Blockchain and FL-based Secure Architecture for Enhanced External Intrusion Detection in Smart Farming

Sushil Kumar Singh (Member, IEEE)[1,*], Manish Kumar[2], Ashish Khanna[3], Bal Virdee[4]

1* Sushil Kumar Singh (Member, IEEE) is with the Department of Computer Engineering at Marwadi University, Rajkot, India, and is a postdoc researcher Center for Communications Technology at London Metropolitan University, United Kingdom. (Email: sushilkumar.singh@marwadieducation.edu.in).
2 Manish Kumar is with the Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul, South Korea. (Email: manish.guptasssss007@gmail.com).
3 Ashish Khanna (Member, IEEE) is with the Department of Computer Science and Engineering at Maharaja Agrasen Institute of Technology (GGSIPU), India. (Email: ashishkhanna@mait.ac.in).
4 Prof. Bal Virdee (Member, IEEE) is the Director of the Centre for Communications Technology research group at London Metropolitan University, United Kingdom (Email: b.virdee@londonmet.ac.uk)

***Abstract*— Smart farming influences advanced technologies to optimize agricultural procedures, yet it meets significant cybersecurity challenges, particularly in External Intrusion Detection (EID). This article proposes a novel architecture combining Blockchain Technology and Federated Learning (FL) to reinforce the security of Smart Farming Systems (SMS) against external threats. The integration of Blockchain ensures data authentication and transparent data storage, while FL enables collaborative model training without compromising data privacy. Our architecture employs Ensemble Learning (EL) for the Local Model at the Ensemble Layer to train each Smart Land's data and offers privacy-prevented security. These devices utilize FL techniques to collaboratively train intrusion detection models while preserving the confidentiality of sensitive data. The Aggregated Model completes data aggregation at the Authentication Layer, and the PoAh Consensus Algorithm is leveraged for smart land's data authentication. The IoT Sensor device's identical information of smart lands is stored at the Macro Base Stations (MBSs). After downloading the aggregated values of the aggregated model, the local model transfers the smart lands information to the Cloud layer for decision-making and decentralized storage. The validation outcomes of the proposed architecture demonstrate excellent performance, with an average processing time of 3.663 secs and 0.9956 accuracy for Smart Land compared to existing frameworks.**

***Index Terms*— Blockchain, Enhance External Intrusion Detection, Smart Farming, Federated Learning, Privacy, and Security.**

I. INTRODUCTION

Smart farming, also known as precision agriculture, transforms traditional agricultural techniques by fusing new emerging technologies to increase efficiency and productivity while reducing resource use. This modern strategy optimizes farming operations by utilizing sensor technologies, actuators, Internet of Things (IoT) devices, data analytics, and automation [1]. Sensors implanted in fields and on equipment collect real-time sensing data on soil moisture, nutrient levels, weather conditions, and crop health, giving farmers essential insights into the state of their crops. IoT devices provide agricultural asset connectivity and remote monitoring, enabling for faster decision-making and more precise control over irrigation, fertilization, and pest management [2]. Data analytics solutions transform large, massive volumes of data into meaningful insights, helping farmers make informed decisions about planting, harvesting, and resource allocation. Automation technologies like drones and self-driving cars improve efficiency by completing tasks like crop monitoring, spraying, and harvesting with greater precision and lower labor costs [3]. Smart farming represents a paradigm shift in agriculture, with the ability to boost yields, reduce environmental impact, and assure long-term food production in the face of increasing global difficulties. While innovative farming systems provide various benefits, they also present new challenges, particularly in terms of cybersecurity. As these systems become more networked and data-driven, they become vulnerable to cyber-attacks, including external intrusion attacks.

External intrusion in farming refers to unauthorized access or activities on agricultural land, which can pose significant risks to the farm's operations, security, and productivity. These intrusions can take various forms, such as theft or vandalism of crops and equipment, poaching, and unauthorized grazing, each with distinct motivations and consequences. As a result, providing security has become one of the significant challenges today. In addition to traditional physical security measures like fencing and patrolling, modern surveillance systems are essential. These include closed-circuit cameras, sensor technologies such as motion and acoustic sensors, and systems for identifying and authorizing individuals accessing the farm, such as employee badges or biometric scanners. Furthermore, installing alarm systems and security lighting can help prevent sudden damage from external intrusions, enhancing the overall protection of agricultural properties. Cutting-edge technologies such as IoT, federated learning, and blockchain can significantly enhance the detection and prevention of intrusions in farming through improved real-time monitoring and collaborative intelligence data security.

Despite the apparent advantages of smart farming, the growing reliance on interconnected devices and the massive amounts of data created severe cybersecurity issues. One crucial part of intelligent farming security is detecting and preventing external intrusions, which can range from unauthorized access to critical infrastructure to tampering with agricultural data and systems. Traditional intrusion detection systems (IDS) frequently require assistance dealing with smart farming contexts' intricacies [4]. These systems are often built using centralized designs, which can lead to single points of failure and scalability difficulties. Furthermore, they may need to effectively manage the privacy problems that come with -

