



Article

Blockchain-Based Cloud-Enabled Security Monitoring Using Internet of Things in Smart Agriculture

Rajasekhar Chaganti ^{1,*}, Vijayakumar Varadarajan ^{2,3,*}, Venkata Subbarao Gorantla ⁴,
Thippa Reddy Gadekallu ⁵ and Vinayakumar Ravi ⁶

¹ Toyota Research Institute, Los Altos, CA 94022, USA

² School of Computer Science and Engineering, The University of New South Wales, Sydney, NSW 2052, Australia

³ School of NUOVOS, Ajeenkya DY Patil University, Pune 412105, India

⁴ Software Developer, Victorville, CA 92395, USA

⁵ Department of Information Technology, VIT University, Vellore 632014, India

⁶ Center for Artificial Intelligence, Prince Mohammad Bin Fahd University, Khobar 31952, Saudi Arabia

* Correspondence: raj.chaganti2@gmail.com (R.C.); v.varadarajan@unsw.edu.au (V.V.)

Abstract: The Internet of Things (IoT) has rapidly progressed in recent years and immensely influenced many industries in how they operate. Consequently, IoT technology has improved productivity in many sectors, and smart farming has also hugely benefited from the IoT. Smart farming enables precision agriculture, high crop yield, and the efficient utilization of natural resources to sustain for a longer time. Smart farming includes sensing capabilities, communication technologies to transmit the collected data from the sensors, and data analytics to extract meaningful information from the collected data. These modules will enable farmers to make intelligent decisions and gain profits. However, incorporating new technologies includes inheriting security and privacy consequences if they are not implemented in a secure manner, and smart farming is not an exception. Therefore, security monitoring is an essential component to be implemented for smart farming. In this paper, we propose a cloud-enabled smart-farm security monitoring framework to monitor device status and sensor anomalies effectively and mitigate security attacks using behavioral patterns. Additionally, a blockchain-based smart-contract application was implemented to securely store security-anomaly information and proactively mitigate similar attacks targeting other farms in the community. We implemented the security-monitoring-framework prototype for smart farms using Arduino Sensor Kit, ESP32, AWS cloud, and the smart contract on the Ethereum Rinkeby Test Network and evaluated network latency to monitor and respond to security events. The performance evaluation of the proposed framework showed that our solution could detect security anomalies within real-time processing time and update the other farm nodes to be aware of the situation.

Keywords: smart contract; AWS cloud; blockchain; IoT security; smart agriculture; security; sensor monitoring



Citation: Chaganti, R.; Varadarajan, V.; Gorantla, V.S.; Gadekallu, T.R.; Ravi, V. Blockchain-Based Cloud-Enabled Security Monitoring Using Internet of Things in Smart Agriculture. *Future Internet* **2022**, *14*, 250. <https://doi.org/10.3390/fi14090250>

Academic Editor: Ishaani Priyadarshini

Received: 28 July 2022

Accepted: 20 August 2022

Published: 24 August 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The surging human population in the world indicates the importance of agriculture and farming to grow and produce food for all the people around the world. Most countries' economies heavily rely on their performance in the agriculture sector [1]. A performance boost in the agriculture sector reinforces a country's economy. However, the profit margins on products and goods obtained by farmers are comparatively less than people working in various other sectors such as computers, construction, education, and more. Consequently, farmers are losing interest in continuing to work in agriculture, as more manpower is required to cultivate goods or food products in the agriculture sector compared to manual work required in many other sectors, and the farmer work incentives are much lower than desired. As a matter of fact, the financial risk associated with agriculture or farming is

also higher due to the direct impact of sudden natural calamities on agriculture if farmers are not prepared for unexpected situations. The emergence of technologies such as the Internet of Things (IoT) changed the landscape of how farming is performed and enhanced operating capabilities in the agriculture sector [2]. The integration of IoT technology within agriculture and farming is termed smart agriculture and smart farming. The global agriculture robot market is predicted to reach USD 15.93 billion by 2028, with an annual compound growth rate of 20.31% during 2021–2028 [3]. The agriculture sector is becoming a soft target for adversaries to launch cyber attacks, as digital infrastructure integration within agriculture is growing and the agriculture economy market is thriving. For instance, a meat processing company, JBS, in food supply suffered a ransomware attack, which resulted in the halting of 13 meat plant operations. The company had to pay USD 11 million dollars ransom to bring back the operations [4]. Therefore, security is considered a massive problem in sectors such as agriculture, and advancement in agriculture security solutions is highly desired.

Smart agriculture and farming may produce high crop yields, and efficient usage of resources to improve productivity [5]. The recent trends in IoT show that smart agriculture is one of the potential applications for IoT for major process improvements [6,7]. Several IoT applications in smart agriculture include soil-state monitoring, pest-control monitoring, crop-growth monitoring, animal-herd monitoring, water-level control, environmental-condition monitoring, and more. Sensor devices are installed on the farm near the premises and surrounding the agriculture area to sense the operating and environmental conditions and convert the sensed analog data into a digital form. Some of the most prominent sensors in smart agriculture include temperature, humidity, light, and pressure and proximity sensors. These sensing devices are connected to the internet through edge gateways or routers to constantly update the sensing information in the cloud. Although communication to the cloud provides data analytics and storage capabilities, a smart device's internet connectivity introduces security and privacy issues. These issues in smart agriculture are not well addressed in the literature [8,9].

The existing security solutions proposed in smart farming and agriculture mostly cover food-supply-chain management [9] and the monitoring of various activities [10] using cloud technologies, ML- and AI-based data-analytic techniques [11], and authentication and authorization solutions for constrained IoT devices [12,13]. Cloud-based monitoring smart agriculture solutions can still have security consequences, if the secured code procedures are not considered during the development and IoT security best practices are not followed. To support the previous statement, we have historically seen that IoT devices exposed to the Internet have been compromised and used as a weapon to perform large-scale denial-of-service attacks or other malicious activities such as manipulating the sensor values to data exposure [14,15]. Therefore, the existing cloud-based solutions or gateway-based security solutions for monitoring smart agriculture applications are not sufficient for providing the full pledged security.

Decentralized applications and storage have security advantages compared to traditional applications and storage in terms of secured events storage, traceability, immutability, and improved security and privacy. Blockchain technology is known to be used for decentralized application development. Apart from blockchain-based digital currency, smart-contract-based applications are popular and used for many applications, including digital identities, financial security, secured storage, and supply chain management [16]. Researchers explored blockchain technology opportunities in resolving IoT security and privacy problems [17], including smart agriculture security. Some of the blockchain applications in smart agriculture are food-production supply-chain management, and secured transaction storage [8,18]. Blockchain enables keeping track of the sequence of events to maintain transparency and, in the end, farmers are fairly treated and gain profits. Considering the blockchain technology advantages in smart agriculture, we were inspired to utilize blockchain technology for implementing a smart farming-security-monitoring solution.

The current security monitoring solutions in smart agriculture either focus on cloud-based options or blockchain technology [10,19]. Furthermore, as discussed earlier, most of the cloud- or blockchain-based solutions mainly address supply-chain issues. The advantages of cloud and blockchain technology can be considered to propose optimal security solutions in smart agriculture. Overall, to overcome the limitations of the existing cloud-based solutions [10] and improve security using blockchain applications, we leveraged a cloud and blockchain solution to constantly process the sensing data in the cloud and store anomalies in blockchain transactions. Additionally, none of the existing solutions provided an end-to-end solution using cloud and blockchain implementation for smart agriculture and evaluating the network latency performance. Therefore, we implemented an end-to-end solution using an Arduino sensor kit with a Wi-Fi module, AWS cloud, and Ethereum smart-contract network for testing real-time application, and evaluated their performance in terms of security, usability, and performance. Ultimately, our contributions to this paper are as follows:

- We implemented an end-to-end smart agriculture security-monitoring prototype using Arduino sensor kit, AWS cloud components, web graphical user interface, and Ethereum smart-contract network.
- We monitored and processed various sensor-type data suitable to generate in a smart-agriculture environment and store the essential monitoring digital data in Ethereum smart contract transactions.
- We presented a cloud- and blockchain-based smart-agriculture architecture, which enables remote monitoring and automation to control the smart-agriculture environment.
- We proposed a smart farmer-community-based monitoring solution to update security alerts to neighbor farmers and disseminate security awareness information across the farming community.
- We evaluated the performance of the proposed architecture and implemented a cloud- and blockchain-based solution and showed that our solution incurs negligible network latency to perform the operations in real time.

