Vol.67: e24230858, 2024
https://doi.org/10.1590/1678-4324-2024230858
ISSN 1678-4324 Online Edition

BABT
Brazilian Archives of Biology and Technology

Article - Engineering, Technology and Techniques

Blockchain Based Secure Data Sharing in Precision Agriculture: a Comprehensive Methodology Incorporating Deep learning and Hybrid Encryption Model

Vinoth Kumar Kalimuthu[1*]
https://orcid.org/0000-0002-8920-4936

Mano Joel PrabuPelavendran[2]
https://orcid.org/0009-0008-7208-2208

[1]Vivekanandha College of Engineering for Women (Autonomous), Department of ECE, Thiruchengode, India; [2]Anjalai Ammal Mahalingam Engineering College, Department of ECE, Thiruvarur, India.

Editor-in-Chief: Alexandre Rasi Aoki
Associate Editor: Fabio Alessandro Guerra

Received: 14-Aug-2023; Accepted: 18-Oct-2023.

*Correspondence: vinodkumaran87@gmail.com; (V.K.K.).

HIGHLIGHTS

- This proposed methodology presents a comprehensive approach for secure data sharing in precision agriculture.
- Deep learning models like Capsule Neural Network (CapsNet), Recurrent Neural Network (RNN), and Bi-directional Long Short-Term Memory (Bi-LSTM) networks provide valuable insights for prediction, classification, and anomaly detection.
- This framework empowers precision agriculture while ensuring secure and efficient data sharing with 98.31% of accuracy.

Abstract: The precision agriculture discipline swiftly adopted blockchain as a key technology in numerous applications. From just smart farms to an internet of smart farms in precision farming, the Internet of Things (IoT) and blockchain is going to boost crop yield in precision agriculture. This proposed methodology presents a comprehensive approach for secure data sharing in precision agriculture. It integrates advanced techniques through multiple layers, including Data Collection, Data Preprocessing, Intelligent Analysis, Security, and Blockchain. IoT sensors collect data on soil moisture, temperature, humidity, crop health, and weather conditions. Preprocessing involves removing outliers, normalizing values, and extracting relevant features, then the required features are selected using the hybrid Sand Cat with Fire Hawk Algorithm (HSCFHA) which is the combination of standard Fire Hawk Optimization (FHO) and Sand Cat Swarm Optimization (SCSO). Deep learning models like Capsule Neural Network (CapsNet), Recurrent Neural Network (RNN), and Bi-directional Long Short-Term Memory (Bi-LSTM) networks provide valuable insights for prediction, classification, and anomaly detection. The blockchain layer establishes a decentralized and tamper-resistant ledger for transparent and immutable data transactions. Smart contracts automate and enforce data sharing

rules. By incorporating optimized clustering, deep learning models, hybrid encryption, and blockchain technology, this framework empowers precision agriculture while ensuring secure and efficient data sharing with 98.31% of accuracy.

Keywords: Precision agriculture; blockchain; Internet of Things; Security; Capsule Neural Network; Bi-directional Long Short-Term Memory.

INTRODUCTION

Precision agriculture, a data-driven farming technique that enables farmers to increase crop yield, has transformed the agricultural industry. With the advancement of technologies like the Internet of Things (IoT) and blockchain in precision agriculture, the significance of secure data sharing has increased. This introduction explores the relationship between blockchain and IoT in the context of secure data sharing for precision agriculture [1], [2], [3]. Large volumes of data are produced by precision farming from a number of sources, including as sensors, drones, weather stations, and satellite photos. Understanding crop health, soil conditions, weather patterns, and resource utilization are all aided by this knowledge [4], [5]. This data has to be exchanged efficiently and securely in order for stakeholders including farmers, researchers, agronomists, and supply chain partners to make informed decisions.

The existing techniques used for crop monitoring mainly rely on the pricey, time-consuming, and labor-intensive process of crop scouting, which entails hand sampling and recording the state of the fields. This old-fashioned method is frequently ineffective and could not give timely and reliable information on the crops. On the other hand, the rise of precision agriculture has created new opportunities by utilizing technology to collect and analyze data straight from the field [6], [7]. The use of cutting-edge technologies to acquire exact data on agricultural activities is referred to as precision agriculture. Utilizing sensors and other data collecting tools to keep track of numerous field factors is a crucial component of precision agriculture [8], [9], [10]. Data from these sensors may be obtained on elements including soil moisture, temperature, nutrient levels, insect infestations, and crop growth stages. However, there are now just a few of these sensors available and functioning, and in certain circumstances, they might not even exist. The absence of complete capabilities for monitoring space, time, and composition is a significant obstacle in the field of precision agriculture [11], [12], [13]. A limited picture of the field's circumstances may be gained from the frequently fine-grained data collected by sensors. This constraint makes it more difficult for farmers to decide what to do and how to do it to maximize crop yield. Additionally, it is challenging to efficiently integrate and analyze the information since the data gathered from sensors is frequently siloed within certain hardware or software.

Farmers frequently employ generalized strategies, such as excessive usage of fertilizers, pesticides, or irrigation water, in the absence of reliable and timely data [14], [15]. These actions may result in financial waste and environmental issues, such as higher expenses and potential ecological harm. Current precision agricultural research and development activities are concentrated on strengthening sensor technology, building thorough monitoring systems, and improving data gathering techniques. The objective is to make it possible for farmers to collect precise, real-time data on a variety of characteristics of their fields, such as soil quality, crop health, and meteorological conditions.

The literature review is provided in section 2 of the paper, and the suggested technique is described in section 3 of the document, the result obtained for the proposed model is discussed in section 4 and at last the conclusion is given in section 5.

LITERATURE REVIEW

An authentication mechanism with drone help is thought to be possible in an IoT-enabled agricultural situation [16]. For IoT-enabled IPA, a new authentication and key management framework known as AKMS-AgriIoT has been presented using the private blockchain-orientedtechnique. The proposed AKMS-AgriIoT systems offers stronger safety, more functionality characteristics, lower communication expenses, and similar computing costs when contrasted with other analogous systems, according to a thorough security analysis and comparative research.

The distributed Ledger (DTL) techniqueson the IoT. The paper provides a DLT-based solution for maintaining IoT detail integrity that safely handle the combined field information [17]. The inherent usage of IOTA's "The Tangle" ledger, which is used to transport and store the data, is what gives it its distinctiveness. Where the Super nodes only gather information and transfer it to the web, where it is controlled by every device in a distributed, decentralized network.

An IoT and blockchain concepts for a distributed process control system extension for a mushroom farm [18]. The paper suggest a theoretical framework for an upgrade to a distributed process control platform for a mushroom farm that integrates IoT and blockchain. That enhancement may not only supplement the present cultivation control system, which is essential for the general efficacy of the agricultural business system used by the team of executives, but will also enable the gathering of shared information on ecological signs inherent to the growing of mushrooms.

A precision agriculture with IoT support using Deep Aerial Semantic Segmentation Framework [19]. In order to detect agricultural patterns in images taken by UAVs, this work presents the powerful neural network framework AgriSegNet. Incorporating a multi scale attention module, a dynamic class weighting loss, and dice loss together with the intended structure enables higher IoU. the training set where there is a class inequality, these modules assist in optimizing the model training.

IoT and blockchain technologies are being used to produce smart farming [20]. the fact whether they are connected or not, this technique offers equal chance to all parties participating in the organic supply of food. To minimise the need for individuals to participate in data collection, capturing, and confirmation, IoT devices are included into the smart model. Compared to our own approach, which does not employ blockchain and only consists of placing IoT sensors in the monitoring field, our unique model's validity is evaluated.

The two-chain approach for Internet of Things network security of agricultural sampling data [21]. That research provide a double blockchain-based Inter Planetary File System (IPFS) storage solution for the safety of agricultural sampling data in an IoT network. To preserve a record of the public in case there are any hostile assaults, block hashes will be created once the data have been saved in ASDC blocks and uploaded to Ethereum's main chain.

