Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.050821

ARTICLE

Security Analysis in Smart Agriculture: Insights from a Cyber-Physical System Application

Ahmed Redha Mahlous*

College of Computer and Information Sciences, Prince Sultan University, Riyadh, 11586, Saudia Arabia

*Corresponding Author: Ahmed Redha Mahlous. Email: armahlous@psu.edu.sa

Received: 19 February 2024 Accepted: 29 April 2024 Published: 20 June 2024

ABSTRACT

Smart agriculture modifies traditional farming practices, and offers innovative approaches to boost production and sustainability by leveraging contemporary technologies. In today's world where technology is everything, these technologies are utilized to streamline regular tasks and procedures in agriculture, one of the largest and most significant industries in every nation. This research paper stands out from existing literature on smart agriculture security by providing a comprehensive analysis and examination of security issues within smart agriculture systems. Divided into three main sections—security analysis, system architecture and design and risk assessment of Cyber-Physical Systems (CPS) applications—the study delves into various elements crucial for smart farming, such as data sources, infrastructure components, communication protocols, and the roles of different stakeholders such as farmers, agricultural scientists and researchers, technology providers, government agencies, consumers and many others. In contrast to earlier research, this work analyzes the resilience of smart agriculture systems using approaches such as threat modeling, penetration testing, and vulnerability assessments. Important discoveries highlight the concerns connected to unsecured communication protocols, possible threats from malevolent actors, and vulnerabilities in IoT devices. Furthermore, the study suggests enhancements for CPS applications, such as strong access controls, intrusion detection systems, and encryption protocols. In addition, risk assessment techniques are applied to prioritize mitigation tactics and detect potential hazards, addressing issues like data breaches, system outages, and automated farming process sabotage. The research sets itself apart even more by presenting a prototype CPS application that makes use of a digital temperature sensor. This application was first created using a Tinkercad simulator and then using actual hardware with Arduino boards. The CPS application's defenses against potential threats and vulnerabilities are strengthened by this integrated approach, which distinguishes this research for its depth and usefulness in the field of smart agriculture security.

KEYWORDS

Smart agriculture; cyber-physical system; IoT; security; temperature sensor; threats; vulnerabilities

1 Introduction

Making sure smart agriculture systems are secure is crucial in a time when digital technologies play a bigger role in agriculture. While integrating innovative technologies like cloud computing, artificial

intelligence, and the Internet of Things (IoT) has many advantages for agricultural practices, it also creates new dangers and weaknesses.

The functioning and integrity of smart agriculture systems can be jeopardized by a variety of risks, such as physical tampering, data breaches, and cyberattacks. Cyberattacks that target these systems' software and network infrastructure pose a serious risk. Distributed denial-of-service (DDoS) attacks, for instance, could be used by hackers to overwhelm the system's servers and interfere with data collection and operation. Furthermore, highly skilled hackers may take advantage of holes in the firmware or software of the system to obtain unauthorized access, alter data, or install malware, endangering the accuracy of gathered data.

Another real risk to smart farm systems is physical manipulation. In the field, sensors, actuators, and other hardware components may be physically tampered with by hostile actors, which could result in erroneous data collection or system failures. For example, manipulating soil moisture sensors may lead to inaccurate irrigation decisions, which may result in crop damage or resource waste. Data leaks are a significant problem for smart agriculture systems. The delicate nature of the data collected—which includes crop yields, weather patterns, and irrigation schedules—means that unauthorized access could have disastrous consequences. Enemies may, for instance, interfere with agricultural operations, steal or modify data for financial gain, or even engage in industrial espionage by selling exclusive farming techniques to rivals. Furthermore, insider threats should not be disregarded in smart agriculture systems, since workers or contractors who have access to confidential information and infrastructure may unintentionally or purposely abuse their rights. This could entail infiltrating the system with software, stealing data, or damaging hardware.

To tackle these threats, this paper provides thorough security analysis and guidelines and best practices for securing smart farm systems against cyber-attacks and ensuring their resilience in dynamic security environments. The methodology used to develop these guidelines involved a comprehensive approach, including thorough literature review of related works in agricultural cybersecurity, conducting risk assessments specific to smart agriculture systems, and designing and testing prototypes to validate security measures. By integrating research methods such as threat modeling, penetration testing, and vulnerability assessments along with analysis techniques like probabilistic risk analysis and threat intelligence, the paper aims to provide actionable insights for stakeholders in the smart agriculture domain such as farmers, agricultural technology companies, researchers, government agencies, policymakers, investors, consumers, and environmental organizations. Through this approach, we aim to enable smart agriculture stakeholders to make well-informed decisions and implement efficient security measures to safeguard data, infrastructure, and procedures in agricultural operations, thereby ensuring food security for future generations.

Related works are reviewed in Section 2. Risk assessment in smart agriculture is covered in Section 3. The prototype design is described in Section 4. Section 5 discusses the security challenges of the prototype, while smart agriculture security analysis is compiled in Section 6. The conclusion is provided in the last section.

2 Related Works

Reference [1] suggested a secure temperature sensor architecture which solves a vital need for robust sensor systems. The sensor exhibits resilience against diverse attacks through the utilization of statistical analysis and complementing current-temperature properties, an essential feature for preserving data integrity in agricultural settings. While reference [1] concentrated on sensor security, reference [2] highlighted the potential of data leakage through communication channels and raises

worries about the vulnerabilities of CPS devices. This emphasizes how sensor and system security are intertwined in smart agriculture, highlighting the significance of a comprehensive cybersecurity strategy.

Reference [3] emphasizes the threats to data integrity and confidentiality associated with the reliance of smart farms on IoT devices. On the other hand, reference [4] focuses on workable approaches to sensor data security, like authentication procedures. Reference [5] explores in greater detail how big data and artificial intelligence (AI) are incorporated into smart agriculture, pointing out security issues and suggesting future paths. Though these studies offer insightful information, none of them specifically address the incorporation of blockchain technology, as described in [6].

By utilizing the decentralized characteristics of blockchain technology, the framework described in [6] provides a novel method for improving security and privacy in intelligent farms. By offering a complete solution for safe data management and real-time threat detection, this closes a research gap. The framework's capabilities for local data processing, communication with IoT devices, and scalable cloud infrastructure for data storage and analysis are further improved by the addition of ESP32 and AWS cloud components. These elements bolster the framework's adaptability and efficacy in tackling security issues in intelligent agriculture.

The authors in [7] introduced PEFL, a Federated Learning (FL) system which makes use of privacy-enhancing techniques including perturbation-based encoding and Long-Short Term Memory-Autoencoder (LSTM-AE). They also developed the FL-based Gated Recurrent Unit Neural Network technique (FedGRU) for intrusion detection. In the ToN-IoT dataset trial results, PEFL beats both non-FL and FL approaches, demonstrating its capacity to distinguish between normal and attack behaviors.

Cybersecurity issues in agriculture was also addressed in [8] and [3]. Authors in [8] concentrated on Smart Farming and Precision Agriculture by detailing security challenges, cyber-attack classifications, and risk mitigation strategies, particularly focusing on Advanced Persistent Threats. In contrast, authors in [9] discussed the broader impact of IoT and smart technologies in agriculture, proposing a multi-layered architecture and outlining potential cyber-attacks. They also suggested future research directions in this domain. Authors in [9] proposed recommendations for farmers and Agriculture Technology Providers (ATPs) to mitigate security risks, categorized into human-centric, technology-based, and physical solutions.

