JOURNAL PUNJAB ACADEMY OF SCIENCES (Peer Reviewed Open Access Journal)
JPAS, 24: 15-32 (January-December 2024)
Available online at www.jpas.in
ISSN 2229-7014 (P)

CYBERSECURITY THREATS AND MITIGATION STRATEGIES IN AGRICULTURE 4.0 AND 5.0: CHALLENGES AND SOLUTIONS IN THE DIGITAL TRANSFORMATION OF AGRICULTURE

Bhagwant Singh[1], Sikander Singh Cheema[2*]
Department of Computer Science and Engineering, Punjabi University, Patiala, Punjab India.
*E-mail: bhagwantsinghresearch@gmail.com[1], *sikander@pbi.ac.in[2]

ABSTRACT

Agriculture's digital evolution through Agriculture 4.0 and 5.0 brings unprecedented technological advancements, notably through IoT, AI, and Blockchain integration, which boost productivity, precision, and sustainability. However, this rapid adoption of connected and intelligent systems also presents a wide range of cybersecurity vulnerabilities that threaten data integrity, operational continuity, and privacy. This review identifies and categorizes key cybersecurity threats in Agriculture 4.0 and 5.0, examining specific risks associated with IoT devices, data privacy, AI models, and Blockchain applications in agriculture. It further explores mitigation strategies such as device encryption, Blockchain security protocols, Explainable AI (XAI) for transparency, and secure data-sharing practices to counteract these risks. By analyzing the interplay between Blockchain and AI, this study highlights synergies that enhance security, transparency, and trust within digital agriculture systems. In discussing ongoing challenges, including economic constraints and scalability issues, this review emphasizes the need for interdisciplinary research and tailored cybersecurity frameworks to safeguard agriculture's digital transformation. Ultimately, securing Agriculture 4.0 and 5.0 is essential for strengthening global food systems, economic resilience, and the long-term sustainability of the agriculture sector.

Keywords: Cybersecurity, IoT in agriculture, Blockchain, AI security, Cyber-threats, Digital Agriculture.

INTRODUCTION

Agriculture 4.0 and 5.0 represent transformative shifts in farming, leveraging technology to address the increasing global demand for food while aiming for sustainable and efficient agricultural practices as shown in fig 1 (Maraveas et al., 2024)(Mesías-Ruiz et al., 2023). As the agricultural sector faces challenges like climate change, soil degradation, and limited resources, these advancements hold promise to enhance productivity and resource management. Agriculture 4.0 is often referred to as "smart farming" or "precision agriculture," driven by the integration of Internet of Things (IoT) devices, big data analytics, and automation. In this phase, farming systems rely on networked sensors, data analytics, and connected machinery to optimize inputs such as water, fertilizers, and pesticides. The result is an increase in crop yields, efficient use of resources, and a reduction in environmental impacts.

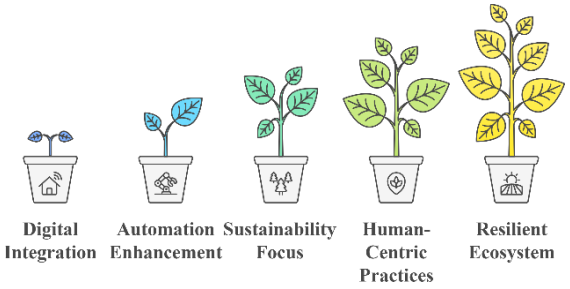

Fig. 1. Progression from Agriculture 4.0 to 5.0.

IoT and Sensor Technology

IoT forms the backbone of Agriculture 4.0, with a range of connected sensors and devices that gather real-time data from fields as shown in fig. 2. Sensors can measure soil moisture, temperature, humidity, and light levels, enabling farmers to monitor and manage field conditions remotely (Dineva & Atanasova, 2022) (Fan et al., 2023). By collecting granular data on crop conditions and soil health, IoT devices allow farmers to make data-driven decisions that optimize inputs.

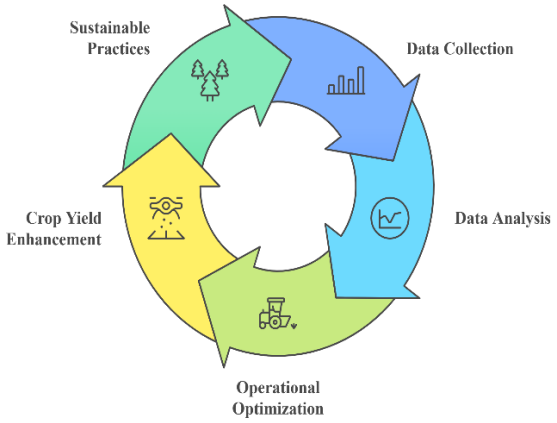

Fig. 2. IoT and Sensor Technology in Agriculture.

2. Data Analytics and Machine Learning

The wealth of data collected through IoT sensors is processed and analyzed using machine learning algorithms, which reveal patterns and provide predictive insights. For example, machine learning models can analyze historical weather patterns and forecast crop yields or identify potential risks like pest outbreaks (Joshi et al., 2023). Predictive analytics empowers farmers to plan ahead, mitigating potential losses and maximizing yields. Data analytics also enhances decision-making for planting schedules, harvest timings, and crop rotations, supporting more strategic and sustainable farming practices.

Automation and Robotics

Automation plays a key role in reducing labor demands and enhancing efficiency in Agriculture 4.0. Autonomous tractors, drones, and robotic systems can perform repetitive tasks like planting, weeding, and monitoring crop health. Drones equipped with multispectral cameras can survey fields, identifying stress areas and assessing plant health at a scale and speed that manual labor cannot achieve (Fei et al., 2023). Meanwhile, robotic harvesters are being developed to address labor shortages and streamline harvesting processes, particularly in crops like fruits and vegetables where manual picking has traditionally been the norm.

Cloud Computing and Connectivity

Agriculture 4.0 heavily depends on cloud computing to store, process, and share vast amounts of data. Through cloud platforms, farmers can access advanced analytics tools and visualizations that provide actionable insights into farm operations. Connectivity remains essential, with mobile apps and dashboards providing real-time data that is accessible from any location. However, one of the challenges for Agriculture 4.0 is reliable internet connectivity in rural areas (Goldstein et al., 2022). Nonetheless, advancements in satellite internet and mobile networks continue to improve connectivity, enabling broader adoption of smart farming technologies.

AGRICULTURE 5.0: THE RISE OF AUTONOMOUS SYSTEMS AND BLOCK-CHAIN IN AGRICULTURE

Agriculture 5.0 builds on the principles of Agriculture 4.0 but advances to an even more autonomous, resilient, and transparent system as illustrated in fig. 3. In this phase, artificial intelligence (AI) and Blockchain play central roles, empowering farmers to harness the full potential of digital tools while ensuring data security, trust, and accountability. Agriculture 5.0 is often characterized by its emphasis on "digital trust" and increased resilience through autonomous, AI-driven systems.

