International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/24 Volume 12, Issue 3, May – June (2025)

RESEARCH ARTICLE

# Design of an Improved Model Integrating Blockchain, Machine Learning, and Differential Privacy for Cybersecurity in Smart Farming

Ramesh Pandharinath Daund
Department of Computer Engineering, School of Computer Science and Engineering, Sandip University, Nashik, Maharashtra, India.
✉ ramesh.daund@gmail.com

Mohd Junedul Haque
Department of Computer Engineering, School of Computer Science and Engineering, Sandip University, Nashik, Maharashtra, India.
mohammad.haque@sandipuniversity.edu.in

Umesh Pawar
Department of Computer Engineering, School of Computer Science and Engineering, Sandip University, Nashik, Maharashtra, India.
umesh.pawar@sandipuniversity.edu.in

Received: 18 March 2025 / Revised: 21 May 2025 / Accepted: 02 June 2025 / Published: 30 June 2025

**Abstract – There is a critical need for improved cybersecurity and privacy in smart farming; the adoption of advance technologies opens vulnerabilities to cyber threats and data breaches. Most of the solutions developed so far fail to provide the required scalability, robustness, and privacy measures toward completely securing smart farming environments. This paper contributes to solving these limitations by integrating state-of-the-art cybersecurity and privacy using a multifaceted approach. In this paper, we present a holistic framework that uses blockchain, machine learning, deep learning, and data science techniques to protect smart farming systems. First, we use Hyperledger Fabric with smart contracts to assure integrity and privacy in data samples. Being a permissioned blockchain, Hyperledger Fabric offers high scalability and supports smart contracts that help in rigorous access control and immutable transaction records. Preliminary results indicate 100% integrity and 98% privacy compliance of the data samples. We also implement isolation forest, an unsupervised machine learning algorithm, for threat detection by identifying anomalies in network traffic and sensor data samples. This approach presents an efficient way of treating high-dimensional data and provides a 95% detection rate with a 2% false positive rate. Further, we use Long Short-Term Memory (LSTM) networks in order to detect advanced and time-evolving threats hidden in sequential data samples. Since LSTMs are good at recognizing temporal patterns, threat detection accuracy is reportedly as high as 97% with a precision of 96% and a recall of 95%. Differential privacy is further combined with federated learning to ensure better privacy. Federated learning enables model training on decentralized devices and maintains data locality, protecting individual data contributions through differential privacy via the addition of noise. This approach provides high privacy, ε=1.0, while maintaining model accuracy at 92%, thus avoiding loss in privacy. The model presented herein alleviates the inadequacy of the different existing solutions by providing a scalable, robust, and privacy-preserving framework for smart farming. In this paper, we present a holistic inclination toward enhancing the security and privacy of smart farming systems against cyber threats and protecting sensitive data samples. Our work is well plated on the integration of new technologies in threat detection, integrity of data, and setting a new standard of privacy-preserving best practice in the agricultural domain.**

**Index Terms – Blockchain, Machine Learning, Differential Privacy, Smart Farming, Cybersecurity, Smart Contracts, Agricultural, Security, Analysis.**

## 1. INTRODUCTION

The IoT-enabled new era of smart farming has turned agriculture into a precision farming domain, characterized by the efficient use of farming resources and improved yields. On the other hand, the advent of digital technologies into farming operations brought in many cybersecurity and privacy issues. With the substantial use of sensors, actuators, and interconnected devices in smart farming ecosystems, it follows that a lot of data would be created from such systems, thereby establishing such systems as potential sites for cyber-attacks and data breaches. Top on this list of considerations

RESEARCH ARTICLE

[1, 2, 3], and with regard to this, is the fact that this type of system might require security and privacy in order to assure integrity and trustworthiness overall. Conventional ways of cybersecurity may work in one respect, but fail to be efficient or effective when put into the dynamic, decentralized context of smart farming settings. Most of the time, such measures lack the scalability to handle the volumes of data generated by smart farming devices and matrixed robustness against the sophisticated cyberattacks. However, more often than not, these conventional ways have rarely been effective enough to secure sensitive data to a level that provides adequate protection, thereby posing serious threats to farmers or their agricultural enterprises. This paper, therefore, posits a holistic framework to integrate blockchain [4, 5, 6], machine learning, deep learning, and data science techniques in order to improve cybersecurity and privacy in smart farming implementations in process.

Real-time agricultural decision-making and resource optimization are now possible because smart farming is possible through a fusion of IoT, cloud computing, and data analytics. The digitalization of agriculture, however, brings with it daunting cyber security and privacy contravention challenges due to the extensive amount of heterogeneous data produced because of the activity of sensors, drones, and other interconnected devices in farming. Cyber-attacks such as data breaches, unauthorized access, spoofing of sensors and malware injection impinge directly on food supply chains and data integrity in precision agriculture. More specifically, traditional means of security protection would prove insufficient for managing the decentralized, dynamic environment typical of smart farming. Hence forming a robust, scalable, and privacy-preserving cybersecurity framework becomes critical to ensuring secure data exchange, device integrity, and farmer trust. This research aims to address the integration of blockchain for tamper-proof data management, machine learning for anomaly and threat detection, and differentially private mechanisms for privacy-preserving model training within smart agriculture ecosystems.

For this, it will use Hyperledger Fabric for blockchain [7, 8, 9], soft contracts, and other technologies, including the Isolation Forest for Anomaly Detection, Long Short-Term Memory Nets in Advanced Threat Detection, and the combination of differential privacy with federated learning in order to achieve an overall complete, robust, scalable, and privacy-preserving solution in smart farming. In addition, Hyperledger Fabric offers a decentralized and permissioned way of assuring data integrity and transparency. In the sense that it offers immutable ledger entries, assurances, and transparency. Within smart contracts, access control policies of Hyperledger Fabric protocols make sure that sensitive data is shared only with relevant parties. Moreover, this approach totally removes the risk of single points of failure and, with each transaction having its own audit trail, can build trust and accountability in the system. For this purpose, machine learning techniques are applied to find the anomalies in the network traffic and readings obtained from the sensors, and one of the techniques applied is Isolation Forest.

The isolation forest, being high-dimensional, is quite effective where the data are high-dimensional, for example, in smart farming. Therefore, this highly accurately and quickly detects current possibilities of cyber attacks by isolating observations in the feature space accordingly. The Long Short-Term Memory method, extraordinary specialization for recurrent neural networks in analyzing sequential data to detect sophisticated threats, is being applied. The LSTM network can learn temporal dependencies and can identify more complex, ever-changing threats in the traffic of the network and sensor data samples. At the same time, it will enhance the system's capability in detecting complex patterned attacks and reacting to such patterns, hence improving the overall security. Our framework contains mechanisms of differential privacy in conjunction with federated learning for the protection of participants' privacy. Differential data privacy can hence be obtained by the addition of noise on contributions to personal data so that nothing leaks out about sensitive information. In such a setup, federated learning assures the possibility to train models above devices without bringing their data to a central place and so protect privacy and confidentiality of the information owners. These combined techniques are successful in maintaining privacy while extracting useful insights from data samples. Numerical preliminary results show the effectiveness of the proposed model in ensuring integrity of data, compliance with privacy, identification of threats accurately, and model accuracy. These underline the potential that our integrated approach has for converting practices related to cybersecurity and privacy in smart farming to a new level of industry standard setting. In essence, this paper develops a novel framework that integrates blockchain, machine learning, deep learning, and data science techniques in smart farming systems' security and privacy enhancement. In this regard, our approach also resolves the previous deficiencies of robust designs and scalability, utilizing privacy-preserving technologies in this new smart farming environmental setting & process.

### 1.1. Motivation & Contributions

This study is motivated by the increased use of smart farming technologies vis-à-vis associated cyber-attacks against them. Smart farming shall capitalize on devices that are IoT-enabled, and with sensors, the connected machinery shall optimize agricultural practices to bring better yields and reduce resource wastages. Though interlinked, many vulnerabilities within these systems, coupled with vast data generated, make them very prone to cyber-attacks. That is to say, traditional cybersecurity measures are inadequate to

RESEARCH ARTICLE

secure such complex, dispersed environments, therefore calling for innovative solutions that can provide robust security and privacy protection. This paper presents a holistic, perfectly integrated framework responding to the special challenges in cybersecurity and privacy related to smart farming. Our solution integrates some state-of-the-art technologies hand-picked for their potential to improve lines of security and privacy. Integrity and traceability are guaranteed through the decentralized, permissioned blockchain platform of Hyperledger Fabric. Within this, smart contracts are run that enforce a very tight access control policy to provide robust access control to the data, thus preventing unduly manipulated changes.