The remainder of the paper is organised as follows. Section 2 discusses the background and work related to the proposed work. Section 5 describes the proposed cloud- and blockchain-based architecture for smart-agriculture security alert monitoring. Section 6 shows the implementation of the end-to-end smart agriculture architecture with a discussion of the different components used in the application. Section 8 includes the discussion and future work on the proposed smart-agriculture solution. Section 9 concludes the paper.

2. Background

In this section, an overview of the IoT applications in agriculture, existing cloud-based security solutions in smart agriculture, and the existing blockchain-based security solutions in smart agriculture are discussed.

2.1. IoT Smart-Agriculture Background

IoT technology offers many benefits in agriculture, including improving productivity and high yields [20]. There are number of prior works discussing the role of IoT in agriculture, IoT applications in agriculture and the advantages of IoT in the agriculture field [5,9,10,20–23]. Olakunle et al. [24] presented a review of IoT integration with smart agriculture and data-analytics benefits and challenges. The future trends and opportunities are categorized based on technologies, applications, business, and marketing. Farooq et al. [23] performed a detailed study of the technologies involved when using IoT in smart agriculture. The technologies covering the network protocols, architecture, cloud computing, and big-data analytics were leveraged to discuss the existing works in IoT-based smart agriculture. Additionally, the security issues, the policies proposed by different countries to support smart agriculture, and the existing smart-device-based applications are presented in the article. Othmane et al. [9] presented a review of the various advanced technologies used in IoT-based smart agriculture solutions. Additionally, various smart-

agriculture applications using IoT are categorized in the article. Furthermore, the existing blockchain solutions for supply-chain management in agriculture are discussed. The articles [25,26] discussed the usage of wireless sensor networks to regulate water and monitor water level in agriculture. The authors emphasized that IoT plays a major role in water management. However, those articles focused on specific water-management applications in agriculture.

The authors of [10] performed a survey of different applications used in smart agriculture with technologies, and cloud computing is used as a backend technology stack for application implementation. Amera et al. [5] also performed a survey on using IoT in smart agriculture. The taxonomy is defined using a smart-agriculture architecture and technologies and classified the literature works based on the taxonomy categories. The authors of [20] also reviewed smart agriculture based on IoT architecture, application, software, hardware, principal advantages, and open research and challenges in the future. Brewster et al. [7] highlighted the data governance, security, and privacy requirements and concluded that a cultural shift is needed to adopt the IoT solutions in agriculture. Overall, based on the state-of-the-art IoT-based smart-agriculture survey, we can conclude that IoT can have many applications in agriculture. IoT technology has already been integrated with smart-agriculture applications. However, there are still many challenges and research issues regarding security and privacy, network issues, regulations, scalability, reliability, and resource optimization.

2.2. Cloud Solutions in Smart Agriculture

Cloud-computing integration with smart agriculture is needed to perform the IoT sensing data storage and analytics, including big-data applications. Researchers proposed solutions to address the issues in IoT-based smart agriculture using cloud computing. Nurzaman et al. [2] proposed a fog-computing-based network architecture for smart farming and agriculture to monitor farms and control agriculture operations. The authors introduced a cross-layer-based channel access and routing solution to optimize the network communication connected to smart-farming endpoints. This improved the network latency of the IoT farming devices connected to the cloud. However, the paper did not discuss the security and privacy aspects of IoT-based smart agriculture. Chen et al. [27] presented an IoT platform to cultivate turmeric outdoors for precision agriculture. The author's application enables the farmers to control the turmeric farm with GUI, improving the quality and productivity of the turmeric while maintaining the network latency that approximately matches real-time communication. However, this work is specific to smart-agriculture turmeric-cultivation application implementation. Ref. [28] proposed an intelligent security system to monitor devices in the agriculture field. The authors implemented the system on Raspberry pi 2. The system can communicate data remotely and send SMS alerts to a remote user. However, the work did not consider blockchain technology to create smart contracts and securely store the data when monitoring the devices in agriculture. Li et al. [11] discussed the limitations of using big-data solutions in IoT-based smart agriculture. The authors use the K-means algorithm to perform the agriculture data analytics and highlighted that data is insufficient to apply big-data solutions. Anandarup et al. [29] proposed a method for detecting link failures between local nodes and master nodes and identifying local nodes from the network packets. The MLP hosted in remote nodes is used to test the identification of the nodes. Overall, the literature indicates that cloud solutions benefit the agriculture industry by remotely monitoring and improving productivity in agriculture. However, the cloud-based solutions are prone to data exposures and may lead to security breaches on the cloud service provider if security controls are not properly implemented.

2.3. Blockchain Solutions in IoT Agriculture

Blockchain technology has advantages such as secure storage, anonymity, and transparency. The user identity and private key will not be disclosed in public, although the user's public key and transaction information can be seen in the public blockchain. Some

researchers explored the usage of blockchain technology in IoT applications [19,30–32]. Ferrang et al. [33] described blockchain protocols in IoT and presented threat models to blockchain protocols in IoT. The IoT application domains for blockchain are discussed, and the state of the art of blockchain technologies in the Internet of things are discussed, emphasizing security and privacy. The research challenges and future directions for utilizing blockchain in IoT are discussed. Ref. [8] studied the security and privacy issues in green IoT-based agriculture. The application of blockchain technology in preserving privacy in green IoT-based agriculture is discussed. Anusha et al. [31] performed a literature review of the information-security research progress in blockchain-based smart-agriculture applications. Oscar et al. [32] performed a detailed study of using blockchain in smart agriculture. The authors highlighted that security and privacy issues are one of the main concerns of smart agriculture. The state-of-the-art review on using the blockchain in agriculture [32] described that most of the works focused on solving the food or agriculture supply-chain problem, and secure data storage, remote monitoring, and automation are the least focused on areas in blockchain-enabled smart agriculture. To sum up, the prior blockchain technology in IoT agriculture review articles indicate that blockchain solutions can improve the security and privacy of smart agriculture. However, challenges such as data storage capacity in blockchain and high network connection rates in rural areas to perform consensus activity still need to be addressed in the agriculture application context.

Saikat [12] proposed a blockchain-based IoT architecture for the food supply chain. RFID sensors captured the identification ID from the product package from different stakeholders in the food supply chain and were added to the blockchain to maintain integrity. Any stakeholder can verify the public blockchain data regarding the products' status. Mubariz et al. [34] introduced blockchain-based cloud nodes to verify the service provided by the edge servers for service authentication to IoT devices. The proof-of-authority (POA) mechanism is considered for maintaining the consensus among blockchain cloud nodes. IoT devices give the rating to the edge servers based on the edge-server service provided and used for determining the service authentication. Mohamed et al. [19] explored blockchain technology to implement security solutions and their performance. The authors highlighted that large throughput and storage capacity are the technical challenges in implementing security solutions. Overall, blockchain solutions have been used in the literature to address some issues in smart agriculture.

3. Related Work

In this section, the relevant state of the art is discussed and it is highlighted how our contributions are important in comparison with the existing works.

The authors of [35] implemented a smart contract based on soil- and climate-condition monitoring metrics in smart agriculture. However, a detailed smart-contract implementation are not provided. Moreover, the real-time experiments sensing the agricultural conditions and testing the proposed smart-contract-based metric monitoring are not performed. Ref. [36] discussed Ethereum blockchain-based smart-agriculture supply-chain data solutions. The authors monitored the agriculture sensor data using Ethereum. However, the solution did not mention data storage usage in the cloud. Ref. [37] performed a proof of concept for implementing the Ethereum blockchain solution to store agriculture sensor details. However, the performance of the implemented solution is not determined in their work. Realistic test experiments by setting the sensor devices are also not performed. Caro et al. [38] proposed AgriBlockIoT, a blockchain-based solution for agriculture food supply-chain management. The Ethereum and hyper ledger blockchain-based implementation is performed to store the Agriculture IoT device's data. The authors showed that the Hyperledger latency is much lower than the Ethereum network latency. However, the end-to-end implementation of the Agriculture blockchain, including enabling the sensors to send data in real time, is missing. Additionally, the message network latency to update the transactions in the blockchain is higher. We address those issues and implemented a

more realistic blockchain-based solution to send the sensor alert data as a transaction in blockchain.

