International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(17s) 2026 pp. 95-113
https://doi.org/10.70917/ijcisim-2026-4708
Article

Analyzing and Mitigation of Cybersecurity Threats and Risks in Precision Agriculture Through IoT and AI Techniques

Shubham Kumar1*, Mohammad Faisal[2]

[1,2]Department of Computer Application, Integral University Lucknow, India
E mail: kshubham@iul.ac.in; mdfaisal@iul.ac.in
*kshubham@iul.ac.in

Abstract: Precision agriculture (PA) increasingly relies on advanced techniques with drone machine based-technique to enhanced agricultural productivity, resource efficiency, and sustainability. Despite these significant, the widespread deployment of interconnected advanced farming systems has presented vital cybersecurity (CS) vulnerabilities that threaten data integrity, operational continuity, and decision-making processes. This researcher study introduced a comprehensive framework for analyzing CS challenges in PA by systematically identification and classification key CS parameters and its sub-parameters, threats, risks, and their potential impacts across advanced technique and drone-enabled agricultural settings. This approach evaluates the severity of CS risks, highlights vital vulnerabilities in existing PA infrastructures, and emphasizes the necessity for domain-specific security mechanism tailored to advanced farming ecosystems. The findings focused on securing interconnected agricultural devices, protecting sensitive farming information, and mitigating emerging cyber threats remain major challenges for sustainable PA deployment. Further, in this study proposes a future research roadmap that integrates advanced security techniques and real-time mitigation mechanisms to improving the resilience, reliability, and trustworthiness of PA systems. The proposed comprehensive framework provides researchers and expert with a structured foundation for strengthening CS and supporting the secure, sustainable adoption of next-generation modern agriculture techniques.
Keywords: Cybersecurity, Threats and Risks, Precision Agriculture, IoT, AI, ML, Risk Migration, Future Research Roadmap

1. INTRODUCTION

Precision agriculture (PA) demonstrate a transformative approach to advanced agriculture that leverages modern techniques to optimize productivity and sustainability [1]. By using a combination of Internet-of-Thing (IoT), Artificial Intelligence (AI), and Machine Learning (ML) technique with drone machine based-communication system. PA authorize farmers to monitor and managed crop production with unprecedented accuracy [4]. IoT device sensors collect real-time data on crop health, soil conditions, and weather patterns. While AI and ML technique to analyze agriculture data to provide operational intelligence, automate decision-making processes and improve resource efficiency [6]. This agriculture combination modern techniques not only enhance agriculture yields and reduces environmental impact but also provides the improving demand for agriculture security in a growing changing world [2][7].

Despite, the improving trustful dependence on modern combination IoT-ML-AI techniques affectations a new CS challenge in the realm. As agricultural operations become highly interconnected, data-driven, and vulnerable to cyberattacks [9]. CS threats have unauthorized access, and infiltration to vital systems affectation critical risks. These PA risks especially affected on vital factors and it sub-factors of agriculture information and infrastructure. Given the potential impact of these CS threats are ranging from financial losses to disruptions in food supply chains system are

ensuring robust CS measures. PA is not only a technical needed but a vital component of world level agriculture security [7][10].

Figure 1. Cybersecurity of Precision Agriculture

However, existing PA researchers mainly emphasis on isolated CS dimensions like IoT vulnerabilities, and AI threat detection strategy [11]. There is a lack of a unified and combination of CSF that simultaneously addresses risks across IoT-AI-ML systems with drone machine based-techniques, and cloud infrastructures. Further, emerging threats like adversarial AI-ML, attacks, and data poisoning vulnerabilities remain insufficiently explored. Moreover, existing PA research inadequately addresses resilience, recovery strategy, and real-time deployment challenges [12].

This research has intended for researchers, farming expert, and CS professionals working at the intersection of PA and secure modern digital ecosystems. To address the identified gaps, this research aims to provide a comprehensive and integrated analysis of CS challenges in PA by integrated IoT-AI-ML and drone based systems.

The main objectives of this research are:

- To systematically identification and classification of CS threats, risks, and their potential impact associated with the integration IoT-AI-ML in PA.
- To analyze the vulnerabilities of agriculture data through holistic perspective integrating IoT devices, and AI-driven ecosystems within PA settings.
- To develop a multi-layered classification of CS parameters and its sub-parameters in PA.
- To analyze the challenges in implementing effective CS measures in PA, with a focus on technique complexity and the evolving threat landscape.
- To propose modern mitigation strategies incorporating AI-driven anomaly detection, and zero-trust architecture in PA.
- To presented a future-research roadmap in CS that addressing emerging threats such as adversarial AI and quantum risks in PA.

Contrary to the other research work which focuses on specific CS issues, this research proposes an integrated and multi-dimensional CSF that integrated IoT-AI-ML and drone ecosystems and includes future-oriented CS approaches. The research contributes to the development of a comprehensive solution of CS risks and mitigation techniques tailored specifically for PA system.

The research contributions of this research study has follows:

- Systematically Identification and classification of parameters and its sub-parameters related to CS in PA.
- Systematically Identification and classification of CS risks and threats in PA.
- Assessment of the potential impact of CS threats on PA.
- Development of risk mitigation strategies to address CS challenges in PA.
- Proposal of a future research roadmap for advancing CS in PA

This research follows a structured analytical approach based on systematic literature synthesis, classification of CS PA parameters and its sub-parameters, and risk mapping across IoT-AI-ML and drone-based systems. The analysis framework enables identification of vulnerabilities and alignment of mitigation strategies without relying on experimental datasets.

This research introduces a scientific review on the benefits, CS risks, threats, parameter classification, and mitigation strategies in PA. The study systematically identifying and classification various domains, including advantages, security issues, IoT-device threats, and novel techniques into distinct sections. Section 3 addresses the identification and classification of CS challenges in PA that focusing on parameters, its sub-parameters, risks, threats, and potential impacts. Section 4 proposed risk and threats mitigation strategies and techniques to address farming challenges. Section 5 proposed a future research roadmap for enhancing CS in PA. Section 6 concludes of the paper.

2. LITERATURE REVIEW

Researchers have extensively explored CS, PA, IoT, and AI/ML that highlighting vulnerabilities in IoT systems and AI's role in intrusion detection, and the need for secure frameworks. However, comprehensive analyses integrating these aspects remain limited.

In this authors [1] have provides a SLR focusing on security threats and countermeasures in smart farming (SF). The review highlights various types of threats, including cyber-attacks targeting agricultural infrastructure, data breaches, and privacy violations. Additionally, proposes a range of countermeasures to mitigate these threats, such as encryption, access control mechanisms, and intrusion detection systems. In this study [2], provided an in-depth analysis of security domains in SF and PA and covers a wide range of topics, including security vulnerabilities in IoT devices, potential attack vectors, and recommended countermeasures. This study provides valuable insights into the evolving CS threat landscape and identifies strategies to strengthen the security resilience of PA systems. In this paper [4], comprehensive evaluation focuses on security and privacy issues specific to PA techniques. Further, authors explored the challenges affectation by data collection and sharing, as well as the necessary for robust authentication and authorization strategy. Furthermore, authors fascinating real-time suspicion for validating security to protect suspicious agriculture data.

In this paper [6], emphasized the important point the improving threat of cyber-attacks focusing agricultural infrastructure with the potential impact on food supply chains systems. Further, investigation of CS measure such as risk assessment, former training, and regular security audits to mitigate the risks affection by malicious actors. In this paper [7], authors identified various issues such as data integrity, and system reliability. further proposed a future research roadmap to identified challenges effectively. In this authors [8], conducted a SLR on agriculture area through AI techniques, while primary focused on security. Further, focused on agriculture security implications of AI adoption such as risk of algorithmic bias and unauthorized access. In this authors [9], identify agriculture risk that provided valuable insights into especially security challenges face. The authors emphasized vital of securing data transmission channels, monitoring for anomalies, and validating encryption techniques to protect suspicious agriculture information from unauthorized access.