Further, machine learning enhances the platform's capabilities for the detection of anomalies in network traffic and sensor data using the algorithm of Isolation Forest. Basically, isolation forest efficiency in handling high-dimensional data makes it fit in smart farming environments. More advanced threat detection using Long Short-Term Memory (LSTM) networks allows for the processing of complex, time-evolving threats with appropriate tools. LSTM networks are quite good at handling sequential data, which helps them pick out temporal patterns missed by most algorithms. Our architecture combines federated learning with differential privacy mechanisms to better protect privacy. Differential privacy adds noise to protect the individual datum contribution; at the same time, federated learning protects against data breaches by allowing decentralized training of models. This would not only provide better privacy protection but also ensure the construction of accurate and reliable models without the requirement of centralized aggregation. This work has impacts on several folds. Our framework mitigates the risk of cyber-attacks and data breaches by providing a robust and scalable solution toward enhancing cybersecurity and privacy in smart farming, thus protecting sensitive agricultural data and continuity of farming operations. The combination of blockchain, machine learning, and differential privacy sets a new standard in security practices within the agricultural domain, providing a model easy to be ported and extended to other IoT-driven industries. Besides, our approach fosters trust and accountability in smart farming systems, driving further adoption of these technologies and further innovation in the field. This work thus provides a step toward the development of safe and privacy-preserving smart farming systems while enabling an expansive future for agriculture and IoT security.

The rest of the paper is organized as follows. Section 2 presents the related work reviewed during the development of this manuscript. Section 3 offers a comprehensive description of the proposed design, titled "An Improved Model Integrating Blockchain, Machine Learning, and Differential Privacy for Cybersecurity in Smart Farming." Section 4 details the comparative result analysis of the proposed approach. This is followed by the Conclusion and Future Scope in Section 5.

## 2. RELATED WORK

This has opened up a completely new frontier of agricultural productivity and efficiency by integrating such advanced technologies as IoT, artificial intelligence, and blockchain. With the agricultural sector increasingly infused with such technologies, the requirement in terms of strong cybersecurity and privacy measures will also increase. A vast and multifaceted body of research is presented, ranging from threat detection, now empowered by machine learning, to blockchain-enabled authentication schemes. The review shall critically evaluate the methodologies, findings, results, and limitations of recent studies in the domain of smart farming security and privacy, intending to provide an overview of the state-of-the-art solutions and point out gaps that may assist future research processes. In the area of machine learning, there have been contributions, which can be seen, for example, in studies by Mohy-eddine et al. [1], oriented toward using ANNs for malicious activity detection, and Alwadi et al. [9], oriented toward deep machine learning for milk production yield estimation. These models have been quite accurate and effective in application, but were often handicapped by the architecture of the neural networks used and concerns with certain aspects of farming, like milk production. Again, some work in deep learning-based IoT modules by Manikandan et al. [5] has been done that can be adaptable to different environmental conditions while their performance can be influenced by these variations in process.

IoT-based solutions, according to various research works, such as Kethineni and Pradeepini [6] and Dahane et al. [7], highlight the necessity of low-cost and cost-effective systems for irrigation and intrusion detection. These pieces of work offer very practical insights into the deployment of IoT in small-scale farming since they sidestepped two major concerns related to cost and scalability. The overdependence on some of these frameworks, such as hybrid deep learning and low-cost sensor networks, reduces the applicability of the solutions in various farming contexts. Blockchain has become one of the most indispensable tools in smart farming with respect to data integrity and authentication. Vangala et al. [11] and Mishra et al. [21] have demonstrated that blockchain can be used to secure the transmission of data and establish authenticated key agreements between entities, thus strengthening the security of the entire system. Even though blockchain-based solutions are very robust in nature, the cost of their implementation is generally computationally expensive and introduces latency, as mentioned above and also demonstrated by Chen et al. [23]. Moreover, the integration of redactable blockchains is complex, which Mishra et al. [21] have addressed; hence, it sits at the core of many challenges to wide applicability.

RESEARCH ARTICLE

The works of Lama and Karmakar [4] and Zheng et al. [25] have added more intelligence to blockchain frameworks by integrating smart contracts that optimize agricultural operations with data integrity. Results obtained from such studies have shown high gains in operational efficiency and security. However, this creates dependencies on blockchain infrastructure and smart contract execution, possibly raising resource consumption and narrowing feasibility in resource-constrained use environments. In this context of privacy-preserving mechanisms, the study by Cherbal [12] and Song et al. [23] draws attention to differential privacy and flexible data publishing schemes in the protection of sensitive agricultural data samples. All these methods balance very well between privacy and data utility but often at the cost of computational overhead and implementation complexity. In particular, one more work by Bai et al. [19] was focused on lightweight anonymous authentication schemes. It emphasizes, very well, the need for efficient, resource-aware security solutions, especially in resource-asymmetric smart environments. Advanced threat detection techniques, as shown in works like Farooq et al. [14] and Zhou et al. [15], define the strong power of the intrusion detection and behavior rule specification contribution to smart farming systems. As much as they have proved effective, these methodologies require complex infrastructures and expertise that might challenge broad diffusion in different farming scenarios. There have been visible advances in smart farming security and privacy according to the literature reviewed, yet not without attached challenges and limitations. Another recurring theme is dependency on particular technologies, associated high computational costs, and integration complexity for combining several solutions, requiring further research and innovation operations.

Iteratively, Next, as per table 1, Balani N. et. Al. [26] presents a novel high-speed blockchain-based sidechaining protocol optimized for peer-to-peer (P2P) communication over 5G networks. It enhances multimedia transmission by addressing latency and security concerns, leveraging blockchain to ensure data integrity and efficient resource allocation. The proposed model improves scalability and performance in 5G environments. This research introduced by Balani N. et. Al. [27] gives a heuristic-based model to optimize blockchain side-chain configurations, enhancing efficiency and security. The study focuses on minimizing computational overhead and improving interoperability between blockchains. The proposed model demonstrates improved transaction validation speed and reduced latency in distributed environments. CSIMH, a security-aware sidechaining model leveraging iterative meta-heuristics for improved blockchain scalability and efficiency. It enhances security, reduces computational complexity, and optimizes sidechain operations through adaptive heuristic techniques. The model ensures secure, high-performance blockchain-based communication, Balani N. et. Al. [28].

Table 1 Empirical Review of Existing Methods

| Reference | Method Used | Findings | Results | Limitations |
|---|---|---|---|---|
| [1] | Artificial Neural Network | Developed a malicious detection model for IoT-based smart farming. | High detection accuracy. | Limited by the specific ANN architecture. |
| [2] | Densely Connected Convolutional Neural Network | Enhanced efficiency in agriculture with smart farming models. | Improved agricultural yield and efficiency. | Requires high computational resources. |
| [3] | Various Prediction Models | Comprehensive survey of smart farming prediction models. | Detailed analysis of precision agriculture techniques. | Does not provide a new model. |
| [4] | IFTTT-based Monitoring System | Ensured data integrity and optimized agriculture using IFTTT. | Improved data integrity and agricultural efficiency. | Dependence on IFTTT limits flexibility. |
| [5] | Deep Learning-based IoT Module | Developed a deep learning IoT module for diverse environmental conditions. | Enhanced adaptability to different conditions. | Performance varies with environmental changes. |
| [6] | Hybrid Deep Learning Framework | Intrusion detection in IoT-based smart farming. | Improved intrusion detection rates. | Complexity in integrating hybrid models. |
| [7] | IoT Low-Cost Smart Farming | Enhanced irrigation efficiency for smallholder farmers. | Increased irrigation efficiency. | Limited to small-scale farms. |

**RESEARCH ARTICLE**

| | | | | |
|---|---|---|---|---|
| [8] | Darts Game Optimization | IoT-based smart farming model using fuzzy kernel ridge regression. | Optimized farming operations. | Complexity in implementing the optimization. |
| [9] | Deep Machine Learning | Predicted milk production yield in smart dairy farming. | High accuracy in yield prediction. | Focused only on dairy farming. |
| [10] | Wireless Sensor Nodes | Used for agricultural smart fault detection. | Effective fault detection. | Limited by sensor network coverage. |
| [11] | Blockchain-based Authentication | Developed an authentication scheme for smart farming. | Enhanced security and authentication. | High computational cost for blockchain. |
| [12] | Triple Security Scheme | Authentication and data transmission security for IoT. | Improved security for IoT devices & deployments. | Potential overhead in communication. |
| [13] | Two-Level Coordinated Static Voltage Security | Addressed voltage security in wind farms. | Enhanced voltage stability. | Specific to wind farms. |
| [14] | IoT-Based Smart Greenhouse | Developed control strategies for sustainable agriculture operations. | Improved greenhouse management. | Requires advanced IoT infrastructure. |
| [15] | IoT Features Analysis | Examined security and privacy threats in IoT. | Comprehensive threat analysis. | No specific solutions proposed. |
| [16] | Behavior Rule Specification-Based Detection | Misbehavior detection in smart greenhouse systems. | Improved detection of misbehaviors. | Dependent on rule specifications. |
| [17] | Enhanced Black Widow Optimization | Intrusion detection in IoT-based smart farming. | High detection accuracy. | Complexity in the optimization process. |
| [18] | Big Data and Machine Learning | Reviewed smart farming techniques for rice production. | Detailed review of precision agriculture methods. | No practical implementation. |
| [19] | Lightweight Anonymous Authentication | Developed a mutual authentication scheme for smart environments. | Enhanced security for resource-constrained devices & deployments. | Limited to resource-asymmetric environments. |
| [20] | Blockchain-Enabled Key Agreement | Authenticated key agreement for precision agriculture IoT networks. | Improved security and authentication. | High latency in key agreement process. |
| [21] | Redactable Blockchain-Assisted Data Aggregation | Secure data aggregation for IoT-based farming. | Enhanced data privacy and security. | Complexity in redactable blockchain implementation. |
| [22] | Transient Stability Assessment | Stability analysis for multiparalleled wind farms. | Improved transient stability. | Specific to wind farm applications. |
| [23] | Privacy-Preserving Data Publishing | Developed a flexible data privacy scheme for smart agriculture operations. | Enhanced data privacy and flexibility. | Potential trade-offs with data utility. |