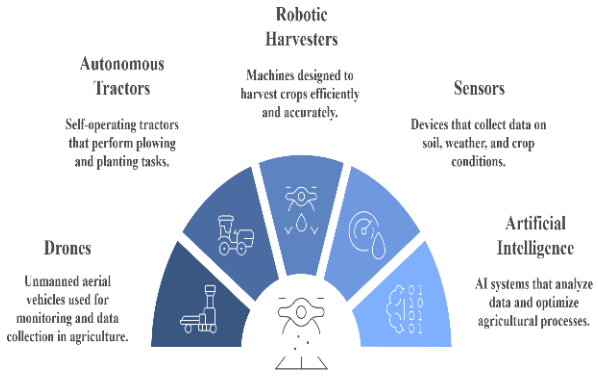

Fig. 3. Agriculture 5.0: The Rise of Autonomous Systems and Blockchain

Artificial Intelligence (AI) and Deep Learning in Agriculture

Agriculture 5.0 moves beyond basic automation by incorporating advanced AI systems that can learn, adapt, and optimize autonomously. Machine learning is refined into deep learning models capable of image

recognition, natural language processing, and predictive modeling at a higher precision. AI enables autonomous decision-making in farm management, as intelligent systems analyze data in real time to adjust operations without human intervention (Lin et al., 2020). For example, AI-powered systems can identify diseases in plants, analyze soil composition, and suggest targeted treatments, thereby reducing chemical use and improving crop quality.

AI also enables prescriptive analytics, where models go beyond predicting outcomes to suggesting specific actions, such as exact quantities of fertilizers for optimal yield. This prescriptive approach minimizes waste, reduces costs, and promotes eco- friendly practices (Lo & Pachamanova, 2023). Additionally, AI-driven chatbots and virtual assistants are being introduced to guide farmers with expert advice based on data from their specific farms, supporting precision farming on an individual scale.

Blockchain for Transparency and Trust

In Agriculture 5.0, Blockchain technology adds a new dimension by addressing issues related to trust, traceability, and data security. Blockchain creates decentralized and tamper-proof records that provide transparency across the agricultural supply chain. Every transaction, from seed purchase to final sale, can be recorded immutably on a Blockchain ledger, ensuring the authenticity and traceability of food products. Consumers, retailers, and regulators gain assurance that food items are produced, processed, and transported according to ethical and safety standards (Gazzola et al., 2023).

For farmers, Blockchain provides a secure platform to track transactions and supply chain logistics without relying on intermediaries. In regions where farmers face challenges in gaining access to fair markets or authenticating product origin, Blockchain enhances credibility and promotes equitable trade practices. Smart contracts self-executing contracts with terms written directly into code further streamline operations, allowing automated payments and data verification in transactions between farmers, suppliers, and buyers.

Integration of IoT, AI, and Blockchain

Agriculture 5.0 leverages the integration of IoT, AI, and Blockchain to create a cohesive, resilient ecosystem. IoT sensors gather data, AI processes it into actionable insights, and Blockchain stores these records securely, ensuring trust and accountability. This integration has transformative implications: in livestock management, IoT devices can monitor animal health metrics while AI predicts health issues, and Blockchain keeps track of each stage of the animal's life cycle, from farm to table. In crop production, data gathered from fields can be securely shared with stakeholders, offering verified information on farming practices and product quality (Wei et al., 2023).

Autonomous Machinery and Robotics in Agriculture 5.0

Autonomous machinery becomes more sophisticated in Agriculture 5.0, with AI enabling machinery to learn and improve over time. Self-driving tractors and drones now work collaboratively, coordinating tasks based on real-time conditions. For example, a tractor equipped with AI may autonomously switch to a different field or adjust its operations based on real-time soil and crop data. Robotics with AI-driven vision systems can identify and manage weeds, pests, or diseases with precise, localized treatments, promoting sustainable pest control practices and reducing pesticide overuse (Rondelli et al., 2022).

Sustainability and Climate Resilience

Agriculture 5.0 also focuses on sustainability by optimizing water, fertilizer, and pesticide use through data-driven insights, thus reducing environmental impacts. Climate resilience is a growing concern, and AI-powered predictive models enable farmers to respond proactively to adverse conditions. By using AI to monitor weather patterns and simulate scenarios, farmers can protect crops from extreme weather events and adjust planting schedules to suit shifting climate conditions. Blockchain enhances these efforts by ensuring that sustainable practices are verifiable and transparent throughout the supply chain (MacPherson et al., 2022).

The evolution from Agriculture 4.0 to Agriculture 5.0 represents a major shift in how agriculture is managed and practiced, with each phase bringing innovative technologies to address the sector's challenges. While Agriculture 4.0 introduced digital tools that increased efficiency and optimized resource use, Agriculture 5.0 pushes the boundaries further with autonomous AI and Blockchain, fostering a transparent and resilient food system. By leveraging IoT, AI, and Blockchain together, Agriculture 5.0 aims to create an interconnected, data-driven framework that enhances productivity, sustainability, and food security. As these technologies continue to develop, they will likely play a crucial role in meeting the agricultural demands of an expanding global population.

SIGNIFICANCE OF SECURING AGRICULTURE 4.0 AND 5.0

The cybersecurity of Agriculture 4.0 and 5.0 is paramount not only to protect digital agricultural systems but also to ensure the overall resilience and sustainability of the global food supply chain. As agriculture increasingly relies on digital systems, any security breach can result in widespread disruptions with severe economic, environmental, and societal consequences. Protecting these systems is critical for food security, as a single cyberattack targeting an essential component of digital agriculture could lead to crop failure, livestock harm, or supply chain breakdowns. For instance, a cyberattack that manipulates sensor data could compromise crop irrigation, leading to water wastage or drought-induced crop losses, ultimately affecting food availability and prices.

The economic resilience of the agriculture sector also hinges on the stability and reliability of its digital systems. Cyber threats could result in significant financial losses due to disrupted operations, loss of sensitive data, and potential litigation arising from breaches. For small- and medium-scale farmers who lack the resources to recover from such setbacks, cybersecurity incidents can be devastating, potentially leading to farm closures and impacting rural economies. The increasing interconnectedness of agriculture with other industries, including logistics, manufacturing, and retail, means that disruptions in agricultural cybersecurity could have a ripple effect, impacting multiple sectors and the broader economy.

Beyond economic and food security, the integrity of Agriculture 4.0 and 5.0 has important implications for societal welfare. Consumers today expect transparency in food sourcing and safety, and secure agricultural systems are essential to maintaining trust. Blockchain, for instance, is a powerful tool for traceability, helping to verify the origins of food products and ensuring that supply chain processes meet regulatory standards. If compromised, however, consumer trust in food quality and safety could deteriorate, affecting market dynamics and public health. Furthermore, a secure agricultural framework supports the development and acceptance of innovative technologies in farming communities, enabling a smoother transition to sustainable practices that can address climate change challenges. Therefore, securing Agriculture 4.0 and 5.0 is not merely a technological requirement but a societal imperative that safeguards food security, economic stability, and environmental sustainability.

RESEARCH SCOPE

This paper focuses on understanding and addressing the cybersecurity challenges posed by Agriculture 4.0 and 5.0 technologies. By systematically categorizing cybersecurity threats and mitigation strategies, this study aims to provide a comprehensive framework for safeguarding the digital transformation in agriculture.