TABLE I
SUMMARY OF COMPARISON WITH EXISTING RESEARCH STUDY

Research Study	Technology	External Intrusion Detection	Data Authentication	Decentralization	Man-in-the-Middle Attack	Environment
Vangala et al. [9]	Blockchain	×	✓	✓	✓	Smart Agriculture
Eddine et al. [10]	Artificial Neural Networks	×	×	×	×	Smart Farming
Vangala et al. [11]	Blockchain, Smart Contract	×	✓	✓	✓	Smart Farming
EL-Ghamry et al. [12]	Convolutional Neural Networks	×	×	×	✓	IoT-based Smart Farming
Berguiga et al. [13]	Feedforward Neural Network	×	×	×	×	Smart Agriculture
Ting et al. [14]	Fuzzy Logic and Blockchain	×	✓	✓	×	Smart Climate Agriculture
Javeed et al. [15]	BCU, LSTM	×	×	×	✓	Edge-envisioned Smart Agriculture
Proposed Work	Blockchain, PoAh, Federated Learning	✓	✓	✓	✓	Smart Farming and Land Architecture

gathering and analyzing sensitive agricultural data. Blockchain technology has received attention as a potential solution to address security and trust challenges in a variety of domains, including agriculture and farming [5]. Blockchain allows for transparent and tamper-resistant record-keeping by utilizing a decentralized, distributed, and immutable ledger with integrated data. Blockchain can improve data integrity, simplify secure transactions, and promote stakeholder collaboration in advanced Smart Applications in Smart Cities. Data authentication in smart city applications such as Smart Farming, Smart Lands, and others uses a variety of consensus techniques, including PoS, PoW, and PoAh. PoAh is the most recent consensus method for data authentication and validation [6].

Federated Learning (FL) has evolved as a privacy-preserving technique to machine learning model training, making it ideal for cases where data privacy is critical. FL enables edge devices to collaboratively train machine learning models (Ensemble Learning) while keeping raw data local and private [7]. This distributed learning paradigm is well-suited to the distributed nature of smart agricultural systems, which prioritize data privacy and security. Local base stations have limited storage and power capacity, so 5G-based macro base stations are used to store identity information for IoT and sensor devices in Smart City Applications such as Smart Farming, Smart Transportation, and others [8]. A summary of the comparison with the existing research study is shown in Table I.

Integrating blockchain technology with FL can provide a secure architecture/ Framework that improves external intrusion detection in smart farming. Such an architecture would use blockchain's openness and immutability to record and validate model updates while maintaining data privacy using FL methods. Smart contracts can also automate governance processes and assure the integrity of transactions in the system. Overall, establishing a blockchain and FL-based safe architecture shows the potential to solve the cybersecurity and external intrusion detection concerns that smart agricultural systems confront. This technique, which improves external intrusion detection capabilities while protecting data privacy and integrity, can help modern agriculture remain resilient and sustainable in an increasingly digitized world.

A. Related Work

Recently, Vangala et al. [9] proposed a generalized blockchain-based secure architecture for IoT-enabled Smart Agriculture, addressing key security considerations and threats. This research offers a secure environment for smart Agriculture, but privacy preservation is not involved. Eddine et al. [10] proposed a malicious intrusion detection model for IoT-oriented Smart Farming Security, addressing smart agriculture security susceptibilities. They developed a novel framework based on the artificial neural network using radial basis functions (RBF), and categorized malicious intrusion activities in the IoT-enabled Smart Farming Networks. However, the research did not provide a decentralized, privacy-preserved environment, low latency, and efficient infrastructure for IoT-enabled Smart Farming. For smart farming, Vangala et al. [11] developed an authentication key agreement scheme based on Blockchain technology using Smart Contracts. A Mutual Authentication mechanism is leveraged for IoT and sensor device-to-device verification. Privacy preservation and external intrusion detection of smart farms are the key challenges of this research.

EL-Ghamry et al. [12] presented a novel intrusion detection system for intelligent farming IoT networks based on Convolutional Neural Networks (CNN) using an NSL KDD data set. Essential features are determined using recursive feature elimination and transformed into square color pictures. Data authentication, decentralization, farming data integrity, and privacy preservation are key research challenges of this study. A novel intrusion detection design model is proposed by Berguiga et al. [13] for Smart Agriculture based on the fusion of Multilayer Perceptron (MLP) and the Gaussian Mixture Model (GMM), both are part of the Feedforward Neural Network, using CIC-DDoS2019 dataset. This technique offers a promised solution for addressing malicious DDoS attacks in the research study. However, this research did not mitigate some challenges in the Smart Agriculture Environment, such as decentralization, privacy preservation, and complexity, which should be addressed by future research.

Ting et al. [14] developed a secure, intelligent framework for IoT-enabled Smart Climate Agriculture System framework

based on two emerging technologies: intelligent Fuzzy Logic and Blockchain. To make a wise decision about the watering necessities of plants, the authors leveraged the intelligent fuzzy logic and security provided by Blockchain technology for IoT-enabled smart farming. Privacy preservation and external intrusion detection are the challenges of this research study. Javeed et al. [15] presented a novel Intrusion Detection System for Edge-envisioned Smart Agriculture in extreme environments based on the convergence of bidirectional gated recurrent unit (BCU), long-short term memory (LSTM) with a softmax classifier to glimpse malicious attacks at the edge of the smart network. In this research, we develop an Ensemble learning-based Federated (ELF) model to detect any extremal intrusion. FL will help to maintain data privacy at the ensemble layer of smart farming. Again, these results are verified with the help of a blockchain-based consensus algorithm at the authentication layer and then saved finally on the cloud layer. Also, issues like data privacy, external intrusion, and data authentication in a combined manner still need to be investigated for smart farming. We know about various consensus algorithms in Blockchain Technology, such as Proof of Work (PoW), Proof of Stack (PoS), Proof of Availability (PoA), and others. However, we leveraged the Proof of Authentication (PoAh) consensus algorithm for Smart Farming (Lands) related Data Authentication for several reasons, such as: The PoAh consensus algorithm provides more security than other consensus algorithms because miner nodes are also verified in this algorithm. For this reason, miner nodes are called Trusted nodes. PoAh is thus suitable for private and permissioned blockchains because it introduces a cryptographic authentication mechanism to replace PoW, PoA, PoS, and others for resource-constrained and authenticated devices and to make blockchain applications such as Smart Farming (Lands).