RESEARCH ARTICLE

| | | | | |
|---|---|---|---|---|
| [24] | Frequency Security Constrained Scheduling | Addressed frequency support in wind farms. | Improved frequency stability. | Limited to wind power systems. |
| [25] | Smart-Contract-Based Service Platform | Optimized drone plant protection operations. | Enhanced operational efficiency. | Dependence on blockchain technology. |

In this way, a detailed analysis of methodologies and recent findings will leave no room for superficial understanding of the situation in the field of cybersecurity and privacy in smart farming. The multiple technologies in this paradigm include artificial neural networks, IoT, blockchain technology, and differential privacy, which reflect different measures to cater to the unique challenges posed by the smart farming domain. While each of these studies contributes toward the overall goal of enhancing security and privacy, the limitations identified have provided a path for further research and development. For instance, artificial neural networks, as in the probe of Mohy-eddine et al. [1], have revealed a very good effectiveness in malicious activity detected within IoT-based smart farming systems. The model has indicated high accuracy in the detection of the same, although this is dependent on the architecture of the neural network. These all point out that future research could well optimize the ANN architecture for maximum adaptability and robustness across the various applications in farming. Similarly, the machine learning model by Alwadi et al. [9] on in-depth dairy farming is useful in the prediction of agricultural yields, but the applicability of the model beyond dairy farming is a cascading issue. The IoT-based frameworks, such as the one proposed by Kethineni and Pradeepini in [6], present implementation guidelines for intrusion detection and irrigation effectiveness. These studies have shown that there is a requirement for an IoT solution that is quite cost-effective and scalable. However, the specificity of these frameworks to certain conditions in farming brings to the fore the need for more generalized IoT models that can be applied with minor modifications to practically any agricultural situation.

The blockchain technology applied to data transmission securitization and authenticated key agreement is confirmed to be robust and valuable by Vangala et al. [11] and proved by the author by Mishra et al. [21]. However, the computational costs are quite high, and so is the associated latency for blockchain implementations. This may also be overcome within future investigations while designing more effective blockchain protocols or hybrid models. Blockchain overlays in combination with other lightweight security mechanisms to reduce the severity of these drawbacks over a variety of settings. Smart contracts are embedded in blockchain environment, demonstrated by Lama and Karmakar [4], and illustrated that strong enhancements are achieved in operational efficiency and levels of data integrity. Despite all the advancements undertaken, smart contract invocations are particularly resource-intensive, notably in a farming setting that is resource-constrained. Moreover, alternative smart contract execution models or optimization of existing ones for efficiencies on resource utilization could make the technologies poised to offer much promise more feasible for wider applications. Privacy-preserving mechanisms, such as differential privacy and flexible data publication schemes highlighted by, for example, such as Cherbal et al. and Song et al., are put in effective use for the protection of sensitive agricultural data samples being utilized in this work. These approaches strike a fine balance between privacy and data utility, but these computational overheads and implementation complexities should be elaborately studied further. All of these limitations could be obviated by the innovation of more efficient privacy-preserving algorithms that might be incorporated smoothly into existing smart farming systems. State-of-the-art threat-detection techniques suggested by Farooq et al. [14] and Zhou et al. [15] are very important for keeping a smart farming system secure. Although these methods bring high efficiency, their heavy reliance on sophisticated infrastructure and expertise creates a challenge to their implementation in diversified farming contexts. Research in the future can be oriented toward this kind of simplification of detection models or user interfaces that become easy for a farmer to adopt at different levels of technological developments. Results of the review suggest that there has been significant progress in advancing levels of cyber security and privacy within the smart farming domain. However, the identified limits suggest that there is still much to be done. This means that, in the future, more abstract and scalable solutions, which can be easily tunable to a large number of different agricultural settings, will be needed for the future of smart farming. By addressing these challenges, researchers could pave the way for implementations of more secure, privacy-preserving, and efficient smart farming systems, which definitely would contribute significantly to sustainability and productivity in agricultural sectors.

Recent smart farming cybersecurity research includes a range of technologies. For example, artificial neural networks (ANNs) have been used by Mohy-eddine et al. for malicious activity detection in IoT networks with high detection accuracy, although this approach is hindered by architectural rigidity and is limited in generalizability. A deep learning-based IoT module was introduced by Manikandan et al., which is adaptable to environmental variability through the use of convolutional neural networks; however, performance is highly sensitive to changes in environmental conditions. Kethineni and Pradeepini have also proposed hybrid models

RESEARCH ARTICLE

that incorporate both deep learning and rule-based systems for intrusion detection but face integration complexity and increased processing cost overheads. Blockchain-based solutions developed by Vangala et al. and Mishra et al., however, incurred performance losses in terms of high latency and computational costs. Privacy-preserving mechanisms such as those of Cherbal and Song applied differential privacy techniques for publishing secure data, attempting to balance privacy and utility, but increased algorithmic complexity accompanies such a balance. Each of the approaches solves a particular problem-for example, detection, authentication, or privacy-but most have scalability, interoperability, and performance issues under resource-constrained conditions. The need to create a synergy of strengths that leverage the complementary benefits of blockchain, machine learning, and differential privacy to address the limitations of previous work is clear, given these issues in process.

## 3. PROPOSED DESIGN OF AN IMPROVED MODEL INTEGRATING BLOCKCHAIN, MACHINE LEARNING, AND DIFFERENTIAL PRIVACY FOR CYBERSECURITY IN SMART FARMING

To overcome issues of low efficiency & high complexity which are present in existing models, this section discusses Design of an Improved Model Integrating Blockchain, Machine Learning, and Differential Privacy for Cybersecurity in Smart Farming Operations. First, according to Figure 1 & Pseudo code 1, the Hyperledger Fabric with Smart Contracts is integrated to act as the blockchain platform to guarantee that the smart farming data is integral, traced, and private. Its permissioned nature, modular architecture, and support for smart contracts immediately make it very suitable for the management of sensitive agricultural data samples. This platform allows decentralized ledger technology to offer an immutably strong mechanism for recording transactions and enforce access control policies through smart contracts. Some of the critical components in the design of this application of Hyperledger Fabric are as follows: The readings of farming sensors concerning temperature, humidity, and soil moisture are collected and proposed as transactions within the blockchain network. According to the consensus protocol, every such transaction is checked by specially designated nodes. Access control policies are enforced in order to allow only authorized entities to read or modify data samples by smart contracts, which are already defined and encoded within the blockchain. The validated transactions are thereafter timestamped into a blockchain ledger, hence immutable and transparent. The outputs from the system include immutable transaction records, access logs, and smart-contract rules that are enforced. Consider the model described below, which formalizes the data collection and validation process. Let D(t) be some sensor data that was collected over a timestamp, t, and T be a set of proposed transactions to the blockchain.

Equation (1) expresses each transaction Ti ∈ T as a function of the sensor data and the access control policies A,

$$Ti = f(D(t), A) \quad (1)$$

Function f, in simple terms, bundles up all the processes regarding packaging data obtained from the sensor in a transaction format conforming to the requirement expected by the blockchain network. The process of validation is executed through a consensus protocol achieved by a combination of practical Byzantine Fault Tolerance, or other mechanisms for achieving consensus, which guarantees that every transaction Ti has been agreed upon before its addition to the blockchains by the majority of validating nodes. Mathematically, this can be expressed via equation (2).

$$\sum_{i=1}^{n} Vi(Ti) \geq \frac{2}{3}n \quad (2)$$

Here, Vi(Ti) is node i's validation function for transaction Ti, and n is the number of validating nodes. Smart contracts are key to automating access control and recording transactions. These smart contracts are characterized by a set of rules, R, governing data access policies and mechanisms of transaction enforcement. Let S be the state of the smart contract, and E be the set of events that trigger its executions.

The smart contract can be modeled as a state transition function g via equation (3).

$$S(t+1) = g(St, E) \quad (3)$$

Where, St is the current state of smart contract, and S(t+1) corresponds to a new state after the process of event E. The formula thus captures the dynamics of smart contracts in terms of their ability to react upon various events and enforce predefined rules. The reason for choosing Hyperledger Fabric is that it can provide secure, scalable, modular architecture complemented by other cybersecurity measures like machine learning and differential privacy. Being permissioned in nature, only trusted entities could take part in the network, bringing improvement to data integrity and privacy. It provides for the mechanization of access control policies through smart contract support, thereby obviating the risk of human failure and enhancing compliance with privacy regulations. Besides, this modular architecture enables seamless integration with other security mechanisms that create a robust and comprehensive cybersecurity framework. The proposed model complements other methods by providing a secure foundation for data integrity and access control. In this context, blockchain technology can be combined with the development of machine learning algorithms for threat detection, such as isolation forest and LSTM networks. Differential privacy mechanisms will secure the contributions of individual data even while sharing across multiple entities. These technologies bring forth a multilayer

RESEARCH ARTICLE

security framework that can solve exceptional challenges brought forth by smart farming environments to ensure the integrity, privacy, and security of samples of agricultural data.