The structure of this paper begins with an exploration of the technological landscape of Agriculture 4.0 and 5.0, emphasizing the roles of IoT, AI, and Blockchain. It details how these technologies function in a digital farming context and why they are critical for modern agricultural productivity and resilience. This section will establish the foundation of the technological landscape within agriculture, highlighting its role in economic and environmental sustainability.

Following the technological background, the paper delves into the specific cybersecurity threats that impact these technologies. This section categorizes threats by technology type IoT, AI, and Blockchain and provides concrete examples of vulnerabilities. For instance, it will discuss common risks associated with IoT devices, such as unauthorized access and DDoS (Distributed Denial of Service) attacks, which can disable large networks of agricultural sensors. In the context of AI, the paper will examine data poisoning and adversarial attacks that target machine learning models, posing threats to the accuracy of agricultural forecasts and recommendations. Regarding Blockchain, the focus will be on potential weaknesses within smart contracts and distributed ledger security that could affect supply chain transparency and food traceability.

Next, the paper explores mitigation strategies for these threats, outlining best practices and innovations to secure digital agricultural systems. In securing IoT networks, solutions include strong encryption methods, two-factor authentication, and hardware upgrades that make devices harder to exploit. AI security measures such as Explainable AI (XAI) and data validation protocols help ensure that machine learning models remain resilient to manipulation. For Blockchain security, strategies include consensus protocols, multi-signature requirements, and robust smart contract development frameworks to safeguard transactions within the agricultural supply chain.

The paper then explores synergies between Blockchain and AI in enhancing agricultural security. For example, Blockchain can record AI-generated data with an immutable timestamp, enhancing traceability and trust. AI, in turn, can monitor Blockchain networks for anomalies, creating a layered security approach that strengthens the resilience of digital agricultural systems.

Finally, the paper addresses ongoing challenges and suggests future research directions. Recognizing that cybersecurity in agriculture is an emerging field, the paper calls for further interdisciplinary research and innovation to address these challenges. By proposing a research agenda, it underscores the importance of continued exploration into tailored cybersecurity measures that can keep pace with the rapidly evolving digital agriculture landscape.

This structured approach ensures that the paper comprehensively addresses both the security challenges and solutions in Agriculture 4.0 and 5.0, emphasizing their significance for sustainable food production, economic resilience, and global food security. Through this study, the agricultural sector can gain insights into building secure, reliable, and scalable systems that enhance productivity without compromising data integrity or system reliability.

PAPER ORGANIZATION

The paper is organize to systematically address cybersecurity in modern agriculture. It begins with an introduction that highlights the significance of digital transformation through Agriculture 4.0 and 5.0, establishing the study's relevance and objectives. Next, the technological landscape is examined, focusing on key innovations such as the Internet of Things (IoT), Artificial Intelligence (AI), and Blockchain, and their roles in enhancing agricultural productivity and sustainability. The paper then identifies and categorizes cybersecurity challenges associated with these technologies, emphasizing vulnerabilities in IoT devices, AI systems, and Blockchain applications. In response to these challenges, the paper outlines mitigation strategies, discussing best practices and innovative solutions for securing IoT networks, protecting AI models, and fortifying Blockchain frameworks. It also explores synergies between technologies, particularly how Blockchain can enhance AI security, promoting a layered security approach. Future research directions are proposed, emphasizing the need for interdisciplinary collaboration to address ongoing cybersecurity challenges in agriculture. The paper concludes by summarizing key findings and underscoring the importance of addressing cybersecurity concerns in the digital agricultural landscape. This concise organization ensures a comprehensive exploration of the opportunities and challenges presented by advanced technologies in agriculture.

TECHNOLOGICAL BACKGROUND AND CYBERSECURITY IN AGRICULTURE

The transition to Agriculture 4.0 and 5.0 marks a shift toward integrating cutting-edge digital technologies that promise to revolutionize agricultural practices as depicts in fig. 4. With these advancements, the sector aims to enhance precision, efficiency, and sustainability. However, alongside the benefits, this digital transformation introduces significant cybersecurity challenges. To maintain the integrity, confidentiality, and availability of agricultural data and systems, a robust understanding of technological applications and potential security risks is essential (Shepherd et al., 2020).

A. Agriculture 4.0: IoT, Cloud Computing, and Data Analytics

IoT Applications in Agriculture 4.0

Agriculture 4.0 primarily revolves around the Internet of Things (IoT), which connects various physical devices across farms sensors, drones, automated machinery, and smart irrigation systems enabling real-time data collection and control. These IoT devices monitor soil conditions, crop health, weather, and livestock, allowing for precise decision-making that can significantly improve yield and resource management. For instance, soil moisture sensors in smart irrigation systems can automate water distribution, ensuring crops receive just the right amount of water based on real-time soil moisture data, saving both water and energy (Ma, 2023).

Cloud Computing and Data Analytics

The data generated from IoT devices is stored, processed, and analyzed using cloud computing. Cloud services facilitate the centralized management of this data, offering scalability and accessibility. Farmers and agronomists can access dashboards and analytics tools on various devices, gaining valuable insights into crop health, resource usage, and potential yield forecasts. Additionally, cloud-based data analytics allows for more sophisticated machine learning models that can predict disease outbreaks, optimize harvest times, and manage supply chain logistics. Data analytics enhances productivity, enabling farmers to act proactively rather than reactively (Méndez-Guzmán et al., 2022).

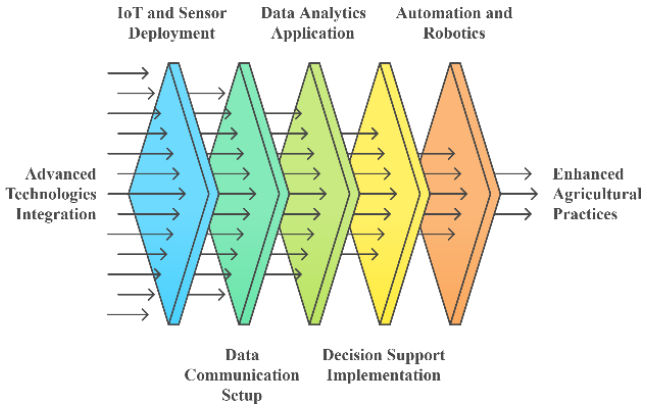

Fig. 4. Enhancing Agriculture through Technology.

Cybersecurity Concerns in Agriculture 4.0

The integration of IoT and cloud computing in Agriculture 4.0 brings multiple security challenges. The widespread use of IoT devices introduces vulnerabilities as these devices often lack built-in security features (Demestichas et al., 2020). Common cybersecurity issues include the following:

- **Data Breaches:** IoT devices collect and transmit sensitive agricultural data, which can include proprietary farming techniques, crop health information, and even personal data about farm workers. Without adequate security protocols, these devices are vulnerable to data breaches that could expose this information to unauthorized parties.
- **IoT Vulnerability:** IoT devices are susceptible to unauthorized access, hijacking, and denial-of-service attacks. For instance, a hacker could take control of irrigation systems, leading to intentional over-watering or under-watering that can harm crop yields.
- **Insufficient Data Encryption:** In many cases, data transmitted between IoT devices and cloud servers are not properly encrypted, exposing it to interception and manipulation during transit.
- **Cloud Security Risks:** Cloud-based data can be targeted by attackers aiming to disrupt access or compromise stored data. As farmers rely more on cloud analytics, the risk of cloud service breaches

such as those resulting from misconfigured permissions or compromised user accounts becomes a serious concern.

