Secure Smart Agriculture Monitoring with Blockchain and Cloud-Enabled IoT Technology

S.Narasimmasubramanian[1]& Dr. S.ArumugaPerumal[2]

[1]Research Scholar (Register Number: 20123152291034), Department of Computer Science, S.T.Hindu College,Nagercoil-629002.AffiliatedtoManonmaniamSundaranarUniversity, Abishekapatti, Tirunelveli, Tamilnadu, India.

[2]Former Associate Professor&Head, Department of Computer Science, S.T. Hindu College, Nagercoil-629002.AffiliatedtoManonmaniamSundaranarUniversity, Abishekapatti, Tirunelveli, Tamilnadu, India.

Email: [1]spkcsns@gmail.com, [2]visvenk@yahoo.co.in

Abstract

The Internet of Things (IoT) and Blockchain has rapidly progressed in recent years and significantly influenced various industries, transforming their operational methods. One notable area benefiting from IoT advancements is smart farming, which leverages this technology to enable precision agriculture, achieve high crop yields, and ensure efficient utilization of natural resources for long-term sustainability. Smart farming integrates sensing capabilities, communication technologies for data transmission, and data analytics to extract meaningful insights, enabling farmers to make intelligent decisions and increase profitability. 7994

However, the incorporation of new technologies in smart farming also brings security and privacy challenges. Without proper implementation, these technologies can inherit vulnerabilities that may compromise the system's integrity. Consequently, security monitoring becomes a crucial component of smart farming. Additionally, the framework includes a Blockchain-based smart-contract application to securely store information about security anomalies and proactively mitigate similar attacks targeting other farms in the community.

The evaluation results demonstrated that the proposed framework could detect security anomalies within a real-time processing window and promptly update other farm nodes about the situation. This proactive approach helps enhance the overall security and resilience of smart farming operations.

In summary, the proposed cloud-enabled smart-farm security monitoring framework integrates IoT, cloud computing, and Blockchain technologies to provide a comprehensive solution for monitoring and securing smart farming environments. This approach ensures the effective detection and mitigation of security threats, thereby supporting the sustainable and profitable operation of smart farms.

The prototype was developed using an Arduino Sensor Kit and ESP32 for sensor data collection and communication. AWS Cloud was used for data processing and storage. A smart contract was implemented on the Ethereum Rinkeby Test Network to manage and store security-anomaly information securely. The performance evaluation focused on network latency to ensure that the system could monitor and respond to security events in real-time. The proposed framework for the system supported to the Monitoring Device Status, Detect Sensor Anomalies, and Mitigate Security Attacks.

Keywords: IoT, Blockchain, Ethereum, Smartfarm.

DOI Number:10.48047/nq.2022.09.NQ44929 **NeuroQuantology 2022;20(9):7994-8007**

1. Introduction

The surging human population worldwide underscores the critical importance of agriculture and farming in producing sufficient food for everyone. Many countries' economies heavily rely on the agriculture sector's performance. Boosting this sector's performance can significantly reinforce a country's economy. However, farmers often earn lower profit margins on their products compared to those working in sectors such as technology, construction, and education. This disparity, combined with the high manpower requirements and lower financial incentives, has led to declining interest in agricultural work among farmers.

Moreover, the financial risks associated with farming are high due to the potential impact of sudden natural calamities, which can devastate crops and livestock if farmers are unprepared. The emergence of technologies like the Internet of Things (IoT) has revolutionized farming practices and enhanced operational capabilities in the agriculture sector. This integration of IoT within agriculture is known as smart agriculture or smart farming.

The global agriculture robot market is projected to reach USD 15.93 billion by 2028, with an annual compound growth rate of 20.31% from 2021 to 2028[1]. As digital infrastructure becomes more integrated within agriculture, the sector has increasingly become a target for cyber attacks. For example, the meat processing company JBS suffered a ransomware attack that halted operations at 13 meat plants, costing the company USD 11 million in ransom to resume operations[2] . This incident highlights the critical need for advanced security solutions in agriculture to protect against such threats. Addressing these challenges through technological integration and enhanced security solutions can help sustain and grow the agriculture sector, ensuring food security and economic stability.

Smart agriculture and farming, leveraging the Internet of Things (IoT), can significantly enhance crop yields and resource efficiency, leading to improved productivity [3]. Recent trends highlight that smart agriculture is a promising application of IoT for process improvements. IoT applications in smart agriculture include soil-state monitoring, pest-control monitoring, crop-growth monitoring, animal-herd monitoring, water-level control, and environmental condition monitoring. Sensors are installed around the farm to capture operational and environmental data, which is then converted from analog to digital form. Prominent sensors used in smart agriculture include temperature, humidity, light, pressure, and proximity sensors. These sensors are connected to the internet through edge gateways or routers, constantly updating the sensing information in the cloud.

However, while cloud communication offers data analytics and storage capabilities, it also introduces security and privacy issues that are not well-addressed in existing literature. Current security solutions in smart farming and agriculture focus on food supply chain management , monitoring various activities using cloud technologies, machine learning (ML), and AI-based data analytics , and authentication and authorization solutions for constrained IoT devices . Despite these efforts, cloud-based monitoring solutions can still have security consequences if secure coding practices and IoT security best practices are not followed. IoT devices exposed to the internet have historically been compromised and used for large-scale denial-of-service attacks or other malicious activities such as manipulating sensor values and data exposure.

The existing cloud-based or gateway-based security solutions for monitoring smart agriculture applications are insufficient for providing comprehensive security [4]. Decentralized applications and storage offer security advantages over traditional methods in terms of secured event storage, traceability, immutability, and enhanced security and privacy. Blockchain technology, known for its use in decentralized applications, has proven effective in addressing IoT security and privacy issues, including in smart agriculture. Blockchain applications in smart agriculture include food production supply chain management and secured transaction storage. Blockchain ensures transparency by keeping track of event sequences, ultimately treating farmers fairly and increasing their profits.