In this paper [10], authors providing on PA strategy and methods for improving trust in IoT device. Further, authors validate trust strategies like device authentication, and data encryption to ensure the integrity and reliability of IoT deployments. In this paper [11], authors introduced SA that in-depth IoT device analysis of security issues including security outcomes, and associated challenges. Additional, authors explored the complexities of securing interconnected IoT devices and proposed adaptive security measures to mitigate threats effectively. In this study [12], authors validate the security and privacy challenges inherent, and identified potential risks like data breaches, tampering with sensor data, and DoS attacks, and validate future prospects for improving security through encryption, authentication, and anomaly detection strategy. In this study [13], authors conducted a survey on security threats in farming IoT and SF. Authors providing a comprehensive overview of the diverse range of security threats targeting IoT devices and networks in SA, providing insights into effective mitigation strategies and risk management practices. In this paper [14-15], authors discussed improving SA through the validation of modern twins, helping a comprehensive review of the potential benefits and challenges.

In this study [16], authors emphasized PA vital of focusing security, privacy, and comprehensive strategies that balance innovation with the protection of sensitive information. In this paper [17], authors focused on farming transformative potential of modern twin techniques. Further, proposed frameworks to facilitate the adoption of these techniques among smaller farming operations. In this study, focused on vital integrating probabilistic ML Method to bolster CS in the evolving landscape of agriculture 5.0, while also addressing the critical unique challenges and threats faced. In this study [18], authors focused on comprehensive study of existing research on CS in agriculture, data-driven techniques, ML applications, and real-time CS models, all of which helping to the development of modern CS model for high-tech agriculture.

An identify that there are vital shortcomings in security issues in SF and PA that lack of combination of across the security dimensions, limited emerging threats such as vulnerabilities of AI-driven cyber-attacks. Lack of discussion on resilience, recovery mechanism, and evidence from validation practical cases. Furthermore, security, and policies that regulate agricultural CS have explored detail. It is vital to address these gaps in ordered to create proactive and combination security plans to ensure effective protection of farming systems and information from emerging threats. Existing research helping vulnerabilities and countermeasures attacks, though they focus on especially parts and fail to consider the IoT-AI-ML technique. Limited real validation cases hinder application, and emerging threats, such as the vulnerabilities of attacks through AI to explored. Furthermore, a lack of focus on resilience methods and recovery strategies and regulatory frameworks hinders the development of highly security models. Applications of needed measures to tackle these gaps have vital to protecting agriculture systems against emerging risks.

3. CYBERSECURITY CHALLENGES IN PRECISION AGRICULTURE

PA harnesses state-of-art advanced technique to enhancing agriculture efficiency and sustainability. Despite, these advanced techniques have vital CS risks that classification, identification, and mitigation vital parameters and its sub-parameters have necessity for improving effective CS strategy to protect agriculture systems. CS challenges assessment into the identification of PA risks and threats [4][6][9][11-12][15-21]. Further, these advancements substantiate their transformative potential to improve the functionality, and data integrity of CS within PA system.

3.1 Classification of Parameters and Sub-Parameters

In this section, the analytical outcomes obtained in the process of identification classification and risk mapping have discussed. The structured mechanism to the identification of CS challenges have structured according to PA data, network, technical and operational aspects, and provides a structured assessment of threats and potential impacts. CS challenges in PA have classified into a structured set of vital criteria and sub-criteria. These classifications provide in identifying the particular criteria that contribute to the overall CS risks in PA systems. The key parameters have techniques components, data security, network infrastructure and operational procedures. Further, parameters have been broken up into sub-parameters to capture granular vulnerabilities and to describe the risk landscape in a more analytical way [2][5][7][8][11-13][15-17][20].

3.1.1 Techniques Components

These criteria through in CS for PA such as IoT devices, drone security, AI and ML systems form the backbone of advanced agricultural system [2][4][6]. These are vital to consider when assessing CS risks because of their ubiquity and interdependencies [15-16][20].

A. IoT Devices

The IoT device security, such as encryption, access controls, and firmware integrity are vital for protecting against unauthorized access and tampering. Likewise, there have been limited authentication and authorization mechanisms vulnerable to compromising these devices and leading to their control by an attacker to disrupt agricultural operations [10-11]. Additional, the physical security of IoT sensors and devices have vital PA challenge. The equipment in open fields is at risk of tampering, theft and sabotage. These threats have affected the integrity of the data and decreased device reliability [13][21].

B. Drones Security

In drone operations security, GPS for navigation is vital, and integrity and communication security are also important leaving them susceptible to spoofing attacks. Such attacks have thrown drones off target, such as in crop spraying and field monitoring [1][2][6][7][9]. Drones also relay huge amounts of data during operations. Unsecured means that communications have not protected. This opens the system to possible attacks or hijacking, jeopardizing the performance and security [11-13] [15-17].

C. AI and ML Systems

Model integrity and data poisoning are significant concerns in AI/ML applications for PA, as ensuring the robustness of AI/ML models against adversarial attacks is vital. These attacks have manipulated data inputs to produced incorrect predictions [17][19]. Furthermore, data poisoning involves attackers feeding corrupted or manipulated data into the models and disrupting the decision-making process. This result in suboptimal resource allocation and inaccurate yield predictions with ultimately impacting the effectiveness of agricultural system [1][2][4][6-8].

3.1.2 Data Security

These CS factor in PA involves safeguarding the vast amounts of data generated and processed by various aspects, such as IoT devices, drones, and AI/ML systems [1][2][4][6][7]. Further, each factor is further divided into sub-factors: data integrity, confidentiality, and availability [11][12][15-23]. The detailed explanations of these sub-factors are provided below:

A. Data Integrity

In, Data gathered through IoT devices and drones need to be accurate for making decisions. These are devices that capture real-time data, which has to be consistent and reliable. Farmers have been fooled by attack to make wrong decisions and predictions based on the farming data [2][7][14-16]. These advanced techniques that prevent tampering are put to the use of securing data transactions. These techniques fascinating to prevent modify in the data while it is being transmitted and stored, which provides to maintain the integrity of the data and ensure reliable operations [21-24].