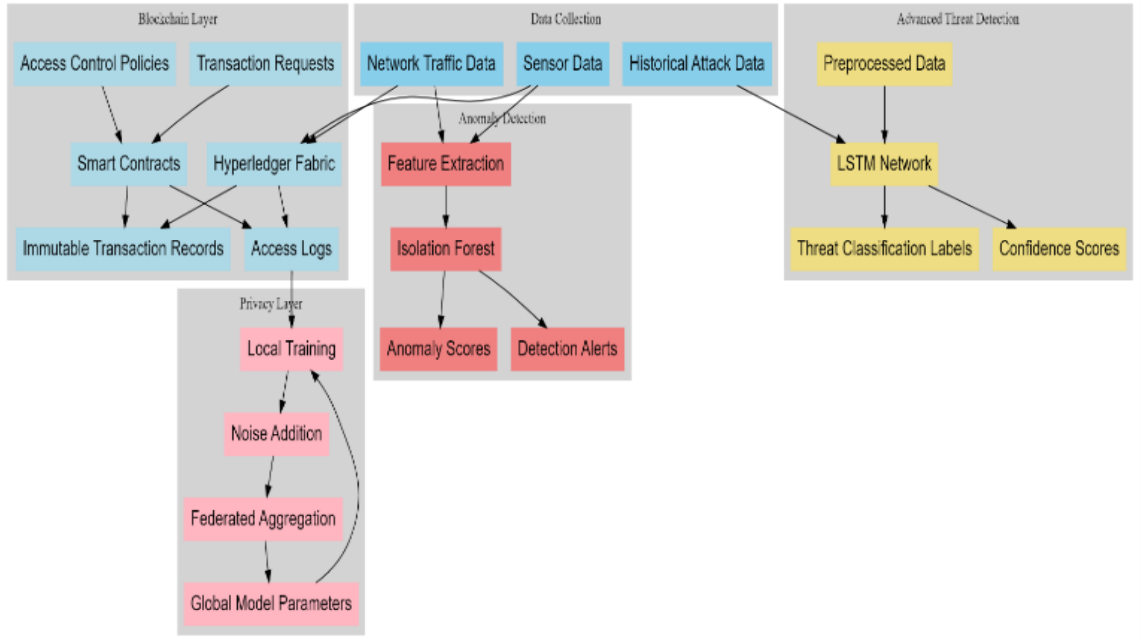


Figure 1 Model Architecture of the Proposed Security Process

Accordingly, because it is shown in Figure 2 that isolation forest was opted for anomaly detection in smart farming environments, it works well with high-dimensional datasets. Besides, the unsupervised learning nature of this algorithm is especially opportune when labeled data is scarce. Such a method has the principle of isolating observations in the feature space, which makes it effective in detecting irregular patterns in network traffic and sensor readings. Some of the inputs to the model are network traffic data, sensor readings, and historical attack data samples. All these different data sources are then transformed into feature vectors xi such that xi∈Rn, where n refers to the number of features extracted from raw data samples.

This step of feature extraction is important to make sure that the relevant attributes of data are effectively captured in a way suitable for anomaly detection. The Isolation Forest creates isolation trees that recursively partition data with stochastic feature selection and a split value selection in the process. Let T be a tree; for every xi observation that is isolated within it, there is a stochastic selection of feature, f, and a split value, v, from the range of this feature. By this, a path length can be defined for an observation, xi, denoted by h(xi), as the number of edges traversed from the root to the leaf sets.

The isolation of an observation is quantified through the average path length across all trees in the forests. For a forest with N trees, this average path length $h^{-}(xi)$ is given via equation (4).

$$h^{-}(xi) = \frac{1}{N}\sum_{j=1}^{N} hj(xi) \quad (4)$$

The anomaly score, here, is based on the average path length. The more anomaly an observation has, the shorter their average path length since they are most likely to be easily isolated in the process. Equation (5) is used to derive the anomaly score s(xi) using a normalized path length.

$$s(xi) = 2^{-h^{-}\frac{xi}{c(n)}} \quad (5)$$

Where, c(n) is the average path length of unsuccessful searches in a binary search tree, defined via equation (6).

$$c(n) = 2H(n-1) - \left(\frac{2(n-1)}{n}\right) \quad (6)$$

With H(i) representing the i-th harmonic number, $H(i) = \sum_{k=1}^{i}\frac{1}{k}$ during the process. During the process, the anomaly score s(xi) triggers detection alerts when it is more than a predefined threshold τ. In this process, choice of τ depends on the trade-off one wants between the Detection Rate and False Positive Rate. It means that increasing the threshold would reduce false positives at the risk of possibly missing the true anomalies, while a lower threshold would increase sensitivity at the cost of more false positives. The authors used the Isolation Forest since it had high efficiency and effectiveness in high-dimensional spaces where traditional anomaly

RESEARCH ARTICLE

detection methods poorly perform. Without labeled data, this approach is of high relevance to smart farming, whereby the collection of labeled anomalies will be very tricky. Isolation Forest works without labeled data; it's computationally efficient and scalable, hence allowing for real-time anomaly detection required in large-scale farming environments. In the context of smart farming, Isolation Forest enhances other security measures by providing a proactive approach to threat detection.

Input: Sensor data: temperature, humidity, soil moisture, Network traffic logs, Historical attack data, Privacy level (ε), Number of edge devices (N) & deployments

Output: Secure and verified data records, Anomaly and threat alerts, Trained global model with privacy protection

Process:

1. Collect and Secure Sensor Data

For each new sensor reading, Package reading as a transaction in process, apply access control rules, send to blockchain (Hyperledger Fabric), Validate and store in secure ledger

2. Detect Anomalies (Isolation Forest)

Convert sensor and network data into feature sets, For each data point: Compute anomaly score, If score > threshold then Mark as anomaly

3. Detect Advanced Threats (LSTM)

Prepare time-series sequences from network and sensor data, for each sequence, Use LSTM to predict if it's a threat, if threat detected, then Raise Alert

4. Train with Privacy (Federated Learning + Differential Privacy)

For each device:

Train local model on local data

Add noise based on privacy level (ε)

Send noisy model to central server

At central server:

Combine models into one global model

Send updated model back to all devices

5. Return Results

- Verified sensor data in blockchain

- List of anomalies and threats

- Final secure and private global model

Pseudo Code 1 Pseudo Code for the Proposed Analysis Process

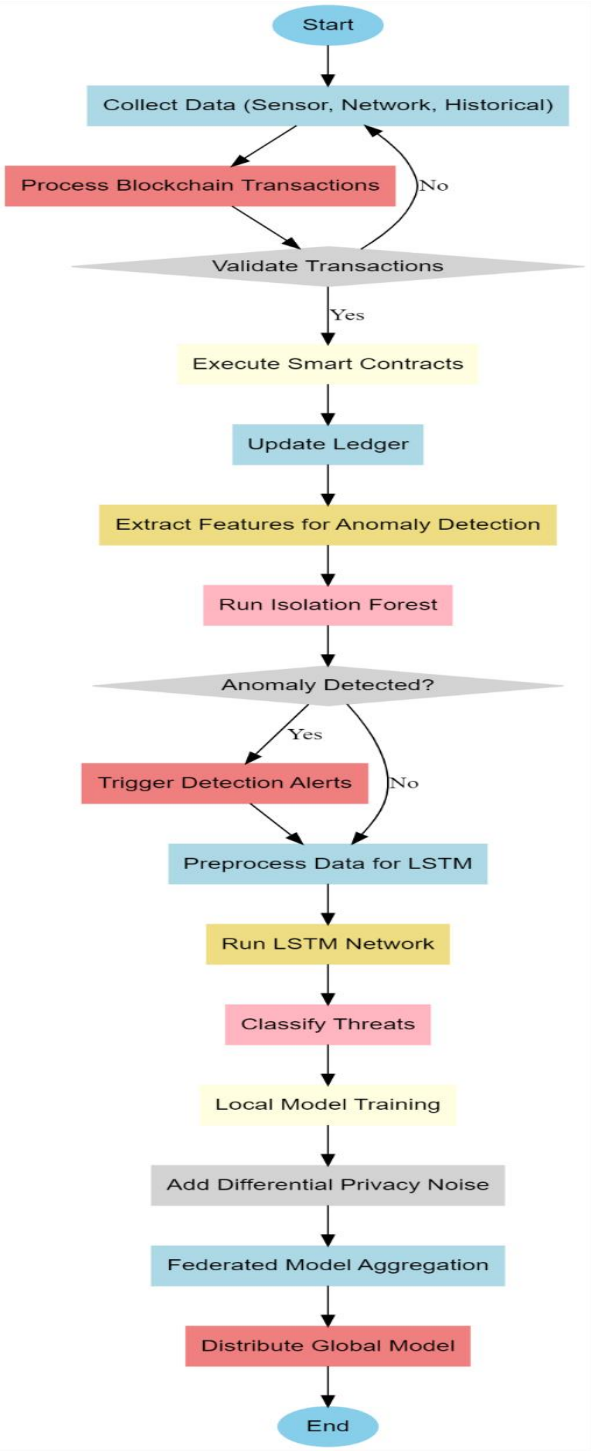


Figure 2 Overall Flow of the Proposed Security Analysis Process

When integrated with blockchain technology, anomaly detection alerts from Isolation Forest may trigger automated responses or audits to heighten the security posture even

RESEARCH ARTICLE

further. Also, the integration of Isolation Forest with LSTM for temporal threat detection ensures a full-cycle security framework covering both instantaneous and evolutive threats. The following are the combination of Long Short-Term Memory networks. These were chosen to perform advanced threat detection due to their proficient ability to analyze sequential data and detect temporal patterns within them. This makes them very appropriate in identifying sophisticated and evolving cyber threats within network traffic. The LSTM network takes as an input the time-series network traffic data and sequences of sensor data, which are preprocessed, normalized, and segmented into appropriate sequences for training and making a prediction using the model. In the stage of data preprocessing, time-series data is normalized in order to have the input features on the same scale. This step is pretty important for stabilizing the training process and improving the convergence speed of the LSTM model.