Inspired by the advantages of Blockchain technology in smart agriculture, we propose a smart farming security monitoring solution utilizing Blockchain. This solution aims to provide robust security for smart agriculture by leveraging the decentralized, immutable, and transparent nature of Blockchain technology.

The current security monitoring solutions in smart agriculture predominantly focus on either cloud-based options or Blockchain Technology. Most of these solutions primarily address supply chain issues. However, leveraging the advantages of both cloud and blockchain technologies can lead to optimal security solutions for smart agriculture. To address the limitations of existing cloud-based solutions and enhance security using Blockchain applications, we propose a combined cloud and blockchain solution. This approach processes sensing data in the cloud and stores anomalies in Blockchain transactions. Unlike existing solutions, we provide a comprehensive end-to-end implementation using both cloud and Blockchain technologies for smart agriculture. Additionally, we evaluate the network latency performance of our solution.

2. Literature survey

2.1.IoT Smart-Agriculture Backgrounds

Benefits of IoT in Agriculture

IoT technology is shown to enhance productivity and yield in agriculture. It has several applications and provides significant advantages in the field, such as improved efficiency and better resource management.

2.2.Prior Works Discussing IoT in Agriculture

Multiple studies have discussed the role of IoT in agriculture, highlighting its applications and benefits. Olakunle et al. [5] reviewed IoT integration in smart agriculture, focusing on data analytics, benefits, and challenges. They categorized future trends and opportunities based on technologies, applications, business, and marketing. Farooq et al. [6] studied the technologies involved in IoT-based smart agriculture, including network protocols, architecture, cloud computing, and big-data analytics. They also discussed security issues and policies supporting smart agriculture, along with existing smart-device applications.

Othmane et al. [7]reviewed advanced technologies used in IoT-based smart agriculture and categorized various smart agriculture applications. They also discussed existing blockchain solutions for supply-chain management in agriculture. Articles focused on the use of wireless sensor networks for water regulation and monitoring in agriculture, emphasizing IoT's role in water management. The authors of one study surveyed different applications used in smart agriculture and highlighted cloud computing as a backend technology stack for application implementation.

Amera et al. [8] performed a survey defining taxonomy for smart agriculture architecture and technologies, classifying literature based on these categories. Another study reviewed IoT-based smart agriculture in terms of architecture, applications, software, hardware, principal advantages, and future research challenges.

Brewster et al. highlighted the importance of data governance, security, and privacy in IoT applications in agriculture, emphasizing the need for a cultural shift to adopt these solutions. Despite the numerous benefits, significant challenges and research issues remain. These include concerns related to security and privacy, network issues, regulations, scalability, reliability, and resource optimization. Addressing these challenges is crucial for the successful integration of IoT in agriculture.

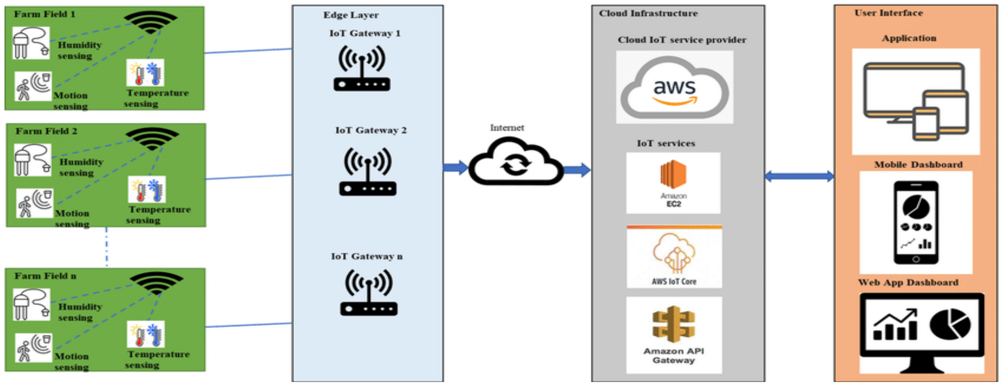


Fig 2.2.1 Cloud based IoT Smart Agriculture Application (Source: Google)

Temperature sensor: The sensor detects temperature changes within the application. The water temperature, the surrounding-air temperature, and plant temperaturemonitoring capabilities improve the effectiveness of agriculture duties.

Humidity sensor: The humidity sensor measures the humidity changes in the agricultural land environment. The humidity sensor helps measure the soil moisture and waterconsumption rate, tracking waterfall trends for future irrigation-requirements estimation. The normal humidity ranges are 0%RH–100%RH.

Light sensor: The light sensors in agriculture monitor the light in the agricultural greenhouse, cloud shadow, and the required light to grow the plants.

Accelerometer sensor: Accelerometer sensors in agriculture help to maintain the agriculture or farming equipment. The movement and vibration changes in the equipment are monitored to detect the equipment replacement needs.

pH sensor: The pH sensors in agriculture improve the productivity of crops. The pH sensor detects the unwanted chemicals in the soil and soil nutrient deficiencies. Soil-pH fluctuation monitoringcanhelpthefarmerstotakeprecaution sandeffectivelygrowplants.

GPS sensors: An animal herd or any objects in the agricultural location can be monitored using a GPS sensor. The remote monitoring and location tracking help to achieve precise agriculture.

Pressure sensor: A pressure sensor in agriculture may be used to monitor pipes and tanks. The pressure sensor improves water management, irrigation management, and precision farming.