The authors of [39] designed a smart-contract-based IoT device-to-device and device-to-gateway authentication mechanism in smart agriculture. The block is formed by the edge server deployed in the IoT environment. The blockchain nodes in the cloud perform the consensus mechanism and add the blocks to the blockchain. A hybrid blockchain hyperledger-sawtooth platform simulates the author's proposed method. Although blockchain and cloud technologies are involved in the author's work, the main focus of their work is on the design of IoT device authentication mechanisms. On the other hand, we focused on monitoring smart agriculture environmental conditions using cloud and blockchain technologies. We implemented an end-to-end production level Ethereum smart-contract solution.

Table 1 compares our work with the prior works using cloud or blockchain technology in smart agriculture. Table 1 shows that prior works either focused on proposing cloud-based smart-agriculture methods or blockchain-based smart-agriculture methods. Cloud-based solutions are required to store sensitive information such as farmer data and environmental-conditions data in the cloud. Securing cloud storage is challenging, as the data is stored in databases or object-based storage solutions. Blockchain-based solutions require decentralized storage, and an agriculture data processing module is necessary to perform the operations on data. A decentralized solution alone is not sufficient to realize the full capabilities of IoT security monitoring using data anomalies. Additionally, none of those prior works implemented end-to-end smart-agriculture monitoring solutions to perform the experiments and evaluate performance and application capabilities. Our work is inspired by the lack of cloud- and blockchain-based solutions for monitoring the smart agriculture environment, whose implementation is realistic while ensuring security when data is processed and stored in the implementation prototype.

Table 1. Our work comparison with the prior state of the art

Authors	Aim of the Paper	Cloud Based	Blockchain Based	Review/ Method
Talavera et al. [22]	Reviewing various IoT applications in agro-industrial and environmental fields	Yes	No	Review
Olakunle et al. [24]	Detailed review of using the Internet of Things (IoT) and data analytics in agriculture	Yes	No	Review
Wen Liang et al. [27]	IoT platform for precision agriculture to cultivate the turmeric in outdoors	Yes	No	Method
Nurzaman et al. [2]	Fog-computing-based network architecture for smart farming and agriculture to monitor the farms	Yes	No	Method
Mohamed et al. [33]	Surveyed the blockchain applications in IoT	No	Yes	Review
Miguel et al. [38]	Blockchain-based solution for food supply chain and digital data storage	No	Yes	Method
Saikat et al. [12]	Blockchain-based IoT architecture for food supply chain	No	Yes	Method
Mubariz et al. [34]	Blockchain-based cloud nodes for the edge servers service authentication	No	Yes	Method
Mohamed et al. [8]	Security and privacy issues in green IoT-based agriculture and blockchain solutions review	Yes	Yes	Review
Voutos et al. [35]	Smart-contract implementation to monitor soil and real-time weather monitoring	No	Yes	Method

Table 1. Cont.

Authors	Aim of the Paper	Cloud Based	Blockchain Based	Review/Method
Pranto et al. [36]	Smart agriculture supply chain using Ethereum blockchain.	No	Yes	Method
Shyamala et al. [37]	Ethereum blockchain for monitoring various sensor data and measure the performance for IoT device	No	Yes	Method
Raj et al. [25]	Regulation of water in agriculture using internet of things	Yes	No	Method
Hassan et al. [21]	Smart-agriculture monitoring factors identified by performing literature review	Yes	No	Review
Our work	Cloud- and blockchain-based security monitoring	Yes	Yes	Method

4. Smart Agriculture, Sensing Technology and Security Attacks

A typical cloud-enabled IoT smart agriculture is shown in Figure 1. The cloud-based architecture is comprised of the IoT device connected to the farms and agricultural land to monitor various physical conditions such as fertilizer usage, proper seed spilling, weather state, food growing quality, and storage environment conditions. Various sensors such as temperature, humidity, and pressure are used to monitor the farming condition. The IoT devices are connected to the common gateway to pass the state information to the third-party cloud vendor, who provides the product services. The gateway can be a generic or dedicated router designed for the smart farm. The cloud provider can be any primary service provider such as AWS, Google Cloud, Microsoft Azure, or a self-managed cloud. The gateway is connected to the cloud resources to process the IoT device requests.

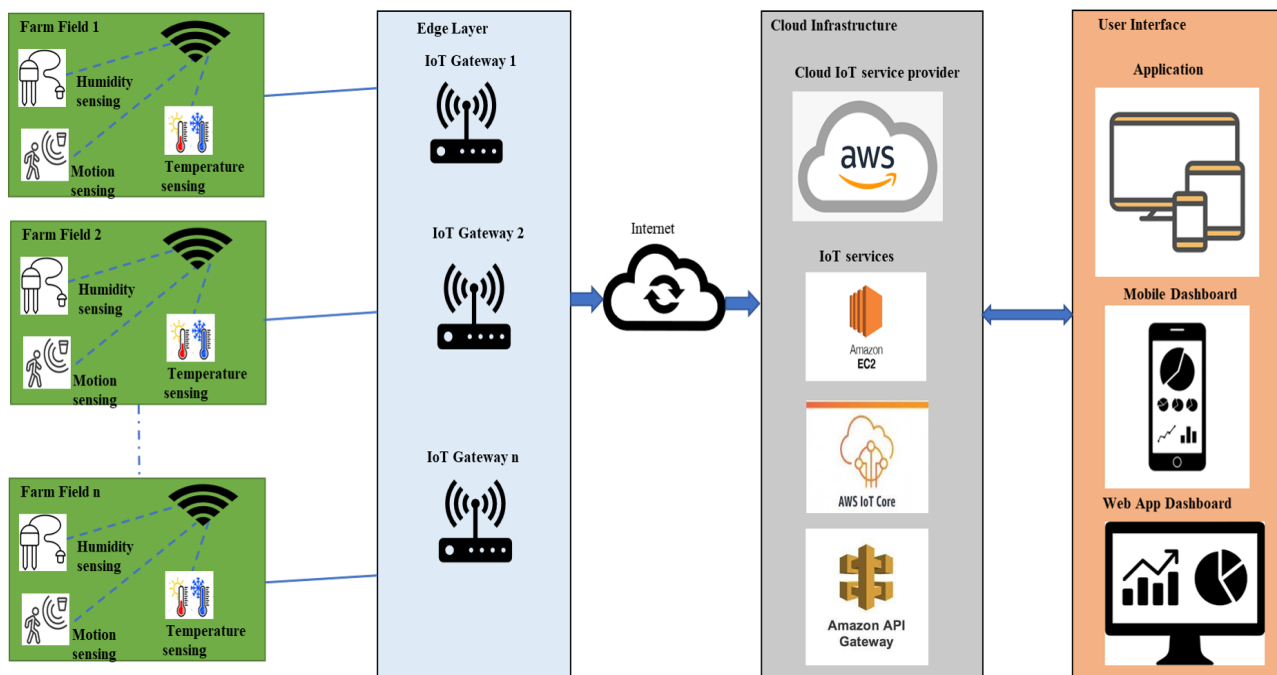


Figure 1. Cloud-based IoT smart-agriculture application.

Table 2 describes the various IoT sensors and their applications in smart agriculture.

Temperature sensor: The sensor detects temperature changes within the application. The water temperature, the surrounding-air temperature, and plant temperature-monitoring 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 water

consumption 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 monitoring can help the farmers to take precautions and effectively grow plants.

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 2. Smart-agriculture sensors and their applications.

