiambo et al., 2020). In order to boost production, precision agriculture, which is a part of Agriculture 3.0, uses automation and information technology in addition to routine yield monitoring. Agriculture 4.0, sometimes referred to as Smart Agricultural production or Smart farming, is an impending revolution in the agriculture industry that would significantly affect the country's economy by utilising technology like the Internet of Things (IoT) (Vangala et al., 2023). Precision agriculture is the perfect application for the IoT due to its highly interoperable, scalable, widespread, and open nature. IoT-derived technologies come in a variety of forms, and they all have benefits of their own, including reducing the danger of vendor lock-in, empowering machines, and enhancing sensing and automation systems (Khriji et al., 2021).

The main IoT applications in the agricultural sector are livestock, greenhouses, and precision farming. Various monitoring domains have been used to group these use cases. Numerous IoT-based sensors and gadgets are used to monitor all of these operations thanks to the deployment of wireless sensor networks (WSN), which enables farmers to gather important data using sensing equipment (Chaudhari Waghulde and Chopade, 2022). Utilising inexpensive electronic equipment and communication protocols, the Internet of Things paradigm enhances human involvement in the physical environment (Rashid et al., 2020). IoT also keeps track of various environmental variables to produce accurate, real-time temperature maps, air pollution, noise level, and hazardous radiation. The user may also receive message alerts or trigger alerts that make recommendations to authorities with information gathered about various environmental parameters (Elmustafa and Mujtaba, 2019). The challenge of maintaining high security requirements with minimal resources is one that WSNs encounter. Node authentication, confidentiality of information, anti-compromise, and traffic surveillance resilience are among the security methods for WSNs. IoT also monitors a variety of environmental variables to provide accurate, real-time temperature, air pollution, noise, and harmful radiation maps (Gharaei, 2022).

Precision soil farming, smart farming, and other IoT applications have recently been implemented for smart agriculture using WSN (Mahajan and Badarla, 2021). Security has been boosted by IoT. At the moment, blockchain technology provides security for precision agriculture (Anand, 2021). Network nodes are organised into groups or clusters using clustering algorithms, with a designated node, the cluster head, in charge of each cluster (Behera et al., 2019). Clustering algorithms have been highly recommended in the context of WSN, but their use in IoT may also be able to address related issues. Clustering would make routing and topology management more energy-efficient by distributing a sizable portion of the communication overhead to the cluster head (Kasturi et al., 2022). Although a lot of research has focused on designing cryptography solutions and device security (Alfa et al., 2021), Numerous issues still exist, particularly with regard to data integrity and the dearth of metrics for device security (Alonso et al., 2020).

The chapters were organised according to the following pattern: The basic introduction is provided in Chapter 1, the theoretical background of the literature review conducted for this research work is provided in Chapter 2, the overview of the proposed

methodology is provided in Chapter 3, the proposed algorithm is used in chapter 4, the experimental results of the same are summarised in Chapter 5, and the research works conclusions are provided in Chapter 6.

2 Literature review

There have already been extensive research projects on writing that focused on Blockchain-IoT based secure data sharing for precision agriculture and multi-objective algorithms based on optimal clustering and hybrid encryption methods. Here are some examples of the reviewed works.

Elijah et al. (2018) had provided an overview of IoT and DA in agriculture. Also discussed about a number of IoT-related topics in relation to agriculture. The review of the literature reveals that there was a significant amount of work was done to develop IoT technology that can be used to boost plant and livestock productivity and operational effectiveness. Then identified and discussed the advantages of IoT and DA as well as open challenges. The agriculture industry can anticipate a number of advantages from IoT.

Haseeb et al. (2020) had proposed an IoT-based WSN framework with various design levels as a smart agriculture application. First, relevant data was collected by agricultural sensors, which then use a multi-criteria decision function to select a set of cluster heads. SNR was also used to measure the signal strength on the transmission links in order to ensure reliable and effective data transmission. Second, data transfer security from agricultural devices to BS was provided by the linear congruential generator's recurrence.

Rangwani et al. (2021) had discussed the most recent user authentication methods for WSNs, their benefits, and drawbacks, and then provided a more secure and efficient three-factor remote authentication solution for WSNs used for agricultural surveillance. The proposed scheme has minimal communication, computation, and memory overheads because ECC was used. Additionally, the suggested scheme makes it simple for a legitimate user to update or modify their password while the gateway was active. A formal security evaluation of the suggested scheme was conducted by widely used Random Oracle Model to assess the level of security of the scheme.

Ali et al. (2018) had suggested a safe remote user authentication system in order to monitor agricultural fields. The proposed was supported by mutual authentication, and used BAN logic to demonstrate that. Additionally, testing our protocol using the AVISPA software ensures that it can withstand both active and passive attacks. The results of the formal and informal security analyses demonstrate that the system can withstand different types of malicious attacks. Therefore, use the scheme in real time and it was effective.

Sharma and Tomar (2021) used cluster head selection to investigate alternative energy-efficient procedures in WSN. There are many well-known clustering protocols, such as LEACH, PEGASIS, and DEC. The stability interval and lifetime of the network of the network system can be shortened by grouping low energy network devices into cluster heads in LEACH. In contrast, it was suggested that the DEC protocol be improved upon because it was a scenario that was close to ideal. The multitier structure and new normal random initialisation were utilised to extend network lifetime and boost the energy efficiency of the conventional DEC protocol.

Alghazzawi et al. (2021) had explained different agricultural models for evapotranspiration. The Penman-Monteith equation was used to assess key variables like

congestion control. In order to divide the relationship between the number of sources evenly, and focused on using more than two references parameters, such as evapotranspiration and humidity, under various conditions. Also demonstrates the MATLAB implementation, which was used to modify values. Similar variations can be produced using the same source value, demonstrating the effectiveness and fairness of the suggested model. Table 1 provides a comprehensive review of the existing works on Blockchain-IoT based secure data sharing for precision agriculture.

Table 1 Review on the existing works

Author	*Aim/process*	*Research gaps*
Rashid et al. (2020)	Outlined the IoT architecture for addressing a range of problems and difficulties in real-world situations	Consumes higher computation and communication cost
Elmustafa and Mujtaba (2019)	Gave a quick overview of the IoT-based environment study areas	Not efficient for large agricultural fields
		Low security in IoT
Gharaei (2022)	A secure inter- and intra-cluster energy-balancing scheme in rechargeable wireless sensor networks for smart city applications	Not applicable for real-time analytics
		Use weak security algorithms with limited memory
Mahajan and Badarla (2021)	Using a Nature-Inspired Algorithm, a Cross-Layer Interface for IoT Smart Farming Systems with WSN Support	High power energy consumption with gateway highly prone to attacks such as forwarding, congestion attack and DoS
Anand (2021)	An IoT-Based Protected and Energy Efficient Precision Agriculture Program Using Blockchains and An Improved Leach Algorithm	Longer execution time
		No description of carrying out clustering
Alonso et al. (2020)	A sophisticated edge-IoT platform for the dairy industry that can monitor livestock and crops	Requires improvement in runtime and scalability
		Consumes huge bandwidth
		Do not have load balancing capability
Haseeb et al. (2020)	A Secure and Energy-Efficient IoT-Based WSN Framework	Doesn't enhance the confidentiality in the cloud
		Do not evade against the privacy breaches
Ali et al. (2018)	Monitoring agriculture with wireless sensor networks using a secure user key-agreement and authentication system	Higher data loss
		Higher computation's time and memory requirements
Song et al. (2020)	Smart Agriculture: A Flexible Data Publishing Scheme for Privacy Protection	Provides only precision values that is not accurate and is not cost efficient