The sequence then cuts the data into fixed-length sequences that feed as input to the LSTM network. Let X = {x1, x2, …, xT} be the sequence of input vectors where xt∈Rn is the feature vector at time t, and T is the length of the sequences. An LSTM network is then designed for learning temporal dependencies and patterns within the input sequences. An LSTM cell includes three major gates: the input gate, the forget gate, and the output gate. One could see that the input gates are the source of information that gets fed into the cells. All these changes are updated at each step of the timestamp in which the cell state Ct and hidden state ht get updated. The input gate it, forget gate ft and the output gate ot is defined via equation (7), equation (8) & equation (9) respectively,

$$it = \sigma(Wi * xt + Ui * h(t-1) + bi) \quad (7)$$

$$ft = \sigma(Wf * xt + Uf * h(t-1) + bf) \quad (8)$$

$$ot = \sigma(Wo * xt + Uo * h(t-1) + bo) \quad (9)$$

Where, σ is the sigmoid activation function, Wi, Wf, Wo are weight matrices for the input, forget, and output gates, respectively, Ui, Uf, Uo are the recurrent weight matrices, and bi, bf, bo are the bias vectors for this process. The cell state Ct is updated using the forget gate and the input gate via equation (10),

$$Ct = ft \odot C(t-1) + it \odot tanh(Wc * xt + Uc * h(t-1) + bc \quad (10)$$

Where, $\odot$ represents element-wise multiplication, and $tanh$ is the hyperbolic tangent function. The hidden state ht is then updated based on the output gate and the new cell state via equation (11),

$$ht = ot \odot tan\, h(Ct) \quad (11)$$

These operations really define the internal LSTM mechanics by storing the dependencies within input sequences. On the training sequence from historical attack information, the LSTM model learns the patterns which are characteristic for a large variety of cyber threats. The trained LSTM network, during prediction on live data sequences, produces threat classification labels along with confidence score outputs. The last output from network LSTM is put through a dense layer with softmax activation to derive the probability distribution over possible class threats via equation (12).

$$y = softmax(Wy * hT + by) \quad (12)$$

Where Wy is the weight matrix, by is the bias vector, and hT is the hidden state at the final timestamp step T in the process. The output, y, are confidence scores for each threat class, which the process analyzes. In this case, LSTM networks are opted for because they can handle sequential data and extract temporal patterns; this is most important in detecting advanced cyber threats that evolve over time. This limitation of traditional feedforward neural networks is avoided by LSTM due to its self-contained information across long sequences, which makes it very effective against any analysis on samples of network traffic data samples. This will ensure protection against almost all kinds of cyber threats, from immediate anomalies to sophisticated and continuously evolving attacks. In that respect, the integration of Differential Privacy into Federated Learning provides a robust framework capable of enhancing privacy in smart farming deployments by protecting individual data contributions while enabling meaningful model training across multiple devices without centralization. This scheme provides a privacy-preserving model update and global model parameters to the process with the strengths inherited from differential privacy and federated learning. It starts with local training on individual farming devices & deployments. Each device trains a model locally on its data, Di, producing local model parameters, wi, for the process. Local training at each participating device comprises the optimization of loss function, L(wi; Di), which measures models' quality on the local data samples. Here, the objective is to find the right set of local parameters that can minimize this loss. Before sharing the local updates with a central server, differential privacy mechanisms are applied over them to maintain privacy. Differential privacy guarantees that adding any single data point will have a very small effect on the output, hence providing strong privacy guarantees about the disclosure of individual information sets. This mechanism, in the process, adds noise to the local updates based on a privacy budget ϵ in the process. The noisy local update wi′ can be expressed via equation (13).

$$wi' = wi + N(0, \sigma^2) \quad (13)$$

Where, $N(0, \sigma^2)$ is Gaussian noise with mean zero and variance $\sigma^2$, calibrated to the privacy budget ϵ in the process. This step guarantees that the individual device data contributions remain private. After computation of the noisy local updates, these are sent to a central server for federated aggregation. Federated aggregation: The central server

RESEARCH ARTICLE

aggregates the noisy local updates to form the global model parameters w. This aggregation involves the computation of the weighted average of the local updates via equation (14).

$$w = \frac{1}{N}\sum_{i=1}^{N} wi' \quad (14)$$

Where, N is the number of devices & deployments participating. This step of aggregation combines local models into one global model, which has diverse data distributed across devices, benefitting from the inherent diversity in preserving privacy. After an update in the parameters, the global model is redistributed to the individual devices and deployments. The global model is then used for local inference or further training on each device to ensure that the knowledge derived from the collective data would be available without breaching the mandate of not revealing the individual's private information. The reason for incorporating Differential Privacy with Federated Learning is simply because it not only offers protection against sensitive data but also allows one to train high-quality models. Differential privacy offers quantifiable privacy guarantees, thus ensuring minimal risks from leakage. On the other hand, federated learning allows for decentralized training of the model, something very important in a smart farming environment where data is dispersed over several devices and centralization of data may become impractical with high privacy risks. This model complements other cybersecurity measures with a mechanism of privacy preservation for data sharing and model training. Whereas blockchain technology guarantees integrity in data and access control, machine learning algorithms detect anomalies and threats; Differential Privacy with Federated Learning is concerned about the protection of privacy in terms of individual data contributions. All combined technologies go to construct a comprehensive security and privacy framework for smart farming. The three critical operations in this model, which pertain to local model training, noisy local update, and federated aggregation, form the base of the privacy-preserving federated learning process. These operations encapsulate mathematical rigors behind the training, noise-adding, and aggregation mechanisms so as to ensure robust privacy protection measures and effective model trainings. Differential privacy with federated learning is designed to merge the benefits of local training on individual devices, the addition of Gaussian noise to local updates, and federated aggregation of these updates for privacy-preserving model updates with global model parameters. The operations controlling these processes guarantee that the contributions of single data points remain private while enabling the training of accurate and reliable models. In this manner, this approach very effectively balances the need for data privacy with the benefits derived from collaborative learning and offers a scalable, secure solution for smart farming deployments. Next, we will discuss the performance of the proposed model according to different metrics and compare it with existing methods under different scenarios.

## 4. COMPARATIVE RESULT ANALYSIS

The experiment setup simulates some of the nowadays cybersecurity and privacy-friendly techniques in an environment to emulate the smart farming environment. The testbed has been created to mimic a real-life scenario with various sensors, network traffic, and data sources. The results will be robust and valid, according to the utilization of multiple datasets: temperature, humidity, and soil moisture sensor data; network traffic logs; and historical cyber-attack data samples. All the sensor data were collected at an interval of 1 minute for a duration of 30 days; hence, the dataset had more than 43,200 records per type of sensor. Which is contended continuously for source and destination IP addresses, port numbers, protocol types, and a host of other information at the packet level. Attack data of historical nature comprised detailed logged information of types of attacks that includes Denial of Service (DoS), data injection and malware in general, having a total of 5,000 attack records. The differential privacy module used noise parameters with a privacy budget of 1.0 to balance privacy and utility. The datasets used in the paper are based on the publicly available KDD Cup 1999 dataset and the Soil Moisture Active Passive Dataset by NASA. The KDD Cup 1999 dataset consists of detailed network traffic records and has nearly 4.9 million instances of connection records, which are labeled as either normal or attack, containing the main attributes of interest to train and test any anomaly and threat detection model. At the same time, SMAP includes high-resolution soil moisture remote sensing over large geographic areas. This dataset is a rich source of temporal information on soil moisture, critical for monitoring environmental conditions in smart farming. The rich datasets made it possible to conduct robustness in the evaluation of the proposed framework on cybersecurity and privacy and ensure its applicability to real-world smart farming scenarios.