Infrared sensor: Infrared sensor integrated with drones monitors the crop and measures the plant's strength. The plants can be adjusted and optimized for the agriculture resources to manage agriculture activities effectively.

Table 1.Smart agriculture sensors and their applications

Sensor type	Sensor Input	Smart agriculture application
Temperature	Heat energy	Plants,air,water
Humidity	Humidity of the surrounding air	Air,water,crop,plant
Camera	Photon detection	Storage area or farm monitor
Light	Light or radiant energy	Fields,crop
pH	Electromechanical	Soil nutrient deficiencies, presence of unwanted chemicals
GPS	Measuring the distance using satellite technology	Keeping track of flocks, highly precise agriculture vehicle guidance
Dielectric soil moisture	Dielectric constant measurements	Water moisture in soil
Passive infrared	Motion detection	Track individuals movement

2.3. Blockchain smart agriculture Background

2.3.1.Prior work discussing in Blockchain with IoT

Oscar et al. [9] conducted a study detailing the use of blockchain in smart agriculture. They highlighted that security and privacy issues are major concerns in this field. Their research found that most efforts were focused on solving supply-chain problems, with less emphasis on secure data storage, remote monitoring, and automation.

Saikat [10] proposed Blockchain-based IoT architecture for the food supply chain. The implementation involved using RFID sensors to capture identification IDs from product packages and adding this information to the Blockchain to maintain data integrity. This architecture enabled stakeholders to verify public blockchain data regarding the status of products.

Mubariz et al. [11] introduced Blockchain-based cloud nodes to verify edge server services for IoT devices. They utilized a proof-of-authority (POA) mechanism to maintain consensus among the Blockchain cloud nodes. Additionally, IoT devices rated edge servers based on the service provided, and this rating was used for service authentication.

Mubariz et al. [11] introduced Blockchain-based cloud nodes to verify edge server services for IoT devices. They utilized a proof-of-authority (POA) mechanism to maintain consensus among Blockchain cloud nodes. Additionally, IoT devices rated edge servers based on the service provided, and this rating was used for service authentication.

Mohamed et al. [12] investigated the use of Blockchain technology to implement security solutions in agriculture. Their research highlighted technical challenges such as large throughput and limited storage capacity.

2.3.2.Key Findings and Challenges

Blockchain solutions can significantly enhance the security and privacy of smart agriculture. However, the limited data storage capacity in Blockchain systems remains a challenge. High network connection rates required for consensus activities pose additional difficulties, especially in rural areas.

Overall, Blockchain technology has been leveraged to address various issues in smart agriculture, particularly in enhancing security and privacy. Nonetheless, challenges related to data storage capacity, network connection rates, and the implementation of blockchain in rural areas need to be addressed for broader adoption. The integration of blockchain with IoT in agriculture presents promising opportunities but requires careful consideration of these challenges to realize its full potential.

3. Proposed system

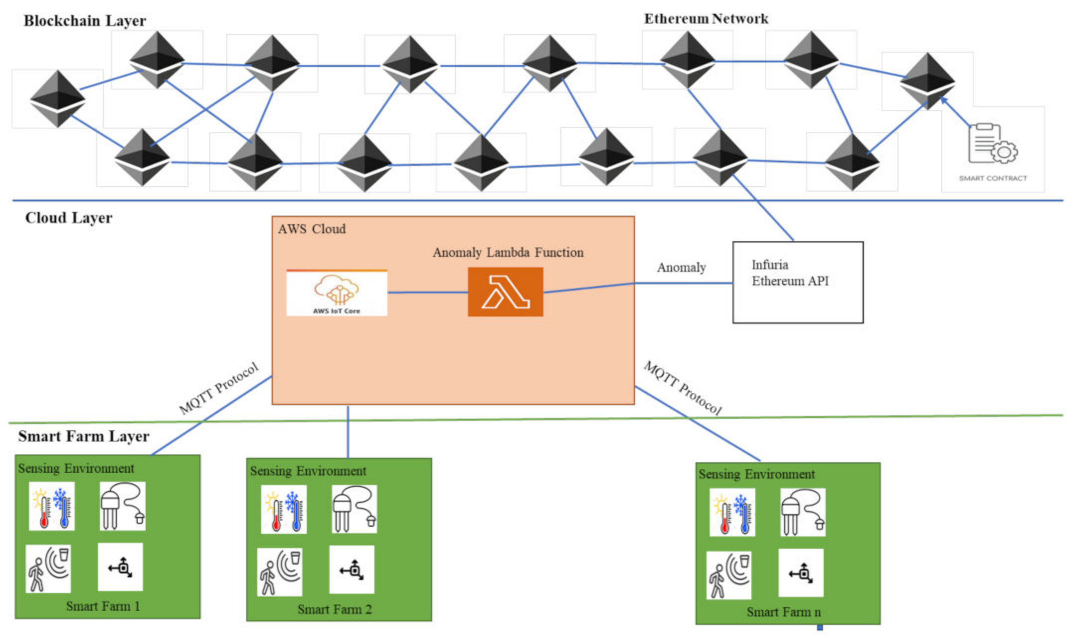


Fig 3.1.Layered Architecture of the Proposed Approach

The Smart farm layer consists of various sensor devices installed on farmland. These sensors monitor critical parameters such as soil moisture, temperature, humidity, and device health, generating continuous event data. This data provides real-time insights into the conditions of the farmland. The Edge Gateway serves the function of transmitting the sensor-generated events to the cloud layer. It acts as a crucial intermediary, ensuring that the data collected by the sensors is communicated effectively to the cloud for further processing.