B. Article Contribution

The main article contribution is as follows:

- Propose a Blockchain and FL-based Secure Architecture for Enhanced External Intrusion Detection in Smart Farming.
- Design an enhanced external intrusion detection mechanism based on Federated Learning at the ensemble learning layer.
- Develop a Blockchain (PoAh)-based Data Authentication Approach at the authentication layer of the proposed work for the secure environment in Smart Farming.
- Finally, we use quantitative and qualitative analysis to validate the proposed framework against existing research studies based on standard parameters such as computational and transactional cost, trust, and security analysis.

The article's organization is as follows: first, section II describes the Proposed Architecture Overview for enhanced external intrusion detection in smart farming and details the methodological flow structure with a step-by-step explanation. Next, Section III presents the experimental results and security quantitative analysis. Finally, the article concludes in Section IV.

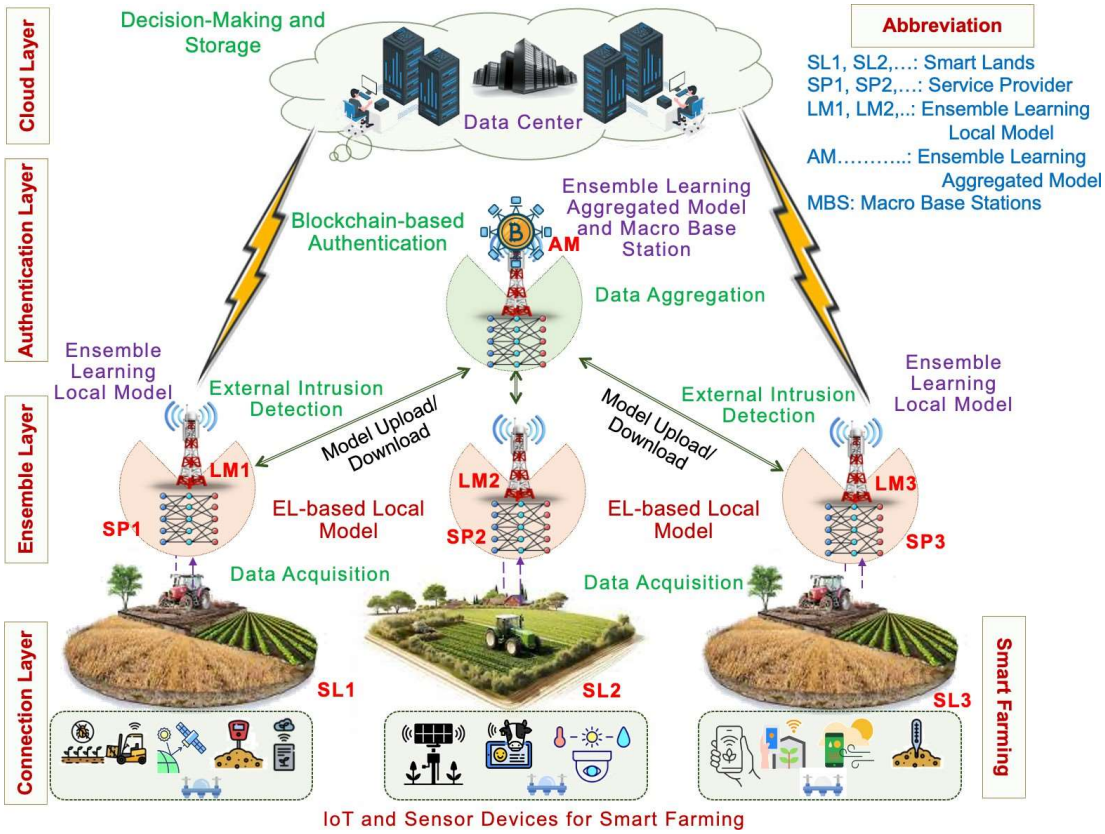


Fig. 1: Proposed Secure Architecture Overview for Secure Smart Farming

TABLE II
ABBREVIATION TABLE

Symbols	Description	Symbols	Description
$\{SP_1, SP_2, ..\}$	Service Provider	$\{t_n\}$	Trusted Nodes
$\{I_1, I_2 ..\}$	IoT Devices	$\{D_i\}$	Bootstrap Samples
$\{SL_1, SL_2, ..\}$	Smart Lands	$f(x)$	Final Prediction
$\{LM_1, LM_2 ....\}$	Local Model	$\{t_{n_1}, t_{n_2}, t_{n_3}\}$	Transactions
$\{MBS\}$	Macro-Base Stations	$\{t_f\}$	Faith value
$\{AM_i\}$	Aggregated Model	$\{AGV_1, AGV_2, ..\}$	Aggregated Gradient Value
FPR	False Positive Rate	MCC	Matthews Correlation Coefficient

II. BLOCKCHAIN AND FL-BASED SECURE ARCHITECTURE FOR SMART FARMING

This section describes and discusses the proposed secure architecture with methodological flow. External intrusion detection is described at the ensemble and authentication layer of the proposed architecture, and data authentication and verification are illustrated at the authentication layer. Therefore, we start with an overview of the architecture and then go through all the parts conferred step by step. The abbreviation table is shown in Table II.