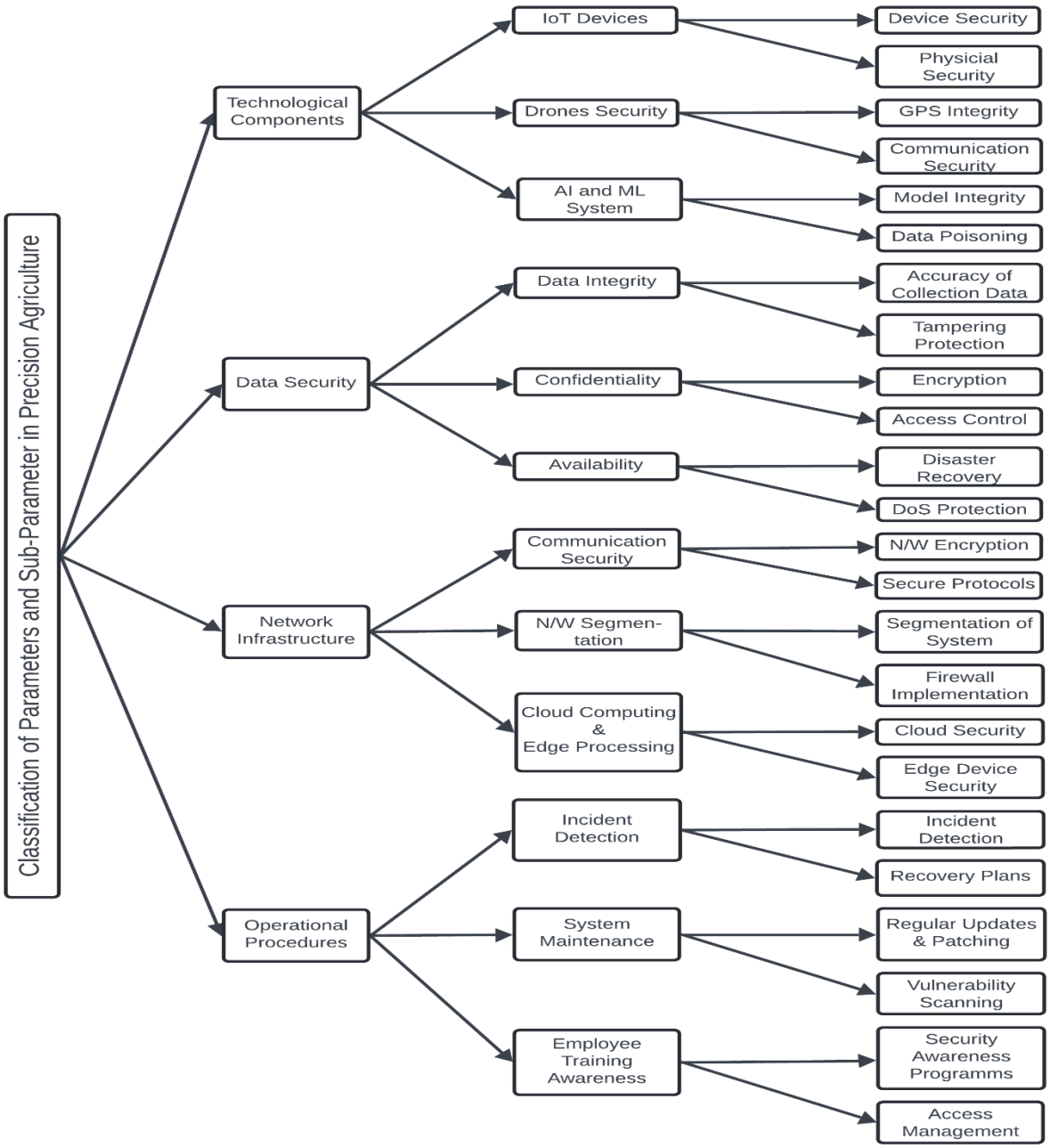

Figure 2. Classification of Cybersecurity Parameters and Sub-Parameters in PA

B. Data Confidentiality

In data confidentiality, Encryption and access controls are elemental in attempting to protected very suspicious cultivating records. The data at rest and in transit need to be encrypted so that unauthorized access and theft [2][4][6-9] have been exposed to malicious actors through insufficient encryption protocols. To ensure that only authorized systems have accessed this suspicious data and to protect it from potential security breaches, further measures were taken [12-17].

C. Data Availability

In data availability, disaster recovery protection are essential aspects in ensuring the availability and reliability of critical agriculture data. In case of cyberattacks, system failure, robust systems of backup and recovery are essential to ensure the availability of data [7][8]. Further, the farms necessity to be defended from DoS attacks that have affected the availability of needed data such as real time monitoring of crops or control of automated systems. These protects are vitl for ensuring the ongoing and effective functioning of PA [14-20].

3.1.3 Network Infrastructure

In network infrastructure, PA systems is responsible for integrate IoT devices, drones, and AI/ML technique with central data processing units. These securing network is vital for managing the integrity and confidentiality of communications between aspects [9][15-16].

A. Communication Security

Encryption of network traffic ensures that data transmitted between devices and central systems cannot be intercepted or altered. Vulnerabilities in encryption protocols have exposed the network to eavesdropping and data manipulation. Further, secure protocols are using secure communication protocols, such as TLS and VPN have protected data transmission between different parts of the PA network [16-20].

B. Network Segmentation

Segmentation of the network into distinct zones reduces the risk of lateral movement by attackers who gain access to a single component. Further, firewall implementation should be deployed to protect sensitive farming operations from unauthorized access and intrusion attempts [2][9][18].

C. Cloud Computing and Edge Processing

These securities in PA increasingly relies on cloud computing for data storage and analysis. Ensuring secure cloud access and protecting data stored in the cloud from breaches are vital sub-factors [1][18]. Further, edge device security computing brings processing closer to the field but it also introduces points of vulnerability. Ensuring the security of edge devices and their ability to process data securely is various to minimizing CS risks [27].

3.1.4 Operational Procedures

In additional to operational procedures, human factors, and technical measures also play a vital role, including policies for device management, incident response, and system maintenance in CS for PA systems [2][17]. Further, each factor is further divided into sub-factors: incident response and recovery, system maintenance, employee training and awareness [2]. The detailed explanations of these sub-factors are provided below:

A. Incident Response and Recovery

These sub-factors have vital for maintained the resilience of PA systems against cyber threats. Real-time detection of cyber incidents has essential for minimizing potential damaged, requiring continuous monitoring of systems for breaches or unusual behavior [1][16]. Addition, Well-defined recovery approaches were recognized as vital for maintaining operational continuity after cyberattacks. The approaches incorporated data recovery, system restoration, and timely vulnerability remediation to enhanced the resilience of PA systems [26][27].

B. System Maintenance

In, the need to secure PA systems have identified as regular software updates, security patch management, and continuous vulnerability evaluations. Exposing vulnerabilities was minimized, as patches have deployed in time across IoT devices, UAVs and AI-ML mechanism, and there have constant evaluations of vulnerabilities to ensure that they have identified and rectified early in the process, enhancing the cyber resilience and protection of vital agricultural operations.

C. Employee Training and Awareness

In, the key themes identified were security awareness programs and access control methods as part of CS in PA. Training programs enhanced stakeholders' understanding of cyber security threats and encouraged good cyber security habits, such as proper password management, software updates and phishing attacks recognition. Further strong access control mechanisms prevented system and data access by anyone other than authorized users, helping to minimize the threat of unauthorized access and security breaches and enhancing PA systems' overall cyber resilience.

3.2 Identification of Risk and Threats

The hybrid of various techniques in PA opens up a broad attack surface for potential CS threats. The potential threats are related to the integration and interdependence of devices, network and data management in advanced farming. A team of researchers has compiled a list of key CS risks and threats faced in PA [1][7][19][26].

3.2.1 IoT Device Vulnerabilities

In IoT device vulnerabilities, the IoT devices employ sensors and smart machinery to gather real-time data and monitor in PA. But, they generally lack adequate security and are an easy target for cyberattacks. The researchers have elaborated the vulnerability of each IoT devices from cyber-attack and the various studies [10][11][13][17].

A. Weak Authentication Mechanisms

There are many IoT devices in agriculture that do not have strong authentication mechanisms. These include multi-layer security factors and making it more accessible for an attacker to gain unauthorized access. After accessing these devices, the attackers have control the devices to affect farm operations such as irrigation and sensor readings [21][22].

B. Unencrypted Data Transmission

These devices may transmit data via unsecured channels, leaving it susceptible to interception and manipulation. This has enabled the stealing of critical farming information including data pertaining to crop health and soil conditions, resulting in the loss of critical and sensitive farming information and faulty or wrong decision making due to corrupted information [23][24].

C. Firmware Exploits

Numerous IoT devices have equipped with outdated firmware that contains unpatched vulnerabilities and making them susceptible to attacks such as malware infections or device hijacking. Hackers have vulnerabilities to take control of these devices and disrupting farm operations by tampering with vital equipment [2] [14].