Wu and Tsai (2019) had suggested Using dark web – based technology to safeguard servers' and blockchains' privacy. To stop DDOS attacks, track the frequency of packet transmission in intelligent agriculture. The system's key characteristics include a method

for identity identification, safe data transmission, the ability to create private blockchains, a speedier, more effective method of blockchain information authentication, and resistant to DDOS attacks. By utilising dark web – based technology, the suggested plan can protect network security for IoT devices as well as servers. By doing so, it can prevent blockchains and server ID addresses from being exposed, which lowers the likelihood of DDOS attack damage.

Song et al. (2020) has established a flexible data gathering plan based on intelligent agriculture that safeguards privacy and permits selective batch processing in the virtual aggregate area. The analysis demonstrates how effective, safe, and privacy-preserving the suggested strategy.

Objectives

- To undergo a literature review on the existing works on IoT-precision agriculture-based data sharing, and to identify the problem statement of the same.
- To design new multi-objective optimisation based optimal clustering and cluster head selection approach.
- To introduce a new hybrid optimisation model for selecting the best node as the CH (optimal CH).
- To introduce a new hybrid cryptographic model for secured data transmission in precision agriculture.
- To undergo a comparative analysis on the proposed work, to validate its efficiency over the existing models.

3 Proposed methodology

Precision agriculture is a technology that uses advanced tools and techniques to optimise crop yields and reduce waste. This is achieved by using IoT devices such as sensors, drones, and precision farming equipment to collect data on factors such as soil moisture, temperature, pH levels, and crop health. This data is then analysed using machine learning and other information technology tools to identify patterns and make predictions about crop growth and yields. Structure of the proposed work is shown in Figure 1.

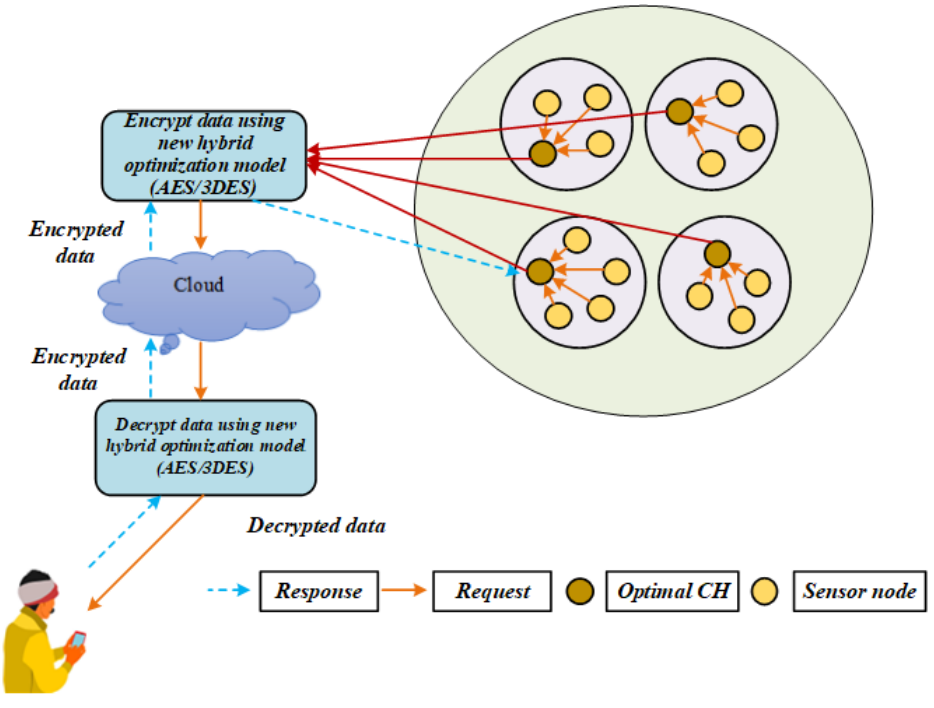
The two major phases of precision agriculture are clustering and data transmission. Clustering involves grouping similar data points together and identifying patterns in the data. This can help farmers to identify areas of their fields that are most productive and target their resources to those areas. The data acquired is safeguarded and shielded against unauthorised access using cryptographic algorithm-based protected data transmission. This is important to protect the privacy and security of farmers and their data. Overall, precision agriculture is a technology that can help farmers to improve crop yields, reduce waste, and optimise their resources. However, the implementation of this technology requires a significant investment in infrastructure, equipment, and expertise.

3.1 Clustering

Clustering is a technique used in machine learning and data analysis to group similar data points together. It is a method of unsupervised learning, which means that the data is not

labelled and the algorithm must find patterns and structure in the data without any prior knowledge. Clustering can be used to identify patterns and trends in large datasets, and is often used in precision agriculture to analyse data collected from sensors and other monitoring devices. There are several different types of clustering algorithms, including centroid-based, density-based, and hierarchical clustering. Centroid-based clustering algorithms, such as k-means, use the mean or median of a group of data points as the centre of the cluster. Density-based clustering algorithms, such as DBSCAN, group data points together that are close to each other in space. Hierarchical clustering algorithms, such as agglomerative and divisive, build a hierarchy of clusters by repeatedly merging or splitting clusters.

Figure 1 Structure of the proposed work (see online version for colours)



Clustering can be utilised in precision agriculture to find patterns in sensor data, such as soil moisture, temperature, and pH levels. For example, clustering can be used to identify areas of a field that have similar soil conditions, which can then be targeted for different types of crop management. Clustering can also be used to identify patterns in crop growth and yields, which can help farmers to optimise their resources and improve crop yields.

3.1.1 Soil moisture

Crop development and yield are significantly influenced by the moisture content of the soil. It is the amount of water present in the soil, and it can vary depending on factors such as precipitation, evaporation, and plant uptake. Crops must have sufficient soil moisture to grow and develop properly, as it provides the water that plants need to absorb nutrients and carry out metabolic processes. In precision agriculture, soil moisture is

typically measured using sensors that are placed in the soil. These sensors can be connected to a wireless network, allowing farmers to monitor soil moisture levels in real-time. Making informed judgements concerning irrigation as well as other water quality management techniques can be done using the data collected by these sensors.

3.1.2 Temperature

Temperature is an important environmental factor that affects the growth and development of crops. The optimal temperature range for most crops is between 15-30 degrees Celsius. However, different crops have different optimal temperature range, for instance, some crops like wheat and corn can tolerate a wide range of temperature whereas some crops like tomatoes and peppers are more sensitive to temperature fluctuations. When the temperature is too high or too low, it can stress the plants and reduce crop yields. In precision agriculture, temperature is typically measured using sensors that are placed in the field. These sensors can be connected to a wireless network, allowing farmers to monitor temperature levels in real-time. The data collected from these sensors can be used to make informed decisions about crop management practices. For example, if the temperature is too high, farmers can take steps to protect the crops from heat stress, such as by providing shade or irrigation.

