Blockchain-Based Smart Farm Security Framework for the Internet of Things

Ahmed Abubakar Aliyu * and Jinshuo Liu

Posted Date: 3 August 2023

doi: 10.20944/preprints202308.0362.v1

Keywords: Blockchain; Poisoning Attacks; Internet of Things; Smart Farming

Article

Blockchain-Based Smart Farm Security Framework for the Internet of Things

Aliyu Ahmed Abubakar [1,2,*] and Jinshuo Liu [1]

[1] School of Cyber Science and Engineering, Wuhan University, Wuhan, China, 430072
[2] Department of computer Science, Faculty of Computing, Kaduna State University, Kaduna 800283, Nigeria
* Correspondence: ahmed.aliyu@kasu.edu.ng

Abstract: Smart farming, as a branch of the Internet of Things (IoT), combines the recognition of agricultural economic competencies, the progress of data and information collected from connected devices with statistical analysis to characterize the essentials of the assimilated information, allowing farmers to make intelligent conclusions that will maximize the harvest benefit. However, the integration of advanced technologies requires the adoption of high-tech security approaches. In this paper, we present a framework that promises to enhance the security and privacy of smart farms by leveraging the decentralized nature of blockchain technology. The framework stores and manages data acquired from IoT devices installed in smart farms using a distributed ledger architecture, which provides secure and tamper-proof data storage and ensures the integrity and validity of the data. The study uses the AWS cloud, ESP32, the smart farm security monitoring framework, and the Ethereum Rinkeby smart contract mechanism, which enables automated execution of pre-defined rules and regulations. As a result of a proof-of-concept implementation, the system can detect and respond to security threats in real time, and the results illustrate its usefulness in improving the security of smart farms.

Keywords: blockchain; poisoning attacks; Internet of Things; smart farming

1. Introduction

Normally, As the population of the world grows, so does our need for agricultural improvement, and farmers work to produce crops that will provide food for people all over the world. The economies of most countries are primarily dependent on the agricultural industry [1]. Many nations have agricultural departments that work to strengthen their country's economy, especially through agriculture. Over the past few decades, it's clear that the growth of IoT has revolutionized the way farming is done and advanced the operational capabilities of the agricultural sector [2, 3]. The integration of the IoT into agricultural growth is known as smart farming, and it is quickly fitting as the new normal as connected devices, smart things and robots exhibited around the globe are expected to be around $15.93 billion in 2028, representing a yearly growth ratio of about 20.31% between 2021 and 2028 [4]. As modern agricultural frameworks are integrated into rural regions, competitors are targeting them for cyberattacks. For example, a ransomware outbreak at the food transportation division of meat management company JBS halted operations at 13 meat industrial sites. To remain operational, the company had to spend approximately $11 million [5]. As a result, we can all agree that security is seen as a key concern in industries such as agriculture, where the advancement of rural security measures is vital.

The cybersecurity structures now advocated in smart farming typically include chain management of food supply and testing of several accomplishments through Machine Learning/Artificial Intelligence-based data analysis techniques, cloud computing technologies as well as verification and authorization arrangements for sophisticated IoT devices [6, 7]. It has also been observed that real IoT devices identified on the Internet were infiltrated And employed as a means to launch full denial-of-service (DoS) assaults and further harmful engagements, such as information

 doi:10.20944/preprints202308.0362.v1

leakage related to management and sensor data [8]. On the other hand, blockchain has emerged and evolved in a fascinating way and is currently being used in decentralized network systems such as IoTs [9]. Researchers have made a separate assessment of the blockchain advancement gaps for IoT security and safety difficulties, and they have advised and urged us to use blockchain-based monitoring for the general security of smart agriculture [10]. Traditionally, in order to extend the limitations of the current system and make progress in terms of security with blockchain-based system needs, we use blockchain arrangements to continuously handle information and store irregularities in blockchain transactions [11, 12]. In this study, AWS cloud, an Arduino gadget package with a Wi-Fi component, and Ethereum smart contract were used as an end-to-end action.