A. Proposed Secure Architecture Overview

The proposed secure architecture has four layers: connection, ensemble, authentication, and cloud, as shown in Fig. 1. Various Smart Lands $\{SL_1, SL_2, SL_3 \ldots\}$ are connected to different types of IoT sensor devices $\{I_1, I_2, I_3 \ldots\}$ smart devices $\{SD_1, SD_2, SD_3 \ldots\}$. These, like a cluster of IoT sensors and smart devices such as cameras, ultra-noise sensors, DHT sensors (Irrigation Control), temperature, soil moisture, light intensity, and humidity, are utilized at the bottom layer (Connected Layer). All IoT sensor devices have specific purposes, such as capturing the image, temperature, water requirement in soil, irrigation, and humidity control. Service providers $\{SP_1, SP_2, SP_3 \ldots\}$ used at the second layer to acquire the smart land data from IoT sensors and smart devices. Federated and Ensemble Learning concepts are also utilized at the ensemble layer for external intrusion detection for Smart Farming. The decision tree model (Local Model $\{LM1, LM2, LM3\}$) is an Ensemble Learning part of the Federated Learning Model. It trains the data and transfers it to an aggregated model $\{AM\}$. By aggregating multiple decision trees, ensemble learning reduces the risk of overfitting and improves the model's generalization across different clients, each of which may have distinct data characteristics. After the aggregation, smart land data is transferred to the Blockchain networks for authentication and validation. Marco base station $\{MBS\}$ and Blockchain (PoAh) consensus algorithm is leveraged at the third (Authentication) Layer of the proposed secure architecture. The macro base station $\{MBS\}$ stores identical information of IoT sensors and smart devices, and the PoAh consensus algorithm completes the smart lands of the proposed secure architecture and data authentication. After data authentication, it is downloaded by local model nodes and transferred to the cloud layer for decision-making and storage.

The top layer (cloud) provides intelligent decision-making and storage purposes in a smart farming environment. It is utilized for smart farming after getting all smart land secure data, such as capturing the image, temperature, water requirement in soil, irrigation, and humidity control. As a result,

smart farming benefits farmers with better-quality and secure services and higher farmer satisfaction. The proposed Secure Architecture's Methodological Flow is shown in Fig. 2.

$$\{I_1, I_2, I_3\} \,\&\, \{SD_1, SD_2, SD_3\} \rightarrow C\ \{SL_1, SL_2, SL_3\} \quad (1)$$

$$\{SP_1, SP_2, SP_3\} \leftarrow data\ acq.\{I_1, I_2, I_3\} \,\&\, \{SD_1, SD_2, SD_3\} \quad (2)$$

B. Enhanced External Intrusion Detection Mechanism

The proposed Federated Learning (FL) algorithm for external intrusion detection leverages Ensemble Learning (EL) and is strategically deployed at the second layer of Smart Farming. The Bagging technique, which combines predictions from multiple Decision Tree (DT) models, is used as the core EL approach in the proposed FL model. This improves the overall performance by reducing the impact of overfitting that can occur in individual Decision Tree models [16]. The mathematical model delineating bagging with DT is as follows: Let D be the original dataset of size N, and D_i be the i^{th} bootstrap samples of size N, obtained by random sampling with replacement. The dataset is prepared on the basis of sensor data like ultrasonic sensors, which can observe the farm boundary and the installed camera response when anything comes to it proximity. The process of creating B bootstrap samples can be represented as:

$$D_i = [(x_{i1}, y_{i1}), (x_{i2}, y_{i2}), \cdots, (x_{iN}, y_{iN})] \quad (3)$$

where, $(i = 1,2,\cdots,B)$ and h_i be the i^{th} DT on the i^{th} bootstrap sample D_i.

$$h_i: X \rightarrow Y \quad (4)$$

Train each DT model on its respective bootstrap sample.

$$h_i = TrainDT(D_i) \quad (5)$$

For the classification tasks, the final prediction $f(x)$ is evaluated by a majority vote among the predictions of individual trees, and it is determined as:

$$f(x) = MajorityVote(h_1(x), h_2(x), \cdots, h_B(x)) \quad (6)$$

The proposed model is built using DT-based EL and employed within the FL framework. FL trains a global model on a decentralized network of clients, where each client contributes to the model training using its local data. Algorithm 1 presents complete design steps for the detection of smart farming. This algorithm highlights all three stages of the proposed FL model: local, global, and aggregate. After completion of the training, we test the trained model with unknown data, i.e., information that does not take part in the training. After testing, the proposed classifier will be validated on the basis of various performance metrics (for example, accuracy, recall, specificity, precision, False Positive Rate (FPR), F1-score, and Matthews Correlation Coefficient (MCC). Using multiple performance metrics provides a comprehensive evaluation of the model by highlighting different aspects of its performance. This is crucial because each metric captures unique information—such as accuracy, recall, precision, and robustness—that helps ensure the model is reliable and meets the specific needs of the application, especially when dealing with imbalanced data or