In the Cloud Layer, components such as AWS IoT Core and AWS Lambda functions play a vital role. AWS IoT Core listens to sensor events, processes the data, and retrieves relevant information using the MQTT protocol for passing data packets. It ensures low latency and high throughput, which supports real-time monitoring. AWS Lambda further processes the collected IoT data, integrating it with the Ethereum Blockchain, and executes backend code without the need for traditional server infrastructure. This setup facilitates efficient data handling and seamless integration with Blockchain technology.

The Blockchain Layer, based on Ethereum, plays a crucial role in running smart contracts and triggering events based on detected anomalies during security monitoring.

It utilizes the Infura API to facilitate Ethereum API services, allowing for the execution of smart contracts and handling transactions without the need to deploy a full Ethereum node. The Ethereum blockchain employs a Proof of Stake (POS) consensus mechanism to approve and add transactions. Transactions are updated with details such as anomaly values and device status, and these updates are propagated across distributed Ethereum nodes to ensure consistency and reliability.

The User Layer features a graphical user interface (GUI) that interacts with the Ethereum Blockchain. It reads transactions from Ethereum nodes through API calls, displays alerts related to smart agriculture, and provides a user-friendly interface for monitoring. This layer allows users to easily track and respond to events detected by the blockchain layer, enhancing the overall effectiveness of the smart agriculture system.

3.1.Work flow of the proposed system

The workflow begins with event generation and transmission. IoT sensor devices in the Smart farm layer generate various events related to soil moisture, temperature, humidity, and other parameters. These events are then transmitted to the cloud layer through an edge gateway.

In the Cloud Layer, AWS IoT Core collects and processes the IoT data received from the sensors. AWS Lambda functions subsequently parse this data, extracting the necessary information for further action. When AWS Lambda detects a security alert or anomaly in the sensor data, it performs a POST request to the Infura API. The Infura API updates the Ethereum Blockchain with the transaction details, including information about sensor anomalies and device statuses. These updated transactions are then propagated across the Ethereum network nodes, ensuring that all nodes reflect the latest data.

Finally, in the User Monitoring phase, the graphical user interface (GUI) retrieves Blockchain transactions through API calls. Users can view smart-agriculture alerts and detailed sensor data via the GUI, providing a comprehensive and user-friendly interface for monitoring the system.

3.2.Main Components of Proposed system

- AWS IoT Core supports the MQTT protocol for efficient IoT message processing, offering low latency and high throughput to enable real-time monitoring of agricultural conditions.
- AWS Lambda serves as a serverless computing service that processes smart-farming data and integrates it with the Ethereum Blockchain, eliminating the need for traditional server infrastructure.
- The Infura API provides a crucial Ethereum API service, facilitating the execution of smart contracts and transaction management without requiring the deployment of a full Ethereum node. This API enables seamless interaction with Ethereum nodes for data storage and transaction processing. On the Ethereum blockchain, sensor data related to farming and environmental conditions is securely stored, utilizing a Proof of Stake (POS) consensus mechanism to ensure transaction validation and network integrity..

3.3.Implementation Components

1. **AWS IoT Core**:
    - Supports IoT message protocols (MQTT) and handles network bandwidth for numerous IoT devices.
    - Provides low latency and high throughput for real-time monitoring.

2. **AWS Lambda**:
   - Server less computing service running backend code.
   - Processes smart-farming data and integrates it with the Ethereum blockchain.
3. **Infura API**:
   - Provides Ethereum API service to run smart contracts and manage transactions.
   - Interacts with Ethereum nodes for data storage and transaction processing.
4. **Ethereum Blockchain**:
   - Stores farming sensor data and monitors environmental conditions.
   - Uses Proof of Stake (POS) consensus mechanism for transaction approval and addition.
   - Ensures data integrity and security for smart agriculture monitoring.

4. Implementation

To evaluate the proposed smart-agriculture security monitoring approach using Blockchain and cloud technologies, we implemented a prototype incorporating several key components. We used the Arduino Sensor kit with Wi-Fi capabilities to simulate various sensors typically deployed in farmland. AWS cloud components were utilized to process the sensor data, while the Ethereum Blockchain was employed to store monitoring alerts and other essential information via smart contracts. Additionally, a web frontend was developed to display these alerts to users.

In our experimental setup, we used hardware and software components including the Arduino sensor kit, an ESP8266 Wi-Fi module, AWS IoT Core, AWS Lambda function, Infura Ethereum API account, and web JavaScript. The Arduino module with Wi-Fi was connected to a home Wi-Fi router to communicate with the cloud. The security monitoring application we developed could function as a product or third-party security tool for IoT devices in smart agriculture.

The Arduino sensor kit includes various sensors such as a potentiometer, light sensor, sound sensor, air pressure sensor, temperature sensor, and accelerometer, which monitor and capture diverse environmental and physical conditions. A breadboard connected these sensors to the communication equipment, specifically the Wi-Fi module, which also acted as the edge gateway for all sensors in the setup. The Arduino code, written in C, was used to connect the Wi-Fi module to the home router and enable communication with remote AWS IoT nodes for event updates.

The AWS IoT Core service was configured in the AWS Cloud with generic settings, running on the FreeRTOS operating system for processing IoT device data and exchanging information using the MQTT protocol. Sensor data was displayed and stored in AWS Cloud storage, such as S3. AWS Lambda functions, written in JavaScript, constantly polled sensor event data from AWS IoT Core, implementing monitoring logic to identify sensor statuses and anomalies. Infura API calls, made by the AWS Lambda function, updated the sensor monitoring data on the Ethereum Blockchain for permanent storage. An Infura account was used to generate the API key and connect to the Ethereum network, ensuring that alert data was updated and stored in Blockchain transactions.