Sensor Type	Smart Agriculture Application	Sensor Input
Temperature	Plants, air, water	Heat energy
Humidity	Air, water, crop, plant	Humidity of the surrounding air
Camera	Storage area or farm monitor	Photon detection
Light	Fields, crop	Light or radiant energy
Accelerometer	Smart-agriculture equipment maintenance	Electromechanical
pH	Soil nutrient deficiencies, presence of unwanted chemicals	Electrochemical
GPS	Keeping track of flocks, highly precise agriculture vehicle guidance	Measuring the distance using satellite technology
Dielectric soil moisture	Water moisture in soil	Dielectric constant measurements
Pressure	Atmospheric pressure in air	Physical pressure
Passive Infrared	Track individuals' movement	Motion detection

The IoT attack surface in smart agriculture opens up a new range of cyber attacks, and few security protection capabilities can be embedded into IoT devices due to processing and memory limitations. Therefore, we may need to rely on gateway- or network-level security detection and protection mechanisms. In this work, we try to address the following attacks using IoT status and anomaly data monitoring solutions.

Denial of service (DoS): An adversary may send malicious network traffic to the victim farmer network to shut down the services, including the sensor devices and routers connected to the network. This may interrupt the operations if we consider that these devices are used for food supply-chain applications. The attack might also originate from diverse source IP addresses, making it difficult to detect and block the attack traffic. DoS attack scenarios in IoT include consuming the IoT device resources, IoT device and gateway communication bottlenecks, or flooded the gateway with malicious attack traffic.

Physical security attacks: Intruders trespass on the agriculture fields and farm premises to destroy the property or with other bad intents such as theft, arson, etc. The camera sensors installed on the farm premises send the data to monitor and alert the farm owners when physical attacks happen in smart agriculture. An adversary may also visit the farm site to install or compromise the farm network.

Sensing-data-manipulation attack: The IoT sensor-data manipulation with malintent prior to going to the destination is another kind of attack seen in IoT. The adversary may perform a man-in-the-middle attack to read the data passing through the communication channel and embed malicious data to perform the attacks. A zero-day vulnerability in the IoT devices can also be exploited to compromise the sensor device and fake the sensor data to hide the malicious activity. There are various ways to get into the network and manipulate the data unless we have good security controls covering the data-link-layer to application-layer protocols.

5. Proposed Approach

The proposed approach improves smart agriculture/farming monitoring and security by incorporating technologies in multi layers of the smart-agriculture architecture. Internet of Things (IoT) technology was added near farming premises to connect with the internet and add intelligence. Cloud technology is used in the data processing layer to support the solution's scalability and achieve production-level performance. The Ethereum blockchain is used in another layer to run the smart contract and trigger events when anomalies are identified during the smart-agriculture security monitoring.

Figure 2 illustrates the layer-wise architecture of the proposed approach. The smart-farm layer contains various sensor devices in the farming premises for different purposes. A smart-agriculture community is formed with IoT sensor devices installed on every piece of farmland. These sensor devices constantly generate events such as device health, device data, etc. The generated events are transmitted to the cloud using an edge gateway or routing device connected to the sensor device. The cloud layer consists of components constantly listening to the sensor events and processing the event data to retrieve the intended information. MQTT is the typical protocol for passing the data in packets from one end to the other. We defined a lambda function in the AWS cloud to parse the data from the AWS IoT core component and extract the required data from the sensor devices connected to the farms. Whenever the lambda function logic determines the security alert observed from the sensor generating data, the lambda function performs POST request infura API to update the Ethereum blockchain. The updated transaction may include the sensor data anomaly values, status of the device, etc. The blockchain contains Ethereum nodes distributed across the network operated by an individual to perform the mining, or someone uses the Ethereum full node for their transaction processing. The infura runs Ethereum nodes and provides APIs to update the transactions from the user's accounts if they have an account with them. The updated blockchain transactions will be updated to all the nodes in the Ethereum network. Although the user layer is not shown in Figure 2, the GUI interface can read the Ethereum node transactions using API calls and display the details in the GUI when the user wants to see the smart-agriculture alerts.

The description of the main components used in the proposed approach is discussed in the following paragraph.

AWS IoT core: A number of IoT sensing devices exist in the smart-farming environment. An IoT message-processing infrastructure is needed to support the IoT message protocols such as MQTT and accommodates the network bandwidth to collect messages from numerous IoT devices. We selected AWS IoT core service to perform the smart-agriculture IoT data processing. The AWS IoT core offers low latency and high throughput performance, and these characteristics support the build of real-time production-level IoT monitoring systems.

AWS Lambda: The collected IoT data should be processed and given as input data to the Ethereum blockchain. Therefore, the AWS Lambda runs the code in the backend and stores the smart-farming information in the Blockchain. AWS Lambda is a serverless computing service to run code virtually without provisioning the server infrastructure.

Infura API: We did not rely on deploying the Ethereum full node to create and run the farming smart contracts. Infura is an Ethereum API service to run smart contracts in

Ethereum nodes and perform Ethereum-based transactions. We leverage the Infura API calls to interact with Ethereum nodes once we collect and process the farming sensor data.

Ethereum: We implement the Ethereum-based smart contract to store the farming sensor data and check the farming environment conditions. The Ethereum first version works on the proof-of-stake (POS) consensus mechanism to approve and add the transactions to the Ethereum blockchain. A Web3 frontend application is implemented to review and alert the farmers when security events are detected.

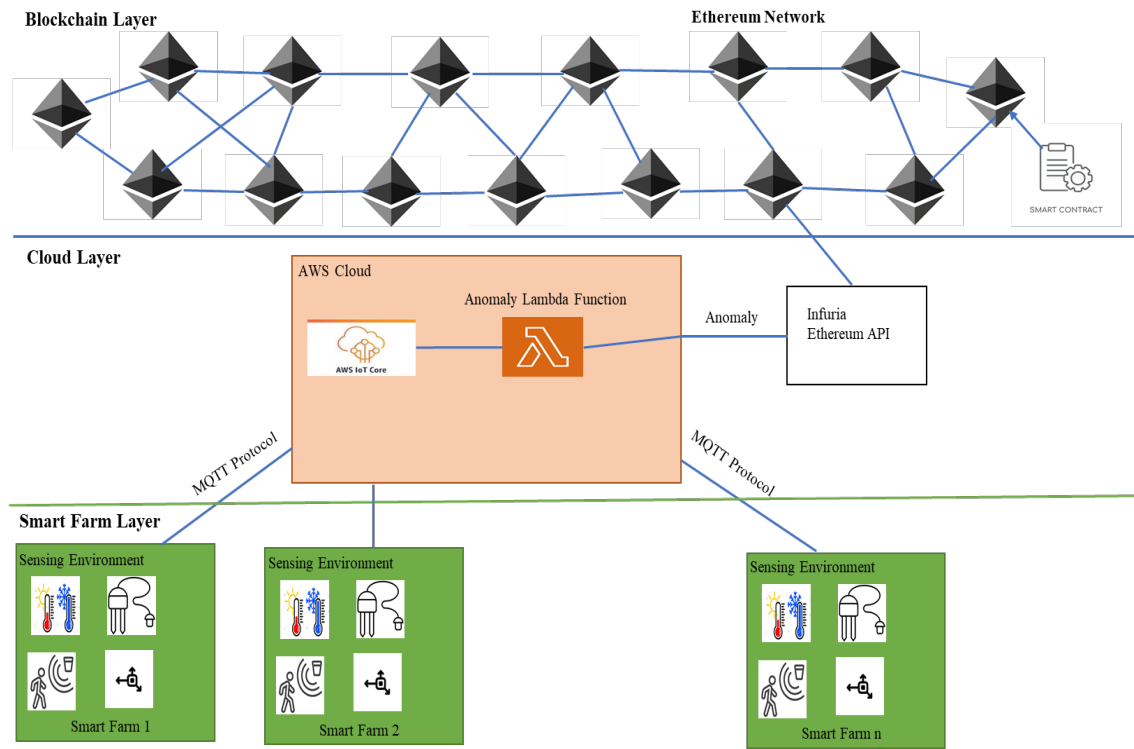


Figure 2. Blockchain cloud-based smart-agriculture application.