3.1.3 pH levels

A solution's acidity or basicity (alkalinity), as determined by its pH. In the case of soil, it measures the acidity or basicity of the soil. The pH scale runs from 0 to 14, with neutral being 7, acidic being less than 7, and basic being more than 7. Different plants have different pH requirements, some plants require acidic soil while others require neutral or alkaline soil. In precision agriculture, pH levels are typically measured using sensors that are placed in the soil. These sensors can be connected to a wireless network, allowing farmers to monitor pH levels in real-time. The data collected from these sensors can be used to make informed decisions about crop management practices such as fertilisation and liming.

For example, if the pH level is too low (acidic), farmers can add lime to the soil to increase the pH level and make the soil more alkaline. If the pH level is too high (alkaline), farmers can add sulphur or other acidic materials to the soil to decrease the pH level and make the soil more acidic.

3.1.4 Energy

Energy is an important factor in precision agriculture as it is required to power the various sensors, equipment, and other technologies used in this field. Sensors, drones, and other precision farming equipment require a steady source of energy to function properly, and the cost of energy can be a significant factor in the overall cost of precision agriculture.

3.1.5 Delay

Delay can occur in precision agriculture due to various reasons, such as communication delays between sensors and the control centre, delays in data processing and analysis, or delays in taking action based on the data. These delays can lead to inefficiencies and can

negatively impact crop yields. To minimise delays, it is important to have a robust and reliable communication network, to use efficient data processing and analysis techniques, and to have a clear plan for how to act on the data in a timely manner.

3.1.6 Execution time

Execution time refers to the amount of time it takes for a task or process to be completed. In precision agriculture, execution time can refer to the time it takes for data to be collected, processed, and analysed, as well as the time it takes for actions to be taken based on the data. The execution time can be affected by various factors such as the complexity of the data processing and analysis algorithms, the speed of the hardware and communication infrastructure, and the amount of data being collected. To minimise execution time, it's important to use efficient data processing and analysis algorithms that can quickly and accurately extract insights from the data. The use of powerful and fast hardware, such as high-performance computing systems, can also help to minimise execution time. Additionally, parallel processing techniques such as distributed computing can also be used to speed up data processing. Another way to minimise execution time is to optimise the data collection process. This can include reducing the amount of data being collected, using more efficient sensors, or using more efficient data transmission methods.

3.1.7 Distance

In precision agriculture, the design and functionality of wireless sensor systems can be significantly influenced by the distances among nodes as well as the distances to the sink node. The Euclidean distance between nodes is a measure of the physical distance between two nodes in a network. This distance can affect the strength of the wireless signal and the amount of energy required to transmit data between nodes. In precision agriculture, the Euclidean distance between nodes can be an important factor in determining the placement of sensors and other network components. For example, if the sensors are placed too far apart, it may be difficult to get accurate and reliable data, and if they are too close, the amount of energy used by the network could be increased.

The distance to the sink node is a measure of the distance between a node and the central hub of the network, known as the sink node. The sink node is typically responsible for collecting, processing, and studying the information coming from every other node in the network. Energy usage and the time it takes for data to be transmitted from nodes to the sink node can both be impacted by the range to the sink node. In precision agriculture, the distance to the sink node can be an important factor in determining the placement of the sink node, such as finding a central location that is close to most of the sensor nodes to minimise the energy consumption and delay.

3.1.8 Residual energy

Residual energy refers to the remaining energy that is available in a wireless sensor node after performing its tasks. In precision agriculture, to gather information about the environment, such as heat, humidity, and moisture levels, wireless sensor devices are employed. These sensors require energy to operate, and the energy consumption of a sensor node can vary depending on the type of sensor, the sink node's location and

sampling frequency. Consideration of a wireless sensor node's residual energy is crucial for the design and operation of such a wireless sensor network. When the residual energy of a sensor node is low, it can lead to a reduction in the network's performance, such as a decrease in the data collection rate, or even failure of the node.

In precision agriculture, in order to maximise the functionality of wireless sensor networks and raise crop yields, it is crucial to take into account elements like reduced energy, lower latency, shorter execution times, and closer proximity.

3.1.9 Lower energy

Lower energy consumption can be achieved by using energy-efficient algorithms, reducing the sampling rate, and using energy harvesting techniques to recharge the nodes. Energy-aware routing algorithms can also be used to route data to the sink node through nodes with higher residual energy.

3.1.10 Lower delay

Lower delay can be achieved by using efficient data processing and analysis algorithms, powerful hardware, and by optimising the data collection process. Additionally, minimising the distance to the sink node can also help to minimise delay.

3.1.11 Lower execution time

Lower execution time can be achieved by using efficient data processing and analysis algorithms, powerful hardware, and by optimising the data collection process.

3.1.12 Lower distance

Lower distance can be achieved by optimising the placement of sensors and other network components. For example, if the sensors are placed too far apart, it may be difficult to get accurate and reliable data, and if they are too close, the energy consumption of the network could be increased.

4 Proposed hybrid optimisation model

4.1 Salp swarm algorithm (SSA)

An optimisation technique known as the salp swarm algorithm (SSA) is based on the behaviour of swarms of salp (a form of plankton) in the ocean. It's a bio-inspired program that imitates salps' movements and social interactions to find the best answers to a given challenge (Mirjalili et al., 2017). The method searches the space of potential solutions using a collection of particles known as a 'swarm'. The method use a mixture of global and local search strategies to direct the swarm of particles toward the ideal answer. Every component in the swarm indicates a possible solution to the issue. Functional optimising, extraction of features, and image processing are just a few of the optimisation issues that SSA has been used to solve.

Step 1: Initialisation

In this step, we initialise the parameters like Energy, Delay, Execution time, Distance, Residual energy

Step 2: Random Generation

After initialisation, the input features are created at random.

Step 3: Fitness Evaluation

$$Z_n^1 = \begin{cases} p_n + r_1\left(\left(U_n - L_n\right)r_2 + l_n\right)r_3 \geq 0 \\ p_n - r_1\left(\left(U_n - L_n\right)r_2 + l_n\right)r_3 < 0 \end{cases} \tag{1}$$

$$r_1 = 2e^{-}\left(-\frac{4a}{A}\right)^2 \tag{2}$$

The coefficient r_1 is crucial for SSA because it balances the capabilities for exploration and exploitation.

To change the followers' position, apply the following equations.:

$$Z_n^m = \frac{1}{2}ce^2 + v_0 e \tag{3}$$

where $m \geq 2$, $c = \frac{v_{Final}}{v_0}$ where $v = \frac{Z - Z_0}{e}$. This equation can be expressed as follows since the time spent optimising equals iteration, the conflict among iterations is equal to 1, and $v_0 = 0$ is taken into consideration.

$$Z_n^m = \frac{1}{2}\left(Z_n^m + Z_n^{m-1}\right) \tag{4}$$

Step 6: Termination

Verify the stopping requirements. Step 4 should be taken if the halting requirements have not been met after the maximum number of iterations.