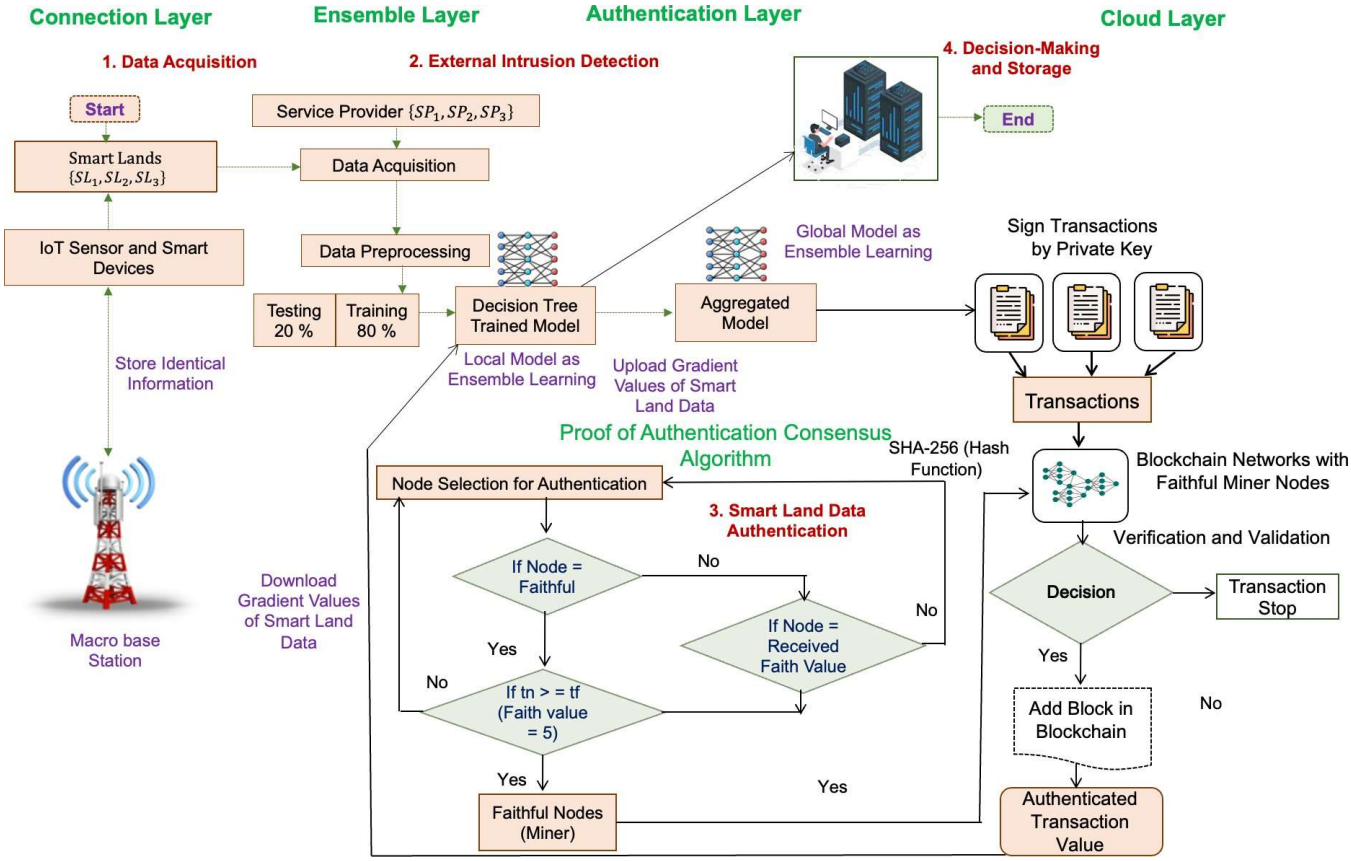


Fig. 2: Proposed Secure Architecture's Methodological Flow

varying costs of errors. The mathematical expression of such metrics is represented as,

$$Accuracy(\%) = \left(\frac{TP+TN}{TP+FN+FP+FN}\right) \times 100 \quad (7)$$

$$Recall = \frac{TP}{TP+FN} \quad (8)$$

$$Specificity = \frac{FP}{FP+TN} \quad (9)$$

$$Precision = \frac{TP}{TP+FP} \quad (10)$$

$$FPR = \frac{FP}{FP+TN} \quad (11)$$

$$F1-Score = 2 \times \frac{Precision \times Recall}{Precison+Recall} \quad (12)$$

$$MCC = \frac{TN \times TP - FN \times FP}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \quad (13)$$

where, TP, TN, FN, and FP are denoting for True Positive, True Negative, False Negative, and False Positive respectively. Table III showcase the hyperparameters of proposed FL technique.

TABLE III
PARAMETERS OF FEDERATED LEARNING CLASSIFIER

Hyperparameters	Values/Type
Number of clients	5
Number of DT to build EL	100
Ensemble Method	Bagging
Data Splitting Method	K-fold cross-validation and value is 2
Number of global model updates	5

Authentication and validation. After the validation of the transaction of gradient values for Smart Land data, one block is added to the blockchain; otherwise, the gradient value transaction has malicious activity (unauthenticated gradient value transaction), and the transaction stops. Then, the local model downloads aggregated and authenticated gradient value, and secure Smart Land data is transferred to the cloud layer for decision-making and storage purposes. Smart Land Data authentication of smart land data is discussed and described in Algorithm 2.

$$\text{Blocks} = tn_1 + tn_2 + tn_3 + \ldots\ldots\ldots \quad (14)$$

$$\text{Private keys } \{M_{keys}\} \rightarrow \text{Blocks}\{Tx_1, Tx_2, Tx_3, \ldots, Tx_i\} \quad (15)$$

$$\text{Blocks } M_{keys} \rightarrow^{\text{Broadcast}} \text{Network } \{TrN_1, TrN_2, TrN_3, ..\}$$

(16) Faithful Miner Nodes←Checks Blocks M_{Keys} ← with N_{Keys} (SHA256 Algorithm); (17)

Algorithm 1: Ensemble Learning-based Federated Model

Input: Providing Smart Farm Sensors-based data and its response, like $D_i = [(x_{i1}, y_{i1}), (x_{i2}, y_{i2}), \cdots, (x_{iN}, y_{iN})]$ for the training of the proposed FL model.