Authors in [10] focused on enhancing security in IoT-based precision agriculture. Addressing cluster key management and web interface configuration challenges, the proposed approach introduces novel methods. It includes cluster key management for enhanced security and a web interface for capturing feedback from IoT sensor nodes, enabling notification management upon signal detection.

In addition, our work presents the use of the RC4 encryption technique, which adds another degree of protection to data storage and transmission in smart agriculture systems. Furthermore, we employ an actual prototype in our study, providing useful verification of our suggested security protocols in an actual farming environment. Incidentally, reference [8] emphasized the necessity of a strong security solution suited to the needs of smart agriculture. This fits well with our present research focus, which attempts to close current gaps in the field by offering thorough guidelines and best practices for protecting smart farm systems from cyber-attacks. We do this by utilizing innovative technologies such as blockchain, as well as doable security measures.

Our study intends to offer deeper insights into the changing environment of smart farm security and practical recommendations for stakeholders by critically analyzing and contrasting these studies.

3 Risk Assessment

A. Asset Identification and Prioritization

We must first make a list of all our assets, both tangible and intangible. When we talk about tangible assets, we mean the actual physical parts of the asset—sensors, wiring, temperature meter, data collection and analysis system, and, in our example, water sprinklers—as well as the area where the action happens. The intangible asset is the data exchanged between the data-analysis system and the CPS device.

The resources are ranked according to how well they support each of the three security pillars identified by the CIA triad (Confidentiality, Integrity, Availability). Data must always be accessible from the sensor and must remain secret and unmodified.

Our Smart Agriculture Scenario primarily centers on data availability. It is imperative to guarantee that crops receive consistent watering and do not overheat; if they do, data must be available to trigger the watering process.

Asset Priority list:

1. The intangible communication that exists between the system and the CPS.
2. The data collection and analysis system.
3. The sensor.
4. The "action based on the data", e.g., the sprinkler system that kicks off when water is required.
5. The wiring components (only a physical attack might cause them harm, which is why this is ranked last on the list).

Asset Prioritization is based on the severity of the attack; however, the order may vary depending on global hacking trends. Man-in-the-middle attacks account for 35% of exploits today [1]. It is possible that in the future, other types of attacks will become more common and simpler to execute; only then will the prioritization order have to be altered.

Not every asset in the Smart Agricultural Environment is as essential to the operations of service providers and stakeholders as others. An asset is considered critical if its disruption would have a major effect on ecosystems and its immediate system. As previously mentioned, the attributes were assessed according to the degree and effect of any interference or attack on their functioning. Table 1 summarizes assets and their priorities within the smart agriculture domain.

Table 1: Assets and their priorities within the smart agriculture domain

Asset	Functionality	Priority
Base shield	Connecting microprocessor's input and output pins	**High**
Arduino UNO	Prototyping the smart agriculture system	**High**
SparkFun soil moisture sensor	Measuring soil moisture	**High**
DHT22 temperature sensor	Sensing the temperature	**High**
PIR sensor	Detecting whether a human or animal has moved in or out of the sensor's range	**High**
Laptop		**High**
Data	Information gathered from sensors	**High**
Code	Controlling the sensors and receiving information	

(Continued)

Table 1 (continued)

Asset	Functionality	Priority
Network	Linking the smart agriculture system's components together	**Medium**

B. Actors and Threats

The threats are identified using a customized method for smart agriculture and inspired from the STRIDE threat model combined with the OWASP top 10. Any individual or group that purposefully causes harm in the digital realm is considered a malevolent actor. By taking advantage of flaws and openings in computers, networks, and other systems, they endanger various people or institutions [11]. Systems for smart agriculture are susceptible to many types of cyberattacks. These attacks carry serious threats to the environment and economy, interrupt agricultural activities, and jeopardize data integrity. The following is a summary of the various attack vectors that can be used against smart agricultural systems:

1) Eavesdropping

The exploit known as "eavesdropping" allows a hacker to intercept any data that the system communicates. Eavesdropping is a passive attack since the attacker just watches the system operate without interfering with it. Smart agriculture systems are susceptible to traffic analysis eavesdropping, which involves intercepting data conveyed in sensor networks that are gathered through monitoring. Additionally, eavesdropping gives the attacker access to private and sensitive data [3,12].

Secure data transmission with strong encryption methods like TLS or SSL is necessary to prevent eavesdropping attacks in smart agriculture. Reducing the possibility of unwanted interception is achieved by using secure communication routes and protocols. Real-time network traffic monitoring is made possible using intrusion detection systems (IDS) and intrusion prevention systems (IPS), which allow for the quick identification of suspicious activity. Frequent penetration tests and security audits find and fix weaknesses in the system, strengthening its defenses. By protecting smart agriculture systems from listening in on users, these tactics maintain the privacy and accuracy of agricultural data and communications.

2) Compromised-Key Attack (CKA)

A key is a code or secret number that is used to verify, decrypt, or encrypt confidential data. Once the key is in the attacker's possession, it is deemed compromised. An attacker can access an encrypted communication with this key without the sender or recipient knowing. With this key, an attacker can also decrypt and alter data. The key can be obtained by an attacker through a variety of techniques, including Brute Force in which the attacker tries every conceivable combination until they locate the key [12]. Social engineering may also be used to trick victims into disclosing the key. Smart agriculture requires strong encryption and key management procedures, such as frequent key rotation and safe cryptographic key storage to defend against compromised-key attacks. To safeguard data throughout its lifecycle, end-to-end encryption, and strong encryption methods like AES or ECC should be used. Connections should be established via secure communication protocols like TLS or SSH, and multi-factor authentication techniques can provide an additional degree of protection. In addition to routine security audits and penetration testing to find and fix vulnerabilities quickly,

intrusion detection systems (IDS) should be installed to monitor network traffic and spot unusual activity. By putting these safeguards in place, smart agriculture systems may protect sensitive data and maintain operational integrity while successfully reducing the danger of compromised-key attacks.

3) Man-in-the-Middle Attack

A cyberattack known as a "man-in-the-middle" (MITM) attack occurs when an attacker surreptitiously intercepts and transfers messages between two parties without the victims' awareness. The attacker deceives the operator by sending false messages, which could lead the operator to act when it is not necessary or to believe that everything is OK and refrain from acting when it is necessary. Serious safety risks and substantial financial losses could result from such an attack [12,13].

MITM attacks can be avoided by using Static Network Configuration, Communication Authenticity, and Network Intrusion Prevention solutions. However, MITM attack success can also be decreased by simply turning off or eliminating pointless network protocols [13].

4) DOS Attack

A cyberattack known as a denial of service (DOS) attack prevents authorized users from accessing a computer or other device. Usually, this is achieved by saturating the targeted host or network with traffic until it becomes unresponsive or fails. The DOS attack stops the system from operating normally or being used. This attack could result in significant data and financial losses [12,14].

The first step in dealing with such an attack is to identify it. A DoS attack can be identified by either a service's unavailability or sluggish network performance. An organization must keep its firewall and antivirus software up to date in order to prevent such an attack. Signing up for a DoS protection service is an additional choice; this service can detect DoS assaults and only send requests that are valid to the system [14].