The study is expected to have a promising significance to farmers, the government and also cybersecurity and assurance specialists as it renders various scenarios of data and information attacks that were encountered by smart farm administrators globally. The research also aimed at recognizing possible cybersecurity alarms in smart farming and presenting scenario-specific cyber-attacks. It also intends to provide a comprehensive evaluation of current cybersecurity analyses, as well as presenting a preventive measure through a blockchain technology consensus in an Intelligent farming ecosystem.

2. Literature Review

The system Recently, Light has been shed [13] on security and safety issues in IoT as a whole and smart farming specifically where coating manufacturing and notable conceivable smart farming cyber threats were displayed. Additionally, their research provides certain cyber-attack situations characterized into data, features, and other attacks. A predominant attack called "The Night Mythical Serpent" is a framework that allows network intruders to get huge amounts of data from several petrochemical corporations. The growing number of connected devices has created lots of safety and security challenges within the smart farming ecosystem in the rural areas, as farmers could not endure severe damage to their crops. Maria and partners' [14] report highlight the importance of data security in smart farming where they explained dangers and potential vulnerabilities in the emerging IoT terrain. Their research focused on security, intelligence, and accessibility models for information security in agriculture, as well as unique advances in smart farm systems, such as on-farm equipment verification, inaccessible sensing approaches, and machine learning. Moreover, the risks associated with the use of IoT technology in agriculture have been clearly identified [15].

Recently, an expert from the security firm Sucuri [16] discovered that a DoS botnet may send 50,000 HTTP requests per second, causing DDoS attacks on many domains. Cloud computing integration with Smart Farming is critical for establishing IoT identifying information capacity and analysis, as well as tallying big data demands. Thus, researchers proposed strategies for solving IoT-based Smart Farming problems using cloud computing [17].

2.1. Cloud Solutions in Smart Farming

A lot of experts have explored the use of blockchain technology for IoT advancement owing to the several benefits it provides which includes green computing [18, 19]. Cloud solutions in smart farming refer to the use of cloud computing technology to enhance farming operations and improve crop yields. Cloud solutions enable farmers to accumulate, store, and evaluate data from multiple sources, such as drones, soil sensors and weather sensors, and then use this information to make data-driven choices about pest control, irrigation and fertilization. With cloud solutions, farmers can access real-time data from anywhere and use it to optimize their farming practices and increase productivity. In addition, cloud solutions can help farmers reduce costs and minimize waste by providing accurate predictions of crop yields and enabling them to fine-tune their operations accordingly. Overall, cloud solutions are becoming an increasingly important part of modern agriculture, helping farmers achieve greater efficiency, sustainability, and profitability.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 3 August 2023 doi:10.20944/preprints202308.0362.v1

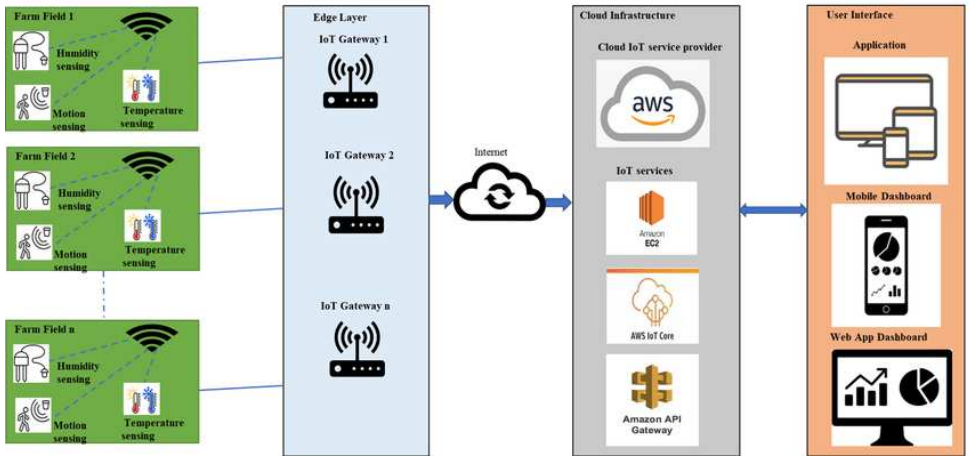

Figure 1. Smart farming application in Cloud-based IoT [8].