Securing Agriculture 4.0 requires addressing these cybersecurity issues through stronger encryption protocols, secure device authentication, and regular security audits for cloud services (Demestichas et al., 2020).

B. Agriculture 5.0: AI and Blockchain Integration

AI in Agriculture 5.0

Agriculture 5.0 builds upon the foundation of Agriculture 4.0 by incorporating artificial intelligence (AI) and machine learning to further optimize agricultural processes. AI models analyze large datasets generated from IoT devices, climate data, and historical agricultural records to improve decision-making. Examples of AI applications in agriculture include precision spraying, automated weed control, yield prediction, and crop disease detection. Through image recognition and data analytics, AI systems can identify specific pests or crop diseases in real time, allowing farmers to take immediate action and reduce crop loss (Oliveira & Silva, 2023).

Blockchain for Data Integrity and Trust

Blockchain technology adds a layer of transparency and security to agriculture by creating immutable records of transactions and data exchanges. In Agriculture 5.0, Blockchain is used to trace the origin and journey of agricultural products, ensuring transparency and accountability within the supply chain. This is particularly beneficial in organic farming and food safety, where end consumers can verify the authenticity of their products. Blockchain also supports secure data sharing, allowing multiple stakeholders such as farmers, distributors, and regulators to access data without the risk of unauthorized alterations.

C. Advanced Cybersecurity Issues in Agriculture 5.0

While AI and Blockchain bring transformative benefits, they also introduce sophisticated cybersecurity challenges:

Adversarial Attacks on AI Models: Adversarial attacks involve introducing subtle manipulations to input data to deceive AI models. In agriculture, an adversarial attack could mislead an AI-based pest detection system into incorrectly identifying a healthy crop as diseased, or vice versa. This vulnerability threatens the reliability of AI applications in agriculture, making it crucial to develop robust AI models resilient to such manipulations.

Blockchain Security Concerns: Although Blockchain offers strong security through its decentralized and immutable nature, it is not immune to attacks. For instance, a "51% attack" could theoretically allow a bad actor to gain control over the Blockchain network, enabling data tampering or double-spending. Smart contracts, which are automated scripts embedded within Blockchain transactions, may also contain vulnerabilities if not properly coded, exposing agricultural supply chains to potential exploitation.

Data Privacy in AI and Blockchain Integration: Blockchain records are permanent, raising concerns over data privacy, especially if sensitive agricultural information or personal data about farm workers is recorded. Data privacy laws, such as GDPR, necessitate careful consideration of how and where agricultural data is stored and who has access to it.

Ensuring the security of AI and Blockchain technologies in Agriculture 5.0 requires robust security measures, including adversarial training for AI models, secure smart contract development practices, and privacy-preserving mechanisms for Blockchain.

D. Importance of Cybersecurity in Agricultural Digitization

The digitization of agriculture holds immense potential to revolutionize the sector, but cybersecurity remains critical to preserving this potential. Real-world cybersecurity incidents in agriculture highlight the devastating impact that security breaches can have on agricultural operations and food supply chains:

Ransomware Attack on a Dairy Cooperative: In 2021, a ransomware attack targeted a large U.S. dairy cooperative, halting production and disrupting supply chains. Cybercriminals encrypted essential data, demanding a ransom for decryption. This incident highlighted the vulnerability of agricultural infrastructure to ransomware and the economic impact of such attacks.

IoT Vulnerabilities in Smart Farms: A 2020 study revealed that many IoT devices in smart farms, such as temperature sensors and irrigation systems, were vulnerable to hacking. In one example, researchers demonstrated how they could take control of an irrigation system remotely, potentially causing significant crop damage by manipulating water flow.

Blockchain Security in the Supply Chain: In an attempt to improve traceability, some agribusinesses adopted Blockchain for supply chain tracking. However, poorly implemented Blockchain solutions faced security issues, such as unauthorized access to sensitive trade data due to weak user authentication protocols. These incidents underscore the need for secure Blockchain implementations in agriculture.

The consequences of such attacks include financial losses, crop damage, and compromised consumer trust. As agriculture becomes more digitized, a proactive approach to cybersecurity is essential. Preventative measures, such as secure IoT device management, Blockchain auditing, and AI model robustness testing, can mitigate these risks and help protect the agricultural sector from cyber threats.

The adoption of digital technologies in Agriculture 4.0 and 5.0 marks a transformative era for the sector. However, without addressing the cybersecurity vulnerabilities that accompany these advancements, the risks may outweigh the benefits. As IoT, AI, and Blockchain become integral to agriculture, protecting data, ensuring system integrity, and maintaining trust among stakeholders become paramount. The development of resilient cybersecurity strategies is critical to safeguarding the future of digital agriculture and securing global food systems.

CYBERSECURITY THREATS IN AGRICULTURE 4.0 AND 5.0

As agriculture advances through the digital integration of technologies such as the Internet of Things (IoT), artificial intelligence (AI), and Blockchain, new cybersecurity threats emerge, exposing this critical sector to unprecedented risks. In Agriculture 4.0 and 5.0, reliance on connected devices, autonomous systems, and data-driven tools transforms how agricultural tasks are conducted but also creates numerous vulnerabilities (Ibrahim & Truby, 2023). Here, we delve into the cybersecurity threats associated with IoT and sensor networks, data privacy, Blockchain, AI, and supply chain management, highlighting specific threats that stakeholders must address to secure the future of agriculture shown in Table 1.

A. IoT and Sensor Networks Vulnerabilities

IoT and sensor networks play a vital role in Agriculture 4.0 by enabling precision farming practices, monitoring environmental conditions, and automating processes like irrigation and fertilization. Despite their benefits, these devices are vulnerable to various security risks due to their connection to open networks and limited computational resources. Key threats include unauthorized data access, Distributed Denial of Service (DDoS) attacks, and device hijacking (Son et al., 2023).

Unauthorized Data Access: In an agricultural setting, sensors collect vast amounts of data, from soil moisture levels to crop health indicators. Unauthorized access to this data poses a significant risk, as intruders can manipulate or misinterpret the information, potentially leading to poor decision-making, yield loss, or market disruptions. Furthermore, sensitive data, such as farm geolocation or proprietary methods, can be exploited if accessed by competitors or malicious entities. Many IoT devices lack advanced encryption protocols, making them easy targets for attackers looking to intercept data.

DDoS Attacks: A DDoS attack overwhelms devices with an excessive volume of requests, rendering IoT devices and networks unable to function. In agriculture, DDoS attacks on IoT networks could disrupt irrigation, pest control, or even harvest schedules, leading to delayed operations and potential crop loss. As IoT networks often rely on cloud services for data storage and analysis, they are particularly vulnerable to such attacks, given that any disruption can have cascading effects on connected systems.