Output: Classifying external intrusion.

Process:

1: Start:

2: Load IoT Sensors dataset

3: Define Input features X and Target labels Y

4: Building FL Model

5: for $\{i = 1\ to\ num-clients\}$

6: Each client updates its local model

$$local\ model\ \{LM1, LM2, LM3\} = fitensemble(client-data\{i\}.X, client-data\{i\}.Y, 'Bag', 100, 'Tree', 'Type', 'classification');$$

7: Combine the local model with the global

$$local-update-model = fitensemble$$

([X; $client-data\{i\}.X$], [Y; $client-data\{i\}.Y$], 'Bag',100,'$Tree$','$Type$','$classification$');

8: Aggregate the local update to the global model

$global-model$ = $compact(fitensemble$ ([X; $client\_data\{i\}.X$], [Y; $client\_data\{i\}.Y$], 'Bag',100,'$Tree$','$Type$','$classification$'));

9: Validate performance of the proposed model with quantitative metrics (e.g.: accuracy, sensitivity, recall, etc.)

10: Save optimal model

10. **END**;

C. *Data Authentication Approach*

In the data authentication approach, various faithful miner nodes are available in the Blockchain networks. The PoAh (Proof of Authentication) consensus algorithm utilizes these nodes for Authentication and Validation purposes. We are leveraging this procedure at the authentication layer of the proposed secure architecture and addressing security and privacy issues. After aggregating gradient values for Smart Lands data as a lot of transactions, all procedures are shown in Fig. 2. Then, the private keys are assigned to the blocks and broadcasted in the blockchain networks. Many faithful miner nodes are available in the Blockchain networks for Authentication and validation. Faithful miner nodes check all these blocks or transactions with the help of the SHA 256 algorithm, which solves the cryptographic puzzles with private keys. Faithful miner nodes are also verified by faithful values based on Algorithm 2 [17]. Faith miner nodes and private keys in the networks achieve the Smart Land Data Authentication and Validation.

Algorithm 2: Smart Land Data Authentication

Input: Aggregated Gradient values $\{AGV_1, AGV_2, AGV_3, ..\}$ of Smart Land, Faithful Miner Nodes, Private Keys $\{M_{keys}\}$, Public Keys $\{N_{keys}\}$.

Output: Authenticated and validated Gradient Value data of Smart Lands

Process:

1: **Start:**

2: $\{tn_1, tn_2, tn_3, \ldots, tn_i\} \leftarrow All\ Block$;

3: Blocks$\{Tx_1, Tx_2, Tx_3, \ldots, Tx_i\} \leftarrow \{M_{keys}\}$;

4: Blocks $M_{keys} \rightarrow^{Broadcast}$ Network $\{TrN_1, TrN_2, TrN_3, ..\}$

5: Select Faithful Nodes ==→ Authentication and Validation

6: **if** (Miner Node = = faithful)

7: **if** ($t_n >= t_f$ (Faith value = 5)); 8: Nodes are faithful

9: **else** 4th Step.

10: **else if** (Normal Node ← Received miner faith value);

11: **else** 6th to 7th Steps;

12: **else** 4th Step.

13: Faithful Miner Nodes←Checks Blocks M_{Keys} ← with N_{Keys} (SHA256 Algorithm);

14: **if** (Validation ==True)

15: Block addition in Blockchain Networks;

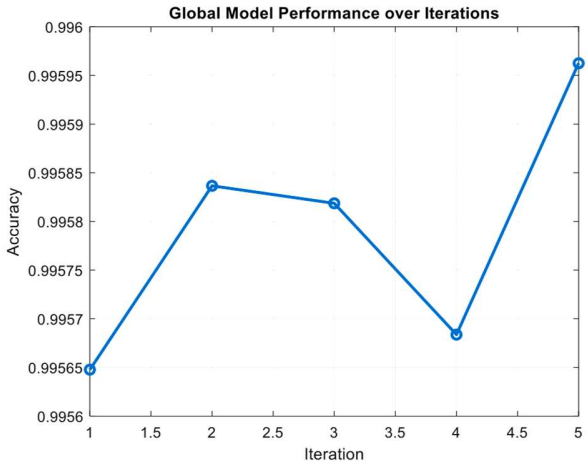
16: **else** Unauthorized Transaction;

17: **END;**

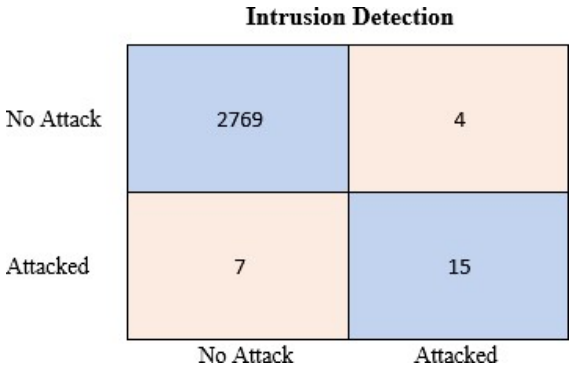
III. Performance and Security Quantitative Evaluation

In this section, we discuss and demonstrate the proposed secure architecture's performance with a security quantitative analysis. The theoretical analysis compares existing research as standard parameters.