A Novel Routing Scheme for Intelligent Agriculture. In order to find a Base Station (BS) path, the proposed technique uses electronic contracts in diverse IoT networks [22]. With the proposed routing protocol, duplicated data is eliminated, IoT architectural attacks are prevented, energy consumption is reduced, and network life is extended. It is compared to our current system to see how well it performs. Internet of Things-based agriculture and LEACH in agriculture.

A Blockchain-Based, Cloud-Based IoT in Innovative Agriculture for Safety Monitoring. That paper offers a system for smart-farm security monitoring, which can efficiently track sensor abnormalities and device status, as well as reduce security threats by observing behavioural trends [23]. Additionally, a blockchain-based smart contract programme was built to safely record data about safety anomalies and prevent similar assaults from happening to other farms in the area.

A Blockchain-Based Authentication Scheme for Smart Farming Based on Smart Contracts. This paper suggests a new authentication method based on smart contracts for a hybrid blockchain-based edge computing-based smart farming architecture [24]. Anonymity and traceability are supported as security characteristics by the proposed approach (SCBAS-SF). Additionally, SCBAS-SF is explicitly tested using the automated validation tool AVISPA protection from man-in-the-middle and replay attacks.

A private blockchain-based intelligent agriculture network security system. This study suggests using dark web technologies to protect the anonymity of servers and blockchains. To avoid distributed denial-of-service (DDOS) assaults, the study will track the frequency of packet transfer in intelligent agriculture [25]. The system's key characteristics are: an identity authentication method; secure information transfer; private blockchain creation; a quicker, more effective authentication system for blockchain information; and resilience to DoS assaults.

The demand for reliable authentication and security solutions has been prompted by the growing integration of IoT technology in agricultural contexts. The security of data integrity, privacy, and effective key management are issues that current authentication techniques must address. Additionally, the rising usage of drones in IoT-enabled agricultural contexts adds new challenges to authentication and safe data transfer. An authentication and key management system based on blockchain has been developed to overcome these issues. In order to improve security, usability, and communication effectiveness in IoT-enabled agricultural situations, this scheme will make use of the advantages of blockchain technology. The plan calls for the creation of encrypted transaction blocks that include GSS-generated signatures when appropriate. To validate and add these blocks to the private blockchain center, cloud servers mine them.

The proposed scheme's security features, must be carefully examined and compared to those of other pertinent systems. Furthermore, research is needed into how distributed ledger technology (DLTs) might be integrated with IoT systems in the agriculture sector. As an alternative to the cloud-centric IoT architecture, a distributed ledger system utilizing IOTA's ledger, referred to as "The Tangle," is suggested. By enabling each Super node to own and store the aggregated field data in a distributed and decentralized database, this node-centric approach seeks to assure data integrity. Additionally, conceptual frameworks and

methodologies are needed for the integration of IoT and blockchain technology in particular agricultural applications, such as distributed process control systems for mushroom farms, precision agriculture, and smart farming. These strategies have to focus on information gathering, environmental monitoring, pattern detection, and general farm management information system improvement.

PROPOSED METHODOLOGY

This proposed methodology presents a comprehensive approach for secure data sharing in precision agriculture by integrating advanced techniques. The methodology consists of multiple layers, including the Data Layer, Data Preprocessing Layer, Intelligent Layer, Security Layer, and Blockchain Layer. Each layer performs specific tasks to ensure efficient and secure data sharing in precision agriculture. The Data Layer focuses on data collection using IoT devices such as sensors that gather information on soil moisture, temperature, humidity, crop health, and weather conditions. The collected data is then preprocessed to remove outliers, normalize values, and extract relevant features. Optimal clustering techniques and feature selection algorithms enhance the data analysis process. The Intelligent Layer utilizes deep learning models such as cascaded CNNs, RNNs, and Bi-LSTM networks to extract valuable insights from the preprocessed data. These models enable accurate prediction, classification, and anomaly detection. The work flow of the proposed secure data sharing model for precision agriculture is shown in Figure 1.

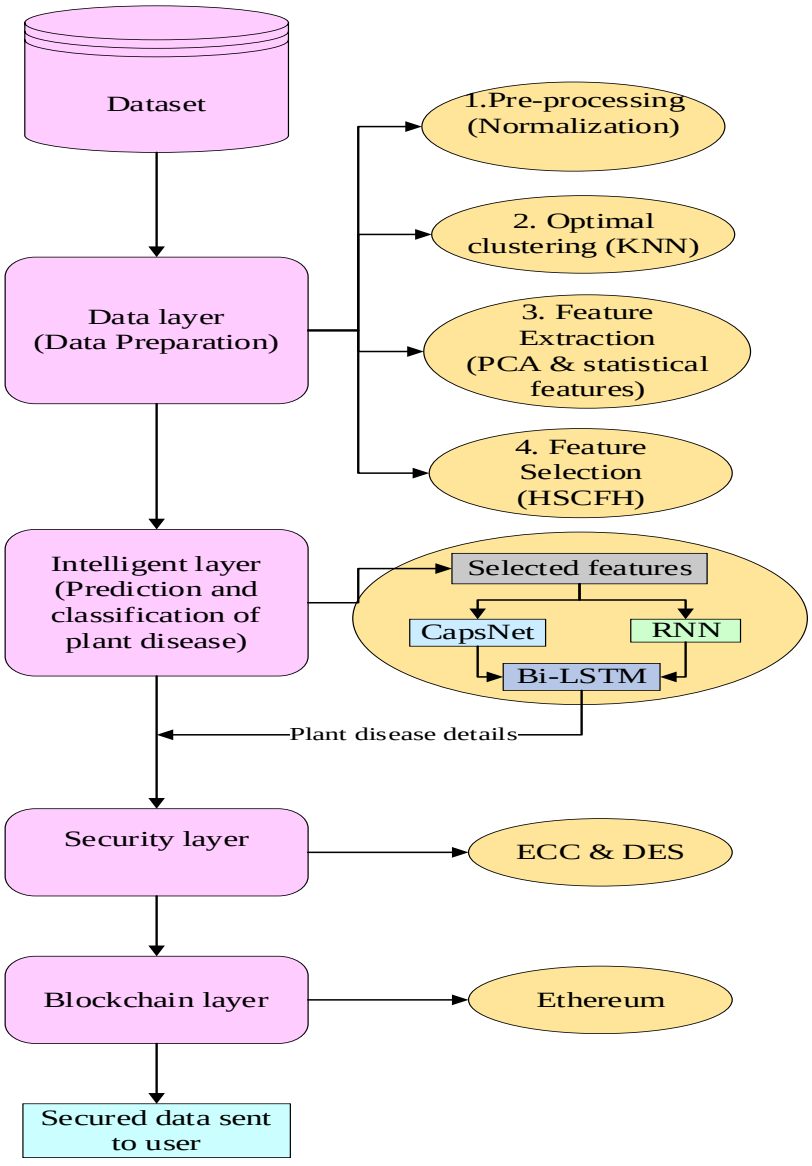

Figure 1. Block diagram of the proposed secure data sharing model.

The Security Layer ensures the confidentiality, integrity, and authenticity of the data through a hybrid encryption algorithm that combines symmetric and asymmetric encryption techniques. This step guarantees data security during transmission and storage. The Blockchain Layer leverages blockchain technology to create a decentralized and tamper-resistant ledger for recording and verifying data transactions. The integration of data sharing transactions onto the blockchain network ensures transparency, immutability, and secure sharing among authorized entities. Smart contracts automate and enforce the rules and conditions of data sharing, enhancing security and efficiency. This proposed methodology provides a comprehensive framework for secure data sharing in precision agriculture, enabling data-driven decision-making, collaboration among stakeholders, and ensuring the privacy and integrity of sensitive agricultural data. By incorporating advanced techniques such as optimized clustering, deep learning models, hybrid encryption, and blockchain technology, this methodology empowers precision agriculture to optimize crop yield, resource management, and sustainable practices.