Device Hijacking: Hackers can take control of IoT devices by exploiting software vulnerabilities, gaining unauthorized access to system settings and controlling devices remotely. Device hijacking in an agricultural setting could lead to unauthorized adjustments to crop treatments, livestock management, or drone applications, all of which can have serious consequences for farm productivity and safety. Moreover, hijacked devices can be used as entry points for broader attacks on farm networks, threatening data security and operational integrity.

B. Data Privacy and Security Concerns

Agriculture 4.0 and 5.0 heavily rely on data, much of which is sensitive and proprietary. Data privacy and security have become central issues, as breaches can have far-reaching consequences for farmers, agribusinesses, and consumers (Raturi et al., 2022).

Threats to Sensitive Agricultural Data: Agricultural operations generate diverse types of sensitive data, such as crop genetics, farm production levels, livestock health metrics, and precise geolocation information. Unauthorized access to this data may result in intellectual property theft, reduced competitiveness, or reputational damage. For instance, competitors who gain access to proprietary farming techniques could use this information to replicate or undermine a producer's competitive advantage.

Impact on Stakeholders: Data breaches not only threaten individual farmers but also the entire agricultural supply chain, impacting agronomists, researchers, suppliers, and consumers. Breaches can compromise trust in food safety, regulatory compliance, and traceability. Additionally, any compromise in data integrity can lead to financial losses, market volatility, and disruptions to production.

Insufficient Data Protection Mechanisms: A major concern in agriculture is the lack of standardized protocols for data security across the diverse range of IoT devices and platforms. Many systems do not incorporate strong encryption, secure authentication, or access controls, making it easier for attackers to breach databases and misuse data. Addressing these gaps requires integrating robust data protection measures, such as end-to-end encryption and multi-factor authentication.

C. Blockchain and Distributed Ledger Threats

Blockchain technology, widely adopted in Agriculture 5.0 for supply chain transparency and data security, also presents unique cybersecurity challenges. Though Blockchain is generally considered secure, specific vulnerabilities like 51% attacks, data manipulation, and smart contract exploitation need to be addressed (Al-Bassam et al., 2018).

51% Attacks: A 51% attack occurs when a single entity gains control over more than half of a Blockchain network's computational power, allowing them to alter the Blockchain ledger. In an agricultural context, this could compromise the authenticity of transactions, leading to fraudulent data or loss of trust. Agricultural Blockchain networks, particularly those that are smaller or decentralized, may be more vulnerable to such attacks.

Data Manipulation: While Blockchain is often immutable, certain Blockchain structures or private Blockchain models may allow participants to manipulate data. This vulnerability could lead to altered records in supply chain transactions or farm data tracking, undermining transparency and trust in the technology. For instance, malicious actors could manipulate pesticide records, certification data, or origin details, potentially impacting food safety and market credibility.

Smart Contract Exploitation: Smart contracts automate transactions based on predefined conditions but can be exploited if poorly coded. In agriculture, smart contracts govern payments, product tracking, and quality certifications. Vulnerable contracts could result in incorrect payments, delays in supply chain transactions, or fake product certifications, disrupting operations and potentially causing significant financial loss.

D. AI and Machine Learning Security Risks

AI and machine learning applications in Agriculture 4.0 and 5.0 contribute to advancements in predictive analytics, autonomous machinery, and precision farming. However, these technologies also bring significant security risks, such as adversarial attacks and data poisoning (Kurniawan et al., 2022).

Adversarial Attacks: Adversarial attacks manipulate input data to deceive AI models. In agriculture, these attacks could lead AI-based monitoring systems to misinterpret crop health, soil quality, or pest presence, resulting in suboptimal farming decisions. An adversarial attack on an autonomous tractor's vision system, for example, could lead to incorrect navigation or inappropriate use of chemicals.

Data Poisoning: AI models are highly dependent on data quality. In data poisoning attacks, malicious actors intentionally inject corrupt or misleading data into an AI system's training dataset, compromising the model's reliability. In agriculture, compromised data could mislead crop yield predictions, pest control strategies, or irrigation planning, causing economic loss and operational inefficiency.

Lack of Explainability: AI models, especially deep learning algorithms, often operate as "black boxes," making it challenging to verify their decisions. This lack of transparency can be exploited by attackers to hide malicious activities or manipulate AI outputs undetected. Ensuring explainability, particularly with Explainable AI (XAI) frameworks, is crucial for maintaining trust and accountability in agricultural applications.

Supply Chain and Smart Contract Vulnerabilities

The agricultural supply chain relies on transparency, trust, and efficiency, increasingly enabled by Blockchain and smart contracts. However, these technologies also introduce unique security vulnerabilities that must be managed (Hameed et al., 2022).

Threats to Supply Chain Integrity: Agriculture supply chains are complex, involving numerous stakeholders and transaction points. Cyber threats can disrupt supply chain integrity by altering transaction data, creating counterfeit records, or delaying deliveries. Such disruptions can cause market fluctuations, delays in food supply, and potential financial losses for stakeholders.

Blockchain-related Supply Chain Issues:

Although Blockchain enhances transparency, the supply chain may still face vulnerabilities if consensus protocols are compromised or participants act maliciously. Blockchain-based systems in agriculture, if misused, can allow data alteration or unauthorized access to records, affecting product traceability and food safety.

Smart Contract Exploitation: Supply chains frequently use smart contracts for automated transactions and quality control checks. Exploited smart contracts could allow unauthorized access to sensitive information, such as shipment routes or pricing, disrupting market conditions and harming stakeholders. Furthermore, if a contract is manipulated, it may lead to incorrect payments, unverified quality certifications, or counterfeit product entries. In conclusion, as Agriculture 4.0 and 5.0 continue to integrate innovative technologies, these systems must account for cybersecurity challenges to protect stakeholders, sustain operational reliability, and build trust in digital agricultural ecosystems.

Mitigation Measures and Security Solutions

As Agriculture 4.0 and 5.0 technologies grow in sophistication, so do the cybersecurity risks associated with their implementation. Addressing these vulnerabilities requires a robust suite of strategies tailored to the unique demands of IoT,

Blockchain, and AI in agriculture. This section explores key mitigation measures, from IoT security practices to advanced techniques in Blockchain, Explainable AI (XAI), data encryption, and secure supply chain management using smart contracts.