3.2.2. AI and ML Risks

AI and ML are vital for predictive and forecasting analytics such as crop yields, pest management, and resource allocation. However, these model exposed to distinct CS risks [8][17][30]:

- **Data Poisoning Attacks:** In this models rely heavily on historical data for training and attackers have introduced malicious data into these datasets. Attackers through data poisoning to manipulated AI outputs and leading to inaccurate predictions, and poor agricultural management decisions, such as incorrect pest control or irrigation plans [2][14].
- **Adversarial Attacks:** In attackers subtly modify the input data provided to AI/ML model and leading to incorrect classifications or predictions. For instance, an attacker may introduce noise into crop health data to trick the AI into diagnosing a healthy crop as diseased and triggering unnecessary pesticide application or resource misallocation.

3.2.3. Drone Threats

Drones are increasingly employed in PA for tasks such as aerial mapping, crop spraying, and field monitoring. While drones contribute to enhanced efficiency and present unique CS vulnerabilities [1][2][13]:

- **GPS Spoofing:** In attackers can manipulate GPS signals to mislead drones and causing them to deviate from their intended path or fail in vital tasks such as pesticide application. This have leaded to incorrect coverage of fields and crop damage or yield loss.
- **Drone Hijacking:** In unauthorized access to a drone's control system allows hackers to take full control of the device. They have employed this access to steal valuable data, such as high-resolution farming images of fields and disrupt operations by causing the drone to crash and malfunction during vital tasks [26].

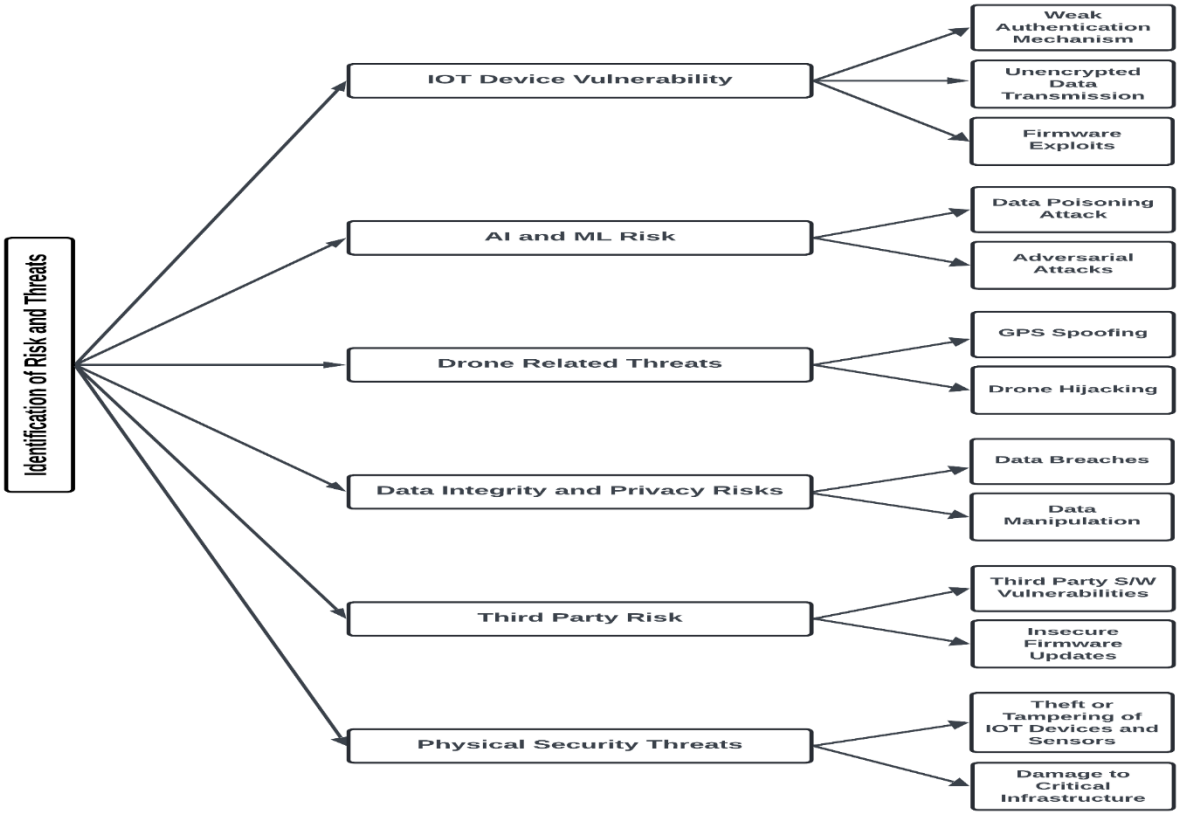

Figure 3. Identification of cybersecurity risks and threats in PA

3.2.4. Data Integrity and Privacy Risks

PA data a central role in decision-making and farming operational efficiency with generating vast amounts of data through IoT devices, drones, and AI/ML systems. Ensuring the integrity and privacy of farming data is vital for maintaining system reliability and protecting sensitive agricultural data [1][6][12][15].

- **Data Breaches:** Insecure networks and devices elevate the risk of unauthorized access to sensitive farming data, including crop yields, financial records, and proprietary management strategies. A breach has compromised a farm's competitive advantage and potential lead to financial losses and market manipulation.
- **Data Manipulation:** Attackers have manipulated vital farming datasets employed in PA and leading to inaccurate predictions and decision-making. Manipulated soil moisture data have misled irrigation systems in causing over- or under-watering and negatively impacting crop health and productivity.

3.2.5. Supply Chain and Third-Party Risks

PA systems often depend on a complex supply chain that involving hardware, software, and third-party service providers. Each component of the supply chain has introduced distinct CS vulnerability [7][21][27][30]:

- **Third-Party Software Vulnerabilities:** In many farming systems depend on software provided from third-party vendors. If the vendor's software contains vulnerabilities or lack proper updated. This issues have serve as a potential entry point for attackers [7].
- **Unsecure Firmware Updates:** In devices and machinery employed in PA often require regular updates to maintain performance. An unsecure update process has introduced vulnerabilities that providing opportunities for attackers to exploit weaknesses in firmware and control software.

3.2.6. Physical Security Threats

In digital farming threats systems are vulnerable to physical security threats. These physical vulnerabilities have leaded to direct CS breaches [7][26][19]:

- **Tampering of IoT Devices and Sensors:** In IoT sensors, drones are frequently deployed in open fields and making them susceptible to tampering and thefts. If an attacker gains physical access to tampering devices and attackers have manipulated data or disrupt farm operations by altering sensor settings or stealing hardware.
- **Damage to Critical Infrastructure:** Physical damage to vital infrastructure, such as servers and control units have leaded to system failures and data loss. Attackers have deliberately sabotage infrastructure to cause widespread operational disruptions.

3.3 Potential Impacts of Cybersecurity Threats

The threats of cybersecurity are under great exposure of CS threats as PA continuously applies multiple techniques such as IoT, Drones, AI/ML, and Cloud Computing. The impact of these threats is far-reaching and have impact farming productivity, economic sustainability and farm security. As pointed out by references [6] and [2] there are several major potential impacts of CS threats [30]:

3.3.1. Operational Disruptions

In operational disruptions, one of the most immediate consequences of CS threats in PA is the disruption of routine farming operations. The vital dependence on automated systems implies that a cyberattack targeting any major aspects including IoT sensor, drone, and farm management platform have halt vital processes [1].