Data layer: Data Collection

In the data collection phase, IoT devices like sensors are deployed to gather data for precision agriculture from multiple sources. These sources include crop health, meteorological conditions, soil moisture, temperature, and humidity. The gathered data serves as the basis for further research and offers insightful knowledge into the agricultural environment.

Data Preprocessing Layer

In order to assure the quality and usefulness of the obtained data for future analysis, the Data preprocessing Layer concentrates on cleaning and preparing it. The steps listed below are part of this layer.

The dataset may be cleaned by eliminating duplicated values, adding missing data, and deleting and repairing undesirable sample-level structures. The dataset must be normalized using the minimum and maximum scaling values as in the following equations after being cleaned:

$$Z_{norm} = \frac{Z\text{-min}(z)}{\max(z)\text{-min}(z)} \quad (1)$$

Where $\min(z)$ is the property Z's minimal value and $\max(z)$ is its highest value, respectively. The feature values Z_{norm} and Z are normalized and original, respectively.

Optimal Clustering

To efficiently group comparable data points together, an optimized clustering technique is used, such as the (proposed) optimized K-means clustering. To increase the precision and effectiveness of clustering findings, the method uses an improved initialization strategy. This process helps to find links and patterns in the data.

The K-means method is an uncomplicated iterative clustering technique. Using the K classes in the data set and the distance as the measurement, determine the distance mean, which will produce the initial centroid and characterize every class. These K-values are optimally selected using new hybrid optimization model called HSCFHA. For a given data collection X with n multivariate information points and a group K to be divided, the clustering aims are to minimise the total of the squares of various sorts, and the Euclidean distance is selected as the similarity metric, shown in Eq. (2).

$$d = \sum_{k=1}^{K} \sum_{i=1}^{n} \|(x_i - u_k)\|^2 \quad (2)$$

where k denotes the number of clusters centers, u_k denotes the center's position, and $x_i$denotes the data set's i^{th} point. The following is the answer to the centroid u_k:

$$\frac{\partial}{\partial u_k} = \frac{\partial}{\partial u_k} \sum_{k=1}^{K} \sum_{i=1}^{n} (x_i - u_k)^2 \quad (3)$$

$$\frac{\partial}{\partial u_k} = \sum_{i=1}^{n} 2(x_i - u_k) \quad (4)$$

Let Eq. (4) be zero; then

$$u_k = \frac{1}{n} \sum_{i=1}^{n} x_i \quad (5)$$

The main principle of the technique is to randomly select K sample points as the first cluster's center: By placing every data point into the cluster that is symbolized by its closest center point, cluster centers are found, with the center of each cluster being the intersection of all sample points inside it. The cluster's center point must remain constant or reach the specified number of iterations before the aforementioned processes should be repeated. The choice of the center point affects the algorithm's output, which leads to unstable outcomes. The centre point is determined by the K value, the algorithm's focus point, and it directly affects the clustering results, such as either worldwide or local the level of optimality.

Feature Extraction

Statistical characteristics and methods like PCA are used to extract pertinent features from the preprocessed data. While maintaining the most crucial features, PCA assists in lowering the dimensionality of the data. Summary statistics that depict the distribution and core patterns of the data are provided by statistical characteristics including mean, median, standard deviation, variance, skewness, and kurtosis.

PCA

A linear dimensionality reduction method known as PCA includes converting high-dimensional data into lower-dimensional data by the lowest dimension's variance should be maximized. The computation of the feature vector's covariance matrix comes first, and its associated eigenvectors are calculated after that. It must implement feature scaling or normalization similar to supervised learning approaches depending on the n-dimensional training data$y^{(1)}, y^{(2)}, \ldots, y^{(n)}$.Eq.(6) is used to compute the mean of each characteristic.

$$\mu_i = \frac{1}{n}\sum_{j=1}^{n} y_i^{(j)} \tag{6}$$

Thatcan scale separate characteristics so that they have comparable ranges of mean values if they possess distinct mean values for different attributes. To guarantee that every y_i value has an absolute zero mean value, then swap out each $y_i$variable with its corresponding $y_i - \mu_i$ value. In the context of supervised learning, this measuring of the i^{th}component is defined by Eq. (7), where $s_i$is the $|\max - \text{mean}|$score of the i^{th} feature.

$$y_i^{(j)} = \frac{y_i^{(j)} - \mu_i}{s_i} \tag{7}$$

It is necessary to determine the mean square error of the data being projected on the m multidimensional vector in order to lower the feature's dimension from N to m (where m×N) and pinpoint the region in a space with N dimensions onto which the projected data are located. It is difficult and outside the scope of this research to computationally verify the computation of these m vectors: $\mu^{(1)}, \mu^{(2)}, \ldots, \mu^{(m)}$ and the anticipated points: $wu^{(1)}, w^{(2)}, \ldots, w^{(N)}$on these vectors. Eq. (3) is used to calculate the covariance matrix, which has the dimensions $N \times 1$ for the $y^{(j)}$vector and $1 \times N$ for the$(y^{(j)})^T$. This results in a covariance matrix with the dimensions $N \times N$. The covariance matrix's eigenvalues and eigenvectors, which stand for the feature vectors' new magnitude and associated directions in the modified vector space, are next calculated. Conversely, eigenvectors with tiny eigenvalues contain relatively little data about the dataset. The covariance matrix is given in Eq. (8),

$$C_v = \frac{1}{N}\sum_{j=1}^{N} y^{(j)} \times (y^{(j)})^T \tag{8}$$

Where C_v is the covariance matrix.As a consequence, the formula $t^{(p)} = y^{(j)}z^{(p)}$ may be used to calculate the score for the p^{th} entire PCA of a data vector, where $z^{(p)}$is the p^{th} eigenvector of the C_v of $y^{(j)}$. As a result, the entire PCA reduction of the vector Y may be represented as $T = Y \times Z$, where Z is the eigenvector of the C_v. Then we establish a cutoff value at which the eigenvalues are deemed valuable and the other ones are eliminated as irrelevant characteristics.

Statistical Features

Make traffic flow statistics calculations at certain times or locations, including the mean, median, standard deviation, variance, skewness, and kurtosis. The formulas are given in Table 1.

Table 1. Formula for Statistical and higher order statistical features

Sl. No	Statistical feature	Formula
1.	Mean	$\frac{\text{Sumofallvalues}}{\text{Totalnumberofvalues}}$
2.	Median	$\begin{cases}\frac{l+1}{2}, & \text{forodd} \\ \frac{l}{2}, & \text{foreven}\end{cases}$
3.	SD (σ)	$\sqrt{\frac{\sum (x_i-\mu)^2}{N}}$
4.	Variance	$\frac{\sum (x_i-\mu)^2}{N}$
5.	Kurtosis (high order)	$\frac{4^{th}\text{Moment}}{4^{th}\text{Moment}^2}$
6.	Skewness (high order)	$\frac{3(\text{Mean-Median})}{SD}$

Feature Selection

For feature selection, a hybrid optimization approach that combines evolutionary algorithms and mathematical programming is used. The objective of this model is to extract the most discriminative and informative characteristics. Feature selection improves the computational effectiveness and interpretability of following analysis processes by lowering the dimensionality of the data. The regular FHO and SCSO are combined to create the hybrid optimization model called HSCFHA.