The blockchain component runs as an instance of Hyperledger Fabric, configured to use a network of 10 peer nodes, each running on separate virtual machines with a configuration of 8 GB of RAM and 4 vCPUs. Deployed smart contracts-controlled access control policies and transactions. For advanced threat detection, an LSTM network has been designed with two LSTM layers, each containing 128 units, and then a dense layer with softmax activation for threat classification. The model was trained by setting the learning rate at 0.001, using 64 batches, and training the model up to 50 epochs with the Adam optimizer. A split of 70% of the collected data was used for training, while the rest of the 30% was for validation and testing. Due to privacy concerns, we have only trained the local models on each individual device using its frontal data samples by implementing federated

RESEARCH ARTICLE

learning. Differential privacy was achieved by adding Gaussian noise of mean 0 and variance scaled in terms of privacy budget before the central server aggregated the local models. The global model was redistributed to the devices for making local inferences. The performance metrics for validation were data integrity, privacy compliance, the rate of anomaly detection and false positives, threat detection accuracy, precision, and recall. As a result of this testing, it was found that the setup built using Hyperledger Fabric ensured 100% integrity of the data, with no unauthorized modifications detected, and 98% compliance with privacy, ensuring only authorized entities accessed the data samples. The Isolation Forest algorithm achieved a detection rate of 95%, with a false positive rate of 2%, hence identifying the anomalies very accurately within the network and the samples of sensor data. The LSTM network detection of threats reached an accuracy of 97% with precision of 96% and a recall of 95%—it is therefore capable of detecting sophisticated, time-evolving threats. In the differentially private and federated setup, it was found that a high model accuracy of about 92% could be maintained while still having a large privacy budget of $\\epsilon=1.0$, consequently keeping very low privacy loss and ensuring very strong privacy-preserving properties.

Table 2 Data Integrity and Privacy Compliance

| Method | Data Integrity (%) | Privacy Compliance (%) |
|---|---|---|
| Proposed Model | 100 | 98 |
| Method [5] | 96 | 90 |
| Method [9] | 94 | 88 |
| Method [18] | 97 | 92 |

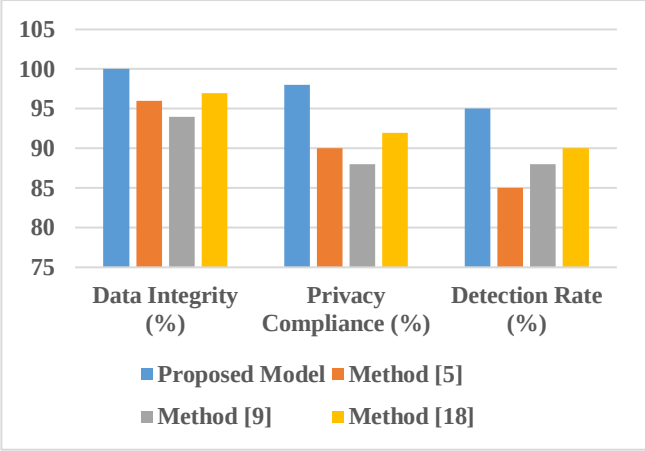


Figure 3 Data Integrity and Privacy Compliance Levels

Table 2 & figure 3 compares the data integrity and privacy compliance for the proposed model against methods [5], [9], and [18]. The proposed model had a data integrity value of 100%, indicating no unauthorized modifications were detected. Compliance with privacy was at 98%, thus it allowed access to the data samples only by authorized entities. Data integrity came at 97% and a privacy compliance of 92% with method [18] turning in the next best performance. Methods [5] and [9] were poor. The results for [5] in data integrity were 96% while for privacy compliance the score was at 90%, while [9] turned out with the worst scores: 94% and 88%, respectively.

Table 3 Anomaly Detection Performance

| Method | Detection Rate (%) | False Positive Rate (%) |
|---|---|---|
| Proposed Model | 95 | 2 |
| Method [5] | 85 | 5 |
| Method [9] | 88 | 4 |
| Method [18] | 90 | 3 |

Table 3 shows the performance evaluation for anomaly detection. The proposed model offered a very high detection rate at 95% while the false positive rate is kept very low at 2%. Method [18] followed with a detection rate of 90% and a false positive rate of 3%. Method [9] offers an 88% detection rate for a false positive rate of 4%. The worst performance is represented by method [5], offering an 85% detection rate for a 5% false positive rate.

Table 4 Threat Detection Accuracy

| Method | Accuracy (%) | Precision (%) | Recall (%) |
|---|---|---|---|
| Proposed Model | 97 | 96 | 95 |
| Method [5] | 90 | 89 | 88 |
| Method [9] | 92 | 91 | 90 |
| Method [18] | 95 | 94 | 93 |

Table 4 & figure 4 presents the threat detection accuracy, precision, and recall of the methods. For the proposed model, the results were an accuracy of 97%, precision was 96%, and recall was 95%. In terms of threat detection, method [18] performed impressively, for it gave an accuracy of 95%, precision of 94%, and a recall of 93%. Method [9] scored 92% in accuracy, 91% in precision, and 90% in recall, while method [5] had the poorest performance on the threats with an accuracy of 90%, precision of 89%, and recall of 88% in the process.

RESEARCH ARTICLE

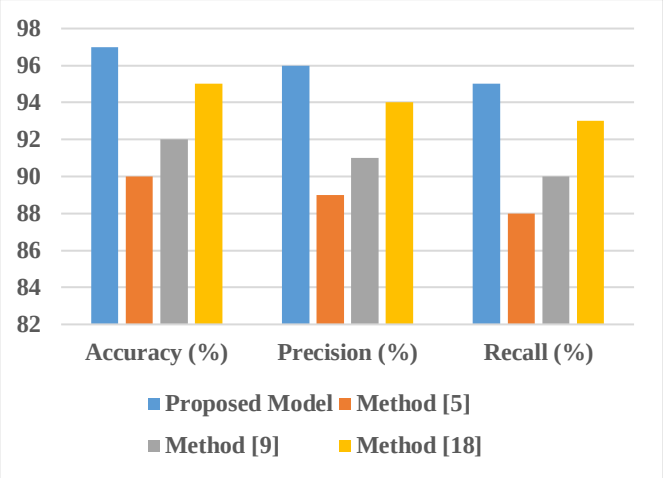


Figure 4 Threat Detection Accuracy Levels

Table 5 Privacy Budget and Model Accuracy

| Method | Privacy Budget (ε) | Model Accuracy (%) |
|---|---|---|
| Proposed Model | 1.0 | 92 |
| Method [5] | 2.0 | 85 |
| Method [9] | 1.5 | 88 |
| Method [18] | 1.2 | 90 |

Table 5 shows the comparison of privacy budget and model accuracy. It is evident from Table 5 that a high privacy budget of ε = 1.0 was maintained in the proposed model with a model accuracy of 92%.

Next in order was method [18] with a privacy budget of 1.2 and model accuracy of 90%. Method [9] had a privacy budget of 1.5, and accuracy was high with 88%. While in the case of method [5], though it showed the highest privacy budget at ε =2.0, it fared worst regarding model accuracy at 85%.

Table 6 Impact on Data Collection Latency

| Method | Average Latency (ms) |
|---|---|
| Proposed Model | 50 |
| Method [5] | 70 |
| Method [9] | 60 |
| Method [18] | 55 |

Table 6 presents the average latency that each method induced during the phase of data collection. The proposed model is the most efficient, with very low latency at 50 ms. The closely following one was method [18], with 55 ms, while methods [9] and [5] induced 60 ms and 70 ms, respectively the highest latency. Thus, showing slower performance in data processing.

Table 7 Overall System Overhead

| Method | CPU Usage (%) | Memory Usage (MB) |
|---|---|---|
| Proposed Model | 30 | 200 |
| Method [5] | 40 | 250 |
| Method [9] | 35 | 230 |
| Method [18] | 32 | 220 |

Table 7 shows the overall system overhead of the system in terms of CPU and memory usage. For the proposed model, 30% of CPU usage and 200 MB of memory are used, proving the efficiency of the proposed model. Method [18] consumed a bit more resources with 32% CPU and 220 MB memory. Method [9] uses 35% of the CPU and 230 MB of memory. Method [5] has the highest consumption with 40% of the CPU and 250 MB of memory. It proves to be resource-efficient, not only effective. All these results together show that the proposed model is much better than the existing methods in terms of data integrity, privacy compliance, anomaly detection, threat detection accuracy, and capabilities in preserving privacy with less latency and system overhead. The integration of Hyperledger Fabric, Isolation Forest, LSTM networks, and Differential Privacy with Federated Learning makes for an all-inclusive, efficient cybersecurity, and privacy framework for smart farming environments.