Advantages of our proposed approach: Our solution inherits the advantage of secured data storage using blockchain. It includes only the authorized farming owners who can see the smart-farming records. The cloud-based data storage poses the security risks of data breaches due to misconfigured access controls. The blockchain allows secured storage of records and no storage maintenance cost. Our solution is scalable in the cloud and offer solutions to various security use cases in smart agriculture

The immutability of the blockchain transaction alert data can be used as evidence for legal proceedings, insurance claims for protecting the farmer's agriculture assets and property, and backing up the security investigation data without data corruption. For instance, natural disasters may have a severe impact on agriculture fields. Evidence of when, what, where, and how can be captured as blockchain transaction data and used for insurance claims. The farms cannot deny the ownership of the transaction once the transaction is added to the blockchain. This property may be used to identify malintent farmer activity and maintain transparency. Some of the smart-agriculture use cases of the proposed approach are discussed below.

Sensor health status: The sensors should constantly monitor the physical conditions in the agricultural land and farms and send this data to the farmers or crop owners to effectively manage the farms for high yield, low loss, and better productivity. The sensors/actuators must work continuously to obtain updates regularly. Sensors are targeted with passive and active attacks. Therefore, the health status monitoring of these device sensors is essential and continuously monitored. The farmer should be notified within a

mobile application whenever the device's health status is off. Then, the farmer may find the root cause and fix the issue.

Sensor data anomalies: Sensor data irregularities can be flagged for attention and to look for anomalies. A threshold can be set up to trigger the alert and monitor the smart-agriculture applications. For instance, the temperature of the farming storage unit is constantly monitored to store commodities safely. A temperature sensor is installed on the storage unit and monitors the storage-unit temperature. Whenever the temperature exceeds the threshold temperature, our blockchain-based monitoring solution sends an alert to the storage unit owner. Similarly, the image sensor installed near the storage unit is used to identify moving objects. An image-processing technique was applied to detect unauthorized access to the storage unit facility. The cloud resources incorporated in our solution can process the images and produce the output.

Community farming blockchain: The crop productivity or quality impact on any single farm may gradually affect other farms in the community or nearby farms in the surrounding area. The effect can be due to the infection of bugs, severe weather disturbing the crop's life cycle or more. Communication of this information to the community farmers may save their crops from infection and stop the infection from spreading. Therefore, the blockchain-based community can use this as a farm blockchain for sharing the latest updates among the farmers and keep connected to be aware of what is happening on the surrounding people's farms for awareness. For instance, a burglar with unauthorized farmland storage access can be reported to the farmers around the premises using the proposed blockchain-based application. The number of applications are numerous using the smart-farm community blockchain.

6. Implementation

In order to evaluate the proposed smart-agriculture security monitoring approach using blockchain and cloud technologies, we implemented a prototype using the Arduino Sensor kit with Wi-Fi capabilities to mimic the various sensors deployed in the farmland, AWS cloud components to process the sensor data, Ethereum blockchain to store the monitoring alerts and other essential information using smart contracts, and developed a web frontend to display the alerts to the users.

Experimental setup: The following software or hardware components such as Arduino sensor kit, EP8266 Wi-Fi module, AWS IoT core component, AWS lambda function, infura Ethereum API Account, and Web Javascript were used to perform the experiments. The Arduino module with Wi-Fi was connected to the home Wi-Fi router for communicating to the cloud. Our security monitoring application can be developed as a product or third-party security monitoring tools for smart-agriculture IoT device's security.

Arduino sensor kit contains Potentiometer, light sensor, sound sensor, air pressure sensor, temperature sensor, and accelerometer sensor to monitor and capture various environmental, physical, and other conditions. The breadboard is used to connect these sensor devices to the communication equipment, i.e., Wi-Fi module. The Wi-Fi module also acts as edge gateway for all the sensor devices mentioned in our experimental setup. The Arduino C language code was written to connect the Wi-Fi module with the home router, and external communication to the remote AWS IoT nodes for event updates. The SSID and password key details of the Wi-Fi home router are provided in the Arduino to connect to the internet. The AWS IoT core service is created in AWS Cloud with few generic configuration settings. The AWS IoT core runs on the Free RTOS operating systems for IoT-device data processing and exchanging the data using the MQTT protocol. The AWS IOT core could display the sensor device data and can be stored in cloud storage such as S3. The AWS Lambda function was written in JavaScript programming language to constantly poll the sensor-events' data from AWS core. The monitoring logic is implemented in the AWS lambda function to identify the sensor status and sensor data anomalies. The infura API calls were also performed using the AWS lambda function to update the sensor monitoring data for permanent storage in the blockchain. The infura account is needed to generate

the API key and establish a connection to the Ethereum network. Therefore, the alert data is updated to the blockchain and stored in the transaction. To implement the end-to-end application, the infura API calls are used to retrieve the alert transaction from the Ethereum blockchain. The farmer may download the mobile application or web app to monitor the farm alerts remotely.

Figure 3 displays the Arduino microcontroller used to control and connect to the IoT sensing devices. The temperature sensor and humidity and light sensor are connected to the microcontroller, and the microcontroller supports a Wi-Fi connection to communicate with cloud services. The sensors can be considered as agriculture application end devices. As shown in Figure 3, the temperature and light sensor positive terminals such as A3, and D3 are connected to the microcontroller PINS. The negative terminals are grounded to prevent short-circuiting issues. The microcontroller is power supplied with 5V, which is shown in Figure 3 with a red wire connection.

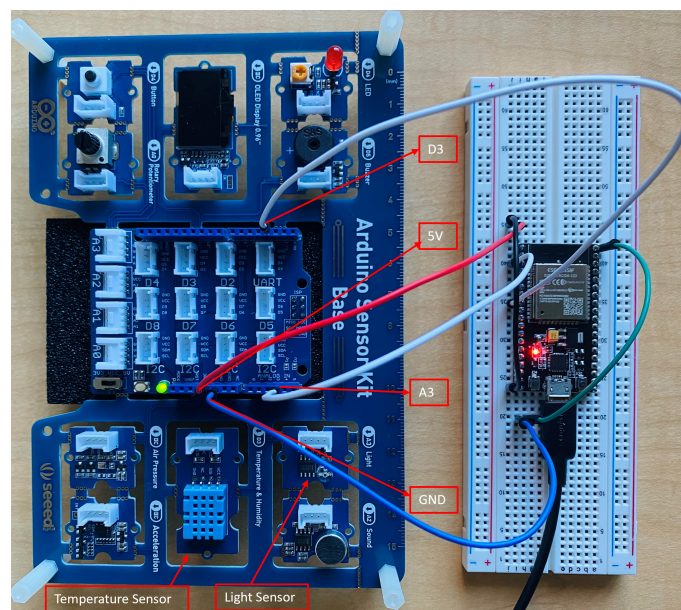


Figure 3. Arduino sensor kit to sense the environment.

As shown in Figure 4, the sensing device's status will be monitored using the desktop application. The Arduino controller is connected to the laptop via wired communication. The sensor measures real-time activity such as temperature and light in the farming. We installed the Arduino software application on the laptop machine to run the C code on the Arduino kit. The code comprises the WIFI connection credentials; AWS IoT Core connection requirements such as Client ID, AWS Host URL; and the MQTT topic name and the programming logic to read the sensor data as an MQTT topic and publish the MQTT topic in the AWS IoT cloud using the network connection. The code is dumped on the Arduino micro-controller to run the application and post the data in AWS IoT Cloud. Figure 4 displays the print statements indicating the Arduino kit connected to the author's home WIFI network "maverickcreek-7-709" and initiating a connection to the AWS Cloud. Once it is connected to the AWS, the sensor data is published as an MQTT topic with values temperature: 26, light: 26, and humidity: 51. The data publish-success message can also be seen in the Figure 4.

```

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 connection 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.
09:37:39.241 ->
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. Sensor devices connected to Wi-Fi and initializing connection to AWS Cloud.

The MQTT publish messages and can also log in to the AWS IoT Core. Figure 5 displays the published IoT sensor data in the AWS Cloud. As seen in Figures 4 and 5, the data publication time in the IoT core cloud is 2 s. The highlighted red boxes in Figure 5 indicate the timestamp and sensing temperature, humidity, and light values in the Arduino kit environment.