Mathematical model

Initialization

In order to accurately simulate the hunting habits of fire hawks, the HSCFHA metaheuristic algorithm considers both the process of igniting and spreading fires as well as gathering food. From a variety of possible solution outcomes (X_i), the initial position coordinates of the fire hawks and prey are selected. Utilizing a random initialization technique, these vectors' beginning positions in the search area are chosen, shown in Eq. (9).

$$X=\begin{bmatrix}X_1\\ \vdots \\ X_i \\ \vdots \\ X_N\end{bmatrix}_{N\times m} = \begin{bmatrix}x_{1,1} & \cdots & x_{1,d} & \cdots & x_{1,m}\\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{i,1} & \cdots & x_{i,d} & \cdots & x_{i,m}\\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{N,1} & \cdots & x_{N,d} & \cdots & x_{N,M}\end{bmatrix}_{N\times m} \quad (9)$$

$$x_{i,j}(0)=x_{i,j}(\min)+\text{rand}.\left(x_{i,j}(\max)-x_{i,j}(\min)\right) \quad (10)$$

Where i=1, 2,…,N, j=1,2,…, d

Where$x_{i,j}(min)$, and $x_{i,j}(max)$ are the minimum and maximum solutions,$X_i$denotes thei^{th} solution candidate in the search space, d denotes the dimension of the problem under consideration, $x_{i,j}$ denotes the j^{th} decision variable of the ith solution candidate, $x_{i,j}(0)$ denotes the initial position of the solution candidates, and$m \times N$ denotes the total number of solution candidates in the search space. In the ways indicated below, these qualities are shown schematically and statistically:

$$\mathbf{PR}=\begin{bmatrix}PR_1\\ \vdots\\ PR_k\\ \vdots\\ PR_m\end{bmatrix},\ k=1,2,\ldots,m \tag{11}$$

$$\mathbf{FH}=\begin{bmatrix}FH_1\\ \vdots\\ FH_l\\ \vdots\\ FH_n\end{bmatrix},\ l=1,2,\ldots,n \tag{12}$$

Where PR_k is the k^{th} prey inside the search space with respect to a total of m preys, and FH_l is the l^{th} fire hawk with respect to a total of $n$fire hawks within the search space.

The total distance (D_k^l)among the Fire Hawks and the prey is computed in the algorithm's subsequent stage is given in Eq. (13),

$$D_k^l=\sqrt{(x_2--x_1)^2+(y_2-y_1)^2} \tag{13}$$

Where m is the total number of preys in the search space, and (x_1,y_1) and (x_2,y_2) indicate the location of the fire hawks and their prey inside the search area. The nearest adjacent prey is utilised to determine the Fire Hawks' domain after using the method outlined above to gauge the total distance between them and their prey.

Search for Prey (Proposed Exploration Stage)

The Fire Hawks gather burning sticks throughout the algorithm's next phase in order to prevent achieving the local optimum; each one's sensitivity range (r) is unique. The HSCFHAalgorithm benefits from the sand cat's low-frequency hearing skills. Because of this, in mathematical modelling, the sensitivity rG is described by Eq.(14). Additionally, the algorithm exploration and exploitation capability are regulated, and the parameter R is generated using Eq. (15).

$$FH_{new}=FH+r^*(r_1+r_G-r_2^*FH_{near}) \tag{14}$$

Where the value of r is shown usingEq. (14) and Eq. (15) of SCSO

$$r_G=S_M-\left(\frac{S_M^*t}{T}\right) \tag{15}$$

$$R=2^*r_G^*rand(0,1)-r_G \tag{16}$$

Where T is the number of iterations over the maximum allowed and S_M is 2.

In the sensitivity range, each sand cat will at random select a new site to look for prey. In this environment, algorithms may be explored and used more effectively. Each sand cat's sensitivity range (r) is unique in order to prevent slipping into the local optimum, based on Eq. (17).

$$r=S_M^*rand(0,1) \tag{17}$$

When the guiding parameter r_G is utilized.Each sand cat will look for the prey's location using the best candidate position (Pos_{bc}), current position (Pos_c(t)), and sensitivity range (r) as a guide. In Eq. (18), the particular Formula is shown.

$$Pos(t+1)=r^*Pos_{bc}(t)-rand(0,1)^*Pos_c(t) \tag{18}$$

Movement of prey inside the territory

The migration of prey within each search agent's area is taken into consideration as a critical aspect of behavioural patterns for the position modifying process in the algorithm's following phase. When the Fire Hawk drops a flaming stick, the prey may probably choose to hide, escape, or will unwittingly move in the direction of the search agent. When updating a location, the following equation might be used to account for various operations:

$$PR_q^{new}=PR_q+(r_3*FH_l-r_4*SP_l) \quad (19)$$

Where $l = 1,2,\ldots,nandq = 1,2,\ldots.,r$, GB is widely regarded as the top option in the primary fire search space; SP_l is a hide place beneath the territory of the l^{th}search agent; and r_3 and r_4 are random integers with a uniform distribution in the range of (0, 1) to predict the motions of prey approaching the search agent and the safe location. When updating a position, the ensuing equation can be utilized to account for these actions.

$$PR_q^{new}=PR_q+(r_5*FH_{alter}-r_6*SP) \quad (20)$$

Where PR_q^{new} is the updated position vector of the q^{th} prey (PR_q)) that is being pursued by the l^{th} fire hawk (FH_l); SP is a secure location beyond the l^{th} Fire Hawk's territory; and r_5 and r_6 have evenly distributed at random in an interval of (0, 1) for predicting the preys' movements towards the other search agent and the secure location beyond the territory. The numerical description of $SP_l$and SP is built on the assumption that the majority of species assemble in a safe region of nature to remain secure during a hazard.

$$SP_l=\frac{\sum_{q=1}^{r} PR_q}{r} \quad (21)$$

$$SP=\frac{\sum_{k=1}^{m} PR_k}{m} \quad (22)$$

Where PR_k is the k^{th} prey in the search area and PR_q is the q^{th} prey being guarded by the lth fire hawk (FH_l).

Attack Prey (Exploitation Stage)

Eq. (23) displays the distance (Pos_{rnd}) between the sand cat and its target in order to replicate the sand cat's attack on its victim. The value of the randomly chosen angle falls between 1 and 1, as it ranges from 0 to 360 degrees. This allows each sand cat to wander through the search area in a variety of circumferential directions. After that, the prey is assaulted using Eq. (24). The dune cat can get to its hunting location more quickly in this fashion.

$$Pos_{rnd}=|rand(0,1)*Pos_b(t)-Pos_c(t)| \quad (23)$$

$$Pos(t+1)=Pos_b(t)-r*Pos_{rnd}*\cos(\alpha) \quad (24)$$

Position updating

By adjusting the adaptive parameters rG and R, the HSCFHA controls the algorithm's exploration and exploitation. Eq. (24) demonstrates that throughout repetition, rG drops linearly from 2 to 0. In light of this, the parameter R has the random value [4, 4]. When R is a multiple of one or fewer, the sand cat will assault its victim. If not, the sand cat will hunt for prey, as shown by Eq. (25).

$$Pos(t+1)=\begin{cases} r*(Pos_{bc}(t)-rand(0,1)*Pos_c(t) & |R|>1;exploration \\ Pos_b(t)-Pos_{rand}*\cos(\alpha)*r & |R|\leq 1;exploitation \end{cases} \quad (25)$$

Each sand cat's updated position during the exploration and exploitation stage is shown in Eq. (25). The sand cat will attack its victim if R is less than 1. Otherwise, the sand cat's job is to scour the entire planet for fresh prey.

Intelligent Layer

The Intelligent Layer analyses the preprocessed data and draws insightful conclusions using machine learning and deep learning techniques. The subsequent actions are part of this layer. A three-tier deep learning framework is employed, consisting of CASPSNet, RNNs, and Bi-LSTM networks. These models are trained on the preprocessed data to perform tasks such as prediction, classification, and anomaly detection. They leverage the extracted features to make accurate and informed decisions.