Threats dispersed throughout the STRIDE threat modeling framework [15] are displayed in Table 2.

Table 2: Threats spread across STRIDE model

Threats	S	T	R	I	D	E
Eavesdropping	✓			✓		
CKA			✓	✓		
MITM	✓	✓	✓	✓		✓
DOS					✓	

Most of these attacks, including MITM attacks, compromised-key attacks, and eavesdropping, are designed to compromise confidentiality and integrity. These assaults aim to alter data or obtain unauthorized access to confidential information. The Denial of Service (DOS) attack, on the other hand, affects availability.

C. Vulnerability Identification

Vulnerabilities signify deficiencies in the security measures of the system. Finding these vulnerabilities is crucial to understanding any threats related to our Smart Agriculture Cyber-Physical System (CPS) application. Vulnerabilities in this environment can impact the functioning, data availability, integrity, and confidentiality of the system [16,17].

A list of a Smart Agriculture system's weak points is as follows:

a) ***Communication in Sensor Networks*:** Eavesdropping attacks may be possible due to the interception of communication channels in sensor networks.
b) ***Encryption Key Management*:** Improper key management raises the possibility of compromised keys, endangering critical data secrecy.
c) ***Data Transfer Procedures*:** The procedures used to move data from sensors to the analysis system could be vulnerable to Man-in-the-Middle attacks, which could jeopardize the integrity and confidentiality of the data.
d) ***Authentication Procedures*:** Our CPS application's authentication procedures may be vulnerable to flaws that allow unwanted access, jeopardizing its integrity and secrecy.
e) ***Network Infrastructure*:** Availability, integrity, and confidentiality may be negatively impacted by a variety of assaults that could target the entire network infrastructure, including wired and wireless components.
f) ***Information Storage and Processing Systems*:** Inadequate security protocols may allow unwanted access, jeopardizing the confidentiality and integrity of the data that is stored.
Actuator Systems: The integrity of the action-taking process may be compromised by manipulation of actuator systems such as water sprinklers which are in charge of acting in response to the data gathered.
Enhancing the resilience and security of the Smart Agriculture CPS application requires identifying and fixing these vulnerabilities [17,18]. Table 3 shows the list of vulnerable components and their corresponding location in the smart agriculture system.

Table 3: Components and Locations of Vulnerabilities

Component	Location of vulnerability
Sensor	◯ The physical component. ◯ Data transmission between the sensor and the system.
System data collection and analysis	◯ Software vulnerabilities in the system. ◯ Communication channels between the system and the CPS device.
Communication between CPS device and system	◯ Vulnerabilities in data transmission. ◯ Encryption and authentication mechanisms.
Water sprinkler system	◯ Remote control functionality and access. ◯ Data dependence for irrigation actions.
Wiring components	◯ Physical wiring that connects sensors and other components. ◯ Wiring tampering or damage.
Intangible asset (Communication)	◯ Weaknesses in encryption methods. ◯ Vulnerabilities in authentication mechanisms.

D. Vulnerability Analysis

1. Sensor Vulnerabilities

1.1 Physical Vulnerabilities: The primary physical vulnerabilities inside our system pertain to the sensors' vulnerability to external causes, such as extreme weather or physical damage. The sensors' ability to perform may be compromised by exposure to extreme weather conditions or physical injury, which could result in malfunctions. Protecting sensors against physical damage and unfavorable environmental conditions is essential to maintaining the system's long-term dependability.

***1.2 Vulnerabilities in Data Transmission*:** One major area of risk is the data flow from sensors to the system. If strong authentication and encryption protocols are not implemented, this data transmission is vulnerable to manipulation or interception. It is important to put in place suitable security measures to protect the confidentiality and integrity of the transferred data. Strong authentication procedures and encryption methods will be essential in preventing unwanted access to or alteration of the data while it is being transmitted, enhancing the system's overall security posture.

2. System Vulnerabilities

2.1 System Vulnerabilities: One weakness in our data collection and processing method is that it could be vulnerable to software attacks. These types of vulnerabilities result from flaws in software components that could be used by bad actors to undermine the system's confidentiality, availability, or integrity. It is essential to use strong cybersecurity safeguards, perform extensive security audits, and update and patch software on a regular basis to manage this issue. By putting these procedures into place, you can help protect the system from attacks and guarantee a safe and reliable method for gathering and analyzing data.

3. Communication Vulnerabilities

***3.1 Man-in-the-middle Attacks*:** This attack can be launched through the communication channel that connects the CPS device to the system. In this case, it would be possible for an unauthorized party to covertly intercept and alter the communication channel between the system and the CPS device. Such assaults put the security and integrity of the data being transferred at serious risk. Putting strong encryption techniques, secure communication routes, and authentication systems in place is crucial to reducing this threat. By protecting data confidentiality and integrity, these procedures make sure that it stays safe during the communication process. Maintaining a strong defense against possible MITM attacks also requires regular monitoring and upgrades to security policies.

4. Water Sprinklers Vulnerabilities

***4.1 Remote Control Vulnerabilities*:** If the water sprinkler system has a remote-control feature, unauthorized people can access it. Vulnerabilities in the system could allow unauthorized users to take over remotely and cause inefficient water use or irrigation process delays. To reduce these risks, strong authentication procedures, secure remote access protocols, and frequent

security audits must be put in place. We can guard against potential misuse by securing the remote-control feature and making sure that only authorized parties have access to the water sprinkler system.

***4.2 Data Dependence*:** Water sprinkler efficiency is dependent on timely and precise data from the CPS application. Any falsification or manipulation of this information might lead to either too little or too much watering, which would be bad for the crops' health. Implementing strict data integrity checks, encryption methods, and secure communication channels between the CPS application and the water sprinkler system is essential to addressing this risk. To ensure appropriate irrigation practices, regular monitoring and validation of the data flow will help to preserve the correctness and dependability of the information used by the water sprinklers.

5. Wiring Vulnerabilities

***5.1 Physical Damage*:** Physical damage to wiring can occur from exposure to external sources or human activity. Such damage can impair control signals and data flow, jeopardizing the system's overall performance. Protective measures such insulation, casing, or electrical routing away from threats should be put in place to alleviate this susceptibility. The integrity of the wiring infrastructure can be ensured by routine maintenance and inspections, which can assist in spotting and quickly repairing any physical damage.

***5.2 Tampering*:** Unauthorized people might try to tamper with the wiring, which could result in problems with connectivity and even data breaches. There are several ways to tamper, such as splicing, purposeful disconnections, or unapproved changes. Physical security measures, like enclosures or locks, must be put in place to limit access to the wire components to reduce this danger. Monitoring programmers and alert systems can also be used to quickly identify and stop any unauthorized tampering. The overall security and dependability of the electrical infrastructure can be improved by providing protection against tampering.

6. Intangible Asset Vulnerabilities

***6.1 Encryption Weakness*:** If encryption is not done correctly or is weak, there is a risk to the communication between the CPS device and the system. In these situations, the secrecy of the transmitted data is compromised by the possibility of eavesdropping or data interception. Strong encryption procedures, current algorithms, and frequent security assessments are necessary to strengthen this intangible asset. By making encryption methods stronger, one may prevent possible eavesdropping efforts and guarantee that confidential information is kept safe during communication.