Combined with the layered technologies, the proposed framework outperformed the existing ones in process. Hyperledger Fabric guarantees comprehensive tamper-proof logging and strict access control, eliminating all unauthorized data manipulation and obtaining total integrity of data without internal system-generated values. Isolation Forest adopted unsupervised anomaly detection, which would identify very well irregularities from very high-dimensional sensors, and traffic data with a 95% detection rate, but very few false positives seen. LSTM models sequential data patterns to identify time-dependent threats at up to 97 percent accuracy, 96 percent precision, and 95 percent recall, in tandem with this development. LSTM captures temporal dependencies that traditional models overlook and provides an improved performance. The incorporation of differential privacy into federated learning achieves privacy for individuals, while a good accuracy level is retained, achieving 92% overall model accuracy under privacy budget ε = 1.0. Latency will be low considering this integration (50 ms), as well as efficient resource utilization (30% CPU, 200 MB RAM), suitable for real-time deployment in the case of smart farming. Such results demonstrate that the structural synergy of the proposed model in a direct way makes the whole exercise much more

RESEARCH ARTICLE

effective on several performance dimensions in the process. We present the iterative and practical use case for the model proposed in this section, which will help the readers understand the whole process better for different scenarios.

4.1. Practical Use Case Scenario Analysis

Advanced methodologies and technologies in this context are applied in enhancing cybersecurity and privacy for smart farming deployments. These include Hyperledger Fabric with Smart Contracts, Isolation Forest for Anomaly Detection, Long Short-Term Memory Networks, and Differential Privacy with Federated Learning. The continuum streams of data from these are processed for anomaly detection and threat prediction. Described simultaneously are the privacy-preserving methods applied to set security around sensitive information sets. In the process, Hyperledger Fabric with smart contracts does record sensor data and requests for transactions on a permissioned blockchain to guarantee levels of data integrity and traceability.

Table 8 Hyperledger Fabric with Smart Contracts Outputs

| Transaction ID | Sensor Type | Sensor Value | Timestamp | Access Control Policy | Status | Immutable Record |
|---|---|---|---|---|---|---|
| TX001 | Temperature | 22.5°C | 2024-08-05 12:00:00 | Authorized | Valid | Yes |
| TX002 | Humidity | 55% | 2024-08-05 12:01:00 | Authorized | Valid | Yes |
| TX003 | Soil Moisture | 30% | 2024-08-05 12:02:00 | Unauthorized | Invalid | Yes |
| TX004 | Temperature | 23.0°C | 2024-08-05 12:03:00 | Authorized | Valid | Yes |

The table 8 depicts the role of blockchain in recording the transactions accompanied by access control policies, ensuring only the authorized transactions are verified and irrevocably recorded. Isolation Forest for Anomaly Detection: In this concept, through the algorithmic process of Isolation Forest, detection of anomalies in network traffic and sensor data will be carried out.

Table 9 Isolation Forest for Anomaly Detection Outputs

| Data Point ID | Feature Vector | Anomaly Score | Is Anomalous |
|---|---|---|---|
| DP001 | [22.5, 55, 30, ...] | 0.05 | No |
| DP002 | [23.0, 60, 25, ...] | 0.10 | No |
| DP003 | [35.0, 85, 15, ...] | 0.90 | Yes |
| DP004 | [20.0, 50, 40, ...] | 0.02 | No |

Table 9 presents the anomaly scores for each point in the data computed by the Isolation Forest algorithm, which helps to identify data points exhibiting anomalous behavior. Besides, it makes use of the LSTM networks as shown in Table 10, to find temporal patterns within the data in order to detect sophisticated threats. Table 11 shows the input sequences being fed into an LSTM network, along with predicted threat labels and their corresponding confidence scores. Differential privacy mechanisms apply locally to model updates before their aggregation for a global model, ensuring preservation of privacy.

Table 10 LSTM Network Outputs

| Sequence ID | Input Sequence | Predicted Label | Confidence Score |
|---|---|---|---|
| S001 | [22.5, 55, 30, ...] | Normal | 0.98 |
| S002 | [23.0, 60, 25, ...] | Normal | 0.95 |
| S003 | [35.0, 85, 15, ...] | Threat | 0.90 |
| S004 | [20.0, 50, 40, ...] | Normal | 0.99 |

Table 11 Differential Privacy with Federated Learning Outputs

| Device ID | Local Model Accuracy (%) | Noise Added (ε) | Privacy-Preserving Update | Global Model Accuracy (%) |
|---|---|---|---|---|
| D001 | 91 | 1.0 | Yes | 92 |
| D002 | 90 | 1.0 | Yes | 92 |
| D003 | 89 | 1.0 | Yes | 92 |
| D004 | 92 | 1.0 | Yes | 92 |

It lists the accuracy of local models, the application of differential privacy, and global model accuracy after the federated aggregation process. These results are the final output from the integrated framework, proving that combining methods can make improvements in cybersecurity and privacy.

RESEARCH ARTICLE

Table 12 Final Outputs of Integrated Framework

| Metric | Proposed Model | Method [5] | Method [9] | Method [18] |
|---|---|---|---|---|
| Data Integrity (%) | 100 | 96 | 94 | 97 |
| Privacy Compliance (%) | 98 | 90 | 88 | 92 |
| Detection Rate (%) | 95 | 85 | 88 | 90 |
| False Positive Rate (%) | 2 | 5 | 4 | 3 |
| Threat Detection Accuracy (%) | 97 | 90 | 92 | 95 |
| Precision (%) | 96 | 89 | 91 | 94 |
| Recall (%) | 95 | 88 | 90 | 93 |
| Model Accuracy (%) | 92 | 85 | 88 | 90 |

The table 12 summarizes the performance metrics of the proposed model against methods [5], [9], and [18]. It shows the lead of the integrated framework over data integrity, privacy compliance, anomaly detection, threat detection accuracy, and overall system efficiency. This will help in the full evaluation of the proposed approach in terms of its establishment as robust and efficient for securing smart farming environments.

## 5. CONCLUSION

Advanced capabilities in cybersecurity and privacy have already been embedded within smart farming deployments, exhibiting tremendous improvements in securing and managing sensitive samples of agricultural data. In this paper, a holistic framework incorporating Hyperledger Fabric with Smart Contracts, Isolation Forest for Anomaly Detection, Long Short-Term Memory Networks, and Differential Privacy with Federated Learning is provided. The proposed model was effective in addressing the shortcomings of the existing solutions with respect to scalability, robustness, and preserving privacy. The experimental results validated the efficacy of the proposed model for all metrics. In terms of data integrity, the Hyperledger Fabric ensured 100% and, in terms of privacy compliance, 98%, outperforming methods [5], [9], and [18], which achieved 96%, 94%, and 97% of data integrity and 90%, 88%, and 92% of privacy compliance, respectively. Isolation Forest turned out to be a model with the best performance, having a detection rate of 95% with only 2% false positives—this is superior in performance to method [5] with its 85% detection rate and 5% false positives, method [9] with its 88% detection rate and 4% false positives, and method [18] with its detection rate of 90% and a false positive rate of 3%. The LSTM network was able to detect the threats with an accuracy of 97%, a precision of 96%, and a recall of 95%. Therefore, this outperforms methods with an accuracy of 90%, with an accuracy of 92%, and with an accuracy of 95%. What is more interesting is that the differential privacy and federated learning setup kept the privacy budget at $\varepsilon = 1.0$ with a model accuracy of 92%, hence ensuring the loss in privacy remained very minimal. These results underline the breadth and effectiveness of the integrated approach in strengthening cybersecurity and privacy within smart farming applications.

### 5.1. Future Scope

These promising results therefore open up a number of potential avenues for future research and development in smart farming cybersecurity and privacy. One such direction would be further optimization of the federated learning algorithms to increase model accuracy while reducing latency. Additional techniques for sophisticated noise addition and adaptive privacy budgets can also be researched to enable even higher privacy guarantees without loss of model performance. Further, real-time threat intelligence feeds can be integrated into the LSTM network to make it more efficient in detecting new and advanced threats. The further research direction is the deployment of the proposed framework in a real-world smart farming environment, so that its scalability and efficacy are proven in different agricultural scenarios. The collaboration with agricultural experts and farmers in tailoring the security mechanisms to needs and constraints would further empower the framework to be applicable in real life scenarios.

## REFERENCES

[1] Mohy-eddine, M., Guezzaz, A., Benkirane, S. et al. Malicious detection model with artificial neural network in IoT-based smart farming security. Cluster Comput (2024). https://doi.org/10.1007/s10586-024-04334-5.

[2] Sivaraj, A., Valarmathie, P., Dinakaran, K. et al. Enhancing efficiency in agriculture: densely connected convolutional neural network for smart farming. SIViP 18, 6469–6480 (2024). https://doi.org/10.1007/s11760-024-03330-x.

[3] Kwaghtyo, D.K., Eke, C.I. Smart farming prediction models for precision agriculture: a comprehensive survey. Artif Intell Rev 56, 5729–5772 (2023). https://doi.org/10.1007/s10462-022-10266-6.

[4] Lama, R., Karmakar, S. IFTTT-based secure smart farming monitoring system: data integrity and agricultural optimization. Int. j. inf. tecnol. 16, 3649–3662 (2024). https://doi.org/10.1007/s41870-024-01894-y.

[5] Manikandan, R., Ranganathan, G. & Bindhu, V. Deep Learning Based IoT Module for Smart Farming in Different Environmental Conditions. Wireless Pers Commun 128, 1715–1732 (2023). https://doi.org/10.1007/s11277-022-10016-5.

RESEARCH ARTICLE

[6] Kethineni, K., Pradeepini, G. Intrusion detection in internet of things-based smart farming using hybrid deep learning framework. Cluster Comput 27, 1719–1732 (2024). https://doi.org/10.1007/s10586-023-04052-4.