CapsNet Architecture

Convolutional, primary, and digit capsule layers make up CapsNet's three major layers. The first step is to utilize the convolutional layer to extract the key characteristics from the input data. Two convolutional layers, with 64 and 128 feature maps each, are employed. Each feature map's output may be calculated in Eq. (26) as follows:

$$y(i,j)=\sum_{m=-N}^{N}\sum_{n=-M}^{M} x(i+m,j+n)*k(m,n) \quad (26)$$

Where x is the convolutional layer's input, k is the filter's kernel (also known as the kernel), and N and M are the kernel sizes. In this instance, we utilize a 33-kernel size and 1 sample for the kernel strides because the input is 40031 in size. Following each convolutional layer, the Rectified Linear Unit (ReLU) is utilized as an activation function, with the following result:

$$Act(y)=max(0,y) \quad (27)$$

The output of the convolutional feature maps is divided into a number of vector representations called capsules u_i for the principal capsule, which produces combinations of the features. By applying a convolutional operation to their input, capsule behaviour is comparable to that of a convolutional layer. With three samples per stride and a kernel size of 3×3, we utilize. The input data, including its orientation and location, are all included in the capsule. Four 16-channel capsules are used in this instance. As a result, $134 \times 1 \times 16 \times 4$ is the form of the capsule layer's output. Because of the vector that the capsule's output is, it is impossible to use the conventional activation function. Consequently, the following Eq. (28) utilizes a non-linear squashing function:

$$v_j=\frac{\|s_j\|^2}{1+\|s_j\|^2} * \frac{s_j}{\|s_j\|^2} \quad (28)$$

Where the capsule j's input and output are s_j and v_j respectively. Short vectors are supposed to be reduced to virtually zero length, while large vectors are supposed to be shrunk to a length just below 1 using the squashing activation function. The third factor is the 2D form of the digit capsule layer. Both the earthquake and noise classifications apply to our issue. Based on the dynamic routing (routing by agreement) idea, the main capsule is connected to the digit capsule. The weighted sum total output contribution $(\hat{u}_{j|i})$ is one way to describe the variable s_j. Following Eq. (29) is the way to calculate the s_j:

$$s_j=\sum_i c_{ij}\hat{u}_{j|i} \quad (29)$$

Hence, in the method for dynamic routing, c_{ij} stands for the coupling coefficient. Following are the steps to acquire the $\hat{u}_{j|i}$in Eq. (30) and c_{ij}Eq. (20):

$$\hat{u}_{j|i}=W_{ij}u_i \quad (30)$$

$$c_{ij}=\frac{\exp(b_{ij})}{\sum_c \exp(b_{ic})} \quad (31)$$

Where W_{ij} stands for the weight matrix and b_{ij} and b_{ic}two capsules' logarithmic prior chances. The routing algorithm uses an iterative process with numerous phases. First, b_{ij} is initialized to zero for all capsules in layer l and capsule$j$ in layer $l+1$, whereas W_{ij} is started at random for the weight matrix. Second, Eq. (31) is used to derive the coupling coefficient c_{ij}. Thirdly, the s_j and v_j are determined using the coupling coefficient c_{ij} and the capsule result layer$(\hat{u}_{j|i})$. Finally, b_{ij} is updated as follows:

$$b_{ij}+(\hat{u}_{j|i}.v_j)\rightarrow b_{ij} \quad (32)$$

The digit caspule's output is in the form of a 2×8 matrix. Using an 8-dimensional vector, each class may be represented. Our routing method goes through three rounds. The margin loss function is minimized using the Adam optimizer, which is utilized to optimize the CapNet network settings, shown in Eq. (33):

$$L_k=T_k max(0,m^+-\|v_k\|)^2+\lambda(1-T_k)max(0,\|v_k\|-m^-)^2 \quad (33)$$

Where T_k equals 1, m^+ = 0.9 and m^-= 0.1. λ denotes the down-weighting of the loss which is constant at 0.5.

RNN

The data utilized in each computation is kept in memory by RNNs. It uses the exact same settings for each input since it provides the same outcome by carrying out the same operation on all inputs or h-layers.

Each Mw_i forecasts the probabilities $g_1, g_2, \ldots, g_n$of each label R for given input Q for input network data, such as Q with n columns and written as $Q = Q_1, Q_2, \ldots, Q_n$. The ensembler combines the Mw_i probability

values to create an ensemble prediction function $f(q)$ that accepts predictions as a vote for the labels from each model. With the given input data Q, Eq. (34) represents the computation of probability predictions.

$$g_i=\tilde{r}_i\left(Mw_i(Q)\right) \tag{34}$$

$$f(q)=\text{argmax}_{r\in R}\sum_{j=1}^{J} I(r=h_j(q)) \tag{35}$$

According to Eq. (35), the prediction function $f(q)$ceives input from the prediction probability values of seven ML models Mw_i for each label. In critical infrastructure, labels that identify the sort of attack or activity being observed may be included in the output of an anomaly detection system. System administrators and security workers can be informed of potential security concerns using these labels, which enable to take the necessary precautions to reduce the risks.

Bi-LSTM

A forward and a backward RNN are both included in each training series of a bi-RNN, and each have an output layer connecting them. At every stage of the input process for the output layer, the whole historical and prospective contextual information is provided. Since there is no data transfer between the forward and the backward postulated layers, the extension of the graph is therefore guaranteed to be non-cyclic.

The Bi-LSTM model has the following layers: input to forward and backward hidden layer weights (w_1–w_3), hidden layer to hidden layer weights (w_2–w_5), and forward and backward hidden layer to output layer weights (w_4–w_6). At each time step, the same six weights are applied. The hidden layer of the Bi-LSTM model must store two values of h_t: one for the forward computation and one for the backward calculation. Following are mathematical equations (Eq. (36)–Eq. (38)) that represent the final output value o_t that is produced by merging the outputs of the two layers:

$$\vec{h}_t=f(w_1x_t+w_2\vec{h}_{t-1}) \tag{36}$$

$$\overleftarrow{h}_t=f(w_3x_t+w_5\overleftarrow{h}_{t+1}) \tag{37}$$

$$o_t=g(w_4\vec{h}_t+w_6\overleftarrow{h}_t) \tag{38}$$

Security Layer

Before sharing the sensitive information with authorized parties, the Security Layer concentrates on securing it. Following is a step included in this layer:

Data Encryption

To guarantee the data's secrecy, integrity, and validity, a hybrid encryption technique is used. Asymmetric and symmetric encryption methods are used in hybrid encryption. ECC and DES are combined to create the hybrid encryption paradigm. The optimal key is generated using the HSCFHA optimization technique. By using encryption, the data is protected both during transmission and storage.

To maximize speed and security, hybrid encryption combines the benefits of symmetric and asymmetric encryption techniques. ECC for key exchange and DES for data encryption and decryption can be used together to create a hybrid encryption method for precision agriculture or any other sector. This is how precision agriculture may benefit from a hybrid encryption system that combines ECC and DES:

Key Exchange

a. The sender creates an ECC key pair with a matching private key and public key.

b. The sender safely sends the recipient's public key across the Internet.

Data Encryption

a. An unpredictable session key is created by the sender for DES encryption.

b. The ciphertext is produced by the sender after the real data is encrypted with the session key and DES algorithm.

c. The receiver's ECC public key is used by the sender to encrypt the session key, creating the encrypted session key.

Data Decryption

a. The recipient uses their private key to decrypt the encrypted session key in order to obtain the original session key.

b. The recipient recovers the original data by decrypting the ciphertext with the DES algorithm and the session key.

The hybrid encryption system guarantees safe key distribution by using ECC for key exchange. Without having to communicate it directly, ECC offers a safe way for sender and receiver to exchange the session key.

Blockchain Layer

With the use of Ethereum blockchain technology, the Blockchain Layer establishes a decentralized, impenetrable ledger for logging and validating data transactions. Our solution ensures the security, privacy, and accuracy of data and transactions by utilizing these components of blockchain technology. The system is protected against unauthorized access, manipulation, and data breaches thanks to the distributed ledger, immutability, consensus procedures, cryptographic security, access control, privacy safeguards, and encrypted data.