```

▼ $aws/things/smartAgriculture/shadow/name/Temp_Humidity
September 26, 2021, 09:38:19 (UTC-0500)

{
  "temp": 26.2,
  "hum": 53,
  "light": 79
}

▼ $aws/things/smartAgriculture/shadow/name/Temp_Humidity
September 26, 2021, 09:37:59 (UTC-0500)

{
  "temp": 26.2,
  "hum": 51,
  "light": 41
}

▼ $aws/things/smartAgriculture/shadow/name/Temp_Humidity
September 26, 2021, 09:37:51 (UTC-0500)

{
  "temp": 26,
  "hum": 53,
  "light": 76
}

```

Figure 5. Sensor data real time recording in AWS Cloud-IoT core service.

The AWS lambda function written in JavaScript reads the AWS IoT Core published data and compares the sensor threshold values for anomaly detection. The code may trigger a sensor device health alert if the data is not received for a specific time interval. To interact with the Ethereum blockchain, the Infura API credentials are stored as variables, and the AWS lambda function reads the credentials to connect with Infura maintained Ethereum main node. The metamask application is used for the software wallet and to interact with the Ethereum blockchain. The wallet details are also provided in the AWS lambda function to perform the transactions in Ethereum. The smart-contract code is written using solidity programming language and sends the alert triggered data as a transaction in the Ethereum blockchain. Figure 6 shows the Ethereum transaction details when the

temperature-threshold-exceeded alert is seen in the AWS IoT core. The transactions include the block number, from and to address, transaction fee, gas price, and timestamp. Based on the timestamps observed in the end-to-end blockchain- and cloud-based implementation, we determined that the time to update the farmer when the agriculture environment anomaly alerts trigger is 9 s. The Ethereum transaction completion time is 7 s. However, we used the Rinkeby testing network to test the Ethereum network, and the overall alert notification network latency will not be the same in the Ethereum production network. Overall, we prove that network latency is minimal when performing agriculture security monitoring using blockchain and cloud services and alerting the farmers.

Transaction Details		
Overview	Logs (1)	Access List State
[This is a Rinkeby Testnet transaction only]		
Transaction Hash:	0x599584b8af7e839d40701c0ced031b0875d10003b8d113810fcc3b28172609c6	
Status:	Success	
Block:	9360680	88 Block Confirmations
Timestamp:	22 mins ago (Sep-26-2021 02:37:58 PM +UTC)	
From:	0x46a1be93a7940252692c47d8201d307be023891	
To:	Contract 0x001aed30b8dabb3e7ccc7a4cb06ad341151ea390	
Value:	0 Ether (\$0.00)	
Transaction Fee:	0.00179555 Ether (\$0.00)	
Gas Price:	0.00000005 Ether (50 Gwei)	
Txn Type:	2 (EIP-1559)	

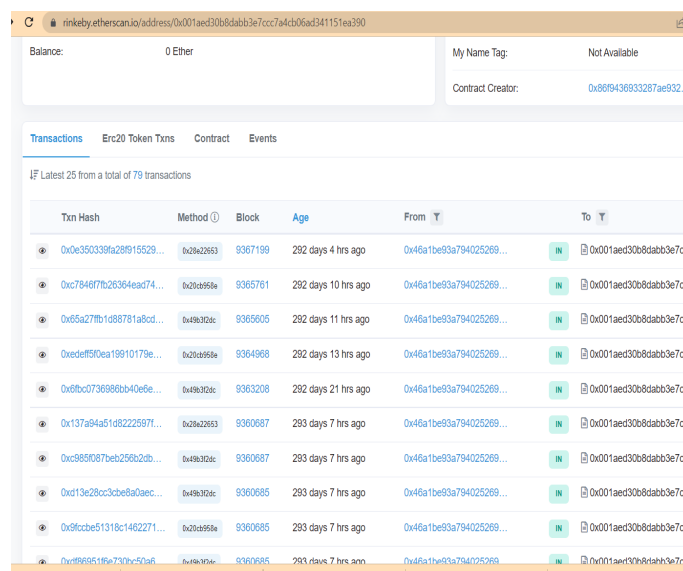
Figure 6. Ethereum smart-contract transaction details.

Figure 7 indicates the data field format in the Ethereum transaction. The sensor threshold value, current value, and alert message are stored in the data transaction. This data will not be tampered with and will be stored securely in the blockchain. The boxes highlighted in red clearly show that the temperature value of 25 does not exceed the threshold value of 26.

[illegible]

Figure 7. Ethereum smart-contract transaction storing the sensor data.

The experimental transaction performed on the rinkeby network can be seen publicly for reader understanding. Figure 8 displays the list of transactions stored in the Ethereum test network. The from and to address, transaction hash value, and the block ID can be seen for each transaction. The details of the transaction can be explored by browsing the URL “<https://rinkeby.etherscan.io/address/0x001aed30b8dabb3e7ccc7a4cb06ad341151ea390> (accessed on 19 August 2022)”.



Txn Hash	Method	Block	Age	From	To
0x0e350339fa28915529...	0x28a2653	9367199	292 days 4 hrs ago	0x46a1be93a794025269...	0x001aed30b8dabb3e7c...
0xc7846f7b26364ead74...	0x28a2653	9367161	292 days 10 hrs ago	0x46a1be93a794025269...	0x001aed30b8dabb3e7c...
0x65a277b1d88781a8cd...	0x4930dc	9365605	292 days 11 hrs ago	0x46a1be93a794025269...	0x001aed30b8dabb3e7c...
0xede5f50dea19910179e...	0x28a2653	9364968	292 days 13 hrs ago	0x46a1be93a794025269...	0x001aed30b8dabb3e7c...
0x8bdc736986bb40e6e...	0x4930dc	9363208	292 days 21 hrs ago	0x46a1be93a794025269...	0x001aed30b8dabb3e7c...
0x137a94a51d2225971...	0x28a2653	9360687	293 days 7 hrs ago	0x46a1be93a794025269...	0x001aed30b8dabb3e7c...
0xc985087beb256b2db...	0x4930dc	9360687	293 days 7 hrs ago	0x46a1be93a794025269...	0x001aed30b8dabb3e7c...
0xd13e28cc3cbe8a0aec...	0x4930dc	9360685	293 days 7 hrs ago	0x46a1be93a794025269...	0x001aed30b8dabb3e7c...
0x9fcbce51318c1462271...	0x28a2653	9360685	293 days 7 hrs ago	0x46a1be93a794025269...	0x001aed30b8dabb3e7c...
0xc985087beb256b2db...	0x4930dc	9360685	293 days 7 hrs ago	0x46a1be93a794025269...	0x001aed30b8dabb3e7c...

Figure 8. Rinkeby Ethereum test-network transactions.

We developed the web frontend application to receive the agriculture security alerts such as anomaly and device-status alerts. The frontend application displays the alert notifications in the form of Ethereum transactions. Figure 9 displays the alert notifications with details about the sensor data and policy violations. For example, block number 9363208 in Figure 9 notifies the farmer regarding the temperature variations in the monitoring environment. When the temperature exceeded the threshold value, the policy violation message was displayed on the frontend test web application. We used vercel web platform to develop our test web application. The web URL “<https://smart-agriculture.vercel.app> (accessed on 19 August 2022)” shows the live experimental data obtained from our smart agriculture end-to-end application.

A user might also want to update the transactions using the frontend application. For instance, the user needs to store the sensing-device anomaly data for future reference purposes. We integrated this functionality into the frontend web app to update the violated sensing data conditions into the blockchain. Figure 10 shows the frontend web application with interactive options to update the transactions in the Ethereum test network. This feature helps the farmer or the web-application operating user to control the blockchain platform used for agriculture security monitoring.

To add a new transaction using the web frontend, the user should be connected to their wallet and fill in the transaction details. The temperature, humidity, and light sensor values and their optimum values are entered and those values submitted using a web application. The infura API is connected with the blockchain node and adds a new transaction when the setup sensor data policies are violated. The other users can see the transaction data once the transaction is updated into the blockchain.

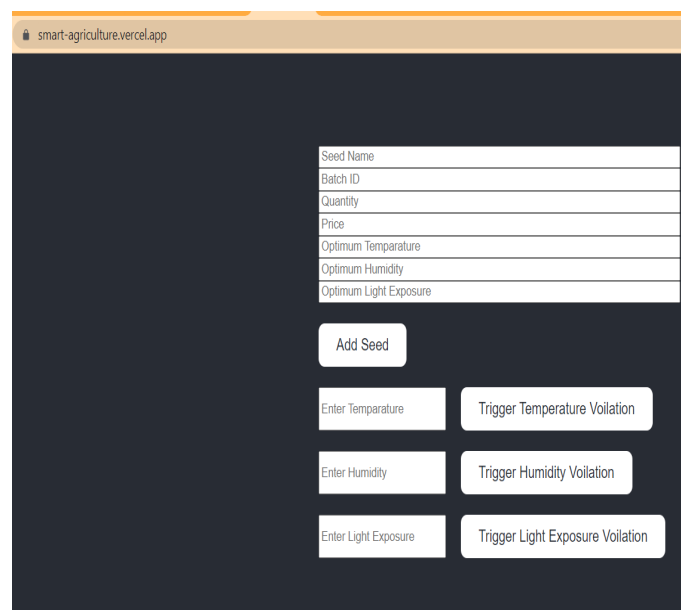


smart-agriculture.vercel.app

You need a crypto wallet installed as a browser extension to add seed or to trigger violations

Block Number	Voilation Type	Voilation Message	Actual Value	Optimum
9367199	HummidityViolation	Hummidity is over the threshold	100	60
9365761	LightExposureViolation	Light exposure is below the threshold	11	38
9365605	TemperatureViolation	Temparature is below the threshold	1	25
9364968	LightExposureViolation	Light exposure is over the threshold	112	38
9363208	TemperatureViolation	Temparature is over the threshold	26	25
9360687	TemperatureViolation	Temparature is over the threshold	26	25
9360687	HummidityViolation	Hummidity is below the threshold	53	60