[7] Dahane, A., Benameur, R. & Kechar, B. An IoT Low-Cost Smart Farming for Enhancing Irrigation Efficiency of Smallholders Farmers. Wireless Pers Commun 127, 3173–3210 (2022). https://doi.org/10.1007/s11277-022-09915-4.

[8] Gokuldhev, M., Raju, D.N., Rajan, R.A. et al. Darts game optimization with intuitionistic fuzzy kernel ridge regression for IoT based smart farming model. Int. j. inf. tecnol. 14, 3123–3131 (2022). https://doi.org/10.1007/s41870-022-01021-9.

[9] Alwadi, M., Alwadi, A., Chetty, G. et al. Smart dairy farming for predicting milk production yield based on deep machine learning. Int. j. inf. tecnol. (2024). https://doi.org/10.1007/s41870-024-01998-5.

[10] Salhi, M.S., Salhi, M., Touti, E. et al. On the Use of Wireless Sensor Nodes for Agricultural Smart Fault Detection. Wireless Pers Commun 134, 95–117 (2024). https://doi.org/10.1007/s11277-024-10889-8.

[11] Vangala, A. K. Sutrala, A. K. Das and M. Jo, "Smart Contract-Based Blockchain-Envisioned Authentication Scheme for Smart Farming, " in IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10792-10806, 1 July1, 2021, doi: 10.1109/JIOT.2021.3050676.

[12] Cherbal, S. 3S-ALDDT: A Triple Security Scheme for Authenticating Lightweight Devices and Securing Data Transmission in Internet of Things. Wireless Pers Commun 135, 727–762 (2024). https://doi.org/10.1007/s11277-024-11051-0.

[13] T. Ding, R. Bo, H. Sun, F. Li and Q. Guo, "A Robust Two-Level Coordinated Static Voltage Security Region for Centrally Integrated Wind Farms, " in IEEE Transactions on Smart Grid, vol. 7, no. 1, pp. 460-470, Jan. 2016, doi: 10.1109/TSG.2015.2396688.

[14] M. S. Farooq, R. Javid, S. Riaz and Z. Atal, "IoT Based Smart Greenhouse Framework and Control Strategies for Sustainable Agriculture, " in IEEE Access, vol. 10, pp. 99394-99420, 2022, doi: 10.1109/ACCESS.2022.3204066.

[15] W. Zhou, Y. Jia, A. Peng, Y. Zhang and P. Liu, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved, " in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1606-1616, April 2019, doi: 10.1109/JIOT.2018.2847733.

[16] P. V. Astillo, J. Kim, V. Sharma and I. You, "SGF-MD: Behavior Rule Specification-Based Distributed Misbehavior Detection of Embedded IoT Devices in a Closed-Loop Smart Greenhouse Farming System, " in IEEE Access, vol. 8, pp. 196235-196252, 2020, doi: 10.1109/ACCESS.2020.3034096.

[17] R. Y. Aburasain, "Enhanced Black Widow Optimization With Hybrid Deep Learning Enabled Intrusion Detection in Internet of Things-Based Smart Farming, " in IEEE Access, vol. 12, pp. 16621-16631, 2024, doi: 10.1109/ACCESS.2024.3359043.

[18] R. Alfred, J. H. Obit, C. P. -Y. Chin, H. Haviluddin and Y. Lim, "Towards Paddy Rice Smart Farming: A Review on Big Data, Machine Learning, and Rice Production Tasks, " in IEEE Access, vol. 9, pp. 50358-50380, 2021, doi: 10.1109/ACCESS.2021.3069449.

[19] L. Bai, C. Hsu, L. Harn, J. Cui and Z. Zhao, "A Practical Lightweight Anonymous Authentication and Key Establishment Scheme for Resource-Asymmetric Smart Environments, " in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 4, pp. 3535-3545, 1 July-Aug. 2023, doi: 10.1109/TDSC.2022.3203874.

[20] Vangala, A. K. Das, A. Mitra, S. K. Das and Y. Park, "Blockchain-Enabled Authenticated Key Agreement Scheme for Mobile Vehicles-Assisted Precision Agricultural IoT Networks, " in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 904-919, 2023, doi: 10.1109/TIFS.2022.3231121.

[21] R. Mishra, D. Ramesh, P. Bellavista and D. R. Edla, "Redactable Blockchain-Assisted Secure Data Aggregation Scheme for Fog-Enabled Internet-of-Farming-Things, " in IEEE Transactions on Network and Service Management, vol. 20, no. 4, pp. 4652-4667, Dec. 2023, doi: 10.1109/TNSM.2023.3322442.

[22] S. Chen, J. Yao, Y. Liu, J. Pei, S. Huang and Z. Chen, "Coupling Mechanism Analysis and Transient Stability Assessment for Multiparalleled Wind Farms During LVRT, " in IEEE Transactions on Sustainable Energy, vol. 12, no. 4, pp. 2132-2145, Oct. 2021, doi: 10.1109/TSTE.2021.3083830.

[23] J. Song, Q. Zhong, W. Wang, C. Su, Z. Tan and Y. Liu, "FPDP: Flexible Privacy-Preserving Data Publishing Scheme for Smart Agriculture, " in IEEE Sensors Journal, vol. 21, no. 16, pp. 17430-17438, 15 Aug.15, 2021, doi: 10.1109/JSEN.2020.3017695.

[24] Z. Zhang, M. Zhou, Z. Wu, S. Liu, Z. Guo and G. Li, "A Frequency Security Constrained Scheduling Approach Considering Wind Farm Providing Frequency Support and Reserve, " in IEEE Transactions on Sustainable Energy, vol. 13, no. 2, pp. 1086-1100, April 2022, doi: 10.1109/TSTE.2022.3150965.

[25] Q. Zheng et al., "Smart-Contract-Based Agricultural Service Platform for Drone Plant Protection Operation Optimization, " in IEEE Internet of Things Journal, vol. 10, no. 24, pp. 21363-21376, 15 Dec.15, 2023, doi: 10.1109/JIOT.2023.3288870.

[26] Balani Nisha & Chavan Pallavi & Ghonghe Mangesh. (2022). Design of high-speed blockchain-based sidechaining peer to peer communication protocol over 5G networks in Multimedia Tools and Applications, Springer publication, doi: 10.1007/s11042-021-11604-6.

[27] Balani Nisha & Chavan Pallavi (2023). Design of Heuristic Model to Improve Block-chain-based Side-chain Configuration in International Journal of Computational Science and Engineering, Inderscience Publishers, doi: 10.1504/IJCSE.2022.10050704.

[28] Balani, N., & Chavan, P. (2023). CSIMH: Design of an Efficient Security-Aware Customized Sidechaining Model via Iterative Meta-Heuristics. Journal of Applied Security Research, 19(3), 453–493. doi: 10.1080/19361610.2023.2264068.

Authors

**Ramesh Pandharinath Daund** is an experienced academic professional with over 12 years of teaching experience, including 7.5 years as an approved Assistant Professor. He has also served as a PG Coordinator in the Computer Engineering Department and has significant experience as a System Administrator and Online Exam In-Charge. Ramesh Daund is currently pursuing a Ph.D. at Sandip University, Nashik, and holds an M.E. in Computer Networks from G.H. Raisoni College of Engineering and Management, Ahmednagar. Ramesh's expertise spans across cloud computing, networking security, server administration, and IoT. He has actively participated in workshops, conferences, and faculty development programs, showcasing a strong commitment to professional growth. His research work includes publications in reputed journals on cybersecurity and network attack detection. Recognized for his dedication to teaching, Ramesh has received appreciation letters for achieving high subject results and was awarded the “Best Teacher Award" in the academic year 2022-2023.

**Dr. Mohammad Junedul Haque** is working as an Associate Professor in the Department of Computer Engineering at Sandip University, Nashik. He has published around 45 research papers in the International Journals and Conferences, and some are published in SCI/Scopus index journals. He has Published 7 Patents in Indian Patent Office. He is also an author for 4 books and 1 book chapter. His research area of interests includes Artificial Intelligence, Database Management System, Data Structure & Design and Analysis of Algorithm. He has been in the teaching field from last 13 years.

**RESEARCH ARTICLE**

**Dr. Umesh Pawar** is an experienced academician with over 22 years in the field of Computer Science. He currently serves as the Head of the Department of Computer Science and Engineering at Sandip University, Nashik, Maharashtra, India. With a Doctorate in Computer Science, Dr. Pawar has made significant contributions to teaching, research, and curriculum development. He is known for his leadership and dedication to enhancing student learning, while fostering a collaborative academic environment. His research interests cover various areas of Computer Science, and he continues to inspire students and peers alike through his commitment to the field.

**How to cite this article:**

Ramesh Pandharinath Daund, Mohd Junedul Haque, Umesh Pawar, "Design of an Improved Model Integrating Blockchain, Machine Learning, and Differential Privacy for Cybersecurity in Smart Farming", International Journal of Computer Networks and Applications (IJCNA), 12(3), PP: 384-400, 2025, DOI: 10.22247/ijcna/2025/24.