Smart Contracts

In order to automate and enforce the terms and conditions of data sharing, smart contracts are created. Between data suppliers and users, these contracts specify the access privileges, authorizations, and financial obligations. As the contracts automatically carry out the agreed-upon terms without the need for middlemen, using smart contracts makes the data exchange process more safe, transparent, and effective.

Each consensus node must carry out the logics that are written into smart contracts, which are published on the blockchain. Smart contracts are contracts that are kept as computer code on the blockchain, much like in the blockchain context. These smart contracts constantly enforce the rules as well as define them. This makes it possible for developers to create their own contracts using logical code that contains the conditions of each party's contract and requires self-execution.

RESULT AND DISCUSSION

In this part, the proposed model's ability to securely share the information in precision agriculture is assessed using several performance measures, including accuracy, sensitivity, specificity, recall, recall, recall, F-Measure, NPV, FPR, FNR, and MCC. The entire amount of data in this dataset is split into training (70%), testing (20%), and validation (10%) categories. Based on a variety of criteria, this dataset enables users to create a prediction model that would suggest the best crops to plant at a certain farm. The Python platform is used to carry out the implementation.

The performance of the proposed model is compared with the existing techniques like Bi-LSTM, RNN, CapsNet. The comparison of the DL model is evaluated in terms of performance metrics, shown in Table 2.

Table 2. Comparison of the proposed and existing techniques

Techniques	Sensitivity	Specificity	Accuracy	Precision	Recall	F-Measure	NPV	FPR	FNR	MCC
Proposed	0.9629	0.9901	0.9831	0.9831	0.9831	0.9831	0.9964	0.0194	0.0556	0.9700
Bi-LSTM	0.9323	0.9934	0.9701	0.9771	0.9771	0.9771	0.9934	0.0285	0.1302	0.9550
RNN	0.9267	0.9964	0.9588	0.9728	0.9728	0.9728	0.9901	0.0751	0.1556	0.8831
CapsNet	0.9002	0.9800	0.9440	0.9690	0.9690	0.9690	0.9800	0.0780	0.1434	0.8736
GRU	0.8204	0.9769	0.9206	0.8901	0.8901	0.8901	0.9769	0.0643	0.2175	0.8083
MLP	0.7963	0.9306	0.8953	0.8866	0.8866	0.8866	0.9306	0.1140	0.2964	0.7432

Among the techniques, the proposed approach demonstrates the highest sensitivity (0.9629) and specificity (0.9901), indicating its ability to accurately identify positive and negative instances. It achieves a high overall accuracy of 0.9831, reflecting its effectiveness in correctly classifying instances. The precision of the proposed approach is also high (0.9831), indicating a low rate of false positives. The recall, or true

positive rate, matches the precision at 0.9831, indicating that a high proportion of positive instances are correctly identified. This is further supported by the F-measure value of 0.9831, which considers both precision and recall.

The NPV of the proposed approach is 0.9964, reflecting its ability to correctly identify negative instances. The FPR is low at 0.0194, indicating a low rate of falsely classifying negative instances as positive. The FNR is also low at 0.0556, suggesting a low rate of falsely classifying positive instances as negative. Finally, the MCC for the proposed approach is 0.9700, which is a measure of the quality of binary classification, taking into account true and false positives and negatives. A higher MCC value indicates a better classification performance.

Comparatively, the other techniques such as Bi-LSTM, RNN, CapsNet, GRU, and MLP also demonstrate varying levels of performance across the evaluation metrics. The graphical representation of sensitivity and specificity is shown in Figure 2.

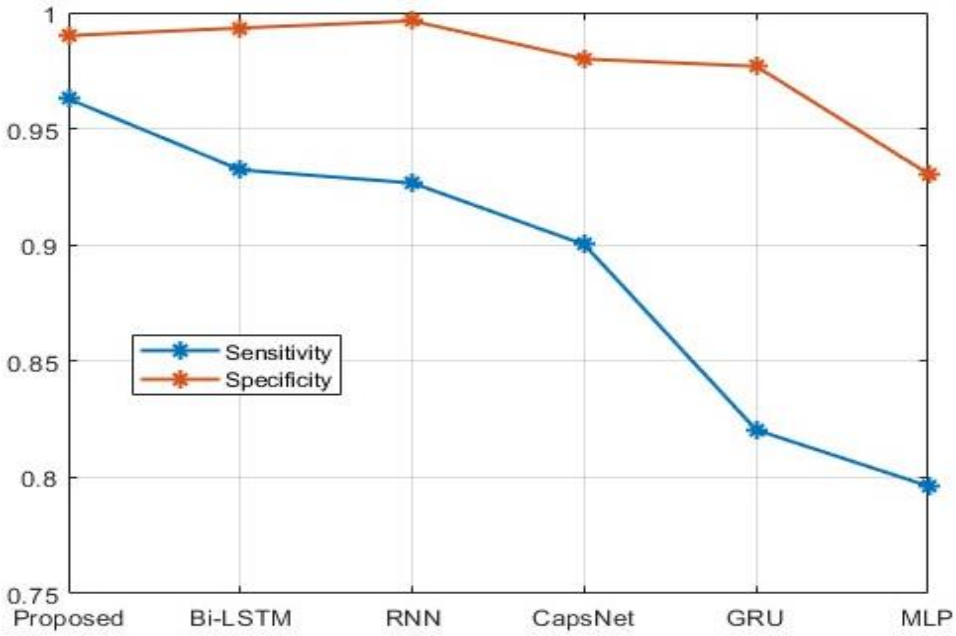

Figure 2. Comparison of sensitivity and specificity

The Bi-LSTM technique achieves a sensitivity of 0.9323, the RNN technique demonstrates a sensitivity of 0.9267, CapsNet achieves a sensitivity of 0.9002, the GRU technique demonstrates a sensitivity of 0.8204, MLP achieves a sensitivity of 0.7963. The specificity of Bi-LSTM is 0.9934,RNN achieves a specificity of 0.9964, CapsNet achieves a sensitivity of 0.9002, the GRU technique demonstrates a sensitivity of 0.8204, and MLP achieves a sensitivity of 0.7963. Figure 3 displays the accuracy and precision in visual form.

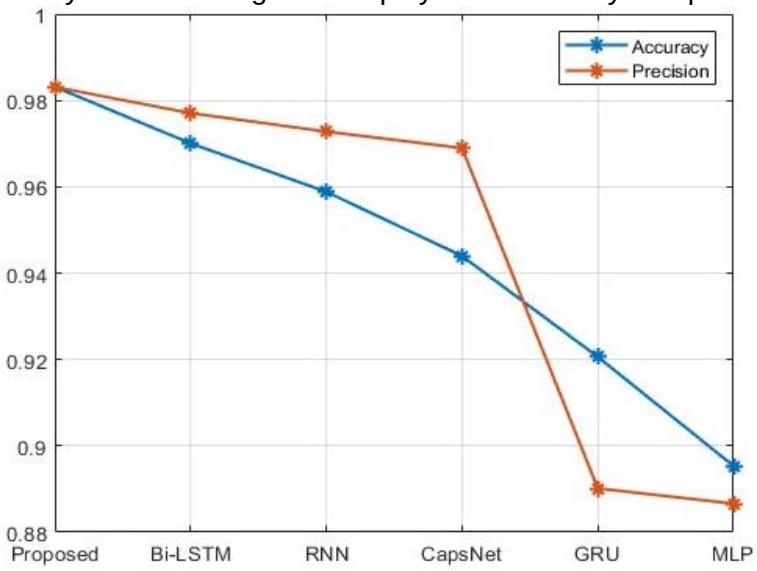

Figure 3. Comparison of accuracy and precision

The proposed approach achieves an accuracy of 0.9831. With anaccuracy of 0.9701, accuracy values range from of 0.9588for the RNN to 0.9440 for CapsNet, 0.9206 for GRU, and 0. 0.8953 for MLP. The proposed approach achieves a precision of 0.9831. Bi-LSTM's precision is 0.9771, which means that 97.71% of the negative cases are accurately identified by it. The precision of RNN is 0.9728, the precision of CapsNet is 0.9690, the GRU method has a precision of 0.8901, and the precision of MLP is 0.8866. Figure 4 displays a visual illustration of recall and NPV.