4.2 Red fox optimisation algorithm (RFO)

The red fox optimisation technique (RFO) is a bio-inspired optimisation technique that draws its inspiration from red fox behaviour in its natural environment. The algorithm is designed to mimic the way that red foxes search for food by using a combination of random and local search techniques (Połap et al., 2021). In RFO, a population of potential solutions is created and the algorithm uses a combination of local search and global exploration to guide the population towards the optimal solution. The algorithm uses a red fox's ability to adapt its search strategy based on the environment to guide the population towards the global optimal solution. RFO algorithm is mainly used for optimisation problems such as function optimisation, feature selection, and image processing.

Step 1: Initialisation

The output of the SSA is given to the input of Red Fox Optimisation Algorithm

Step 2: Random Generation

After initialisation, the input features are created at random.

Step 3: Fitness Evaluation

Step 4: In search for food – global search phase

In the suggested method, we presuppose that the best person has travelled to the most fascinating places and can impart this knowledge to a family. As a result, we first sort the population by fitness level, as well as for $\left(\bar{X}^{best}\right)^t$. The Euclidean distance square between every person in the population is calculated as

$$D\left(\left(\bar{X}^i\right)^t, \left(\bar{X}^{best}\right)^t\right) = \sqrt{\left\| \left(\bar{X}^i\right)^t - \left(\bar{X}^{best}\right)^t \right\|} \tag{5}$$

and we direct population members toward the most effective one.

$$\left(\bar{X}^i\right)^t = \left(\bar{X}^i\right)^t + \alpha\, Sign\left(\left(\bar{X}^{best}\right)^t - \left(\bar{X}^i\right)^t\right) \tag{6}$$

where $\alpha \in \left(0, D\left(\bar{X}^i\right)^t, \left(\bar{X}^{best}\right)^t\right)$ is a randomised growth hyperparameter set once for every cycle for the overall population.

Step 5: Traversing through the local habitat – local search phase

$$\begin{cases} Move\,closer & IF\ \mu > 0.75 \\ Stay\ and\ disguise & IF\ \mu \le 0.75 \end{cases} \tag{7}$$

If the parameter μ indicates that the population should move during this every cycle, we apply a modified Cochleoid equation to show how each person will travel.

$$r = \begin{cases} a\dfrac{\sin\left(\phi_0\right)}{\phi_0} & IF\ \phi_0 \neq 0 \\ \theta & IF\ \phi_0 \neq 0 \end{cases} \tag{8}$$

Where θ is denoted as a randomly generated value between 0 and 1 that is set once at the start of the process and represents the impact of bad weather.

$$\begin{cases} X_0^{new} = ar \cdot \cos\left(\phi_1\right) + X_0^{actual} \\ X_1^{new} = ar \cdot \sin\left(\phi_1\right) + ar \cdot \cos\left(\phi_2\right) + X_1^{actual} \\ X_2^{new} = ar \cdot \sin\left(\phi_1\right) + ar \cdot \sin\left(\phi_2\right) + ar \cdot \cos\left(\phi_3\right) + X_2^{actual} \\ \cdots \\ X_{n-2}^{new} = ar \cdot \sum_{k=1}^{n-2} \sin\left(\phi_k\right) + ar \cdot \cos\left(\phi_{n-1}\right) + X_{n-2}^{actual} \\ X_{n-1}^{new} = ar \cdot \sin\left(\phi_1\right) + ar \cdot \sin\left(\phi_2\right) + \cdots + ar \cdot \sin\left(\phi_{n-1}\right) + X_{n-1}^{actual} \end{cases} \tag{9}$$

Whereby every angular value for each point is randomised according to $\phi_1, \phi_2, ...\phi_{n-1} \in (0, 2\pi)$

Step 6: Termination

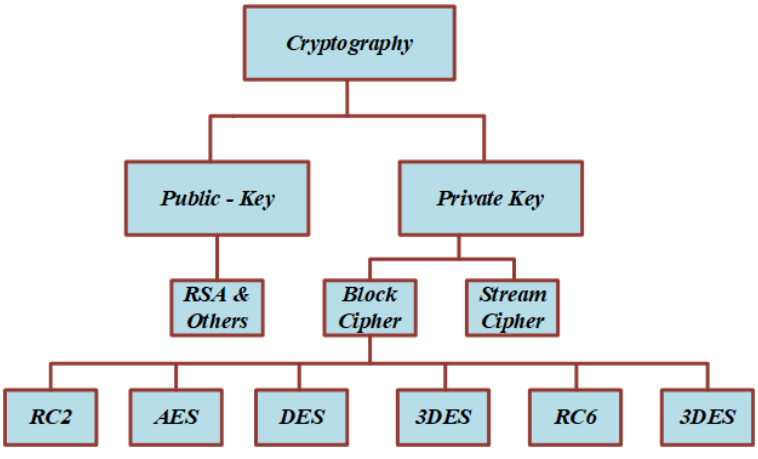
Verify the stopping requirements. Step 4 should be taken if the halting requirements have not been met after the maximum number of iterations.

4.3 Hybrid cryptographic model

4.3.1 Cryptography

Cryptography is the practice of securing communication and information by transforming it into a code or cipher that can only be read by authorised parties. It serves as a safeguard against unauthorised access, alteration, and disclosure of data. Numerous uses for cryptography exist, including those related to confidentiality, integrity, identification, and non-repudiation. Symmetric and asymmetric cryptography are the two primary categories. The same secret key is employed in symmetric cryptography for both decryption and encryption. AES is the most popular symmetric encryption algorithm. Two separate keys are utilised for decryption and encryption in asymmetric cryptography, commonly referred to as public key cryptography. The data is encrypted using a public key and decrypted with a private key. The most widely used asymmetric encryption algorithm is RSA. Cryptography is used in many different fields, including computer science, telecommunications, and finance, and is essential for secure online communication and transactions. Structure of Cryptography is given in Figure 2.

Figure 2 Structure of cryptography (see online version for colours)



Depending on how many keys are utilised, cryptographic algorithms can be categorised as symmetrical or asymmetric (public key) (secret key). In symmetric key encryption, also known as secret key encryption, both the transmitter and the receiver use the same key. Data encryption standard (DES), 3DES, and Encryption Algorithm are a few examples of symmetric key encryption techniques (AES). Asymmetric key encryption uses two different keys (public and private keys) for encryption and decryption. While the public key is utilised for encryption, the secret key is utilised for decryption. Elliptic

Curve Cryptosystem and Rivest-Shamir-Adelman (RSA) are two asymmetric key algorithms (ECC). Five components make up a symmetric cryptosystem:

I *Plain text*

This is the first information or message that will be transmitted and is used as input by the algorithm.

II *Encryption algorithm*

On the plaintext, the algorithm applies different transformations and substitutions.

III *Secret key*

The value of the secret key is independent of the plaintext and is another input to the algorithm. The outcome of the algorithm will vary depending on the individual key.

IV *Cipher text*

The result of the message's encryption or scrambling is shown here. For this output, the plaintext and private keys are necessary.