For end-to-end application implementation, Infura API calls were used to retrieve alert transactions from the Ethereum Blockchain. Farmers could then download a mobile application or use a web app to monitor farm alerts remotely. Figure 3 illustrates the Arduino microcontroller used to control and connect to the IoT sensing devices. The temperature, humidity, and light sensors were connected to the microcontroller, which supported Wi-Fi connectivity for cloud communication. The sensors, as agricultural application end devices, had their positive terminals connected to microcontroller pins, while negative terminals were grounded to prevent short-circuiting. The microcontroller was powered with 5V, as indicated by a red wire connection in Figure 4.1.1.

4.1.Experimental Setup

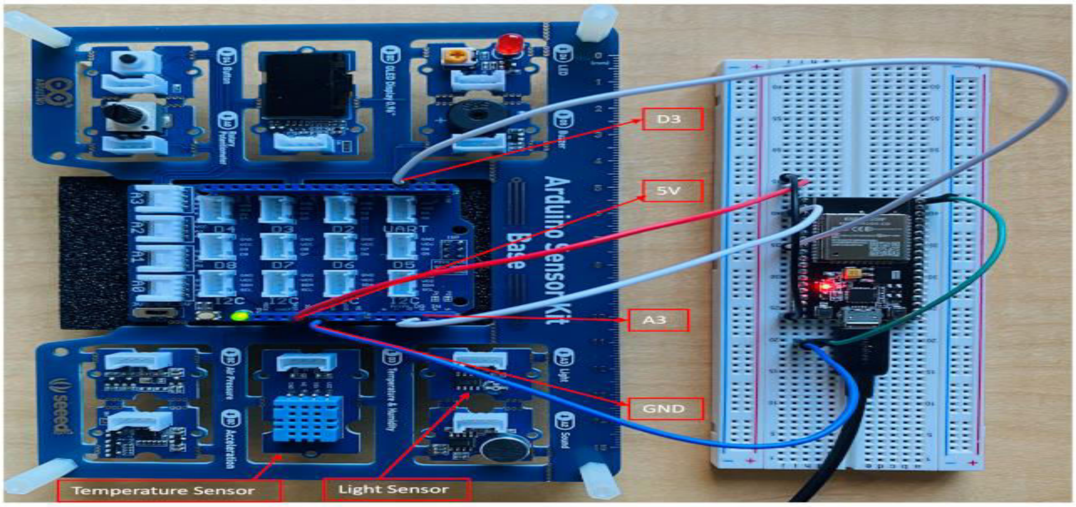


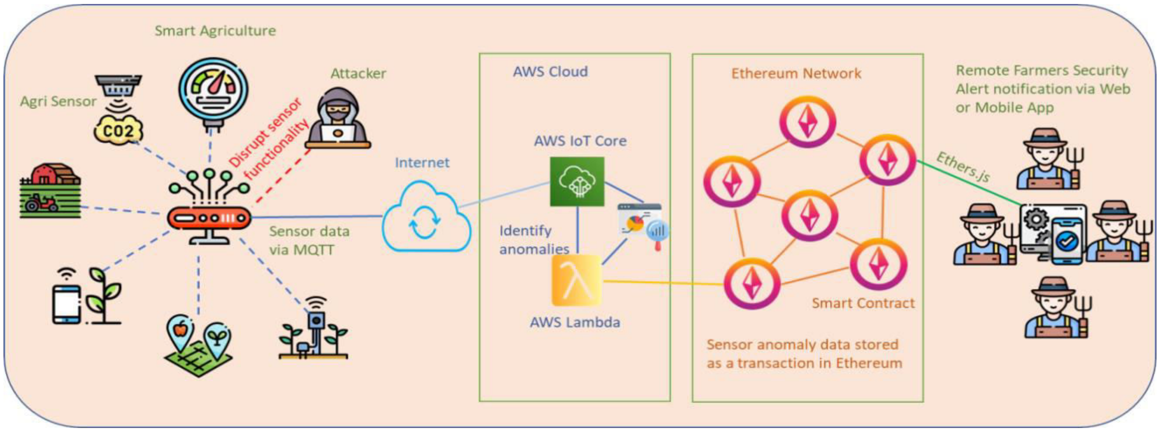
Figure 4.1.1. Arduino sensor kit to sense the environment

4.2.Hardware and Software Components

- **Arduino Sensor Kit**: Includes potentiometer, light sensor, sound sensor, air pressure sensor, temperature sensor, and accelerometer to monitor environmental and physical conditions.
- **EP8266 Wi-Fi Module**: Connects the Arduino to a home Wi-Fi router for communication with the cloud.
- **AWS IoT Core**: Processes sensor data and handles IoT device communication.
- **AWS Lambda**: Executes code to process sensor data and interact with the blockchain.
- **Infura Ethereum API Account**: Provides API calls to interact with the Ethereum blockchain.
- **Web Frontend**: Developed in JavaScript to display alerts to users.

4.3.Implementation Process

The sensor data collection and communication system is designed to integrate Arduino with AWS IoT Core, AWS Lambda, and Blockchain technology, providing real-time monitoring and alerting capabilities. The setup involves connecting sensors to an Arduino board via a breadboard, with Arduino C code facilitating the Wi-Fi module's connection to the home router using SSID and password credentials. The sensor data is transmitted to AWS IoT Core, which serves as an edge gateway using the Wi-Fi module. AWS IoT Core is configured with generic settings and operates on FreeRTOS, an operating system tailored for IoT device data processing. It employs the MQTT protocol for data exchange and has the capability to display and optionally store sensor data in AWS S3.