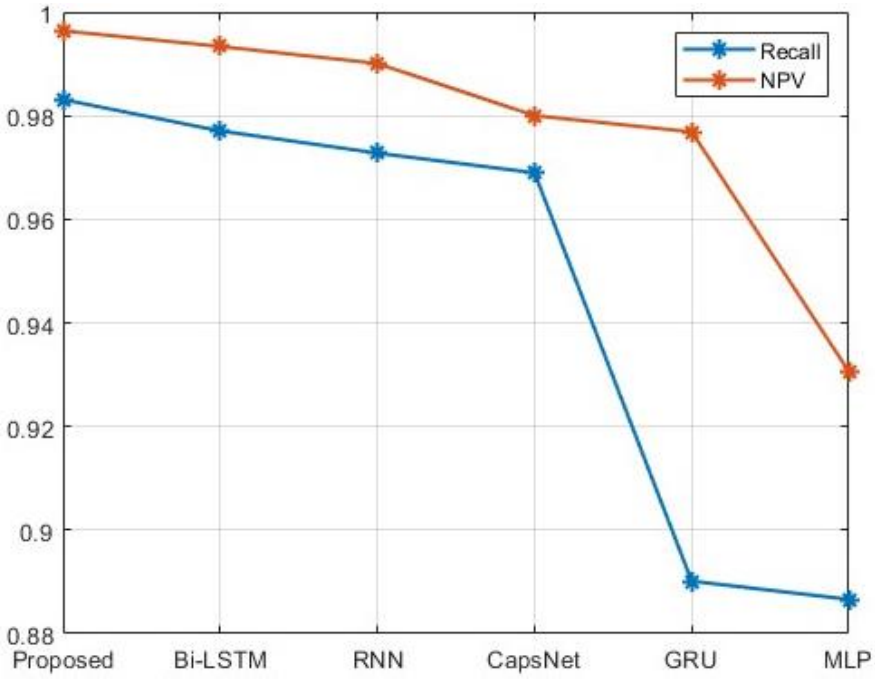

Figure 4. Comparison of recall and NPV

The proposed approach achieves a recall of 0.9831. A recall of 0.9771 means that the Bi-LSTM method accurately detects 97.71% of the positive cases. CapsNet obtains a recall of 0.9690, RNN achieves a recall of 0.9728, GRU achieves a recall of 0.8901, and MLP earns a recall of 0.8866. The proposed approach achieves an NPV of 0.9964. Bi-LSTM properly distinguishes 99.34% of the negative cases, according to its NPV of 0.9934. NPV for RNN is 0.9901, NPV for CapsNet is 0.9800, NPV for the GRU method is 0.9769, and NPV for MLP is 0.9306. Figure 5 displays F-measure and MCC as a graphical depiction.

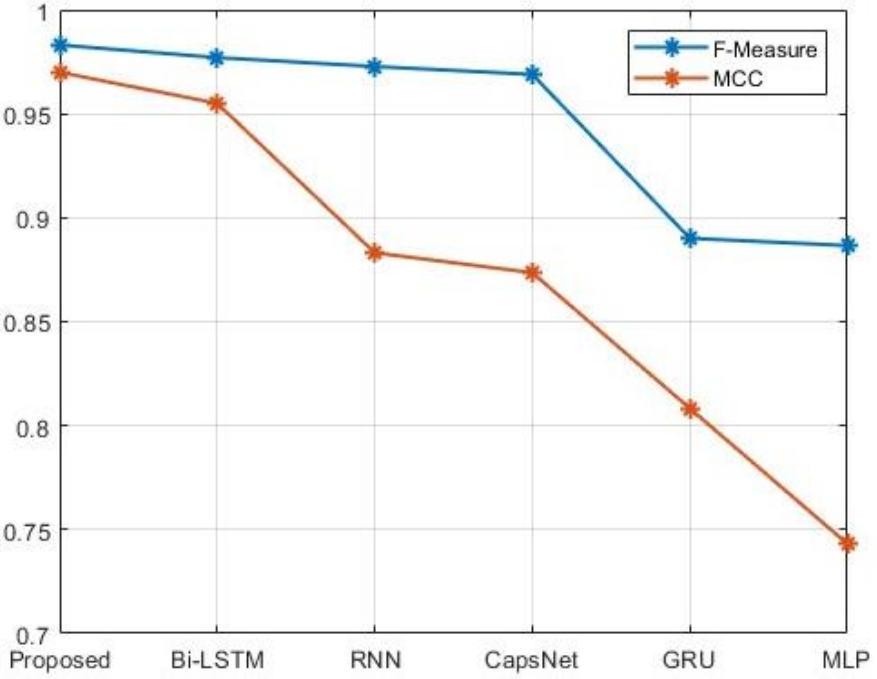

Figure 5. Comparison of F-measure and MCC

The proposed approach achieves an F-measure of 0.9831. Bi-LSTM successfully recognizes the F-measure of 0.9771. The RNN method obtains a F-measure of 0.9728, CapsNet accomplishes a F-measure of 0.9690, GRU accomplishes a F-measure of 0.8901, and MLP accomplishes a F-measure of 0.8866. The proposed approach achieves an MCC of 0.9700. The Bi-LSTM's MCC value is0.9550. The MCC of the RNN is 0.8831, the MCC of CapsNet is 0.8736, the MCC of the GRU method is 0.8083, and the MCC of MLP is 0.7432. Figure 6 displays a graphical representation of FNR and FPR.

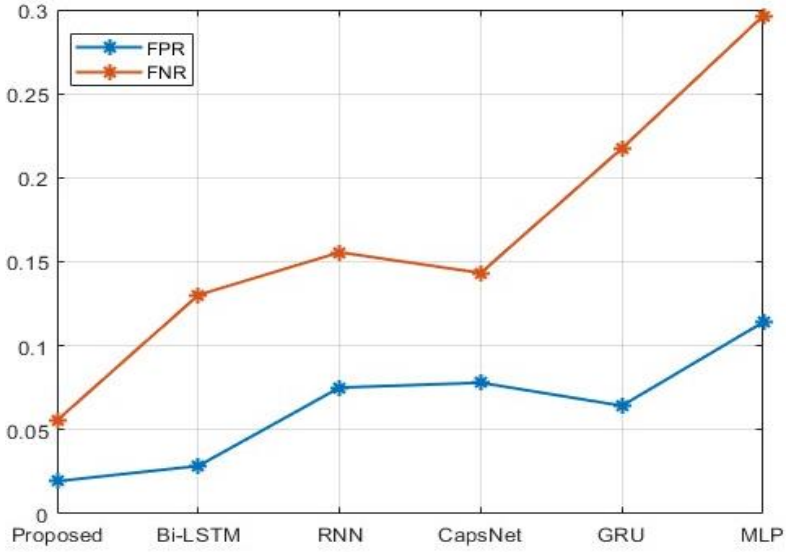

Figure 6. Comparison of FNR and FPR

The FNR and FPR are the error metrics, the lower values of FNR and FPR indicates that the proposed model achieve lower error rate compared to the existing Bi-LSTM, RNN, CapsNet, GRU and MLP.

Comparison of security measures

Based on the Table3, the proposed encryption technique demonstrates relatively faster encryption and decryption times compared to DES, ECC, Blowfish, and RSA.