V *Decryption algorithm*

Essentially, this is the block cipher reversed. It accepts the ciphertext and private keys as input and outputs the genuine plaintext.

4.3.2 AES algorithm

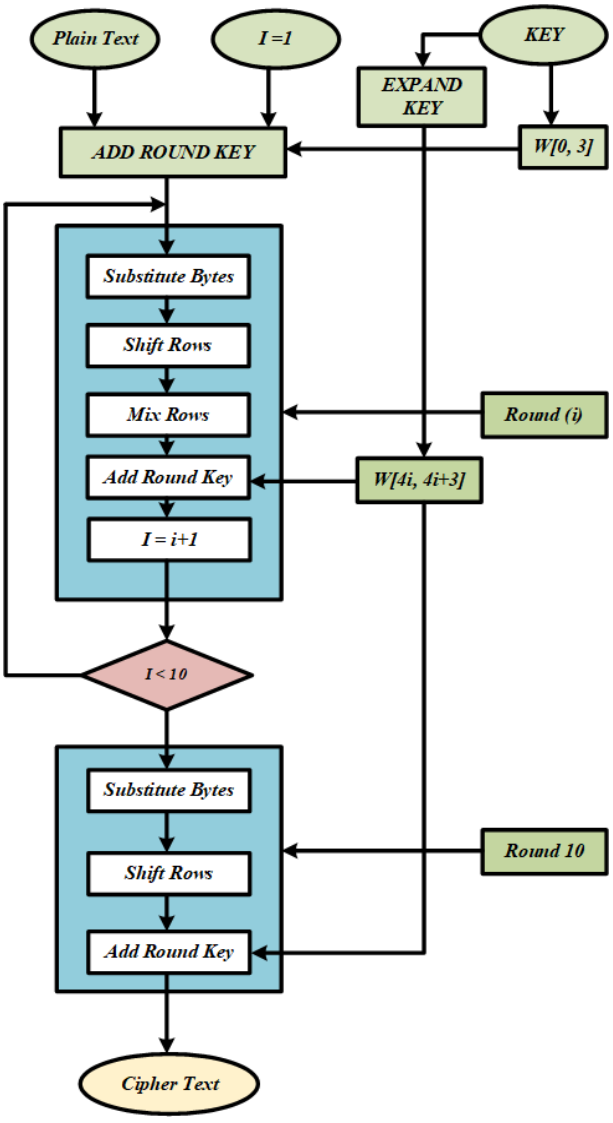
The US government originally used the symmetric encryption method known as advanced encryption standard (AES) in 2001. It is a block cypher that uses a secret key with a predetermined length to encrypt and decrypt data in fixed-size blocks (128 bits) (128-bits, 192-bits, or 256-bits). AES uses a process known as substitution-permutation network (SPN) to encrypt data. The encryption process includes several rounds of substitution and permutation operations, each of which transforms the plaintext in a specific way. The key schedule, which is a part of the algorithm, generates a series of round keys that are used in each round. The encryption method uses the exact same round keys as the decryption process, but they are used in the opposite sequence. Flow of AES is shown on Figure 3.

AES is utilised in a number of applications, such as strong encryption, file encryption, and protection of information, and is thought to be very efficient and secure. It is also widely supported by hardware and software vendors, making it a popular choice for encryption.

4.3.2.1 Bytesub transformation

It is a multiplicative inverse and affine transformation-generated substation table (s-box)-based nonlinear byte substitution.

Figure 3 Flow of advanced encryption standard (AES) (see online version for colours)



4.3.2.2 Shiftrows transformation

It is a simple byte transposition in which the bytes inside the agency's final three rows are circularly shifted based on the row location; the left shift might be anywhere between zero and three bytes.

4.3.2.3 Mixcolumns transformation

This round equates to multiplying each state's column by a matrix. A fixed matrix is multiplied by each column vector. Instead of treating the bytes as numbers, his operation treats them as polynomials.

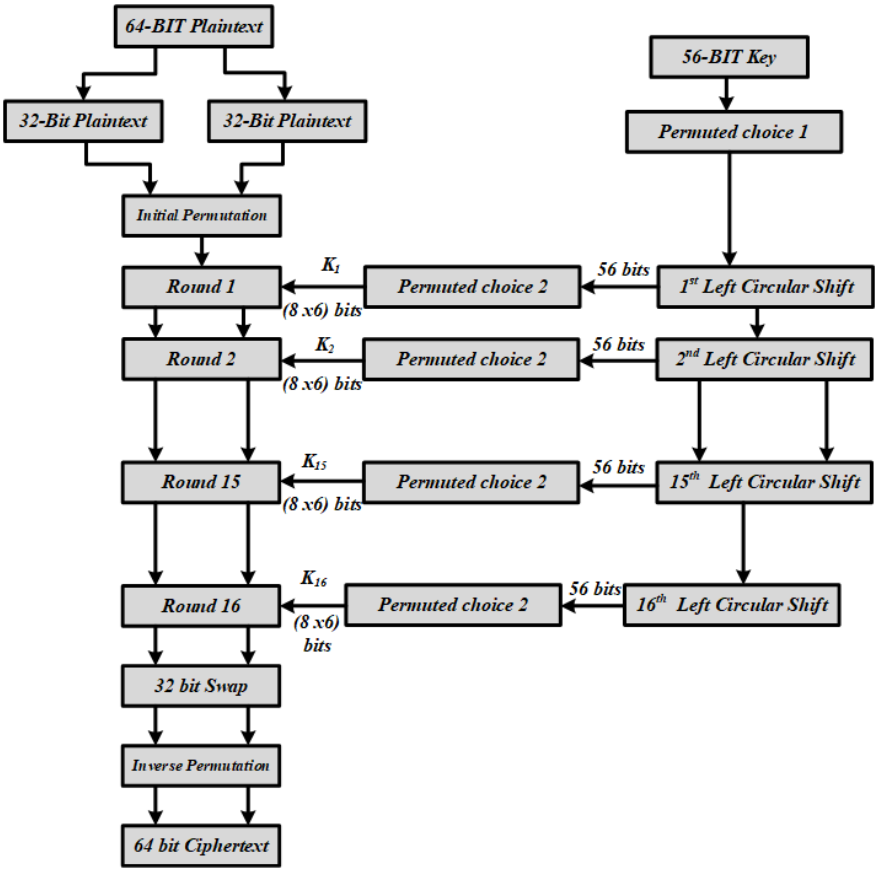
4.3.2.4 Addroundkey transformation

The round key and the current state are simply XORed. This transformation is the inverse of itself. There are various processes involved in the encryption process. The addroundkey operation is followed by applying a round function to the data block. This round process is performed repeatedly depending on the key's size (Nr times). The decryption process follows the exact same series of transformations as the encryption algorithm. According to the modifications Inv-Bytesub, Inv-Shiftrows, Inv-Mixcolumns, and Addroundkey, the key schedules' forms can be similar for encryption and decryption.