Table 1. Cybersecurity Threats In Agriculture 4.0 And 5.0

Author, Year	Cybersecurity Threat	Threat Description	Impact	Mitigation Strategies	Research Gaps
(Son et al., 2023)	IoT and Sensor Networks Vulnerabilities	IoT devices in agriculture collect and transmit sensitive farm data but are often poorly secured	Unauthorized access to data, potential disruptions in real-time monitoring, and control of farm operations	Implementing device authentication, regular firmware updates, and network segmentation to reduce unauthorized access.	Enhanced security frameworks for resource-constrained IoT devices in agricultural environments.
(Raturi et al., 2022)	Data Privacy and Security Concerns	Large volumes of data, including sensitive farm data and business intelligence, are stored digitally.	Exposure of sensitive data, privacy breaches, and potential misuse of farm management strategies by attackers.	Data encryption, secure storage solutions, and compliance with data privacy regulations (e.g., GDPR, CCPA)	Developing effective privacy-preserving methods tailored to the unique needs of agricultural data.
(Al-Bassam et al., 2018)	Blockchain and Distributed Ledger Threats	Blockchain is used for secure data sharing and smart contracts in agriculture, yet can be exploited.	Exploits in smart contracts and vulnerabilities in consensus protocols can disrupt trust and operations.	Smart contract audits, formal verification, and using hybrid consensus mechanisms to ensure secure transactions.	Investigating lightweight, secure consensus algorithms suited to decentralized agricultural data.
(Kurniawan et al., 2022)	AI and Machine Learning Security Risks	AI algorithms analyze vast agricultural data for decision-making, but can be vulnerable to attacks.	Potential for adversarial attacks leading to inaccurate predictions, mismanagement, or farm operational risks.	Adversarial training, robust model evaluation techniques, and secure data pre-processing methods.	Exploring interpretability and robustness in agricultural AI to ensure reliable, explainable models
(Hameed et al., 2022)	Supply Chain and Smart Contract Vulnerabilities	Integrated supply chains rely on smart contracts, creating vulnerabilities in logistics and traceability.	Supply chain disruptions, fraud, and counterfeit products affecting agricultural operations and food safety.	Secure multi-party computations, zero-knowledge proofs, and enhancing Blockchain-based supply chain traceability.	Advancing secure, scalable smart contract frameworks specific to agricultural supply chains

IOT AND SENSOR SECURITY STRATEGIES

The Internet of Things (IoT) is integral to Agriculture 4.0 and 5.0, enabling real-time data

collection from sensors and devices distributed across vast agricultural landscapes. However, IoT's interconnectivity makes it highly vulnerable to cyber threats, necessitating stringent security practices (Trnka et al., 2022).

Encryption: Encryption is fundamental to protecting data transmitted between IoT devices. By converting information into unreadable formats without decryption keys, encryption secures data against interception and unauthorized access. Lightweight encryption protocols, such as TinySec or SIMON/SPECK, are especially effective for low-power IoT devices used in agriculture, as they balance security with resource efficiency.

Authentication: Authentication mechanisms are vital for verifying the identities of users and devices within IoT networks. Techniques like multi-factor authentication (MFA) and biometric verification ensure only authorized users can access the network. Mutual authentication, where both devices authenticate each other before data exchange, adds another layer of protection, particularly for sensitive agricultural data.

Hardware-level Security: Hardware-based security solutions strengthen IoT devices against physical tampering and unauthorized reprogramming. Secure hardware enclaves and Trusted Platform Modules (TPMs) are widely adopted to protect encryption keys and other sensitive data directly on IoT devices. In agriculture, securing IoT hardware is critical, especially when sensors and devices are deployed in remote or unmonitored locations.

Regular Firmware Updates and Patch Management: As new vulnerabilities in IoT firmware are frequently discovered, keeping devices updated with the latest firmware patches minimizes potential attack vectors. Automated patch management systems ensure all devices remain secure, reducing the chances of cyberattacks exploiting outdated software.

BLOCKCHAIN SECURITY MECHANISMS IN AGRICULTURE

Blockchain technology has emerged as a powerful tool for enhancing trust, traceability, and data integrity in Agriculture 5.0, especially within data-sharing ecosystems. Yet, Blockchain itself is susceptible to attacks such as double-spending, 51% attacks, and smart contract vulnerabilities. Implementing strong Blockchain security mechanisms is essential for agriculture's digital security (Song et al., 2023).

Consensus Mechanisms: Consensus protocols, such as Proof of Work (PoW) and Proof of Stake (PoS), are integral to Blockchain's security. They prevent malicious actors from manipulating data by requiring network consensus for any transaction. While PoW is resource-intensive, PoS offers an energy-efficient alternative, making it suitable for agricultural applications where sustainability is a priority. These mechanisms ensure that only validated data is recorded on the Blockchain, enhancing trust across the agricultural value chain.

2. Multisignature Protocols: Multisignature (or multisig) protocols add a layer of security to Blockchain transactions by requiring multiple parties to sign off before a transaction is executed. This ensures that no single entity has control over data or resources within the Blockchain, reducing the risk of fraud or unauthorized transactions. In agriculture, multisig protocols provide safeguard for sensitive operations, such as transferring ownership of digital assets or accessing critical data in shared networks.

Blockchain-based Auditing: Blockchain's inherent immutability offers a reliable framework for data auditing. By maintaining a transparent and unalterable record of transactions, Blockchain auditing enhances traceability, which is crucial for food safety and regulatory compliance in agriculture. Blockchain-based auditing also aids in identifying security breaches or anomalies in real-time, allowing quick remediation and enhancing overall network security.

ARTIFICIAL INTELLIGENCE SECURITY AND EXPLAINABLE AI (XAI) IN AGRICULTURE

Artificial intelligence (AI) is pivotal in Agriculture 5.0, driving predictive analytics, automated

decision-making, and crop monitoring. However, AI's complexity also introduces risks, including adversarial attacks where malicious actors manipulate input data to mislead AI algorithms. Explainable AI (XAI) mitigates these threats by providing transparency and interpretability in AI-driven decision processes (Lahza et al., 2023).

Role of XAI in Agriculture Security: XAI frameworks make AI decision-making processes understandable, enabling users to trace the logic behind AI-driven outcomes. This transparency is crucial in agriculture, where AI is used to manage resources, predict crop yields, and monitor pests. XAI helps identify anomalies or inconsistencies in AI predictions, flagging potential threats or inaccuracies that may arise from adversarial manipulation.

Reducing Vulnerability to Adversarial Attacks: XAI mitigates the risks of adversarial attacks by allowing stakeholders to verify and trust AI outputs. For instance, if an AI model suggests unusual irrigation levels for a crop, XAI can provide insights into why the recommendation was made. This clarity helps identify potential attacks early and ensures AI models are resilient against data manipulation.

Ethics and Bias Mitigation: XAI also plays a critical role in minimizing bias, a prevalent issue in machine learning models that can lead to flawed or discriminatory decisions. In agriculture, unbiased AI decisions are vital for fair resource allocation and management, making XAI a valuable tool for both security and ethical AI deployment.

CHALLENGES IN AGRICULTURAL CYBERSECURITY

The adoption of digital technologies in agriculture, such as IoT, AI, and Blockchain, has revolutionized traditional farming practices by enhancing precision, efficiency, and productivity. However, integrating these technologies also brings cybersecurity challenges that can impact data integrity, operational continuity, and trust in digital agricultural systems. Addressing these challenges effectively requires acknowledging both current barriers to cybersecurity in agriculture and exploring avenues for future research and interdisciplinary collaboration depicts in Table 2.

A. Challenges in Cybersecurity Adoption

Economic and Logistical Constraints

The agricultural sector faces significant economic and logistical hurdles in implementing effective cybersecurity measures, especially given its unique characteristics and diverse stakeholders. Most agricultural operations have limited budgets, particularly smaller and medium-sized farms, making it challenging to invest in sophisticated cybersecurity solutions. High upfront costs for secure IoT devices, Blockchain infrastructure, and AI solutions may be prohibitively expensive, particularly when farmers are already burdened with costs related to equipment, labor, and fluctuating market conditions. In regions where agriculture is the primary economic activity, allocating funds to cybersecurity may be viewed as a lower priority compared to investments in productivity-enhancing technologies.