Data processing is handled by an AWS Lambda function written in JavaScript, which continuously polls data from AWS IoT Core. This function includes monitoring logic to assess sensor status and detect anomalies. When anomalies are detected, the function makes Infura API calls to update the Ethereum Blockchain with the sensor monitoring data. The Blockchain interaction is facilitated through Infura API, where an Infura account is used to generate API keys and establish connections to the Ethereum network. This enables the updating of Blockchain transactions with sensor alert data for permanent storage. Smart contracts deployed on the Ethereum Blockchain manage and store monitoring alerts and essential information.

Additionally, a web application developed in JavaScript retrieves alert transactions from the Ethereum Blockchain via Infura API calls. This web app provides real-time alerts and monitoring data, accessible to the farmer remotely through a mobile app or web browser, ensuring that the farmer can stay informed about the sensor data and alerts at all times.

4.4. Prototype Workflow Output

```
09:37:30.248 ->
09:37:30.248 -> Initializing thing Temp_Humidity_DHT11_0
09:37:30.248 ->
09:37:30.248 ->   Initializing WIFI: Connecting to MaverickCreek-7-709
09:37:30.355 ->   ..........
09:37:35.377 ->   Connected.
09:37:35.377 ->   Done
09:37:35.377 ->
09:37:35.377 ->   Initializing DHT11...  Done.
09:37:35.377 ->
09:37:35.377 ->   Initializing connetction to AWS....
09:37:39.206 ->   Connected to AWS
09:37:39.206 ->   Done.
09:37:39.206 ->   Done.
09:37:39.206 ->
09:37:39.206 -> Done.
09:37:39.206 ->
09:37:39.241 ->
09:37:39.241 ->
09:37:39.241 -> Publishing:-
09:37:39.241 -> { "temp":26.20, "hum": 53.00, "light": 78 }
09:37:39.241 -> Failed!
09:37:39.241 ->
09:37:49.255 ->
09:37:49.255 ->
09:37:49.255 -> Publishing:-
09:37:49.255 -> { "temp":26.00, "hum": 53.00, "light": 76 }
09:37:49.255 -> Success
09:37:49.255 ->
09:37:59.295 ->
09:37:59.295 ->
09:37:59.295 -> Publishing:-
09:37:59.295 -> { "temp":26.20, "hum": 51.00, "light": 41 }
09:37:59.295 -> Success
09:37:59.295 ->
09:38:09.307 ->
09:38:09.307 ->
```

Figure 4.4.1.Sensor devices connected to Wi-Fi and initializing connection to AWS Cloud

The log provided illustrates the initialization process and data publishing attempts of a device named \`Temp_Humidity_DHT11_0\`. Here is the paragraph summarizing the key information:

The device \`Temp_Humidity_DHT11_0\` underwent an initialization process that included connecting to the WiFi network \`MaverickCreek-7-709\` and successfully establishing a connection to AWS. Following this, the device attempted to publish data readings of temperature, humidity, and light levels. The first publishing attempt, with data values of temperature 26.00°C, humidity 53.00%, and light level 78, failed. A subsequent attempt with similar temperature and humidity readings but a slightly lower light level of 76 was successful. Another successful publishing followed with temperature 26.20°C, humidity 51.00%, and light level 41. This summary captures the main events and outcomes from the log, including connection success; initial publishing failure, and subsequent successes with specific data readings.

The MQTT publish messages can also be logged in the AWS IoT Core. Figure 5 shows the published IoT sensor data in the AWS Cloud. As shown in Figures 4 and 5, the data publication time in the IoT core cloud is 2 seconds. The red highlighted boxes in Figure 5 indicate the timestamp and sensor readings for temperature, humidity, and light values in the Arduino kit environment.

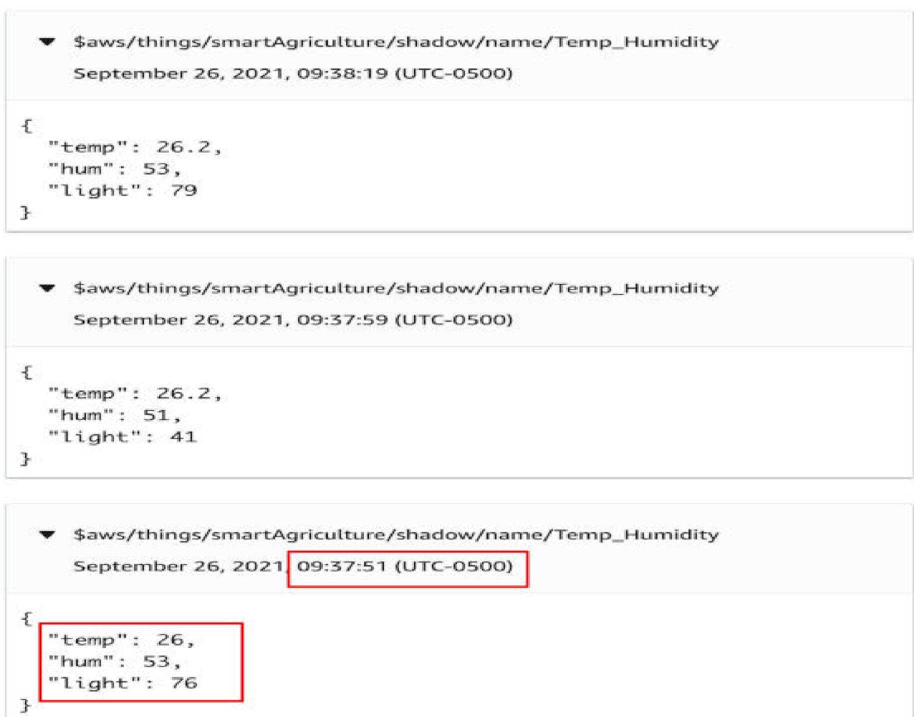


Figure 4.4.2. Sensor data real time recording in AWS Cloud-IoT core service

The AWS Lambda function, written in JavaScript, reads data published by AWS IoT Core and compares it with sensor threshold values for anomaly detection. If data is not received within a specified time interval, the code may trigger a sensor device health alert. To interact with the Ethereum Blockchain, Infura API credentials are stored as variables. The AWS Lambda function uses these credentials to connect to an Infura-maintained Ethereum main node. The MetaMask application is used as a software wallet to interact with the Ethereum Blockchain. Wallet details are provided in the AWS Lambda function to perform transactions on Ethereum.