3. Materials and Method

The proposed methodology aims to improve the security and monitoring of the smart agriculture system. The Ethereum blockchain is used to track smart contracts and trigger events when discrepancies in security checks are detected. Figure 2 shows the layered design of the proposed approach. These IoT devices continuously generate events, such as device status, device information, and so on. The generated events are sent to the cloud through a wireless gateway or switch connected to the device. The cloud layer consists of components that continuously monitor the device events and process the event data to extract the required data in the system. MQTT is the industry standard for end-to-end packet data transmission. In the AWS cloud, we developed a Lambda function to analyze data from the AWS IoT main component and extricate the relevant data from sensor devices attached to the farms. When the Lambda identifies a security warning in the device data generation, Lambda initiates an Infura API POST request to update the Ethereum blockchain. Moreover, the improved exchange may include anomalous values of device information, device location, etc. Infura operates Ethereum hubs and provides an API for upgrading ex-variations from customer accounts, if they have one. Also, an upgraded blockchain ex-variations will be made available on all Ethereum hubs. Though, Figure 2 did not illustrate the client layer, the GUI could examine transactions from the Ethereum hub by means of an API call.

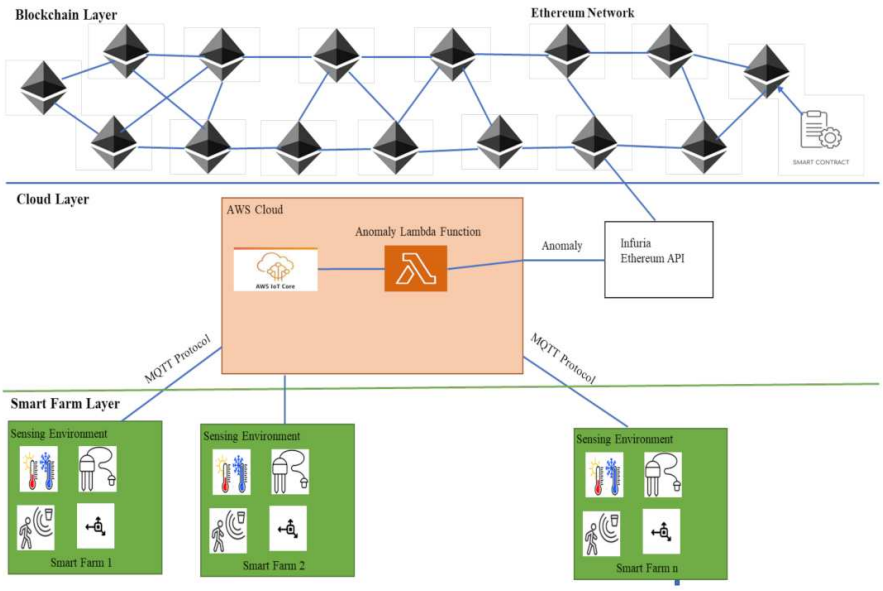

Figure 2. Blockchain-based solution in smart farming [8].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 3 August 2023 doi:10.20944/preprints202308.0362.v1

The portrayal of the most parts utilized within the projected approach is discussed below:

Ethereum: Form works on the POS agreement component to favor and incorporate ex-variations to the Ethereum blockchain. When a safety event is detected, a Web3 frontend request is conducted to survey and warn the farmers.