Additionally, logistical barriers complicate cybersecurity adoption in agriculture. Many farms and agricultural sites are located in rural or remote areas with limited internet access, which can restrict the implementation of robust, cloud-dependent security systems. Ensuring that cybersecurity solutions are accessible, operable, and maintainable in these regions is a major logistical challenge. Furthermore, the decentralized nature of agriculture, where operations are spread (Lahza et al., 2023). Across vast geographical areas, complicates centralized management of cybersecurity. For instance, securing IoT sensors and devices across thousands of acres requires both physical and digital monitoring, which can be resource-intensive.

Limited Awareness and Technical Knowledge

Cybersecurity literacy among farmers and agribusiness operators remains low, making it challenging to implement and maintain secure systems. Many farmers may not be aware of the cybersecurity risks associated with using IoT devices and digital platforms, leading to insufficient or inconsistent security practices. As a result, even if

sophisticated security systems are put in place, they may not be used or monitored effectively. This gap in cybersecurity knowledge extends to understanding the importance of regular software updates, password management, and the secure handling of sensitive data (Nurse, 2021).

Fragmented Regulatory Framework

Cybersecurity regulations in agriculture are often fragmented and underdeveloped, which complicates efforts to establish industry-wide standards. Unlike sectors such as finance or healthcare, agriculture lacks a unified regulatory framework governing cybersecurity practices. Existing policies are often region-specific or industry-specific, leading to inconsistencies in security standards and practices across the agricultural supply chain. This lack of regulatory uniformity also means that farmers and agricultural organizations have limited guidance on how to effectively secure their digital assets (Simone Stephen et al., 2023)(Martin Otieno, 2023).

Table 2. Challenges in Agricultural Cybersecurity

Author, Year	Challenges	Challenge Description	Impact on Agricultural Sector	Potential Solutions	Future Research Directions
(Lahza et al., 2023)	Economic and Logistical Constraints	High costs associated with secure IoT devices, AI, and Blockchain solutions make cybersecurity measures less accessible to small and medium-sized farms. Geographical isolation of farms limits access to reliable internet, impacting security implementation	Increased vulnerability to cyber-attacks in smaller farms; limited ability to deploy advanced security infrastructure, leading to uneven protection.	Explore subsidies or financial incentives for small farms; develop cost-effective, offline-capable cybersecurity solutions that work in rural and remote settings.	Research cost-effective cybersecurity technologies tailored for resource-constrained, decentralized agricultural environments.
(Nurse, 2021)	Limited Awareness and Technical Knowledge	Low cybersecurity awareness among farmers and agribusinesses results in poor security practices, such as weak password management and infrequent software	Cybersecurity risks go unmanaged; even high-tech systems may become vulnerable due to improper use, potentially disrupting farm operations.	Initiate cybersecurity training programs for farmers; provide user-friendly security interfaces on IoT and digital platforms for ease of use.	Study effective methods of cybersecurity education for non-technical users in agriculture, assessing long-term impacts.

		updates, making farms more vulnerable to attacks.			
(Simone Stephen et al., 2023)	Fragmented Regulatory Framework	The absence of unified cybersecurity regulations in agriculture creates inconsistencies, with varying standards based on region or industry sector, complicating secure practices across the agricultural supply chain.	Lack of clear regulatory guidance can lead to compliance challenges and security gaps, weakening overall security posture in the sector.	Develop a standardized cybersecurity framework tailored for agriculture; encourage global cooperation on agricultural cybersecurity standards	Investigate frameworks for harmonizing agricultural cybersecurity policies, especially for cross-border supply chain security.

CONCLUSIONS

The digital transformation of agriculture brings immense potential for enhancing productivity and sustainability but also introduces complex cybersecurity challenges that require comprehensive solutions. Economic and logistical constraints, limited cybersecurity knowledge, and a fragmented regulatory framework are some of the primary barriers to cybersecurity adoption in agriculture. Future research into scalable Blockchain solutions, lightweight encryption, and Explainable AI can address many of these challenges. Collaborative, interdisciplinary approaches that involve experts from computer science, agronomy, and policy-making are essential for developing holistic and effective cybersecurity frameworks that can safeguard agriculture's digital future. Agriculture 4.0 and 5.0 have revolutionized traditional farming practices by integrating IoT, AI, Blockchain, and data analytics, providing transformative improvements in productivity, efficiency, and sustainability. However, these advancements bring a suite of cybersecurity risks that threaten the reliability, confidentiality, and availability of agricultural systems. Major threats identified include vulnerabilities in IoT devices and sensor networks, which are prone to data breaches, unauthorized access, and Distributed Denial of Service (DDoS) attacks. Since IoT devices often lack robust security measures, they present a gateway for attackers to manipulate operational data, disrupt farming processes, and cause potential damage to crops and livestock management. The review also examined data privacy risks arising from the vast amounts of sensitive data generated by digital agriculture systems. These risks are compounded by inadequate encryption standards and weak authentication protocols, creating opportunities for data theft and privacy breaches.

Additionally, the deployment of AI in agriculture, though beneficial for predictive analytics and decision-making, introduces its own vulnerabilities. Adversarial attacks, data poisoning, and model manipulation are significant threats, potentially compromising the accuracy and reliability of AI-driven decisions. Blockchain, while promising as a tool for transparency and traceability, is also susceptible to security challenges, such as 51% attacks, smart contract vulnerabilities, and double-spending. Smart contracts, commonly used to

automate transactions in agricultural supply chains, are particularly vulnerable to exploitation if not properly coded, resulting in potential financial losses or compromised trust among stakeholders.

To counter these threats, a range of mitigation measures were explored. Securing IoT devices with advanced encryption, multi-factor authentication, and regular software updates is essential to safeguard data transmitted within interconnected farming systems. Data privacy can be strengthened through techniques like privacy-preserving data sharing and homomorphic encryption, ensuring that sensitive information remains protected even when shared across platforms. For AI security, the implementation of Explainable AI (XAI) enhances transparency, allowing for improved oversight and a better understanding of machine learning decisions. This approach helps mitigate risks associated with adversarial attacks and enhances trust among users. Furthermore, Blockchain specific solutions, such as consensus algorithms, robust smart contract auditing, and multi-signature wallets, were highlighted as effective measures to address Blockchain's inherent vulnerabilities and strengthen data integrity in agriculture.

FUTURE RESEACH DIRECTION

To fully secure Agriculture 4.0 and 5.0, ongoing research and investment in cybersecurity are essential. As threats continue to evolve in sophistication, so must the security measures designed to counter them. One of the pressing research needs is the development of lightweight encryption and security solutions tailored specifically to IoT devices used in agriculture, as conventional security solutions often demand high processing power and are unsuitable for low-power IoT sensors. Additionally, there is a need for AI models that are not only explainable but also resilient to adversarial attacks. This can be achieved through research into defensive machine learning techniques, which make AI systems more robust against data manipulation.