The smart contract, written in Solidity, sends alert-triggered data as a transaction on the Ethereum Blockchain. Figure 4.4.3 shows the Ethereum transaction details when a temperature-threshold-exceeded alert is seen in AWS IoT Core. The transactions include the block number, from and to addresses, transaction fee, gas price, and timestamp.

Based on the timestamps observed in this end-to-end blockchain and cloud-based implementation, it takes 9 seconds to update the farmer when an agriculture environment anomaly alert is triggered. The Ethereum transaction completion time is 7 seconds. However, this testing was done on the Rinkeby test network, and the overall alert notification network latency may differ on the Ethereum production network. Overall, the system demonstrates minimal network latency when performing agriculture security monitoring using Blockchain and cloud services, effectively alerting farmers in a timely manner.

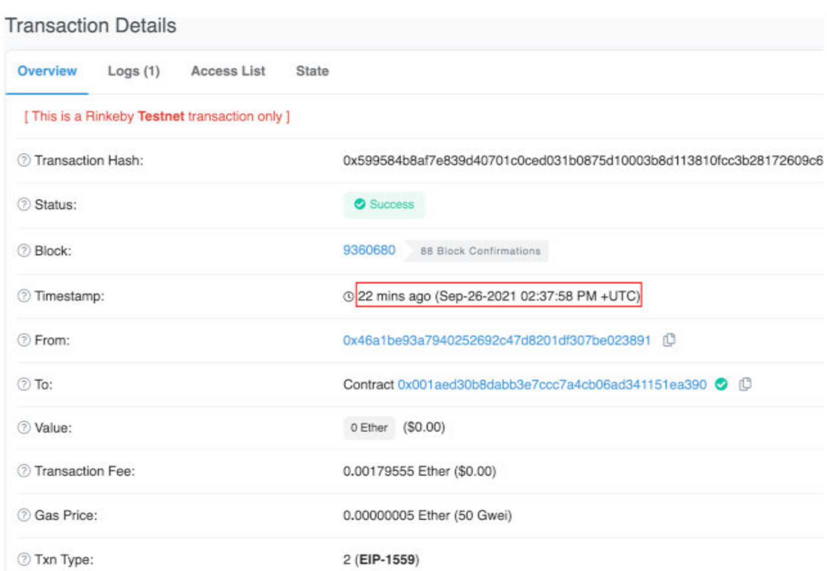


Figure 4.4.3. Ethereum smart-contract transaction details

Figure 4.4.4 illustrates the data field format in an Ethereum transaction. The sensor threshold value, current value, and alert message are stored within the data transaction. This information is securely stored in the Blockchain, ensuring it cannot be tampered with. The red highlighted boxes clearly indicate that the temperature value of 25 does not exceed the threshold value of 26.