- **System Downtime:** in system downtime, cyberattacks, such as DoS and ransomware have disrupted vital agriculture systems including irrigation control, crop monitoring, and automated machinery. Even brief periods of downtime have leaded to crop damage and missed optimal growth windows that impacting farming productivity.
- **Drone Interference:** GPS Spoofing or drone infringement on equipment has led to poor coverage in the field, incorrect data collection, and interference with essential activities like pesticide application or soil surveys. This has caused agricultural management to be inefficient and operations to be delayed.

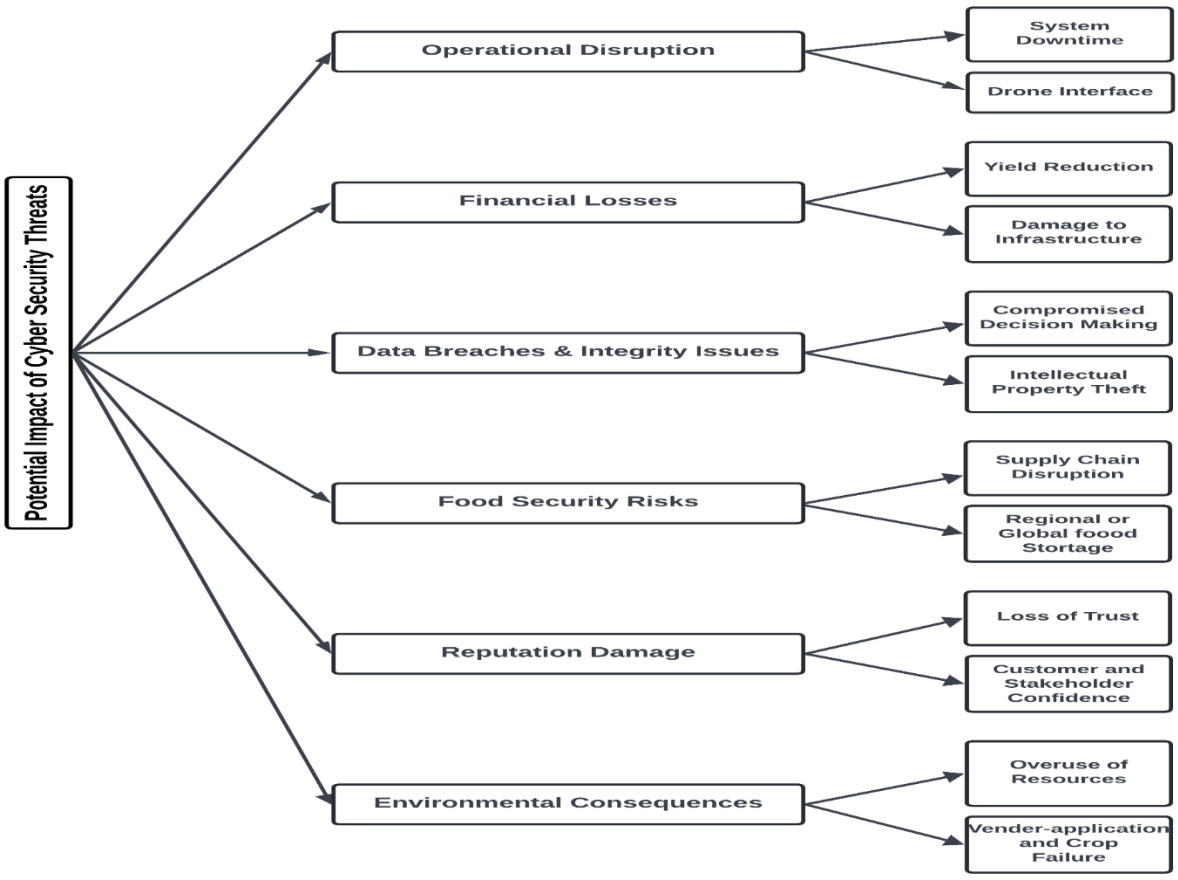

Figure 4. Potential Impact of Cybersecurity Threats in PA

3.3.2. Financial Losses

CS incidents have both direct and indirect financial costs in PA. An important cost is the recovery expenses after an attack. Further, the loss of during and after these events, productivity have significantly affected, with consequences on the profitability of farms.

- **Yield Reduction:** Incorrect decisions have been made due to attacks that corrupt and modified critical data, such as using the wrong irrigation schedule, nutrient allocation, and pest management. All of this makes for inefficiencies and eventually yields lower productivity and significant losses**.**
- **Damage to infrastructure:** When the devices, drones and machinery associated with IoT are damaged by a cyber-attack, it has cost millions of dollars to repair and replace. These damages have more than just equipment issues, affecting entire crop cycles, and adding to losses.

3.3.3. Data Breaches and Integrity Issues

PA relies much on accurate information for the critical decision making process. Disruption of the integrity of data caused by cyber threats can have wide and far-reaching consequences [16] [31].

- **Compromised Decision Making:** When an attacker alters critical farm information like weather, soil and crop health information. Farmers have made wrong decisions, which adversely affect the growth and yield of crops. Some of the decisions might involve over-irrigating, under-fertilizing and not responding to pests in time.

- **Intellectual Property Theft:** High-tech farming methods, strategies, algorithms, optimized techniques, and even hybrid patents are all susceptible to intellectual property theft. Leading to loss of competitive advantage and jeopardizing future profitability due to data breaches when this sensitive information is exposed to competitors.

3.3.4. Food Security Risks

In food security, the integrity of PA systems is vital role in ensuring food security at a broader scale, particularly in regions heavily dependent on high-efficiency agriculture practices to meet their agriculture demands [30].

- **Supply Chain Disruption (SCD):** In SCD, PA often integrates with broadly level supply chains to coordinate planting, harvesting, and distribution schedules. Cyberattacks mainly focusing vital systems have case in significant disruptions, and spoilage that impacting local and global agriculture supply chains.
- **Regional or Global Food Shortages:** A coordinated cyberattack focus on agriculture systems across a world level that impact farming production on broader level. Such an incident has reduced food supply, drive up prices, and exacerbate food insecurity in developing countries.

3.3.5. Reputational Damage

CS incidents extend beyond tangible operational and financial impact. They causing significant to farms, agricultural companies, and even entire regions [10].

- **Loss of Trust:** farming data breaches and attacks on infrastructure have undermined the trust between farmers and the technology providers they depend on. Such incidents can create hesitant among farmers to adopt advanced modern techniques. This hesitation is driven by concern over potential security vulnerabilities.
- **Customer and Stakeholder Confidence:** Large-scale data braches and operational disruption caused by CS issues can undermine consumer and stakeholder confidence in a farm and agricultural firm. These incidents can negatively affect future business opportunities. Further, they can deter investments, and jeopardize long-term partnerships.

3.3.6. Environmental Consequences

PA aims to enhance resource efficiency and reduce environmental impacts. However, cyberattacks target on PA systems could inadvertently lead in ecological damage [28].

- **Overuse of Resources:** A cyberattack that corrupts irrigation and fertilization schedules could lead to over-application of water, fertilizers, and pesticides. This misuse has cause environmental impact like soil degradation, water contamination, and a loss of biodiversity.
- **Crop Failure and Under-application:** A disruption in critical systems has led to the under-application of necessary resources this imbalance has result in crop failure and waste of farming inputs.

The effects of cyber security risks in PA are far-reaching. These result in substantial economic loss, loss of data, loss of data integrity, food security issues, reputation issues and environmental damage. The far-reaching ramifications highlight the importance of bolstering CS systems against maintaining the resilience of agricultural systems in a more technologically interdependent future. The reliability, efficiency and sustainability of advanced farming methods is ensured by the solution of these questions.

PA CS challenges are complex and numerous and have multiple impacts on operational efficiency, profitability and the security of farms. By identifying potential risks and threats, classifying vital parameters and sub-parameters, and understanding the potential impacts, stakeholders can better prepare for and mitigate CS threats and risk. Protecting the techniques infrastructure, data, and networks supported in PA is needed to farming in the digital time.