***6.2 Authentication Flaws*:** Authentication weaknesses present a grave concern since they facilitate unauthorized access for potential attackers. To mitigate these vulnerabilities, it is imperative to strengthen authentication procedures, implement multi-factor authentication, and update access credentials on a regular basis. The integrity and secrecy of the communication between the CPS device and the system can be strengthened by fixing authentication problems, guaranteeing that only authorized parties have access to vital information and functionality.

E. Risk Estimation and Calculation

A thorough risk assessment and calculation procedure is essential to determine the possible impact and possibility of security issues within the Smart Agricultural CPS application. The following components are considered in this risk analysis [18].

1. ***Man-in-the-Middle Attacks*:** The attack's frequency in the current threat landscape, as noted in the previous section, indicates that there is a moderately high chance that it will occur. Therefore, High (Impact) × Moderately High (Likelihood) is the calculation used to determine the overall risk [18].
2. ***Data Collection and Analysis System Vulnerabilities:*** There is a serious concern about vulnerabilities in the data collection and analysis system. A security flaw in this system could lead to erroneous data analysis and affect the CPS application's operations. A breach of this kind could have a moderate impact since it could result in improper decisions being made based on compromised data or wasteful watering. The efficacy of the system's security protocols and their current state of updating determine the probability of these vulnerabilities being exploited. Thus, Moderate (Impact) × Depends on Security Measures (Likelihood) is the computed overall risk.
3. ***Sensor Security:*** Although sensor attacks are rare, they can result in erroneous temperature readings and corrupted data. Such attacks have a negligible potential impact, altering the accuracy of the data and resulting in wasteful irrigation decisions. While considered unlikely, sensory assaults are nevertheless a possibility and should not be disregarded. The total risk is therefore computed as follows: Moderate (Impact) × Relatively Low (Likelihood).
4. ***Water Sprinkler System*:** Unauthorized access to the water sprinkler system is considered to pose a moderate risk. It can lead to improper irrigation decisions, endangering the health of crops if it is affected or damaged. The probability of these types of assaults is dependent on the security controls put in place within the system. Consequently, Moderate (Impact) × Depends on Security (Likelihood) is the computation used to determine the overall risk.
5. ***Wiring Component Vulnerabilities*:** The least vulnerable parts are those that involve wiring, as they have less potential to affect things and little chance of being exploited. The formula to compute the overall risk is Risk = Low (Impact) × Low (Likelihood).

Each vulnerability must be evaluated thoroughly, considering both likelihood and potential consequence. The risk associated with each vulnerability can be estimated using the risk calculation formula: $\boldsymbol{Risk} = \boldsymbol{Impact} \times \boldsymbol{Likelihood}$. Usually, the level of risk is categorized as Low, Moderate, or High based on the generated risk assessment.

Periodic evaluations and revisions of the risk assessment are necessary to take into consideration the changing threats and vulnerabilities present in this industry. Within the context of smart agriculture, stakeholders should proactively address emerging risks and make sure their security measures continue to be effective against new and changing threats specific to agricultural systems by routinely reviewing and updating the risk assessment process. In response to the constantly shifting cybersecurity landscape, this proactive approach makes it possible to identify potential flaws and apply the required adjustments to strengthen the resilience of smart agriculture systems.

Cyberattacks against smart farming infrastructure give attackers the ability to remotely operate and take advantage of autonomous vehicles (drones, tractors, etc.) and on-field sensors, leading to a dangerous and inefficient farming environment. For instance, employing smart drones to overspray chemicals, damage entire crop fields, or flood farmlands are examples of exploits that can result in hazardous consumption and economic decline. Such "Cyber Agroterrorism" is a serious threat

to the economies of countries that depend heavily on agriculture. Agriculture was listed as a vital infrastructure sector in a US Council of Economic Advisors study that included 11 cyber incidents in 2016. A joint report from the FBI and USDA also listed a number of dangers to precision agriculture [19]. The intricacy and interdependence of contemporary agricultural systems are the fundamental sources of vulnerabilities in smart agriculture. Cyber threats have access to a large attack surface due to the plethora of networked devices, sensors, and software applications. Vulnerabilities are further increased by insufficient security measures such as default passwords and incompatibilities between older and more modern systems. These vulnerabilities are demonstrated by real-world hacks, such as those that affect crop yields and resource allocation by compromising data integrity in agricultural management software or attacking smart irrigation systems. Stakeholder education, continuous risk assessments, and strong cybersecurity protocols are necessary considering the growing ubiquity of cloud-based platforms and IoT devices, which present new avenues for exploitation. Robust authentication methods, robust encryption frameworks, frequent security assessments, and educating stakeholders on cybersecurity best practices are essential for guaranteeing the sustainability and resilience of smart agriculture systems against constantly changing cyber threats.

4 Designing a Smart Agriculture System Prototype

4.1 Architecture Overview

It takes careful planning, hardware assembly, programming, testing, and integration with edge-to-cloud systems for real-time decision-making to create a physical prototype utilizing Arduino boards. A board acts as the key processing unit, facilitating coordination and communication amongst different components. The way Arduino boards communicate with other components, including the resistor, LED lights, digital temperature sensor, and sound device, is determined by the design goals and specifications of the prototype. A key component is the digital temperature sensor, which senses the surroundings, records information, and initiates actions based on temperature ranges. A green LED illuminates when the temperature is between 40 and 50 degrees; a yellow LED illuminates when the temperature is between 50 and 60; and a red LED illuminates along with an alert to indicate an elevated temperature if the temperature surpasses 60.

The continuous communication and cooperation among components made possible by this interconnection guarantees the effective operation of the smart agriculture system.

The next step is to program the Arduino boards to perform the desired functions when the hardware has been constructed. Writing code to read sensor data, operate actuators, and manage decision-making or logic-based processes is required for this. Debugging code faults, maximizing efficiency, and integrating third-party libraries or APIs are some of the challenges that come with programming. The prototype is then put through a thorough testing process to make sure it works as planned, with an emphasis on temperature sensor readings and overall system performance. Calibration of sensors, power usage optimization, and finding and fixing hardware or software flaws are some of the challenges that testing may present.

We might integrate the prototype with an edge-to-cloud platform for real-time data analysis and decision-making, in addition to assessing the hardware and software. This entails putting algorithms for real-time analytics into place, securely transferring sensor data, and creating connectivity between the Arduino boards and the cloud platform. Regretfully, lack of resources prevented us from taking this action.

The Tinkercad simulator [20] was used to reduce the possibility of breaking actual physical components while assembling hardware. Tinkercad is a useful tool for virtual experimentation and prototyping. It provides an intuitive environment for developing, simulating, and testing Arduino-based prototypes, allowing for rapid iteration and development without requiring physical hardware, even if it is not an exact duplicate of real-world settings.

4.2 Subsystems Overview

Our prototype has a number of parts that work together to create a crucial subsystem for effective temperature control and monitoring. The high-precision temperature sensor at the center of this system was carefully engineered to detect minute changes in ambient temperature that are essential to plant health and growth. Through its link with a specific module power supply [21], this sensor ensures dependable and continuous operation—even in isolated farming locations. Subsequently, the temperature signal is subjected to rigorous signal conditioning and conversion procedures [1], which improve its accuracy and digital system compatibility. With the help of this conversion, smart agriculture platforms may be seamlessly integrated, allowing for real-time data analysis and well-informed decision-making. The subsystem meets the many requirements of contemporary agriculture by offering both analogue and digital outputs [22]. Precision farming is encouraged by digital outputs that make data logging and cloud-based AMIS (Automated Methods for Integrating Systems) integration easier. Analogue outputs give farmers instant insights for on-site modifications.