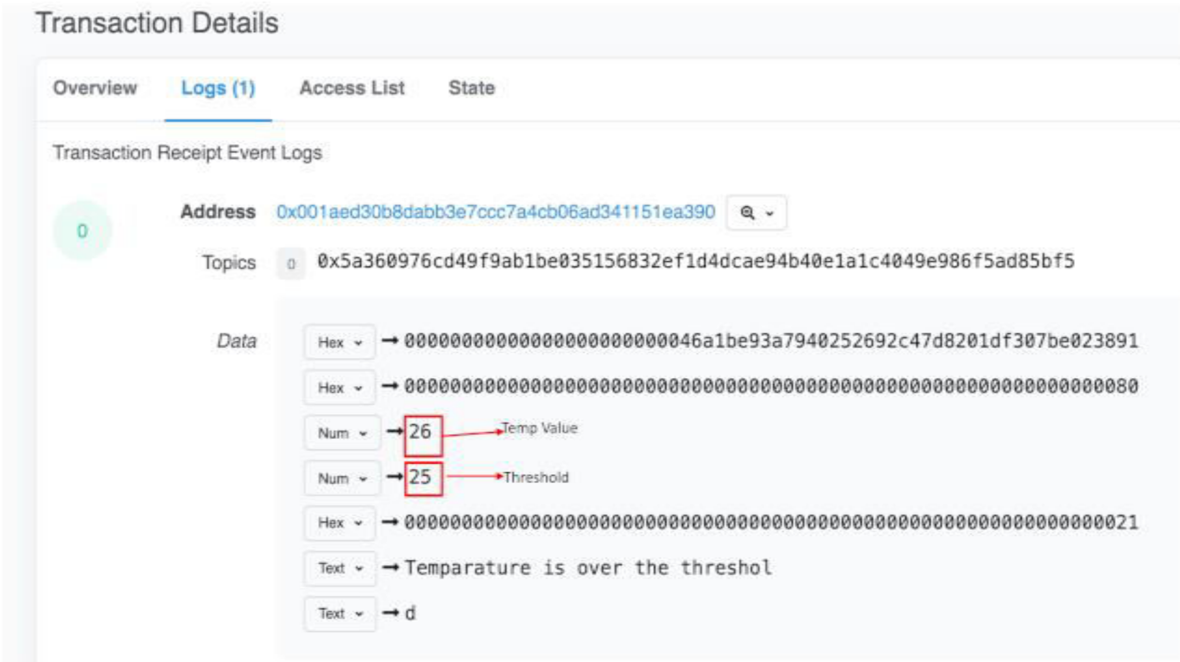


Figure 4.4.4. Ethereum smart-contract transaction storing the sensor data

5. Discussions, Limitations &future work

We created a real-time agriculture security monitoring system that tracks the health status of sensor devices and detects anomalies to support precision agriculture and productive farming. However, we did not deploy these sensors in actual agricultural fields to monitor real farmland conditions. We believe that network latency will be minimal, thanks to the widespread availability of the internet in rural areas. Our solution can monitor agricultural conditions in rural areas as long as there is an internet connection. In our work, we did not implement an IoT gateway. Instead, we used a home router as the IoT gateway and connected the IoT sensor devices to the network via home WiFi. This is a limitation of our work.

Future improvements include implementing an IoT network with an actual IoT gateway and various sensing devices to better simulate a realistic smart agriculture environment. Currently, our implementation operates on the Ethereum proof-of-work (POW) Blockchain. Future work will involve transitioning to the Ethereum 2.0 network, which uses the proof-of-stake (POS) consensus mechanism.

There are numerous IoT applications for monitoring environments, including agriculture, smart homes, smart health, and smart transportation. We envision that our prototype can also be used for monitoring solutions in these other fields. Network traffic can be collected from a smart agriculture edge gateway and stored in the cloud. This data can then be analyzed using machine learning (ML) and deep learning (DL) techniques to identify anomalies in network traffic within a smart agriculture network.

One future direction involves implementing ML- and DL-based network security monitoring solutions in smart agriculture and using Blockchain to store network anomaly events as transactions. The gas prices on the production Ethereum Blockchain are high. Therefore, we are considering using Blockchain technologies like Cardano and Solana to design low network-latency applications and reduce transaction costs for end users and farmers in smart agriculture.

6. Conclusion

In this Research article, we proposed a cloud- and Blockchain-based security monitoring solution for smart agriculture IoT applications. The end-to-end application prototype was implemented using an Arduino sensor kit, AWS cloud components, a web application GUI, and an Ethereum blockchain smart contract to alert farmers about security anomalies and sensor device statuses. The prototype successfully provided real-time alerts to farmers, enabled remote monitoring of the farm and agricultural environment, and facilitated communication within the farming community via blockchain. The performance evaluation indicated nominal network latency with our prototype, and we noted that the delay could be further reduced by implementing high-performance Blockchain technologies such as Cardano. We also discussed the limitations of our current implementation and future opportunities to enhance the security of smart agriculture.

References:

1. Steve, C. Cyber Threats Are a Real Threat to Modern Agriculture's Expanding Digital InfrastructureAgWeb. 2022. Available online: https://www.agweb.com/news/business/technology/cyber-threats-are-real-threat-modern-agricultures-expandingdigital (2022).

2. Nicole, S. JBS Paid $11 Million to Hackers after Ransomware Attack—CBS News. 2020. Available online: https://www.cbsnews.com/news/jbs-ransom-11-million/.

3. Badran, A.I.; Kashmoola, M.Y. Smart Agriculture Using Internet of Things: A Survey. In Proceedings of the 1st International Multi-DisciplinaryConferenceTheme: SustainableDevelopment andSmartPlanning,IMDC-SDSP,Cyperspace,28–30June 2020; p. 10.

4.Friha,O.;Ferrag,M.A.;Shu,L.;Maglaras,L.A.;Wang,X. InternetofThingsfortheFutureofSmartAgriculture: AComprehensive Survey of Emerging Technologies. IEEE CAA J. Autom.Sin. 2021, 8, 718–752.

5. Elijah, O.; Rahman, T.A.; Orikumhi, I.; Leow, C.Y.; Hindia, M.N. An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. IEEE Internet Things J. 2018, 5, 3758–3773.

6.Farooq, M.S.; Riaz, S.; Abid, A.; Abid, K.; Naeem, M.A. A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. IEEE Access 2019, 7, 156237–156271.

7. Friha,O.;Ferrag,M.A.;Shu,L.;Maglaras,L.A.;Wang,X. InternetofThingsfortheFutureofSmartAgriculture: AComprehensive Survey of Emerging Technologies. IEEE CAA J. Autom.Sin. 2021, 8, 718–752.

8. Badran, A.I.; Kashmoola, M.Y. Smart Agriculture Using Internet of Things: A Survey. In Proceedings of the 1st International Multi-DisciplinaryConferenceTheme: SustainableDevelopmentandSmartPlanning,IMDC-SDSP,Cyperspace,28–30June 2020; p. 10.

9. Bermeo-Almeida, O.; Cardenas-Rodriguez, M.; Samaniego-Cobo, T.; Ferruzola-Gómez, E.; Cabezas-Cabezas, R.; Bazán-Vera, W. Blockchain in agriculture: A systematic literature review. In Proceedings of the International Conference on Technologies and Innovation, Guayaquil, Ecuador, 6–9 November 2018; pp. 44–56.

10. Mondal, S.; Wijewardena, K.P.; Karuppuswami, S.; Kriti, N.; Kumar, D.; Chahal, P. Blockchain inspired RFID-based information architecture for food supply chain. IEEE Internet Things J. 2019, 6, 5803–5813.

11. Rehman, M.; Javaid, N.; Awais, M.; Imran, M.; Naseer, N. Cloud based secure service providing for IoTs using blockchain. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp.1–7

12.Torky, M.; Hassanein, A.E. Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges. Comput.Electron.Agric. 2020, 178, 105476.