9360685	TemperatureViolation	Temparature is over the threshold	26	25
9360685	TemperatureViolation	Temparature is over the threshold	26	25
9360685	LightExposureViolation	Light exposure is over the threshold	69	38
9360684	TemperatureViolation	Temparature is over the threshold	26	25

Figure 9. Smart-contract web-application frontend—alert notifications.



smart-agriculture.vercel.app

Seed Name

Batch ID

Quantity

Price

Optimum Temperature

Optimum Humidity

Optimum Light Exposure

Add Seed

Enter Temperature

Trigger Temperature Voilation

Enter Humidity

Trigger Humidity Voilation

Enter Light Exposure

Trigger Light Exposure Voilation

Figure 10. Smart-contract web application—frontend GUI.

Our blockchain solution can be used on the farming community blockchain platform. As shown in Figure 10, a farmer can update the real-time agriculture environment condition to fellow farmers so that fellow farmers do not have to visit the farming location and can effectively make decisions from home to perform daily agriculture and farming operations. Although we only used three sensors to test our prototype, our solution can be easily tweaked to support processing multi-sensor data and our implementation used for various IoT applications.

7. Performance Evaluation

Monitoring system performance: The end-to-end system performance needs to be evaluated to estimate the solution's effectiveness. The network latency and throughput are the indicators seen in the literature as performance factors for blockchain-based applications. The time taken to receive the sensor alert when an anomaly occurs in the sensor environment directly indicates the network latency. Our test results on Rinkeby show that

the network latency is a few seconds. The network throughput was not tested using our implementation due to the infura API free-access limitation.

Performance comparison with existing works: Our solution performance is compared with the existing works using blockchain in smart contracts. Although none of the existing works implemented the end-to-end solutions with AWS cloud and smart contracts, we included the closely related smart-contract implementation for smart agriculture. Table 3 depicts the message network latency comparison of our work with existing works. The authors [38] implemented Ethereum-based smart contracts to update the IoT sensing data to the blockchain and evaluated the network latency of issuing a transaction in the blockchain. The authors reported a total network latency of 16.55 s. This work is closely related to our work in terms of adding the IoT sensor data into the blockchain. Our solution performed much better than the work [38] because we used real-time implementation applications, including IoT core and smart contracts using Infura API. The additional latency in [38] can also be caused by the blockchain node running in the virtual machine. The work [27] performed simulations to test the IoT devices sending updates to the blockchain and estimated the network latency. They considered 4G as a communication medium to model the communication link and obtained less than 0.2 s latency. We utilized the home WiFi to perform the experiments and obtained the matchable performance with [27]. The authors [34] also used Ethereum to build the agriculture smart contract. The authors reported that it took 272 s to complete one transaction. The high network latency may be caused by the usage of the real Ethereum network. Our solution reported a total network latency of 0.11 s, which is real-time alert reporting. We also determined the mean time to detect (MTTD) when the 95% confidence interval is used. The MTTD is reported as 0.115 with a margin of error of 0.00919 and a standard deviation of 0.016.

Table 3. Performance comparison with existing works.

Authors	Implementation	Device-to-Cloud Latency (Second)	Cloud-to-Blockchain Latency (Second)	Blockchain-to-Client-Console Latency (Second)	Alert Total Latency (Second)
[38]	Ethereum	-	-	-	16.55 *
[27]	Simulations	<0.02 (4G)	-	-	-
[34]	Ethereum	-	272 *	-	-
[37]	Ethereum	4	-	-	-
Our Work	Ethereum	0.02 (Wifi)	0.07	0.02	0.11

*—partially matches our work.

8. Discussion, Limitations and Future Work

We implemented a real-time scenario agriculture security-monitoring system, which monitors the sensor device's health status and sensor anomalies to perform precision agriculture and productive farming. However, we did not deploy the sensors in the agriculture field to capture the farmland environment conditions. We envision that the network latency will be negligible, considering the wide spread of the internet in rural areas. Our solution can even monitor the agricultural conditions in rural areas as long as an internet connection is available.

We did not implement the IoT gateway in our work. We used the home router as an IoT gateway and connected the IoT sensor devices to the network via home WiFi. This is one of the limitations of our work. Implementing an IoT network with an IoT gateway and various sensing devices to mimic the realistic smart-agriculture environment is one of the extensions of our work.

The current implementation only works on the Ethereum proof-of-work (POW) consensus mechanism blockchain. One future work will be implementing the current solution in the Ethereum 2.0 network, which is supported by the proof-of-stake (POS) consensus.

There are numerous IoT applications to monitor the IoT environment, including agriculture applications, smart homes, smart health, smart transportation applications, etc. Therefore, we envision our prototype will also be used to implement the monitoring solutions in other fields.

The network traffic can be collected from a smart-agriculture edge gateway and store the network events data in the cloud. The network events can be used to apply machine-learning and deep-learning techniques and identify the anomaly network traffic in a smart-agriculture network. One future work will be implementing ML- and DL-based network-security monitoring solutions in smart agriculture and using blockchain to store the network anomaly events as transactions.

The production Ethereum blockchain gas price is high. Therefore, blockchain technologies such as Cardano and Solano-based blockchain implementation are considered to design low network-latency applications and reduce the end user/farmer transaction cost in smart agriculture.

9. Conclusions

In this 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, web application GUI, and the Ethereum blockchain smart contract to alert the farmers of security anomalies and sensor-device status. The prototype was able to alert the farmers in real-time, allow remote monitoring of the farm and agriculture environment, and enable the farming community to communicate via blockchain. The performance evaluation in terms of network latency is shown to be nominal with our prototype and it could be stated that the delay can even be reduced with the implementation of high-performance transaction blockchain technologies such as Cardano. We discussed the limitations and future opportunities to improve the security of smart agriculture.