The proposed FL-based classifier is executed in the Matlab-2023a software environments, and the computer hardware specification is the 12th Generation Intel Core-i5-12400 processor, 16 GB of RAM, and a 2.50 GHz clock frequency. Hyperledger Fabric 1.3 on VMware 14 Pro and Ubuntu operating system is utilized for PoAh-based Smart Lands data authentication. Node.js v8.9.1 (version 6.8.0) is applied for test interpretation of multiple node tests and transmission processes for successful data authentication with mining nodes in the blockchain network. The sensor data was collected throughout February 2024, with events logged every 15 minutes. A total of 2784 entries were recorded from diverse sensors installed across different fields in Rajkot, primarily utilizing ultrasonic and camera data. This dataset was utilized to develop the proposed FL-based intrusion detection model. Entries were labeled as either 'No Attack' or 'Attack', with 'Attack' denoting the presence of unwanted animals or humans in the agricultural fields.



(a)



(b)

Fig. 3: Global Model Performance Measures (a) Accuracy Comparison (b) Confusion Matrix

TABLE IV.
PERFORMANCE MEASURES

TECHNIQUES	ACCURACY	RECALL	SPECIFICITY	PRECISION	FPR	F1-SCORE	MCC
DT-BASED ENSEMBLE LEARNING	0.9327	0.8755	0.9477	0.9129	0.0126	0.8149	0.8125
PROPOSED-FL	0.9956	0.9189	0.9844	0.9599	0.0044	0.9031	0.8754

TABLE V.
POAH AUTHENTICATION TIME DURATION

Iteration (Number of Transaction)	10	20	30	40	50	60	70	80	90	100
Time (Sec.) in block validation	3.32	3.81	3.62	3.32	2.61	4.20	4.32	3.82	3.90	3.71

TABLE VI.
COMPUTATIONAL COST ANALYSIS

Iterations (Number of Transaction)	Iteration (Number of Transaction)	10	20	30	40	50	60	70	80	90	100
Computational Cost	NON-FL	200	380	490	760	1000	1100	1170	1220	1400	1520
	PROPOSED FL	260	240	490	730	800	890	1020	1100	1360	1500

Fig. 3 depicts the performance of the proposed FL-based classifier in terms of accuracy across different iterations and presents the associated confusion matrices. Specifically, Fig. 3 (a) shows the FL-based classifier's accuracy over iterations, reaching a peak of 99.56% in iteration 5. Accuracy variation across iterations arises from factors like heterogeneity of client data and randomness in local model training. This heterogeneity, influenced by factors such as geographical location and device characteristics, leads to diverse data distributions among clients. Additionally, stochastic optimization algorithms like gradient descent introduce randomness, causing local models to converge towards slightly different solutions. These discrepancies contribute to variations in the global model's performance after aggregating the local models. Similarly, Fig. 3 (b) illustrates the confusion matrix of the proposed FL model, showcasing its ability to successfully detect 'No Attack' 2769 times. However, there were four instances where it was misclassified as 'Attack,' indicating the potential presence of unwanted animals or humans. Similarly, it accurately identified the presence of external intrusions 15 times but erroneously classified the same event as 'No Attack' 7 times. The confusion matrix data shows that the proposed FL-based model provides an accuracy of up to 99.56%.

Likewise, Table IV represents the performance of both the proposed DT-based ensemble learning model and the proposed FL-based model. Apart from accuracy, various other performance metrics were evaluated, such as recall, specificity, precision, false positive rate (FPR), F1-Score, and Matthews Correlation Coefficient (MCC). These data were also assessed based on the confusion matrix, which shows that the federated learning-based technique not only provides superior accuracy but also offers a robust, scalable, and privacy-preserving solution for farmland intrusion detection. Leveraging decentralized data processing, real-time analytics, and collaborative learning enhances agricultural operations' security and efficiency, helping farmers protect their valuable resources and assets. Since the whole process of handling sensitive sensor and image data of the farm remains on local devices (e.g., edge devices or local servers), it minimizes the risk of data breaches and protects the privacy of the farmers. Additionally, DHT sensor data is processed, and soil humidity and temperature data can be used to control the irrigation of the farmland.

We are using an extension version of the consensus algorithm (Proof of Authentication-PoAh), which is part of Blockchain Technology. To simulate the proposed secure architecture, we leveraged six nodes, three of which are trusted nodes available in the decentralized and distributed Blockchain network and utilized 100 iterations. According to these iterations, we investigated the performance results and provided Smart Land data authentication as gradient values at the authentication layer after aggregation with the ensemble learning model; 35 bytes are used for each block size. All network nodes have public keys for encrypting the transactions of gradient values and developing signature certificates using private keys and node IDs used by trusted valuable nodes. These nodes validate the blocks with the authentic signature but use and deploy their public key. After confirmation, trusted and valuable nodes are again broadcast to all nodes in the blockchain-based network to preserve and validate a replica of the block in their ledger. PoAh consensus mechanism or algorithm-based Smart Land Data Authentication as Gradient value is shown in Table V with specific time duration, based on various transactions. We evaluate the average time duration for block Gradient authentication with the PoAh consensus mechanism and algorithm, which is 3.663 secs, employing a maximum of 100 iterations and following all steps of Algorithm 2 of the proposed secure architecture. Additionally, we compare the computational cost of the proposed secure architecture with traditional architecture and analyze which is better, as shown in Table VI; it also utilizes a maximum of 100 iterations.