We used wired connections in our prototype, which is depicted in Figs. 1 and 2 (made with Tinkercad to connect the sensor—which oversees monitoring the outside world—to a control center. This control center is made up of a laptop and the Arduino IDE, which are used for logic, computing, and information presentation. Additionally, we have an Arduino board base station that is used to connect the sensor and LED lights, creating an essential network inside the Smart Agricultural Environment prototype. This network is linked to a laptop that manages and interprets the information gathered. We put in place an encryption method and related libraries to guarantee information security. Sensors can be linked to the control center more easily with the use of USB cables and wired connections. Table 4 displays the characteristics of the prototype's components.

We employed the RC4 encryption algorithm to encrypt and decrypt data collected from the sensors for the subsystems requiring security features. Operating on one byte at a time, RC4 is a stream cipher that uses a variable-length key method. We identified an algorithmic implementation that works with the Arduino IDE, and we selected RC4 due to its simplicity and accessibility from the library within the Arduino IDE.

The speed advantage of the RC4 algorithm comes from its easy to understand and effective implementation. In contrast to more sophisticated encryption algorithms like AES which require complicated mathematical calculations, RC4 uses a pseudo-random number generation procedure in conjunction with a simple key scheduling technique. Because of its simplified methodology, RC4 can encrypt and decrypt data with less computing overhead, which leads to quicker processing times. Furthermore, RC4's lightweight architecture uses less computational power, which makes it especially appropriate for settings with constrained memory or processing power. Because of this, RC4 is frequently chosen in situations where efficiency and speed are critical, such as in embedded systems, Internet of Things devices, and applications needing encryption and decryption in real-time.

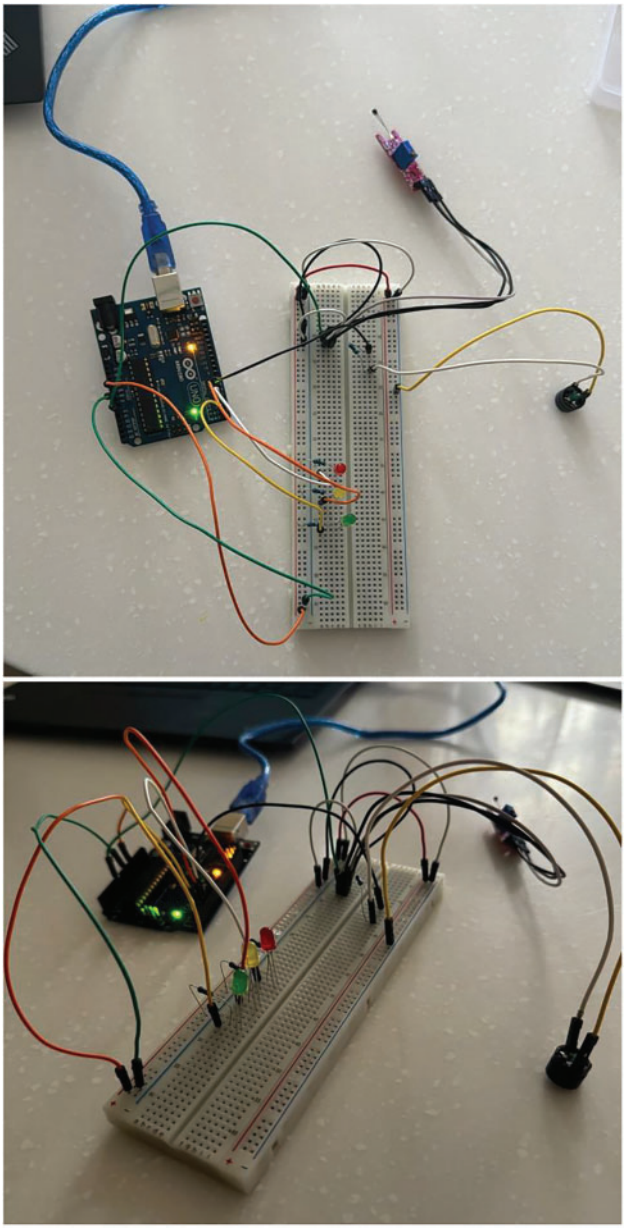

Figure 1: Smart agriculture system prototype

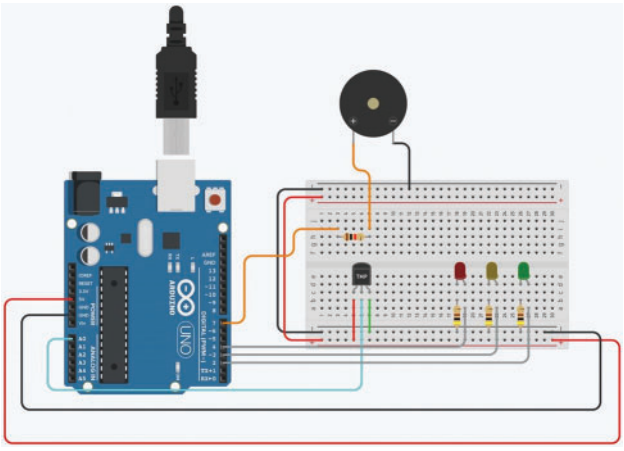

Figure 2: Prototype designed using Tinkercad

Table 4: Characteristics of prototype components

Component	Specification
Arduino	UNO
Breadboard	NA
Temperature sensor	DHT22
Led	400 Ohm Resistor
Buzzer alarm	1 KOhm Resistor

The control system, a Windows 10 Desktop, is protected against security threats by firewalls and antivirus software.

A firewall configuration is essential for defending smart agriculture systems against online attacks. Because they enable administrators to govern traffic flow based on source and destination IP addresses, ports, and protocols, access control lists (ACLs) are essential. ACLs reduce the danger of unauthorized network access by specifying explicit rules that permit or refuse access. By keeping an eye on the status of active connections and applying security policies appropriately, stateful packet inspection, or SPI, improves security. This aids in the detection and blocking of malicious traffic that aims to take advantage of weaknesses. By hiding internal IP addresses from external networks, Network Address Translation (NAT) fortifies security even more by keeping attackers from recognizing and focusing on certain devices.

An extra line of defense against online threats is provided by Intrusion Prevention Systems (IPS) that are integrated with the firewall and give real-time threat detection and mitigation capabilities. To guarantee defense against changing threats, firewall firmware and signature databases must be updated on a regular basis. Administrators may also analyze network traffic, spot anomalies, and react quickly to security problems identified by logging and monitoring services. Firewalls are essential for safeguarding smart farm systems and their assets from various cyber threats because of these security setups.