3.4. Discussion

The results highlight that while protecting individual devices and communication routes is important to cyber security in PA, it is no longer the end objective. Rather, it rests on the creation of an interwoven systems entry that integrates the technology of sensors with the power of AI and ML, UAVs and the cloud, as they all continually share information and inform one another's choices. As these technologies have become closely coupled, failing of one component will impact the security and reliability of the entire farming system.

The identified challenges are the most exposed ones by far, being IoT devices. However, they are not always able to implement more sophisticated authentication and encryption protocols due to their limited processing power, energy and the heterogeneous deployment. Consequently, these devices provide attractive avenues for attackers as reported by [2] and [13]. But unlike intended existing study target on IoT security, and this study takes into account the vulnerabilities with IoT and threats associated with AI and ML, thereby giving a greater idea of the CS risks in modern PA settings.

PA also focus on improving security threat of AI/ML techniques. While there are many applications of these techniques, such as anomaly detection, prediction of crop conditions, and optimization of resource use, they are new attack surfaces. Prediction and decision making errors have been caused by changes in model behavior, triggered by adversarial and data poisoning attacks. The consequences of these attacks are downstream on irrigation scheduling, pest detection and forecasting, yield estimation, and fertilizer recommendations, and ultimately on yield and operational expenses. These findings demonstrate that AI has been seen not only as a CS solution but also as a part that needs special attention during its lifecycle to meet CS requirements.

UAVs are also recognized as a nascent source of cyber-physical risk in the study. Drink volumes are the used by PA for the monitoring of crops, field mapping, pesticide spraying and data collection efforts are becoming more and more a staple in the fleet of drones PA is increasingly using in their operations. But attacks like GPS spoofing, communication spoofing and control have already caused flight disruptions and endanger data integrity. Although the use of UAVs in agriculture is gaining traction, these security concerns have only been investigated a bit more than their use in agronomy, thus leaving a great room for future research.

Cyber events have regarded not only as technical failures, but also as incidents that have significant effects on farm productivity, farm income, and environmental sustainability since data integrity loss or disruption of automatic processes in the farm and access to farm data by unauthorized persons have very much impacted the farm world. With the growing trend towards data-driven agricultural systems, CS is becoming a crucial component to guarantee effective decisions, secure the digital infrastructure, and inclusive food security.

The findings of this study have certain restrictions. The proposed cyber security framework has not been so far tested by experimental implementation and real world deployments and is conceptually designed. Furthermore, the threats are constantly evolving and unknown attacks can be created that are not covered by the current framework. Furthermore, certain new era security measures, like the zero trust framework, blockchain or FL, present challenges for implementation in today's conditions where many farming areas have limited computing power, occasional network connectivity and price limitations.

It fills the gap on literature by collating different issues related to the integration of the following challenges: IoT, AI/ML, UAV, cloud and cyber-physical security in a single analytical framework. The study combines these separate research areas into a single base to formulate CS strategies to ensure the survival of PA system and further experimental validation to real PA systems.

4. MITIGATION OF CYBERSECURITY RISKS AND THREATS IN PA

Cyber security in PA has its own set of unique and complex challenges to overcome, particularly in regard to the different ways that IoT, AI, drones and other technologies are emerging. These risks and threats require a systematic approach to be properly managed, and more emphasis needs to be placed on enhancing of technical

infrastructure by implementing mitigation strategies. These mitigation measures also mention better operational practices, and making through of advanced approach of enhancing system resilience. In further, we have listed the problems by systematic identified PA threats and risks, and provided the mitigations to give a more general overview of the CS issues. [1-2][13][26][34].

4.1. Mitigation of IoT Device Vulnerabilities

IoT devices form the backbone of PA systems but are often resource-constrained and prone to various cyberattacks. Effective mitigation methods include [2]:

- **Device Security Enhancements:** Implementing lightweight encryption protocols and secure boot mechanisms have needed to prevent unauthorized access and protect IoT devices from malware injection.
- **Secure Communication Protocols:** Employ end-to-end encryption through TLS methods for data transmission to ensure both confidentiality and integrity.
- **Regular Updates and Patching:** Regularly implement timely firmware updates and apply vulnerability patches to IoT devices to enhance security and mitigate potential risks.
- **Anomaly Detection Systems (ADS):** Implement AI-IDS to monitor IoT networks in real time for enabling the detection of abnormal behavior patterns and potential threats.

4.2. Addressing AI and ML Risks

In, AI and ML systems, despite their capabilities are vulnerable to adversarial attacks and biased decision-making. Mitigation measures include [2]:

- Model Robustness: Develop adversarially robust models by employing techniques such as adversarial training to enhance resistance against manipulation attempts.
- Federated Learning: Utilized federated learning techniques to train models locally. This technique ensuring sensitive and maintaining data privacy during the training process.
- Data Quality Assurance: Utilize diverse and high-quality datasets to reduce risks associated with biased or incomplete training data. Ensuring data variety and reliability improve the robustness and fairness of AI models in PA.

4.3. Mitigating Drone-Related Threats

Drones are increasingly utilized in PA but are vulnerable to both physical and cyber threats. Mitigation strategies include [1][2][13][31]:

- Secure Communication Channels (SCC): Encrypt communications between drones and ground stations to protect against interception and hijacking [29].
- Drone Systems Security: In, ensure drone systems have multi-layer security mechanisms for drone access as well as drone control systems, to enhance security and encase unauthorized access.
- Physical Protection: Implement geofencing and hardware protection against unauthorized drone flight and protect drone operation zones [16][31].
- Anomaly-Based Surveillance: Incorporate AI-powered anomaly detection into monitoring drone activities that swiftly detect and respond to abnormal behavior.

4.4. Data Integrity and Privacy Protections

In, data integrity and breach are main concerns with PA systems. Mitigation measures include [1-2][13][26][31][36]:

- **Blockchain Solutions:** Adopt the blockchain technique to guarantee the unchangeability of information, safe allocation and considerate sources of shared information.
- **Security Measures:** Ensure that sensitive farming data is not accessed by unauthorized personnel by implementing fine-grained security access policies and RBAC.
- Data Encryption: Encrypt sensitive data both at rest and in transit to sprotect against farming breaches sensitive data.
- Privacy-Preserving Technologies: Utilize differential privacy and secure multiparty computation techniques to facilitate data sharing while ensuring the preservation of privacy.

4.5. Managing Supply Chain and Third-Party Risks

In, supply chain and third party vulnerabilities are critical to the integrity of the whole PA ecosystem, with approach for the mitigation of these vulnerabilities including: [1][19][30]:

- **Third-Party Audits (TPA):** Periodically test third-party vendors for adherence to cyber security standards and protocols.
- **Blockchain in Supply Chains (BSC):** Use blockchain to gain access to secure and transparent supply chain and prevent data leakages and complexities.
- **Third Party Integrations:** Take a zero-trust approach for Third Party Integrations to ensure access request is tightly verified before granting access.

4.6. Strengthening Physical Security

Prevention of unauthorized access to farming devices and systems by physical security is extremely vital. Some approach for mitigation are: [1][7][1][37-42]:

- Access Control Systems: In, install biometric and card-based access systems to secured areas housing vital devices and data.
- Surveillance Systems: In, deploy CCTV cameras and IoT-device monitoring to real-time surveillance and improve physical security.
- Regular Maintenance: Conduct periodic inspections of farming devices and systems to identify and potential physical vulnerabilities and implement corrective measure to mitigate risks.
- Data Backups: Maintain secure off-site backups of vital data to ensure its recovery in case of data theft, damage and system failures.