Infura API: This is a feature of Ethereum API that allows Smart contracts to be performed in Ethereum hubs and performs Ethereum-based ex-variations. Once we have collected and prepared the farming device data, we use the Infura API calls to connect with Ethereum hubs.

AWS IoT core: Several IoT devices sensors are available in the smart agricultural environment. To gather messages from diverse IoT devices, a message-processing framework is necessary to supplement IoT message protocols such as the MQTT and suits the organized transfer speed. Furthermore, to benefit from the Smart agricultural IoT data preparation, we chose AWS IoT core. The AWS IoT core enables minimal inactivity and maximum throughput execution, which aids in the development of real-time production level IoT monitoring frameworks.

AWS Lambda: The IoT data should be collected, prepared, and sent into the system as input data. As a result, AWS Lambda performs the cryptography in the background and saves the smart farming data to the Blockchain. AWS Lambda may be a serverless computing utility that allows you to run programs without the need for a framework.

4. Results Discussion

The data were obtained from the phase of triggering the device alarm when the organized sleep is in seconds, to verify the number of blockchain transactions accepted based on smart farming requests. The tests were carried out in six phases, and the data obtained are shown below:

Table 1. showing varying data trends.

Time Taken to Induce Device Alarm (In seconds)	Number of Accepted Blockchain Transactions on Smart farming Requests	Testing Phases
4.78	189,000	1
6.79	114,900	2
6.12	109,450	3
4.89	176,000	4
3.33	194,670	5
1.02	290,786	6

The data above showed a varying trend based on a series of tests carried out. The number of accepted blockchain transactions on smart farming requests fell from 189,000 to 109,450 after carrying out the first three tests (phases 1 to 3).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 3 August 2023 doi:10.20944/preprints202308.0362.v1

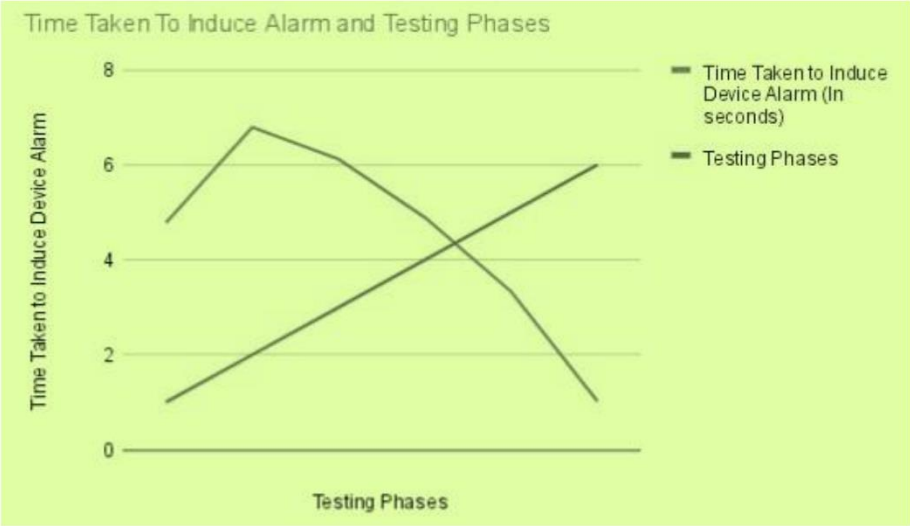

Figure 2. Testing stages and the time taken to induce the device alarm.