To safeguard smart farm systems against dangerous software and cyber threats, antivirus software is essential. Antivirus software configuration parameters can be adjusted to improve security in

smart agriculture setups. Real-time scanning is a crucial tool that keeps an eye out for malware by continuously monitoring system activity and incoming data. Scheduled scans may be set up to check removable devices, apps, and system files for security risks on a regular basis. Another important setting is heuristic analysis, which enables the antivirus to identify undiscovered threats by analyzing their traits and behavior, offering proactive protection against newly discovered malware.

Threats that are identified are isolated and neutralized by quarantine and automatic removal settings, keeping them from damaging the system. To provide protection against the most recent threats, antivirus software should also be set up to receive regular updates to its virus definition database and software patches. In smart agriculture networks, centralized management consoles can simplify antivirus setup and deployment across several devices while giving administrators centralized control and monitoring powers. Antivirus software may successfully defend smart agriculture systems against a variety of cyberthreats by putting certain security configurations into place, guaranteeing the availability and integrity of agricultural activities.

Putting in place strong physical security measures in addition to conventional cybersecurity measures like firewalls and encryption can increase the resilience of smart agriculture systems. A variety of tactics are included in physical security measures with the goal of safeguarding the assets and physical infrastructure used in agricultural operations. Controlled access points and surveillance systems, for example, can be used to monitor and prevent unwanted access to vital agricultural equipment and facilities. Furthermore, physical tampering and sabotage can be prevented by implementing tamper-evident seals and locks on hardware components like sensors and control systems. Sensitive data and equipment can be protected from theft, vandalism, and environmental damage in secure storage facilities with backup power supplies and environmental controls.

Agricultural areas can also be further protected against incursions and unauthorized entry by utilizing security systems including perimeter fencing, lights, and alarms. Through the integration of physical security measures with digital protections, smart agriculture systems may enhance risk mitigation and guarantee uninterrupted operations against a range of threats.

4.3 Security Risks and Vulnerabilities of the Designed Prototype

The subsystems of the prototype are vulnerable to the following weaknesses:

- The sensors are vulnerable to external assaults like denial of service and jamming, since the encryption technique only protects the integrity and confidentiality of the data that is collected. By using cable connections with sensors rather than wireless ones, such attacks are limited to the control system or local access. Cable connections limit the extent of vulnerabilities because they require physical proximity to be compromised, unlike wireless sensor networks that are susceptible to remote threats. This design decision keeps threats near to the sensor, increasing sensor robustness. But depending only on cable connections does not mean that there are no risks; this emphasizes the necessity for comprehensive cybersecurity methods to protect against constantly changing threats.
- The accuracy of sensor measurements may be impacted by a temporary drop in the usual supply voltage caused by an under-powering glitch attack on the power supply [1]. The physical accessibility of the amplifier circuit renders it vulnerable to security threats, and any compromise may lead to imprecise sensor signals [1]. These weaknesses draw attention to how inadequate the security controls are at this architectural level.
- Inaccurate sensor readings could result from amplifier circuit compromise, which would compromise the accuracy of the data that was gathered [1].

- There are further security risks associated with interacting with external systems, such as linking the CPS application to a server for data processing and the internet backbone. The integrity and dependability of the system could be seriously impacted by unauthorized access or attacks on these external connections that result in data breaches, loss of confidentiality, or data manipulation.
- The integrity of the entire system may be at danger if the sensor subsystem is breached. Attackers could tamper with or change the data collected by the sensors, causing the control system to calculate and send inaccurate data to the monitor. The decision-making of the operator might potentially have a detrimental effect on farming and agriculture, which would undermine the dependability of the system.
- Should an intruder manage to crack the cryptography and find the RC4 key, the system's confidentiality would be jeopardized.

It becomes necessary to address these vulnerabilities if smart agriculture is to continue in the future. The system's security can be improved by putting in place secure communication protocols, data encryption, and access control measures. To manage new threats and vulnerabilities, regular security audits and updates are essential. Moreover, considering developments in hardware security, adding secure components or hardware-based security modules can offer a strong defense against physical assaults, guaranteeing the integrity and dependability of the system over the long run. Sustaining the system's resilience over time will need constant observation and adjustment to changing security threats.

Adding a hashing algorithm to cyber/physical systems can protect the integrity of collected data and improve security even more at the design level. Denial-of-service attacks on the control system can also be prevented by installing firewalls on it.

5 Smart Agriculture prototype Security Analysis

To evaluate the security of a smart agriculture prototype, one must have a thorough grasp of how asset placement within the architecture affects the likelihood of an exploit. Despite having a lower exploit probability for remote cyberattacks, physical assets are vulnerable to physical manipulation or attacks since they are an essential part of the system's architecture. On the other hand, cyber assets, which include systems for gathering and analyzing data, are more susceptible to cyberattacks, which raises the possibility of exploitation. Likewise, because of their engagement in data interchange and associated vulnerabilities, assets positioned at the communication layer, such as communication components, are more vulnerable to cyberattacks and have a higher likelihood of exploitation.

Designing efficient security solutions that are suited to the unique vulnerabilities of each asset requires an understanding of the location-based probability of asset exploitation [17]. Different assets are found in the physical, cyber, and communication layers of the smart agriculture system [17]. Additional resources may be inherently relevant to various levels, even while specific resources like sensors, data gathering systems, and communication components are expressly identified. Over-concentration of assets in one region increases the danger of a single point of failure, hence strategies to improve redundancy or disperse resources equitably must be put in place as well as an assessment of the possible outcomes must be made.

Furthermore, the concentration of multiple assets in one place may result in intricate inter-dependencies, highlighting how crucial it is to comprehend and efficiently manage these linkages to reduce risks. The Actuation Subsystem of the Physical Layer, which houses the Water Sprinkler

System, is susceptible to physical attacks for remote control and data manipulation that could impact irrigation. As they are in the Physical Layer, Wiring Components run the danger of being physically damaged or tampered with, which could impair data transport. Furthermore, the Intangible Asset within the Communication Subsystem of the Cyber Layer is vulnerable to gaps in authentication and encryption protocols, making it open to cyberattacks and communication vulnerabilities.

Stakeholders may ensure the resilience and integrity of the system by creating strong security measures to protect against potential threats and vulnerabilities by thoroughly evaluating the location and interaction of assets within the architecture of the smart agricultural prototype.

5.1 Prototype's Subdomain

To thoroughly describe the essential characteristics of digital temperature sensors, we have chosen three primary subdomains:

5.1.1 Technology Subdomain: An explanation of the many kinds of electronic temperature sensors and the working mechanics behind them.

5.1.2 The Communication Protocol Subdomain: It addresses the communication between these sensors and other devices, which is a key factor in deciding interoperability and interchangeability.

5.1.3 Accuracy and Precision Subdomain: Concentrates on the primary function of the sensor, which is to provide precise and accurate temperature readings.

When combined, these subdomains offer a thorough perspective that considers both practicality and technological intricacy.

Our selection of these subdomains provides a fair appraisal of the important concerns. "Technology" gives customers knowledge about how sensors work, empowering them to choose a sensor that best suits their needs. The 'Communication Protocol' makes it simple to integrate the sensor with other systems while taking data transport and interoperability into account. The important topic of temperature sensing is covered in "Accuracy and Precision," with a focus on measurement quality—a critical component in precision applications. This choice makes it possible to evaluate the sensor's technological capabilities in detail, as well as its compatibility with the system and accuracy of temperature information.