4.7. Operational and Procedural Enhancements

Human nature and flawed protocol can make for higher exposure risks of CS. To address involve problem(s) [1][2]:

Conducting CS training for farmers, operators and stakeholders is critical in fostering safe practices, which include the "Training Programs". It includes methods for educating people to recognize phishing attempts; generating and utilizing robust passwords; and adhering to secure procedures to manage vital farming information.

It is crucial to have Incident Response Plans and regularly update them to ensure rapid initial response and effective reaction to cyber incidents. While ensuring a potential cyber incident does not have too much impact, these strategies should also have predetermined roles, responsibility and SCC to reduce cyber security impacts.

- **Regulatory Compliance:** adjusting operations to be able to follow both local and global CS regulations is crucial to ensure it is done in a best way. This means adhering to farming data protection legislation, common practices and security systems to reduce risks, strengthen the resilience of farming systems.

These focused mitigation steps will be fascinating PA stakeholders successfully tackle IoT, AI/ML, and emerging techniques CS challenges and threats. These methods not only provide to manage service operations and ensure the robustness of data but also they nourish indigenous trust and enhancing PA ecosystems resilience.

5. FUTURE ROADMAP IN CYBERSECURITY FOR PA

In future roadmap in cybersecurity is vital to utilizing proactive methods in CS, alongside through of IoT, AI-ML, drones, and emerging techniques. This roadmap for the future will be prioritized adapting to the changing nature of the threat and new techniques as well as resilience, adaptability, and sustainability in farming operations. The following is a strategic of the major areas of interest for future research and development in PA CS:

- **Advanced IoT Security Solutions:** Future work should concentrate on developing efficient, yet powerful, security solutions suitable for the particular challenges of IoT devices in PA. Research have explored quantum-safe cryptographic protocols to prepare for the advent of quantum computing that ensuring long-term security. Further, developing lightweight ML models to on-device anomaly detection will help secure devices with limited computational resources.

- **Resilient AI and ML Frameworks**: Adversarial attacks and biases should be taken into consideration when designing AI and ML systems. Future research should emphasize federated and decentralized learning frameworks that ensure data privacy without compromising analytical capabilities. Further, modern in XAI will be vital for fostering trust and accountability among stakeholders that making AI decisions more interpretable and actionable.

- **Enhanced Drone Security and Monitoring:** As drones become increasingly prevalent in PA, their CS must be continually improved. Further efforts should focus on implementing blockchain-based drone authentication solutions for improved trust and traceability. Studies also could include self-healing autonomous drones that adapt to threats so they could safely function in hostile environments.

- **Data Governance and Privacy Frameworks**: Future studies should focus on establishing secure data sharing mechanisms using privacy-preserving methods like homomorphic encryption and secure multiparty computation to handle data integrity and privacy issues, and also on creating standardized data governance frameworks to PA to ensure interoperability and prevent misuse or data breaches in the farming sector.

- **AI-Powered Physical and Environmental Security: In, t**he future roadmap should incorporate AI-powered surveillance systems capable of monitoring physical and environmental security in real-time. These systems will be detected unauthorized access, environmental anomalies, and tampering with farming equipment. Coupled with IoT-based alert approach that ensure proactive and responsive protection measures.

By aligning these future directions and roadmap with the unique needs of PA. This roadmap for CS will be ensure that sector remains resilient to cyber threats. Emphasizing innovation, collaboration, and proactive measures will prevent the integrity, reliability, and sustainability of PA in an increasingly connected global.

6. CONCLUSION

The rapid adoption of advanced technique and drone machine based-technique has transformed PA into a data-driven and highly connected ecosystem. While these advanced techniques enhance productivity, resource utilization, decision-making, and also introduced complex CS challenges that have compromised system reliability, data confidentiality, and operational continuity. This research developed a comprehensive CS framework to analyze, classification, identification, CS threats and risks, also financial losses in PA that evaluate technical, data-centric, and

operational security dimensions. The analysis identified vital vulnerabilities associated with connected modern technique with drone based-communication systems, and data integrity, demonstrating the need for security approaches especially designed for modern PA settings.

These finding focused on cyberattacks in PA have led to significant consequences, including service interruptions, financial losses, altered agricultural data, reduced food security, and diminished stakeholder trust. To address these risks, the study provides a combination of technical and organizational countermeasures, such as strengthening IoT security, improving the robustness of AI models, securing drone machine based-communication system, implementing privacy-preserving techniques, adopting zero-trust security architectures, and leveraging emerging modern techniques to enhance data integrity and supply chain transparency. These measures collectively enhance the resilience of interconnected agriculture systems while supporting secure farming operations.

Future work will implement and validate the proposed CS framework through real-world PA data by integrating advanced technique such as IoT, AI, ML, drones, FL, digital twins, and quantum-resistant cryptography to develop a secure, scalable, and resilient SF ecosystem.

SDG ALIGNMENT

This research contributes to SDG 2 (Zero Hunger), SDG 9 (Industry, Innovation and Infrastructure), SDG 12 (Responsible Consumption and Production), SDG 13 (Climate Action), and SDG 15 (Life on Land) by promoting secure, sustainable, and AI- and IoT-enabled precision agriculture.

SDG Keywords: SDG 2, SDG 9, SDG 12, SDG 13, SDG 15, Precision Agriculture, IoT, AI, Cybersecurity, Sustainable Agriculture.

7. Acknowledgment

Author would like to acknowledge the MCN NO: IU/R&D/2026-MCN0004856

REFERENCES

1. Ahmadi, S. (2023). *A systematic literature review: Security threats and countermeasure in smart farming*. Authorea Preprints.
2. Yazdinejad, A., Zolfaghari, B., Azmoodeh, A., Dehghantanha, A., Karimipour, H., Fraser, E., & Duncan, E. (2021). A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures. *Applied Sciences*, *11*(16), Article 7518.
3. Shrivastava, A., Praveen, R. V. S., Vemuri, H. K., Peri, S. S. S. R. G., Sista, S., & Hasan, M. M. (2027). Future directions and challenges in smart agriculture and cybersecurity. In *Sustainable agriculture production using blockchain technology* (pp. 265–276).
4. Sagar, S., & Birje, M. N. (2025). Precision agriculture using Internet of Things and cloud computing: A review. *SN Computer Science*, *6*(4), Article 3833.
5. Shinwari, A. K., Hameed, S., Akhter, M. S., Hassan, F. U., & Sani, A. (2026). A vision for the future: The next wave of innovation in precision agriculture. In *Advancing precision agriculture with AI and IoT* (pp. 427–456). IGI Global Scientific Publishing.
6. Ongadi, P. A. (2024). A comprehensive examination of security and privacy in precision agriculture technologies. *GSC Advanced Research and Reviews*, *18*(1), 336–363.
7. Angyalos, Z., Botos, S., & Szilágyi, R. (2021). The importance of cybersecurity in modern agriculture. *Journal of Agricultural Informatics*, *12*(2), 604.
8. de Araujo Zanella, A. R., Da Silva, E., & Albini, L. C. P. (2020). Security challenges to smart agriculture: Current state, key issues, and future directions. *Array*, *8*, Article 100048.
9. Elbasi, E., Mostafa, N., AlArnaout, Z., Zreikat, A. I., Cina, E., Varghese, G., & Zaki, C. (2022). Artificial intelligence technology in the agricultural sector: A systematic literature review. *IEEE Access*, *11*, 171–202.
10. Window, M. (2019). *Security in precision agriculture: Vulnerabilities and risks of agricultural systems* [Bachelor's thesis, Luleå University of Technology]. DiVA Portal.
11. Otieno, M. (2023). Review of the techniques and mechanisms for enhancing trust in Internet of Things for smart agriculture. *Global Journal of Engineering and Technology Advances*, *15*(1), 50–63.
12. Vangala, A., Das, A. K., Chamola, V., Korotaev, V., & Rodrigues, J. J. (2023). Security in IoT-enabled smart agriculture: Architecture, security solutions and challenges. *Cluster Computing*, *26*(2), 879–902.