4.3.3 DES/Triple DES algorithm

The symmetric key encryption method known as DES was once widely used but has largely been supplanted by AES. Using a 56-bit key, it encrypts the data in 64-bit blocks. Similar to AES, the encryption method involves numerous rounds of permutation and substitution operations. Figure 4 illustrates the DES encryption procedure.

Figure 4 Encryption process of DES



DES was considered to be very secure when it was first adopted in 1977, but with the advancement of technology, it became clear that the 56-bit key size was no longer

sufficient to provide adequate security. Triple DES (3DES), a DES variant, was created as a solution to this problem. Using two or three distinct keys, Triple DES runs the Homomorphic encryption three times on each block of data. This increases the key size to 112 or 168 bits, making it more secure than standard DES. Since DES has a flexible nature, it can function in any cryptographic mode. Like other cryptographic algorithms, DES encrypts and decrypts data using permutation and substitution processes. While permutation reorders the places of the bits in the input data, substitution substitutes one value for another. The number of times these procedures are repeated is referred to as a round, and it is generally accepted that the algorithm's strength increases with the number of rounds.

The DES algorithm is a symmetric-key encryption algorithm that operates on 64-bit blocks of data using a 56-bit key. The algorithm consists of 16 rounds, each of which performs a series of mathematical operations on the data. The overall process of the DES algorithm can be broken down into the following steps:

1 *Initial permutation (IP)*: The 64-bit data block is rearranged according to a predefined permutation table.

2 *Key generation*: The 56-bit key is expanded to 48 bits using a key schedule.

3 *Round function*: In each round, the data is divided into two 32-bit blocks, the right block (R) and the left block (L). The R block is then passed through a function (F) that takes the R block and a 48-bit key as input. The output of this function is then XORed with the L block to produce a new R block. The L and R blocks are then swapped, and this process is repeated for a total of 16 rounds.

4 *Inverse initial permutation (IP^-1)*: The final R and L blocks are then rearranged according to a reverse permutation table to produce the encrypted data.

For Triple-DES (3DES), the process is similar but instead of one key and one encryption process, it uses three keys and encrypts the data three times. The algorithm can either use three different keys (3-key 3DES) or two different keys (2-key 3DES). Accordingly, the data is first encrypted with the initial key, subsequently decoded with the second key, and then encrypted once more with the third key. This process makes the algorithm more secure but also slower than the original DES.

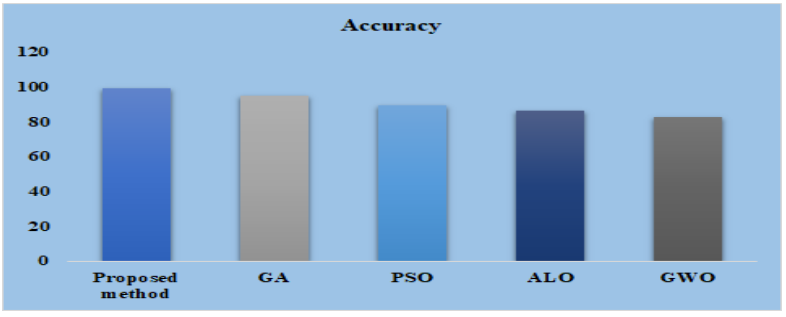
5 Result and discussion

In summary, the proposed system for secure data sharing in precision agriculture combines IoT and blockchain technology to improve agricultural productivity. The system uses clustering to group similar sensor nodes together and a multi-objective optimisation approach to select the optimal cluster head. The collected data is then stored in the cloud and protected using a hybrid encryption algorithm (AES and 3DES/TDEA). The encrypted data is then transmitted via the blockchain network to ensure secure and tamper-proof transmission. At the receiver end, the data is decrypted using the same hybrid encryption algorithm. The overall system aims to provide a secure and efficient way to collect, transmit and analyse data in precision agriculture.

Accuracy analysis is shown in Figure 5. Here the accuracy of proposed method is 98.97, the GA method is 94.86, the PSO method is 89.26, the ALO method is 86.54, the

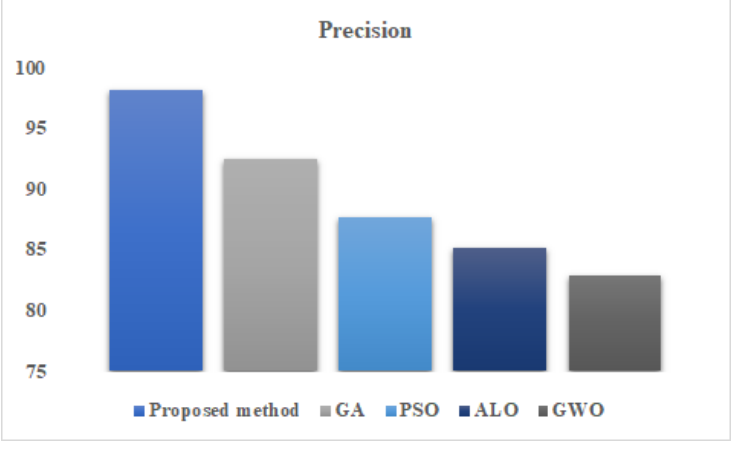
GWO method is 82.45. The outcome of the proposed method is high compared to the existing technique in accuracy.

Figure 5 Accuracy analysis (see online version for colours)



Precision Analysis is shown in Figure 6. Here the Precision of proposed method is 98.23, the GA method is 92.54, the PSO method is 87.63, the ALO method is 85.21, the GWO method is 82.87. The outcome of the proposed method is high compared to the existing technique in precision.

Figure 6 Precision analysis (see online version for colours)



Recall analysis is shown in Figure 7. Here the Recall of proposed method is 97.92, the GA method is 95.62, the PSO method is 93.87, the ALO method is 90.65, the GWO method is 88.12. The outcome of the proposed method is high compared to the existing technique in recall.

Analysis of F measure is shown in Figure 8. Here the F measure of proposed method is 97.68, the GA method is 94.12, the PSO method is 91.87, the ALO method is 90.55, the GWO method is 89.21. The outcome of the proposed method is high compared to the existing technique in E measure.

Analysis of NPV is shown in Figure 9. Here the NPV of proposed method is 97.98, the GA method is 95.32, the PSO method is 92.16, the ALO method is 91.52, the GWO method is 89.23. The outcome of the proposed method is high compared to the existing technique in NPV.