5.2 Subdomains Security Analysis

When understanding and assessing digital temperature sensors, the three subdomains that were chosen to have separate roles to play. "Technology" reveals the sensor's innermost workings, helping consumers understand the nuances of temperature measurement. The term "Communication Protocol" describes the sensor's ease of integration by explaining how it connects with other systems or devices. On the other hand, the 'Accuracy and Precision' domain assesses how consistently the sensor provides correct temperature measurements, which is important for applications that depend on accuracy. When taken as a whole, these duties enable consumers to choose a digital temperature sensor that best suits their requirements.

Digital temperature sensors rely heavily on resources that are impacted by the "Technology," "Communication Protocol," and "Accuracy and Precision" subdomains. In the "Technology" subdomain, the choice of sensor type—such as thermocouples, thermistors, or infrared sensors—directly affects sensitivity and response to temperature changes. The sensor's capacity to connect with other systems and devices is determined by the "Communication Protocol" subdomain, which also affects interoperability and integration properties. Furthermore, the credibility of sensor data is determined by

the "Accuracy and Precision" domain, which has a substantial impact on temperature reading dependability. These subdomains work together to define the sensitivity, interoperability, and reliability assets that determine the efficacy of digital temperature sensors in a range of applications.

Security problems might arise from mistakes in these subdomains. Shortcomings in the "Technology" subdomain, such as the use of inappropriate sensor types, can lead to vulnerabilities that jeopardize the accuracy of data and the responsiveness of important applications. Errors in the "Communication Protocol" can lead to security gaps if the selected protocol does not include the necessary authentication and encryption, leaving the sensor open to manipulation and unwanted access. This may allow temperature data to be compromised in transit. Furthermore, in systems that depend on precise temperature data, faults in "Accuracy and Precision" can negatively impact decision-making and jeopardize safety and dependability. To solve potential security vulnerabilities in the usage of digital temperature sensors, a comprehensive and secure approach to these subdomains is necessary.

5.3 Other Security Enhancements

A layered strategy to improve temperature sensor security in smart agriculture necessitates different tactics at every security tier.

At the physical layer, temperature sensors and other physical assets must be protected from theft, vandalism, and manipulation by putting in place physical security measures. This entails taking precautions like using security cameras, locking up sensor enclosures, and limiting physical access to sensor installations. Temperature data integrity and reliability can be ensured by reducing the danger of unauthorized access or manipulation through adequate physical asset security.

Temperature data confidentiality, integrity, and availability in the cyber domain depend on safeguarding digital assets and sensor networks against cyberattacks. Strong cybersecurity defenses against cyberattacks on sensor infrastructure include the use of firewalls, intrusion detection systems (IDS), and encryption methods. To minimize the impact on agricultural operations, security breaches can be quickly detected and responded to through the continuous monitoring of system logs and network traffic. Ensuring the secure transmission of temperature data between sensors, cloud platforms, and central management systems requires the establishment of secure communication routes. Data transmissions can be encrypted using encryption protocols like SSL/TLS to guard against tampering or unwanted access during conversation.

Furthermore, the security and integrity of temperature data are improved by establishing secure communication channels via Virtual Private Networks (VPNs) or putting secure communication protocols into place, which reduces the possibility of malevolent actors manipulating or intercepting the data.

To guarantee the resilience and integrity of temperature data in smart agriculture applications, stakeholders can effectively mitigate security threats by implementing a tiered security approach that addresses the physical, cyber, and communication layers. In addition to providing defense against threats and weaknesses, this multipronged approach improves the quality and dependability of temperature data, which is essential for maximizing agricultural output and sustainability.

Adopting more sophisticated security techniques and technologies, such as machine learning, in the context of smart agriculture has the potential to improve cybersecurity defenses. Large volumes of sensor data and network traffic can be analyzed using machine learning algorithms, which can then be used to spot trends that could indicate abnormal behavior or security risks. Machine learning models can autonomously detect and respond to cybersecurity problems in real-time, decreasing the

need for manual involvement and improving overall threat detection capabilities. These models do this by continuously learning from historical data and adapting to evolving threats.

Furthermore, anomaly detection—the process of identifying departures from typical system behavior as security breaches—can be enhanced by machine learning. Unauthorized access or efforts at tampering, for instance, may be indicated by anomalies in temperature readings or irregularities in sensor data transmission patterns. By comparing recent observations with past data, machine learning algorithms can identify these anomalies and take proactive steps to mitigate security threats before they become serious attacks.

By predicting probable future cyber risks based on past trends and patterns, machine learning can also support predictive security analytics. Machine learning models can offer insights into new threats and vulnerabilities by examining historical security events and finding recurring attack pathways. This enables organizations to proactively deploy countermeasures and strengthen their defenses against predicted cyberattacks.

Machine learning can also improve the adaptability and robustness of defense systems in smart agriculture security frameworks. Machine learning-driven security systems can change over time and remain effective against both known and undiscovered cyber threats by continuously learning from new data and adapting to shifting threat environments. Furthermore, the scalability of machine learning algorithms makes it possible for them to manage the increasing amount and complexity of security data produced by networked agricultural systems, guaranteeing reliable protection in a variety of settings and deployment situations.

Given the circumstances, incorporating machine learning technologies into smart agriculture security frameworks is a promising way to strengthen cybersecurity posture and provide quick incident response, proactive threat detection, and adaptive defenses to protect vital agricultural infrastructure and assets.

6 Security Analysis of a Smart Agriculture System

This section delves into detailed approaches to protect the smart agriculture space, acknowledging the difficulties and risks associated with incorporating digital technologies into farming operations. Through targeted concerns, we hope to strengthen the security posture of smart farm systems, protecting private agricultural data and maintaining critical operations. Every component is essential to building a strong and safe base for smart agriculture, from domain-specific concerns to workable solutions. Table 5 delves into the many strategies for safeguarding the smart agriculture space, covering both technical and procedural elements to create a comprehensive and resilient security system.

Table 5: Domains of concerns & security measures

Domain of concern	Proposed security measures
Domain-specific security	◯ Recognize and tackle security issues specific to the smart agriculture space. ◯ Consider legal and regulatory obligations concerning the safeguarding of agricultural data.

(Continued)

Table 5 (continued)

Domain of concern	Proposed security measures
Exclusive subdomain vulnerabilities	◯ Analyze vulnerabilities unique to the smart agriculture system's subdomains, like irrigation control and soil monitoring. ◯ Put specific security procedures in place to deal with vulnerabilities particular to each subdomain.
Past vulnerability mistakes	◯ Take note of past security incidents and weaknesses in comparable systems. ◯ Integrate the lessons learnt into the present design to avoid making the same mistakes twice.
Design	◯ Look for any design errors in the system architecture. ◯ Make sure the architecture is scalable and modular to enable security updates and changes.
Availability	◯ Implement redundancy measures to ensure the availability of the system. ◯ Develop contingency plans for potential system failures or disruptions.
Security and privacy	◯ Put data integrity and confidentiality first to manage security issues. ◯ Put privacy measures in place to safeguard user data and abide by applicable privacy laws.
Data encryption	◯ Make sure that sensitive data is encrypted from beginning to finish while it is being transported and stored. ◯ Examine encryption techniques with an eye towards efficiency and security concerns.
Authentication and access control	◯ Establish strong authentication protocols for users and system elements. ◯ Using roles and responsibilities as a basis, define and implement access control policies.
Network security	◯ Install intrusion detection/prevention systems and firewalls to protect network integrity.
Physical security	Audit network configurations frequently to look for security flaws.
Incident response plan	◯ Create a thorough incident response strategy to address security breaches. ◯ Evaluate and update the incident response protocols on a regular basis.
Privacy	Verify adherence to privacy laws concerning agricultural data. Educate users on data collecting procedures and, if required, secure consent.