Table 3. Comparison of the security metrics

Techniques	Encryption Time (Sec)	Decryption Time (Sec)	Security (%)
Proposed	1.728258028	0.85494808	99.05
DES	2.816889785	1.789568713	90.36
ECC	2.693018101	1.888595158	93.64
Blowfish	3.689735555	2.705795568	89.34
RSA	3.941046446	3.014292112	87.36

CONCLUSION

In conclusion, the proposed methodology presents a comprehensive and advanced approach for secure data sharing in precision agriculture. By integrating multiple layers including the Data Layer, Data Preprocessing Layer, Intelligent Layer, Security Layer, and Blockchain Layer, the methodology ensures efficient and secure handling of agricultural data. this methodology empowers precision agriculture by enabling data-driven decision-making, fostering collaboration among stakeholders, and ensuring the privacy and integrity of sensitive agricultural data. By incorporating advanced techniques such as optimized clustering, deep learning models, hybrid encryption, and blockchain technology, this comprehensive framework contributes to optimizing crop yield, improving resource management, and promoting sustainable practices in precision agriculture. By adopting this methodology, stakeholders in precision agriculture can harness the full potential of data while maintaining security, trust, and efficiency throughout the data sharing

process. The integration of advanced techniques and the use of blockchain technology provide a solid foundation for the development and growth of precision agriculture, leading to improved productivity and sustainability in the agricultural sector.

Funding: The authors declare they have no funding applied.
Conflicts of Interest: The authors declare they have no conflicts of interest to report regarding the present study.

REFERENCES

1. Demestichas K, Daskalakis E. Data lifecycle management in precision agriculture supported by information and communication technology. Agron. 2020;10(11):1648.https://doi.org/10.3390/agronomy10111648
2. Dong M, Yu H, Zhang L, Sui Y, Zhao R. A PCA-SMO Based Hybrid Classification Model for Predictions in Precision Agriculture. TV/TG, 2023; 30(5):1652-1660. https://doi.org/10.17559/TV-20230530000682
3. McLennon E, Dari B, Jha G, Sihi D, KankarlaV. Regenerative agriculture and integrative permaculture for sustainable and technology driven global food production and security. J. Agron. 2021;113(6):4541-59.https://doi.org/10.1002/agj2.20814
4. Mateja O, Vojislav S, Nevena T, Emil V, Ivan Z, Nenad G. Analyzing Site-Specific Tractor Draft Force in Different Passes during Plowing. TV/TG, 31, 1(2024):228-232. https://doi.org/10.17559/TV-20230614000733
5. Hemming S, de Zwart F, Elings A, Righini I, Petropoulou A. Remote control of greenhouse vegetable production with artificial intelligence—greenhouse climate, irrigation, and crop production. Sens. 2019;19(8):1807.https://doi.org/10.3390/s19081807
6. Tantalaki N, Souravlas S, Roumeliotis M. Data-driven decision making in precision agriculture: The rise of big data in agricultural systems. J. Agric. Food Inf. 2019; 20(4):344-80. http://dx.doi.org/10.1080/10496505.2019.1638264
7. Ayaz M, Ammad-Uddin M, Sharif Z, Mansour A, Aggoune EHM. Internet-of-Things (IoT)-based smart agriculture: Toward making the fields talk.IEEE accs.2019; 7:129551-83. https://doi.org/10.1109/ACCESS.2019.2932609
8. Sanjeevi P, Prasanna S, Siva Kumar B, Gunasekaran G, Alagiri I, Vijay Anand R. Precision agriculture and farming using Internet of Things based on wireless sensor network. Trans. Emerg. Telecommun. Technol. 2020; 31(12):e3978.https://doi.org/10.1002/ett.3978
9. Akhter R, Sofi SA. Precision agriculture using IoT data analytics and machine learning. J. King Saud Univ. - Comput. Inf. Sci. 2022; 34(8):5602-18.http://dx.doi.org/10.1016/j.jksuci.2021.05.013
10. Popescu D, Stoican F, Stamatescu G, Ichim L, Dragana C. Advanced UAV–WSN system for intelligent monitoring in precision agriculture. Sens. 2020; 20(3):817.https://doi.org/10.3390/s20030817
11. Kong J, Wang H, Wang X, Jin X, Fang X, Lin S. Multi-stream hybrid architecture based on cross-level fusion strategy for fine-grained crop species recognition in precision agriculture. Comput. Electron. Agric. 2021; 185:106134.http://dx.doi.org/10.1016/j.compag.2021.106134
12. Lloret J, Sendra S, Garcia L, Jimenez JM. A wireless sensor network deployment for soil moisture monitoring in precision agriculture. Sens. 2021; 21(21):7243.https://doi.org/10.3390/s21217243
13. Vinoth KumarK,Duraisamy B. Efficient Privacy-Preserving Red Deer Optimization Algorithm with Blockchain Technology for Clustered VANET. TV/TG, 29, 3(2022), 813-817. https://doi.org/10.17559/TV-20211216115635
14. Linaza MT, Posada J, Bund J, Eisert P, Quartulli M, Döllner J, et al. Data-driven artificial intelligence applications for sustainable precision agriculture. Agron. 2021; 11(6):1227.https://doi.org/10.3390/agronomy11061227
15. Thiruvenkatasamy S, Sivaraj R, Vijayakumar M. Blockchain Assisted Fireworks Optimization with Machine Learning based Intrusion Detection System (IDS). Technical Gazette. 2024;31(2):596-603. doi: 10.17559/TV-20230712000798.
16. Bera B, Vangala A, Das AK, Lorenz P, Khan MK. Private blockchain-envisioned drones-assisted authentication scheme in IoT-enabled agricultural environment.Comput. Stand. Interfaces. 2022; 80:103567.http://dx.doi.org/10.1016/j.csi.2021.103567
17. Lamtzidis O, Pettas D, Gialelis J. A novel combination of distributed ledger technologies on internet of things: Use case on precision agriculture. Appl. Syst. Innov. 2019; 2(3):30. https://doi.org/10.3390/asi2030030
18. Branco F, Moreira F, Martins J, Au-Yong-Oliveira M, Gonçalves R. Conceptual approach for an extension to a mushroom farm distributed process control system: IoT and blockchain. New Knowledge in Information Systems and Technologies, Springer. 2019; 1:738-47. http://dx.doi.org/10.1007/978-3-030-16181-1_69
19. Anand T, Sinha S, Mandal M, Chamola V, Yu FR. AgriSegNet: Deep aerial semantic segmentation framework for IoT-assisted precision agriculture. IEEE Sens. J. 2021; 21(16):17581-90.
20. Awan SH, Ahmed S, Safwan N, Najam Z, Hashim MZ, Safdar T. Role of internet of things (IoT) with blockchain technology for the development of smart farming. J. mech. continua math. sci.2019;14(5):170-188.http://doi.org/10.26782/jmcms.2019.10.00014
21. Ren W, Wan X, Gan P. A double-blockchain solution for agricultural sampled data security in Internet of Things network. Future Gener. Comput. Syst. 2021; 117:453-61.http://dx.doi.org/10.1016/j.future.2020.12.007
22. Awan SH, Ahmed S, Nawaz A, Sulaiman S, Zaman K, Ali MY,Khan ZN, Saeed SI.BlockChain with IoT, an emergent routing scheme for smart agriculture. Int. J. Adv. Comput. Sci. Appl.2020; 11(4):420-9.http://dx.doi.org/10.14569/IJACSA.2020.0110457

23. Chaganti R, Varadarajan V, Gorantla VS, Gadekallu TR, Ravi V. Blockchain-based cloud-enabled security monitoring using Internet of Things in smart agriculture. Future Internet.2022;14(9):250.https://doi.org/10.3390/fi14090250
24. Vangala A, Sutrala AK, Das AK, Jo M. Smart contract-based blockchain-envisioned authentication scheme for smart farming. IEEE IoT- J.2021; 8(13):10792-806.https://doi.org/10.1109/JIOT.2021.3050676
25. Ramamoorthi R, Ramasamy A. Block Chain Technology Assisted Privacy Preserving Resource Allocation Scheme for Internet of Things Based Cloud Computing. Tehničkivjesnik. 2023;30(6):1943-50. doi: 10.17559/TV-20230404000503.