Figure 7 Recall analysis (see online version for colours)

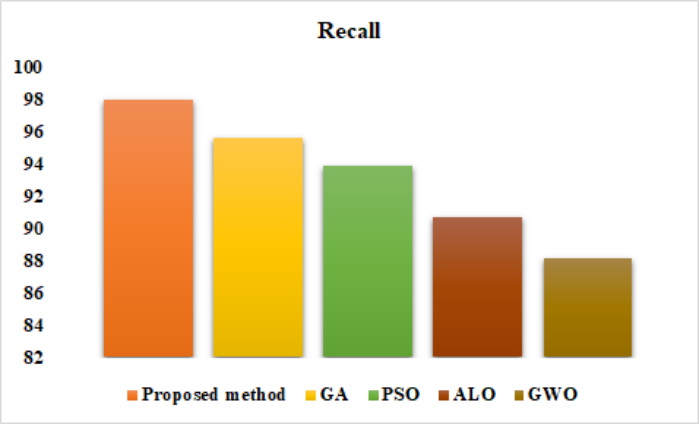


Figure 8 Analysis of F measure (see online version for colours)

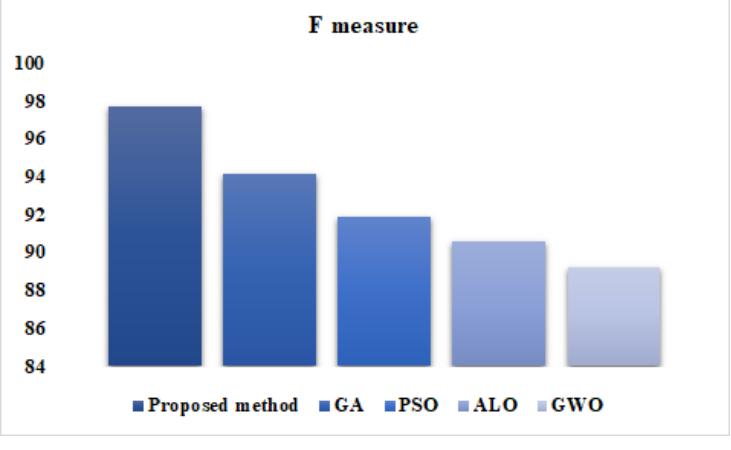
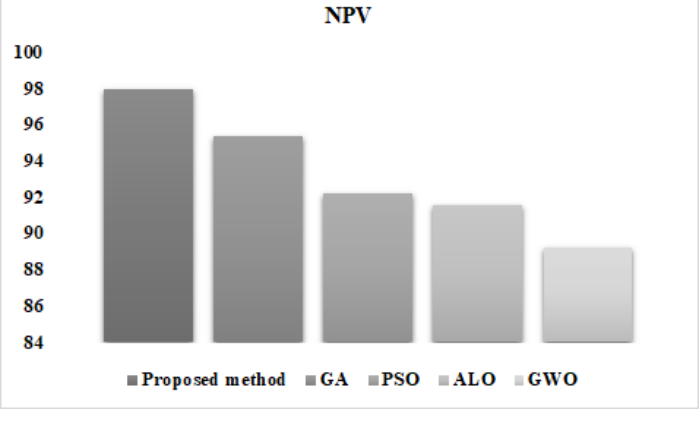
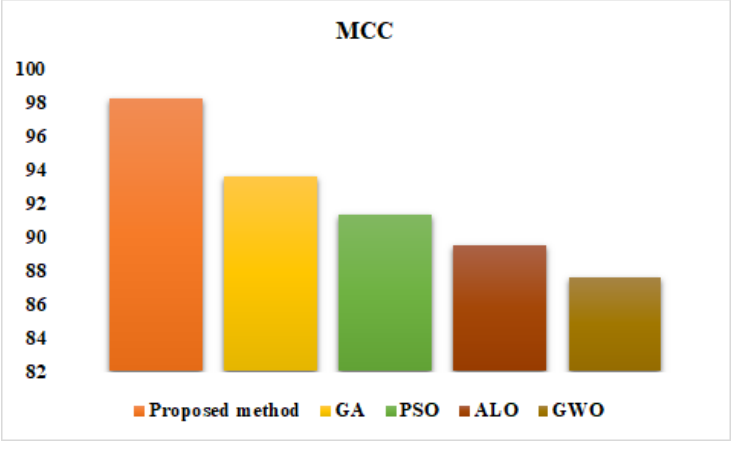


Figure 9 Analysis of NPV



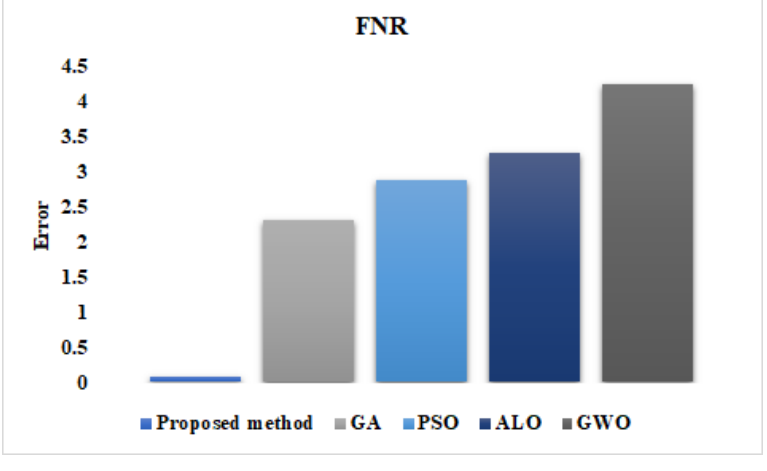
Analysis of MCC is shown in Figure 10. Here the MCC of proposed method is 98.25, the GA method is 93.62, the PSO method is 91.33, the ALO method is 89.47, the GWO method is 87.55. The outcome of the proposed method is high compared to the existing technique in MCC.

Figure 10 Analysis of MCC (see online version for colours)



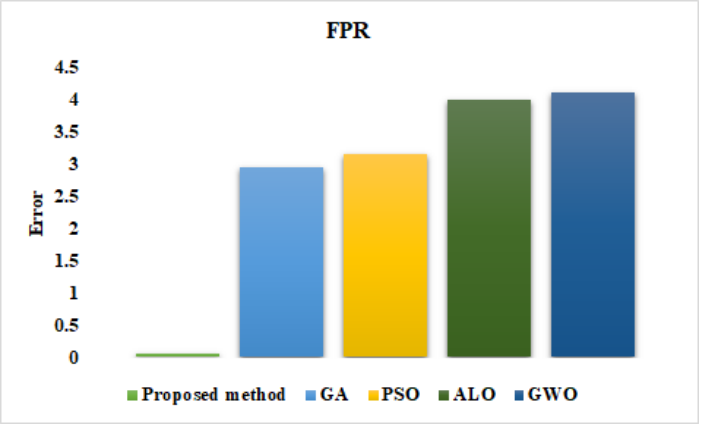
Analysis of FNR is shown in Figure 11. Here the FNR of proposed method is 0.07, the GA method is 2.31, the PSO method is 2.88, the ALO method is 3.26, the GWO method is 4.25. The outcome of the proposed method is low compared to the existing technique in FNR.

Figure 11 Analysis of FNR (see online version for colours)



Analysis of FPR is shown in Figure 12. Here the FPR of proposed method is 0.05, the GA method is 2.95, the PSO method is 3.15, the ALO method is 3.98, the GWO method is 4.11. The outcome of the proposed method is low compared to the existing technique in FPR.

Figure 12 Analysis of FPR (see online version for colours)



6 Conclusion

In this paper, the proposed system for secure data sharing in precision agriculture using blockchain and IoT technology, along with optimal clustering and a hybrid encryption algorithm, aims to improve agricultural productivity by providing a secure and efficient way to collect, transmit, and analyse data. The system utilises clustering to group sensor nodes and a multi-objective optimisation approach to select the optimal cluster head. The collected data is then stored in the cloud and protected using a hybrid encryption algorithm (AES and 3DES/TDEA) before being transmitted via the blockchain network to ensure secure and tamper-proof transmission. The proposed system can be a valuable tool for precision agriculture, providing farmers and researchers with accurate and secure data to make informed decisions and improve crop yields.