(Continued)

Table 5 (continued)

Domain of concern	Proposed security measures
Supplier and third-party security	◯ Perform comprehensive security evaluations for external components and services. ◯ Create procedures to guarantee that vendors follow security guidelines.
Documentation	◯ Ensure that security configuration and measure documentation is clear and current. ◯ Document security practices to make future audits and assessments easier.

7 Conclusion

The main goal of this study is to improve the usability of agricultural information systems by automating tasks and controlling temperature in a way that is optimal for safe, healthy, and successful farming activities. Our examination of security protocols, which includes the deployment of firewalls, antivirus software, and the RC4 encryption technique, emphasizes how vital it is to protect these systems' digital and physical components. A wired connection is vulnerable to flaws even though it offers some protection from potential external attackers. Although there has been progress in strengthening smart agricultural subsystems, there are still issues to be resolved, especially regarding sensor weaknesses which makes them susceptible to outside threats like jamming and denial-of-service attacks. The system's overall integrity is determined by how secure these weak spots are.

Adding further security measures like hashing algorithms and continuous monitoring will be essential to increasing the robustness of these systems in the future.

As smart agriculture advances, maintaining a careful balance between innovation and security will become increasingly important. It is necessary to integrate secure communication protocols, conduct frequent security audits, and respond to emerging threats to maintain the integrity and dependability of smart agriculture systems. By addressing these security concerns head-on, we provide the groundwork for a strong and dependable foundation that will increase the sustainability and productivity of modern farming practices.

Acknowledgement: The author would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The author confirm contribution to the paper as follows: The whole draft manuscript preparation, analysis and conclusion: Ahmed Redha Mahlous. The author reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: No data was used in this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. A. Kajol, M. M. R. Monjur, and Q. Yu, "A circuit-level solution for secure temperature sensor," *Sensors*, vol. 23, no. 12, pp. 5685, Jun. 2023. doi: 10.3390/s23125685.

[2] A. N. Alahmadi, S. U. Rehman, H. S. Alhazmi, D. G. Glynn, H. Shoaib and P. Solé, "Cyber-security threats and side-channel attacks for digital agriculture," *Sensors*, vol. 22, no. 9, pp. 3520, May 2022. doi: 10.3390/s22093520.

[3] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and privacy in smart farming: Challenges and opportunities," *IEEE Access*, vol. 8, pp. 34564–34584, 2020. doi: 10.1109/ACCESS.2020.2975142.

[4] K. V. V. Venkata *et al.*, "A PUF-based approach for sustainable cybersecurity in smart agriculture," in *19th OITS Int. Conf. Inf. Technol. (OCIT)*, Bhubaneswar, India, 2021, pp. 375–380. doi: 10.1109/OCIT53463.2021.00080.

[5] A. Rettore de Araujo Zanella, E. da Silva, and L. C. Pessoa Albini, "Security challenges to smart agriculture: Current state, key issues, and future directions," *Array*, vol. 8, pp. 2590, 2020. doi: 10.1016/j.array.2020.100048.

[6] A. Vangala, A. K. Das, V. Chamola, V. Korotaev, and J. J. P. C. Rodrigues, "Security in IoT-enabled smart agriculture: Architecture, security solutions, and challenges," *Cluster Comput.*, vol. 26, no. 2, pp. 879–902, 2022. doi: 10.1007/s10586-022-03566-7.

[7] P. Kumar, G. P. Gupta, and R. Tripathi, "PEFL: Deep privacy-encoding-based federated learning framework for smart agriculture," *IEEE Micro.*, vol. 42, no. 1, pp. 33–40, 2021. doi: 10.1109/MM.2021.3112476.

[8] A. Yazdinejad *et al.*, "A review on security of smart farming and precision agriculture: Security aspects, attacks, threats, and countermeasures," *Appl. Sci.*, vol. 11, no. 16, pp. 7518, 2021. doi: 10.3390/app11167518.

[9] M. Hazrati, R. Dara, and J. Kaur, "On-farm data security: Practical recommendations for securing farm data," *Front. Sustain. Food Syst.*, vol. 6, pp. 615, 2022. doi: 10.3389/fsufs.2022.884187.

[10] S. Anand and A. Sharma, "AgroKy: An approach for enhancing security services in precision agriculture," *Measur.: Sens.*, vol. 24, pp. 100449, 2022.

[11] B. Lenaerts-Bergmans, "What is a cyber threat actor?," Feb. 2023. Accessed: May 16, 2024. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/threat-actor/

[12] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui and K. P. Chow, "Security issues and challenges for cyber physical systems," in *Proc. 2010 IEEE/ACM Int. Conf. Green Comput. Commun. & Int. Conf. Cyber, Phy. Soc. Comput.*, Hangzhou, China, 2010, pp. 733–738. doi: 10.1109/GreenCom-CPSCom.2010.36.

[13] K. Yasar, "Man-in-the-middle attack (MitM)," Apr. 2022. Accessed: May 16, 2024. [Online]. Available: https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM

[14] The Investopedia Team, "Denial-of-Service (DOS) attack: Examples and common targets," May 2023. Accessed: May 16, 2024. [Online]. Available: https://www.investopedia.com/terms/d/denial-service-attack-dos.asp#:~:text=A%20DoS%20

[15] Microsoft, "The STRIDE Threat Model|Microsoft Learn," Dec. 2009. Accessed: May 16, 2024. [Online]. Available: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN

[16] M. V. Ruthvik Raja, "Cyber physical system security vulnerabilities," Jun. 2021. Accessed: May 16, 2024. [Online]. Available: https://dev.to/ruthvikraja_mv/cyber-physical-system-security-vulnerabilities-4bak

[17] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges, and solutions," *Comput. & Secur.*, vol. 68, no. 2, pp. 81–97, Jul. 2017. doi: 10.1016/j.cose.2017.04.005.

[18] Blog, "Calculating risk scores for project risk analysis," Jun. 2019. Accessed: May 16, 2024. [Online]. Available: https://intaver.com/blog-project-management-project-risk-analysis/risk-scores-2/

[19] FBI, "FBI cyber bulletin: Smart farming may increase cyber targeting against US food and agriculture sector," Mar. 2016. Accessed: May 16, 2024. [Online]. Available: https://publicintelligence.net/

[20] Tinkercad-Dashboard. Accessed: May 16, 2024. [Online]. Available: https://www.tinkercad.com

[21] A. M. Shojaei, "Interfacing KY-028 temperature sensor module with Arduino-Electropeak," Accessed: May 16, 2024. [Online]. Available: https://electropeak.com/learn/interfacing-ky-028-temperature-sensor-module-with-arduino/

[22] "KY-028 Temperature sensor (thermistor)," Accessed: May 16, 2024. [Online]. Available: https://sensorkit.joy-it.net/en/sensors/ky-028