13. Gupta, M., Abdelsalam, M., Khorsandroo, S., & Mittal, S. (2020). Security and privacy in smart farming: Challenges and opportunities. *IEEE Access*, *8*, 34564–34584.
14. Demestichas, K., Peppes, N., & Alexakis, T. (2020). Survey on security threats in agricultural IoT and smart farming. *Sensors*, *20*(22), Article 6458.
15. Peladarinos, N., Piromalis, D., Cheimaras, V., Tserepas, E., Munteanu, R. A., & Papageorgas, P. (2023). Enhancing smart agriculture by implementing digital twins: A comprehensive review. *Sensors*, *23*(16), Article 7128.
16. Bissadu, K., Hossain, G., & Vajpayee, P. (2024, May). *Agriculture 5.0 cybersecurity: Monitoring agricultural cyber threats with digital twin technology*. 2024 IEEE World AI IoT Congress (AIIoT), IEEE, (pp. 0252–0258).
17. Adewusi, A. O., Chikezie, N. R., & Eyo-Udo, N. L. (2023). Cybersecurity in precision agriculture: Protecting data integrity and privacy. *International Journal of Applied Research in Social Sciences*, *5*(10), 693–708.
18. Kuppusamy, P., & Khang, A. (2024). An advanced cybersecurity model for high-tech farming using machine learning approach. In *Agriculture and aquaculture applications of biosensors and bioelectronics* (pp. 461–495). IGI Global Scientific Publishing.
19. Kumar, S., Kumar, A., Kumar, S., & Chaurasia, P. K. (2023, September). *Comprehensive analysis of cloud security: Issues & challenges*. 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), IEEE, (Vol. 6, pp. 622–627).
20. Ali, G., Mijwil, M. M., Buruga, B. A., Abotaleb, M., & Adamopoulos, I. (2024). A survey on artificial intelligence in cybersecurity for smart agriculture: State-of-the-art, cyber threats, artificial intelligence applications, and ethical concerns. *Mesopotamian Journal of Computer Science*, *2024*, 53–103.
21. Kumar, S., Chaurasia, P. K., & Khan, R. A. (2022, December). Securing transmission of medical images using cryptography steganography and watermarking technique. In *International Conference on Cryptology & Network Security with Machine Learning* (pp. 407–420). Springer Nature Singapore.
22. Ansar, S. A., Kumar, S., Khan, M. W., Yadav, A., & Khan, R. A. (2020). Enhancement of two-tier ATM security mechanism: Towards providing a real-time solution for network issues. *International Journal of Advanced Computer Science and Applications*, *11*(7).
23. Kumar, S., Devi, M., Singh, S., Chaurasia, P. K., & Khan, R. A. (2023, September). *Prioritization of medical image security features: Fuzzy AHP approaches*. 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), IEEE, (Vol. 6, pp. 540–545).
24. Kumar, S., Singh, S., & Chaurasia, P. K. (2023, November). Enhancing security of medical image transmission: An innovative Fuzzy-AHP approach. In *International Conference on Trends in Computational and Cognitive Engineering* (pp. 471–483). Springer Nature Singapore.
25. Prosper, J. (2025). *Artificial intelligence and cryptographic protocols for secure data management: Applications in smart cities, mobile platforms, and precision agriculture*.
26. Kumar, S., Srivastava, A., Chaurasiya, P. K., Kushawaha, A., & Vishal, V. (2022, December). *DCT and SVD-based watermarking technique for imperceptibility and robustness of medical images*. 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), IEEE, (pp. 2335–2339).
27. Maraveas, C., Rajarajan, M., Arvanitis, K. D., & Vatsanidou, A. (2024). Cybersecurity threats and mitigation measures in Agriculture 4.0 and 5.0. *Smart Agricultural Technology*, *9*, Article 100616.
28. Kumar, S., & Faisal, M. (2024, November). *Critical review of cybersecurity risks in precision agriculture*. 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES), IEEE, (pp. 1–7).
29. Parvathala, B. R., & Kolli, S. (2025). Cyber biosecurity solutions for protecting smart agriculture and precision farming. In *Computer vision in smart agriculture and crop management* (pp. 25–55). Wiley.
30. Sharma, I., & Khullar, V. (2025). Blockchain-enabled federated learning-based privacy preservation framework for secure IoT in precision agriculture. *Journal of Industrial Information Integration*, *44*, Article 100765.
31. Russell, C., Botschner, J., Duncan, E., Dehghantanha, A., & Fraser, E. D. (2025). "I grow food, IT people do cybersecurity": Addressing cybersecurity risks in Canada's agri-food sector. *Smart Agricultural Technology*, *10*, Article 100866.
32. Zangana, H. M., Luckyardi, S., Mustafa, F. M., & Li, S. (2025). Enhancing agricultural cybersecurity: Leveraging deep learning and large language models for smart farming protection. In *Revolutionizing cybersecurity with deep learning and large language models* (pp. 307–338). IGI Global Scientific Publishing.
33. Addanki, U. K., Devareddi, R. B., Kamarajugadda, K. K., Pavani, M., & Gera, P. (2025). Machine learning-powered intrusion detection system for Agriculture 4.0: Securing the next generation of farming. *International Journal of Innovative Research and Scientific Studies*, *8*(1), 1964–1978.
34. Javed, N., Sadia, H., Ahmed, T., & Faisal, M. (2024). Blockchain technology-based framework to build cyber-secured smart cities. In *Intelligent networks* (pp. 198–215). CRC Press.
35. Daund, R. P., Haque, M. J., & Pawar, U. (n.d.). *Design of an improved model integrating blockchain, machine learning, and differential privacy for cybersecurity in smart farming*.
36. Kumar, S., Ahmad, M., Maurya, S. K., Pratap, R., Chaurasia, P. K., & Khan, R. A. (2025). Soft computing-driven framework for enhanced security in medical image transmission. *Proceedings of the National Academy of Sciences, India Section A: Physical Sciences*, 1–13.

37. Ahamad, M. K., & Bharti, A. K. (2021, March). *Prevention from COVID-19 in India: Fuzzy logic approach*. 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), IEEE, (pp. 421–426).
38. Ahmad, M., Pratap, R., Maurya, S. K., Iqbal, M. S. A., & Kumar, S. (2025). A unified framework for classifying big data security algorithms: A healthcare perspective. *Proceedings of the National Academy of Sciences, India Section A: Physical Sciences*, 1–11.
39. Sudha, S. P., & Loret, J. B. (2026). A review on machine learning-based precision agriculture techniques for crop farming monitoring with IoT. *Discover Environment*, *4*(1), Article 10.
40. Pandit, V., Sravya, M., Ravali, C., Fiaz, S., Tariq, A., & Chatterjee, S. (2026). Precision agriculture in the era of technological advancement. In *Artificial intelligence and data sciences for precision agriculture* (pp. 159–186). Springer Nature Switzerland.
41. Afaq, S. A., Izhar, S. K., & Srivastava, S. (2023). The IoT farming revolution: Enhancing efficiency and sustainability in agriculture. International Journal of Engineering Sciences & Emerging Technologies, 11(2), 160–170.
42. Afaq, S. A., Husain, M. S., Bello, A., & Sadia, H. (2023). A critical analysis of cyber threats and their global impact. In Computational intelligent security in wireless communications (pp. 201–220). CRC Press.