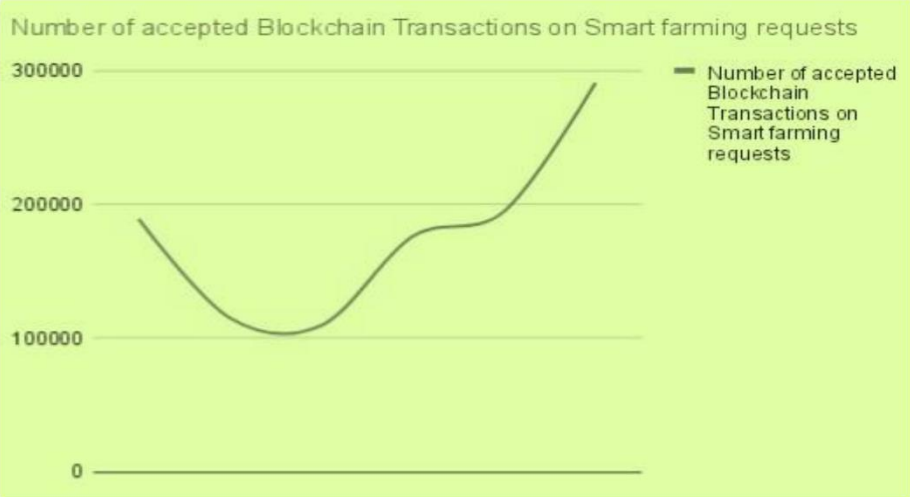

Figure 2. Number of accepted blockchain-based transactions on requests.

However, the next three testing phases showed a rise in the number of blockchain transactions accepted on smart farming requests from 176,000 to 290,786. We further observed that the lesser the time taken to induce the device alarm, the higher the number of blockchain transactions accepted on smart farming requests. This demonstrates the efficacy of blockchain-based poisoning attack mitigation in smart farming. The device alarm helps minimize poisoning attacks on the blockchain network concerning smart farming requests.

5. Conclusion

In this study, we presented a different method to mitigate and prevent poisoning attacks in the smart farming system, which notifies farmers of security and safety concerns, as well as the status of sensor devices. The end-to-end query implementation as demonstrated used an Arduino device pack, an AWS cloud environment, Ethereum blockchain smart contract, and a web application GUI. The system can provide real-time notifications to farmers, enable remote observation of the cultivation and farming ecosystem, and connect the farming society through this smart farm blockchain-based security framework. In our approach, the execution evaluation in terms of organized idleness becomes obvious, and it can be stated that the delay can be avoided by executing powerful exchange blockchain such as Cardano. In addition, the six test results showed varying trends in the number of

accepted blockchain transactions and the time taken to induce the device alarm system. The first three tests revealed a decline in the number of accepted Blockchain transactions and a rise in the time taken to induce device alarm. However, the last three tests revealed a rise in the number of accepted blockchain transactions and a fall in the time taken to induce device alarm. The lesser time it takes to induce a device alarm, the higher the number of accepted blockchain transactions on smart farming requests and vice versa. This further validates the prevention of blockchain based poisoning in smart farming and also enhances Blockchain transactions and development. We also investigated the security constraints and future potential of smart farming.

Acknowledgments: The research described in this paper was financially supported by the Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University.

Conflict of Interest Disclosure: This research declares no conflict of interest.