Author Contributions: Conceptualization, R.C. and V.S.G.; Data curation, R.C., V.S.G. and V.R.; Formal analysis, V.S.G.; Funding acquisition, V.V.; Investigation, R.C., V.S.G. and V.R.; Methodology, R.C. and V.S.G.; Project administration, V.V.; Resources, R.C. and V.R.; Software, R.C. and V.S.G.; Supervision, V.V. and T.G.R.; Validation, R.C.; Visualization, V.S.G.; Writing—original draft, R.C.; Writing—review & editing, T.R.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Dutta, S. Top 25 Agricultural Producing Countries in the World. 2020. Available online: <https://www.yahoo.com/video/top-20-agricultural-producing-countries-151350776.html?guccounter=1> (accessed on 15 July 2022).
2. Ahmed, N.; De, D.; Hussain, I. Internet of Things (IoT) for smart precision agriculture and farming in rural areas. *IEEE Internet Things J.* **2018**, *5*, 4890–4899. [CrossRef]
3. Steve, C. Cyber Threats Are a Real Threat to Modern Agriculture's Expanding Digital Infrastructure | AgWeb. 2022. Available online: <https://www.agweb.com/news/business/technology/cyber-threats-are-real-threat-modern-agricultures-expanding-digital> (accessed on 13 August 2022).
4. 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/> (accessed on 13 August 2022).
5. Badran, A.I.; Kashmoola, M.Y. Smart Agriculture Using Internet of Things: A Survey. In Proceedings of the 1st International Multi-Disciplinary Conference Theme: Sustainable Development and Smart Planning, IMDC-SDSP, Cyperspace, 28–30 June 2020; p. 10.

6. Baskar, C.; Balasubramanian, C.; Manivannan, D. Establishment of light weight cryptography for resource constraint environment using FPGA. *Procedia Comput. Sci.* **2016**, *78*, 165–171. [\[CrossRef\]](#)
7. Brewster, C.; Roussaki, I.; Kalatzis, N.; Doolin, K.; Ellis, K. IoT in agriculture: Designing a Europe-wide large-scale pilot. *IEEE Commun. Mag.* **2017**, *55*, 26–33. [\[CrossRef\]](#)
8. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. *IEEE Access* **2020**, *8*, 32031–32053. [\[CrossRef\]](#)
9. Friha, O.; Ferrag, M.A.; Shu, L.; Maglaras, L.A.; Wang, X. Internet of Things for the Future of Smart Agriculture: A Comprehensive Survey of Emerging Technologies. *IEEE CAA J. Autom. Sin.* **2021**, *8*, 718–752. [\[CrossRef\]](#)
10. Mekala, M.S.; Viswanathan, P. A Survey: Smart agriculture IoT with cloud computing. In Proceedings of the 2017 international conference on microelectronic devices, circuits and systems (ICMDCS), Vellore, India, 10–12 August 2017; pp. 1–7.
11. Li, C.; Niu, B. Design of smart agriculture based on big data and Internet of things. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 1550147720917065. [\[CrossRef\]](#)
12. 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. [\[CrossRef\]](#)
13. Song, T.; Li, R.; Mei, B.; Yu, J.; Xing, X.; Cheng, X. A privacy preserving communication protocol for IoT applications in smart homes. *IEEE Internet Things J.* **2017**, *4*, 1844–1852. [\[CrossRef\]](#)
14. Chaganti, R.; Gupta, D.; Vemprala, N. Intelligent network layer for cyber-physical systems security. *Int. J. Smart Secur. Technol. (IJSST)* **2021**, *8*, 42–58. [\[CrossRef\]](#)
15. Chaganti, R.; Ravi, V.; Pham, T.D. Deep Learning based Cross Architecture Internet of Things malware Detection and Classification. *Comput. Secur.* **2022**, *120*, 102779. [\[CrossRef\]](#)
16. Geroni, D. Top 12 Smart Contract Use Cases—101 Blockchains. 2021. Available online: <https://101blockchains.com/smart-contract-use-cases/> (accessed on 16 July 2022).
17. Chaganti, R.; Bhushan, B.; Ravi, V. The role of Blockchain in DDoS attacks mitigation: Techniques, open challenges and future directions. *arXiv* **2022**, arXiv:2202.03617.
18. Li, X.; Wang, D.; Li, M. Convenience analysis of sustainable E-agriculture based on blockchain technology. *J. Clean. Prod.* **2020**, *271*, 122503. [\[CrossRef\]](#)
19. 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. [\[CrossRef\]](#)
20. Sinha, B.B.; Dhanalakshmi, R. Recent advancements and challenges of Internet of Things in smart agriculture: A survey. *Future Gener. Comput. Syst.* **2022**, *126*, 169–184. [\[CrossRef\]](#)
21. Hassan, S.I.; Alam, M.M.; Illahi, U.; Al Ghamdi, M.A.; Almotiri, S.H.; Su’ud, M.M. A systematic review on monitoring and advanced control strategies in smart agriculture. *IEEE Access* **2021**, *9*, 32517–32548. [\[CrossRef\]](#)
22. Talavera, J.M.; Tobón, L.E.; Gómez, J.A.; Culman, M.A.; Aranda, J.M.; Parra, D.T.; Quiroz, L.A.; Hoyos, A.; Garreta, L.E. Review of IoT applications in agro-industrial and environmental fields. *Comput. Electron. Agric.* **2017**, *142*, 283–297. [\[CrossRef\]](#)
23. 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. [\[CrossRef\]](#)
24. 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. [\[CrossRef\]](#)
25. hari Ram, V.V.; Vishal, H.; Dhanalakshmi, S.; Vidya, P.M. Regulation of water in agriculture field using Internet Of Things. In Proceedings of the 2015 IEEE Technological Innovation in ICT for Agriculture and Rural Development (TIAR), Chennai, India, 10–12 July 2015; pp. 112–115.
26. Postolache, O.; Pereira, M.; Girão, P. Sensor network for environment monitoring: Water quality case study. In Proceedings of the 4th Symposium on Environmental Instrumentation and Measurements 2013, Lecce, Italy, 3–4 June 2013; pp. 30–34.
27. Chen, W.L.; Lin, Y.B.; Lin, Y.W.; Chen, R.; Liao, J.K.; Ng, F.L.; Chan, Y.Y.; Liu, Y.C.; Wang, C.C.; Chiu, C.H.; et al. AgriTalk: IoT for precision soil farming of turmeric cultivation. *IEEE Internet Things J.* **2019**, *6*, 5209–5223. [\[CrossRef\]](#)
28. Baranwal, T.; Nitika; Pateriya, P.K. Development of IoT based smart security and monitoring devices for agriculture. In Proceedings of the 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence), Noida, India, 14–15 January 2016; pp. 597–602.
29. Mukherjee, A.; Misra, S.; Raghuwanshi, N.S.; Mitra, S. Blind entity identification for agricultural IoT deployments. *IEEE Internet Things J.* **2018**, *6*, 3156–3163. [\[CrossRef\]](#)
30. Yadav, V.S.; Singh, A. A systematic literature review of blockchain technology in agriculture. In Proceedings of the International Conference on Industrial Engineering and Operations Management, Toronto, ON, Canada, 23–25 October 2019; pp. 973–981.
31. Vangala, A.; Das, A.K.; Kumar, N.; Alazab, M. Smart secure sensing for IoT-based agriculture: Blockchain perspective. *IEEE Sens. J.* **2020**, *21*, 17591–17607. [\[CrossRef\]](#)
32. 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.
33. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet Things J.* **2018**, *6*, 2188–2204. [\[CrossRef\]](#)

34. 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.
35. Voutos, Y.; Drakopoulos, G.; Mylonas, P. Smart agriculture: An open field for smart contracts. In Proceedings of the 2019 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Piraeus, Greece, 20–22 September 2019; pp. 1–6.
36. Pranto, T.H.; Noman, A.A.; Mahmud, A.; Haque, A.B. Blockchain and smart contract for IoT enabled smart agriculture. *PeerJ Comput. Sci.* **2021**, *7*, e407. [[CrossRef](#)]
37. Shyamala Devi, M.; Suguna, R.; Joshi, A.S.; Bagate, R.A. Design of IoT blockchain based smart agriculture for enlightening safety and security. In Proceedings of the International Conference on Emerging Technologies in Computer Engineering, Jaipur, India, 1–2 February 2019; pp. 7–19.
38. Caro, M.P.; Ali, M.S.; Vecchio, M.; Giaffreda, R. Blockchain-based traceability in Agri-Food supply chain management: A practical implementation. In Proceedings of the 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany), Tuscany, Italy, 8–9 May 2018; pp. 1–4.
39. Vangala, A.; Sutrala, A.K.; Das, A.K.; Jo, M. Smart contract-based blockchain-envisioned authentication scheme for smart farming. *IEEE Internet Things J.* **2021**, *8*, 10792–10806. [[CrossRef](#)]