Data availability statement

Not Applicable

Funding

No fund received for this project

Conflicts of interest

The authors declare that they have no conflict of interest.

References

Alfa, A.A., Alhassan, J.K., Olaniyi, O.M. and Olalere, M. (2021) 'Blockchain technology in IoT systems: current trends, methodology, problems, applications, and future directions', *Journal of Reliable Intelligent Environments*, Vol. 7, No. 2, pp.115–143.

Alghazzawi, D., Bamasaq, O., Bhatia, S., Kumar, A., Dadheech, P. and Albeshri, A. (2021) 'Congestion control in cognitive IoT-based WSN network for smart agriculture', *IEEE Access*, Vol. 9, pp.151401–151420.

Ali, R., Pal, A.K., Kumari, S., Karuppiah, M. and Conti, M. (2018) 'A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring', *Future Generation Computer Systems*, Vol. 84, pp.200–215.

Alonso, R.S., Sittón-Candanedo, I., García, Ó., Prieto, J. and Rodríguez-González, S. (2020) 'An intelligent edge-IoT platform for monitoring livestock and crops in a dairy farming scenario', *Ad Hoc Networks*, Vol. 98, p.102047.

Anand, S.J. (2021) 'IoT-based secure and energy efficient scheme for precision agriculture using blockchain and improved leach algorithm', *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, Vol. 12, No. 10, pp.2466–2475.

Behera, T.M., Mohapatra, S.K., Samal, U.C., Khan, M.S., Daneshmand M. and Gandomi, A.H. (2019) 'Residual energy-based cluster-head selection in WSNs for IoT application', *IEEE Internet of Things Journal*, Vol. 6, No. 3, pp.5132–5139.

Chaudhari Waghulde, S.S. and Chopade, J.J. (2022) 'Role of (internet of things) IoT in agriculture monitoring system', *International Journal of Multidisciplinary Educational Research*, Vol. 11, No. 6, part 1.

Elijah, O., Rahman, T.A., Orikumhi, I., Leow, C.Y. and Hindia, M.N. (2018) 'An overview of internet of things (IoT) and data analytics in agriculture: benefits and challenges', *IEEE Internet of Things Journal*, Vol. 5, No. 5, pp.3758–3773.

Elmustafa, S.A.A. and Mujtaba, E.Y. (2019) 'Internet of things in smart environment: concept, applications, challenges, and future directions', *World Scientific News*, Vol. 134, No. 1, pp.1–51.

Eyo, U.E. (2019) *Between Religion and Agriculture: A Roadmap to Revamping Nigeria's Economy*.

Gharaei, N. (2022) *A Secure Inter-and Intra-Cluster Energy-Balancing Scheme in Rechargeable Wireless Sensor Networks for Smart City Applications*, Available at SSRN 4187010.

Haseeb, K., Ud Din, I., Almogren, A. and Islam, N. (2020) 'An energy efficient and secure IoT-based WSN framework: an application to smart agriculture', *Sensors*, Vol. 20, No. 7, p.2081.

Kasturi, S.B., Reddy, P.V., VenkataNagendra, K., Madhavi, M.R. and Jha, S.K. (2022) 'An improved energy efficient solution for routing in IoT', *Journal of Pharmaceutical Negative Results*, pp.1683–1691.

Khriji, S., El Houssaini, D., Kammoun, I. and Kanoun, O. (2021) 'Precision irrigation: an IoT - enabled wireless sensor network for smart irrigation systems', *Women in Precision Agriculture*, Springer, Cham, pp.107–129.

Mahajan, H.B. and Badarla, A. (2021) 'Cross-layer protocol for WSN-assisted IoT smart farming applications using nature inspired algorithm', *Wireless Personal Communications*, Vol. 121, No. 4, pp.3125–3149.

Mirjalili, S., Gandomi, A.H., Mirjalili, S.Z., Saremi, S., Faris, H. and Mirjalili, S.M. (2017) 'Salp swarm algorithm: a bio-inspired optimizer for engineering design problems', *Advances in Engineering Software*, Vol. 114, pp.163–191.

Odhiambo, J., Weke, P. and Ngare, P. (2020) 'Modeling Kenyan economic impact of corona virus in Kenya using discrete-time Markov chains', *Journal of Finance and Economics*, Vol. 8, No. 2, pp.80–85.

Połap, D. and Woźniak, M. (2021) 'Red fox optimization algorithm', *Expert Systems with Applications*, Vol. 166, p.114107.

Rangwani, D., Sadhukhan, D., Ray, S., Khan, M.K. and Dasgupta, M. (2021) 'An improved privacy preserving remote user authentication scheme for agricultural wireless sensor network', *Transactions on Emerging Telecommunications Technologies*, Vol. 32, No. 3, p.e4218.

Rashid, M., Nazeer, I., Gupta, S.K. and Khanam, Z. (2020) 'Internet of things: architecture, challenges, and future directions', *Emerging Trends and Impacts of the Internet of Things in Libraries*, IGI Global, pp.87–104.

Sharma, D. and Tomar, G.S. (2021) 'Energy efficient multitier random December routing protocols for WSN', *Agricultural. Wireless Personal Communications*, Vol. 120, No. 1, pp.727–747.

Song, J., Zhong, Q., Wang, W., Su, C., Tan, Z. and Liu, Y. (2020) 'FPDP: flexible privacy-preserving data publishing scheme for smart agriculture', *IEEE Sensors Journal*, Vol. 21, No. 16, pp.17430–17438.

Vangala, A., Das, A.K., Chamola, V., Korotaev, V. and Rodrigues, J.J. (2023) 'Security in IoT-enabled smart agriculture: Architecture, security solutions and challenges', *Cluster Computing*, Vol. 26, No. 2, pp.879–902.

Vougioukas, S.G. (2019) 'Agricultural robotics', *Annual Review of Control, Robotics, and Autonomous Systems*, Vol. 2, No. 1, pp.365–392.

Wu, H.T. and Tsai, C.W. (2019) 'An intelligent agriculture network security system based on private blockchains', *Journal of Communications and Networks*, Vol. 21, No. 5, pp.503–508.

Nomenclature

Abbreviation	*Description*
AES	Advanced encryption standard
AVISPA	Automated validation information security protocols and applications
BS	Base stations
BAN	Burrows–Abadi–Needham
CH	Cluster head
DA	Data analytics
DEC	Deterministic energy efficient
DDoS	Distributed denial of service
DoS	Denial of service
ECC	Elliptic curve cryptography
GDP	Gross domestic product
IoT	Internet of Things
LEACH	Low-energy adaptive clustering-hierarchy
PEGASIS	Power-efficient gathering for the sensor info-systems
RFO	Red fox optimization
SSA	Salp swarm algorithm
SNR	Signal to noise ratio
TDEA	Triple DEA
WSN	Wireless sensor networks