IV. CONCLUSION

In this article, we proposed a Blockchain and FL-based Secure Architecture for Enhanced External Intrusion Detection in Smart Farming. Federated Learning is utilized for privacy preservation-based external intrusion detection-based ensemble learning and Smart Land data authentication as the PoAh consensus algorithm offers aggregated gradient values, which is part of Blockchain technology. We compared the proposed secure architecture's performance with parameters such as accuracy, average processing time, recall, precision, FPR, F1-

score, MCC, and computational cost, which is better than existing works. The average processing time is 3.663 secs, and the accuracy is 0.9956 of the proposed secure architecture. In the future, we will extend our work with an advanced version algorithm for more accuracy and less average processing time.

ACKNOWLEDGMENT

This research was supported by a Research Seed Grant from Marwadi University, Rajkot, Gujarat (MU/R&D/22-23/MRP/FT13). The technical aspects were additionally supported by the Center for Communications Technology at London Metropolitan University, London, UK, under the supervision of Prof. Bal Virdee.

REFERENCES

[1] Glaroudis, D., Iossifides, A., & Chatzimisios, P. (2020). Survey, comparison and research challenges of IoT application protocols for smart farming. Computer Networks, 168, 107037.

[2] Zhang, W., & Wang, L. (2024). Advancing Agricultural Practices through IoT-Driven Crop Field Monitoring and Automated Irrigation Systems for Seamless Farm Management. Advances in Urban Resilience and Sustainable City Design, 16(02), 1-17.

[3] Mohamed, E. S., Belal, A. A., Abd-Elmabod, S. K., El-Shirbeny, M. A., Gad, A., & Zahran, M. B. (2021). Smart farming for improving agricultural management. The Egyptian Journal of Remote Sensing and Space Science, 24(3), 971-981.

[4] El-Ghamry, A., Darwish, A., & Hassanien, A. E. (2023). An optimized CNN-based intrusion detection system for reducing risks in smart farming. Internet of Things, 22, 100709.

[5] Singh, S. K., Azzaoui, A. E., Choo, K. K. R., Yang, L. T., & Park, J. H. (2023). Articles A Comprehensive Survey on Blockchain for Secure IoT-enabled Smart City beyond 5G: Approaches, Processes, Challenges, and Opportunities. Hum.-Centric Comput. Inf. Sci, 13, 51.

[6] Rahman, W., Hossain, M. M., Hasan, M. M., Iqbal, M. S., Rahman, M. M., Hasan, K. F., & Moni, M. A. (2024). Automated Detection of Harmful Insects in Agriculture: A Smart Framework Leveraging IoT, Machine Learning, and Blockchain. IEEE Transactions on Artificial Intelligence.

[7] Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Poor, H. V. (2021). Federated learning for internet of things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 23(3), 1622-1658.

[8] Habbal, A., Goudar, S. I., & Hassan, S. (2019). A Context-aware Radio Access Technology selection mechanism in 5G mobile network for smart city applications. Journal of Network and Computer Applications, 135, 97-107.

[9] Vangala, A., Das, A. K., Kumar, N., & Alazab, M. (2020). Smart secure sensing for IoT-based agriculture: Blockchain perspective. IEEE Sensors Journal, 21(16), 17591-17607.

[10] Mohy-eddine, M., Guezzaz, A., Benkirane, S., & Azrour, M. (2024). Malicious detection model with artificial neural network in IoT-based smart farming security. Cluster Computing, 1-16.

[11] Vangala, A., Sutrala, A. K., Das, A. K., & Jo, M. (2021). Smart contract-based blockchain-envisioned authentication scheme for smart farming. IEEE Internet of Things Journal, 8(13), 10792-10806.

[12] El-Ghamry, A., Darwish, A., & Hassanien, A. E. (2023). An optimized CNN-based intrusion detection system for reducing risks in smart farming. Internet of Things, 22, 100709.

[13] Berguiga, A., Harchay, A., Massaoudi, A., Ayed, M. B., & Belmabrouk, H. (2023). GMLP-IDS: A Novel Deep Learning-Based Intrusion Detection System for Smart Agriculture. Computers, Materials & Continua, 77(1).

[14] Ting, L., Khan, M., Sharma, A., & Ansari, M. D. (2022). A secure framework for IoT-based smart climate agriculture system: Toward blockchain and edge computing. Journal of Intelligent Systems, 31(1), 221-236.

[15] Javeed, D., Gao, T., Saeed, M. S., & Kumar, P. (2023). An intrusion det ection system for edge-envisioned smart agriculture in extreme environ ment. IEEE Internet of Things Journal.

[16] F. Farooq, W. Ahmed, A. Akbar, F. Aslam, and R. Alyousef, "Predictiv e modeling for sustainable high-performance concrete from industrial w astes: A comparison and optimization of models using ensemble learner s," Journal of Cleaner Production, vol. 292, p. 126032, 2021.

[17] Singh, S. K., Kumar, M., Tanwar, S., & Park, J. H. (2024). GRU-based digital twin framework for data allocation and storage in IoT-enabled sm art home networks. *Future Generation Computer Systems*, *153*, 391-402 .