References

1. Z. Shen, T. Baležentis, and G. D. Ferrier, "Agricultural productivity evolution in China: A generalized decomposition of the Luenberger-Hicks-Moorsteen productivity indicator," *China Economic Review*, vol. 57, p. 101315, Oct. 2019, doi: 10.1016/j.chieco.2019.101315.
2. X. Xu, K. Zhou, and H. Ma, "The Impact of Agricultural Mechanization on Industry-Agriculture Coordinated Development in China," SSRN, preprint, 2023. doi: 10.2139/ssrn.4462200.
3. Y. Zhang and X. Diao, "The changing role of agriculture with economic structural change – The case of China," *China Economic Review*, vol. 62, p. 101504, Aug. 2020, doi: 10.1016/j.chieco.2020.101504.
4. C. STEVE, "Cyber Threats Are A Real Threat To Modern Agriculture's Expanding Digital Infrastructure," *AgWeb*, Jan. 11, 2022. https://www.agweb.com/news/business/technology/cyber-threats-are-real-threat-modern-agricultures-expanding-digital (accessed Jun. 26, 2023).
5. K. Hayes, "Ransomware: a growing geopolitical threat," *Network Security*, vol. 2021, no. 8, pp. 11–13, Aug. 2021, doi: 10.1016/S1353-4858(21)00089-1.
6. S. Mondal, K. P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal, "Blockchain Inspired RFID-Based Information Architecture for Food Supply Chain," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5803–5813, Jun. 2019, doi: 10.1109/JIOT.2019.2907658.
7. Z. Jana, B. Reiner, R. Sebastian, and W. S. Roland, "Perceived risks and vulnerabilities of employing digitalization and digital data in agriculture – Socially robust orientations from a transdisciplinary process," *Journal of Cleaner Production*, vol. 358, p. 132034, Jul. 2022, doi: 10.1016/j.jclepro.2022.132034.
8. R. Chaganti, V. Varadarajan, V. S. Gorantla, T. R. Gadekallu, and V. Ravi, "Blockchain-Based Cloud-Enabled Security Monitoring Using Internet of Things in Smart Agriculture," *Future Internet*, vol. 14, no. 9, Art. no. 9, Sep. 2022, doi: 10.3390/fi14090250.
9. A. A. Aliyu, J. Liu, and E. Gilliard, "BLOCKCHAIN-BASED POISONING ATTACK PREVENTION IN SMART FARMING," *Scientific and practical cyber security journal*, 2023, Accessed: Apr. 18, 2023. [Online]. Available: https://journal.scsa.ge/papers/blockchain-based-poisoning-attack-prevention-in-smart-farming/
10. R. Chaganti, B. Bhushan, and V. Ravi, "The role of Blockchain in DDoS attacks mitigation: techniques, open challenges and future directions." arXiv, Feb. 07, 2022. doi: 10.48550/arXiv.2202.03617.
11. A. Aliyu, J. Liu, and E. Gilliard, "Increased Accuracy in Blockchain-Based Intrusion Detection and Prevention System," Preprints, preprint, Jun. 2023. doi: http://doi.org/10.22541/au.168628693.37072204/v1.
12. M. S. Mekala and P. Viswanathan, "A Survey: Smart agriculture IoT with cloud computing," *2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS)*, pp. 1–7, Aug. 2017, doi: 10.1109/ICMDCS.2017.8211551.
13. M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges," *IEEE Access*, vol. PP, Feb. 2020, doi: 10.1109/ACCESS.2020.2973178.
14. O. Friha, M. A. Ferrag, L. Shu, L. Maglaras, and X. Wang, "Internet of Things for the Future of Smart Agriculture: A Comprehensive Survey of Emerging Technologies," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 4, pp. 718–752, Apr. 2021, doi: 10.1109/JAS.2021.1003925.
15. C. Li and B. Niu, "Design of smart agriculture based on big data and Internet of things," *International Journal of Distributed Sensor Networks*, vol. 16, no. 5, 2020, doi: 10.1177/1550147720917065.
16. T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes," *2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)*, pp. 519–524, Oct. 2016, doi: 10.1109/IIKI.2016.3.

17. N. Ahmed, D. De, and I. Hussain, "Internet of Things (IoT) for Smart Precision Agriculture and Farming in Rural Areas," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4890–4899, Dec. 2018, doi: 10.1109/JIOT.2018.2879579.
18. M. Torky and A. E. Hassanein, "Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges," *Computers and Electronics in Agriculture*, vol. 178, p. 105476, Nov. 2020, doi: 10.1016/j.compag.2020.105476.
19. A. Vangala, A. K. Das, N. Kumar, and M. Alazab, "Smart Secure Sensing for IoT-Based Agriculture: Blockchain Perspective," *IEEE Sensors J.*, vol. 21, no. 16, pp. 17591–17607, Aug. 2021, doi: 10.1109/JSEN.2020.3012294.