Another critical area for development is the refinement of Blockchain solutions to improve scalability, transaction speed, and energy efficiency. Current Blockchain implementations can be resource-intensive, which poses challenges for large-scale agricultural applications where high transaction volumes are common. Research into alternative consensus mechanisms, such as Proof of Stake (PoS) or hybrid models, can help make Blockchain more viable and environmentally sustainable for agriculture. Enhanced smart contract auditing tools are also necessary to ensure the reliability of automated contracts in agricultural supply chains. Interdisciplinary collaboration will be essential to address these challenges effectively. Cybersecurity research in agriculture should integrate insights from agronomy, data science, and policy-making to create holistic solutions that are technologically sound and practically implementable. Policy-level interventions are also crucial; governments and regulatory bodies must establish frameworks that mandate cybersecurity standards in agricultural technology, similar to regulations seen in sectors like finance and healthcare. Furthermore, industry partnerships are needed to ensure that innovative cybersecurity measures are adopted at scale. Investing in cybersecurity training for farmers and agricultural technology providers can build awareness and capacity for implementing secure practices at the ground level. Large agricultural firms and technology developers should collaborate to create accessible cybersecurity solutions that cater to the varied needs of the agriculture sector. Public-private partnerships and incentives for adopting advanced cybersecurity solutions could help accelerate this shift, ensuring that agricultural systems remain protected against cyber threats.

REFERENCES

Al-Bassam, M., Sonnino, A., Bano, S., Hrycyszyn, D., & Danezis, G. (2018). Chainspace: A Sharded Smart Contracts Platform. *25th Annual Network and Distributed System Security Symposium, NDSS 2018, February*. https://doi.org/10.14722/ndss.2018.23241

Demestichas, K., Peppes, N., & Alexakis, T. (2020). Survey on security threats in agricultural iot and smart farming. *Sensors (Switzerland)*, *20*(22), 1–17. https://doi.org/10.3390/s20226458

Dineva, K., & Atanasova, T. (2022). Cloud Data-Driven Intelligent Monitoring System for Interactive Smart Farming. *Sensors*, *22*(17). https://doi.org/10.3390/s22176566

Fan, J., Li, Y., Yu, S., Gou, W., Guo, X., & Zhao, C. (2023). Application of Internet of Things to Agriculture—The LQ-FieldPheno Platform: A High-Throughput Platform for Obtaining Crop Phenotypes in Field. *Research*, *6*, 1–17. https://doi.org/10.34133/research.0059

Fei, S., Hassan, M. A., Xiao, Y., Su, X., Chen, Z., Cheng, Q., Duan, F., Chen, R., & Ma, Y. (2023). UAV-based multi-sensor data fusion and machine learning algorithm for yield prediction in wheat. *Precision Agriculture*, *24*(1), 187–212. https://doi.org/10.1007/s11119-022-09938-8

Gazzola, P., Pavione, E., Barge, A., & Fassio, F. (2023). Using the Transparency of Supply Chain Powered by Blockchain to Improve Sustainability Relationships with Stakeholders in the Food Sector: The Case Study of Lavazza. *Sustainability (Switzerland)*, *15*(10). https://doi.org/10.3390/su15107884

Goldstein, A., Fink, L., & Ravid, G. (2022). A Cloud-Based Framework for Agricultural Data Integration: A Top-Down-Bottom-Up Approach. *IEEE Access*, *10*, 88527–88537. https://doi.org/10.1109/ACCESS.2022.3198099

Hameed, H., Zafar, N. A., Alkhammash, E. H., & Hadjouni, M. (2022). Blockchain-Based Formal Model for Food Supply Chain Management System Using VDM-SL. *Sustainability (Switzerland)*, *14*(21). https://doi.org/10.3390/su142114202

Ibrahim, I. A., & Truby, J. M. (2023). FarmTech: Regulating the use of digital technologies in the agricultural sector. *Food and Energy Security*, *12*(4), 1–15. https://doi.org/10.1002/fes3.483

Joshi, A., Pradhan, B., Gite, S., & Chakraborty, S. (2023). Remote-Sensing Data and Deep-Learning Techniques in Crop Mapping and Yield Prediction: A Systematic Review. *Remote Sensing*, *15*(8). https://doi.org/10.3390/rs15082014

Kurniawan, A., Ohsita, Y., & Murata, M. (2022). Experiments on Adversarial Examples for Deep Learning Model Using Multimodal Sensors. *Sensors*, *22*(22). https://doi.org/10.3390/s22228642

Lahza, H., Naveen Kumar, K. R., Sreenivasa, B. R., Shawly, T., Alsheikhy, A. A., Hiremath, A. K., & Lahza, H. F. M. (2023). Optimization of Crop Recommendations Using Novel Machine Learning Techniques. *Sustainability (Switzerland)*, *15*(11), 1–18. https://doi.org/10.3390/su15118836

Lin, N., Wang, X., Zhang, Y., Hu, X., & Ruan, J. (2020). Fertigation management for sustainable precision agriculture based on Internet of Things. *Journal of Cleaner Production*, *277*. https://doi.org/10.1016/j.jclepro.2020.124119

Lo, V. S. Y., & Pachamanova, D. A. (2023). From Meaningful Data Science to Impactful Decisions: The Importance of Being Causally Prescriptive. *Data Science Journal*, *22*(1), 1–18. https://doi.org/10.5334/dsj-2023-008

Ma, X. (2023). Smart Agriculture and Rural Revitalization and Development Based on the Internet of Things under the Background of Big Data. *Sustainability (Switzerland)*, *15*(4). https://doi.org/10.3390/su15043352

MacPherson, J., Voglhuber-Slavinsky, A., Olbrisch, M., Schöbel, P., Dönitz, E., Mouratiadou, I., & Helming, K. (2022). Future agricultural systems and the role of digitalization for achieving sustainability goals. A review. *Agronomy for Sustainable Development*, *42*(4). https://doi.org/10.1007/s13593-022-00792-6

Maraveas, C., Rajarajan, M., Arvanitis, K. G., & Vatsanidou, A. (2024). Cybersecurity threats and mitigation measures in agriculture 4.0 and 5.0. *Smart Agricultural Technology*, *9*(September). https://doi.org/10.1016/j.atech.2024.100616

Martin Otieno. (2023). An extensive survey of smart agriculture technologies: Current security posture. *World Journal of Advanced Research and Reviews*, *18*(3), 1207–1231. https://doi.org/10.30574/wjarr.2023.18.3.1241

Méndez-Guzmán, H. A., Padilla-Medina, J. A., Martínez-Nolasco, C., Martinez-Nolasco, J. J., Barranco-Gutiérrez, A. I., Contreras-Medina, L. M., & Leon-Rodriguez, M. (2022). IoT-Based Monitoring System Applied to Aeroponics Greenhouse. *Sensors*, *22*(15). https://doi.org/10.3390/s22155646

Mesías-Ruiz, G. A., Pérez-Ortiz, M., Dorado, J., de Castro, A. I., & Peña, J. M. (2023). Boosting precision crop protection towards agriculture 5.0 via machine learning and emerging technologies: A contextual review. *Frontiers in Plant Science*, *14*(March), 1–22. https://doi.org/10.3389/fpls.2023.1143326

Nurse, J. R. C. (2021). Cybersecurity Awareness. *Encyclopedia of Cryptography, Security and Privacy*, 1–4. https://doi.org/10.1007/978-3-642-27739-9_1596-1

Oliveira, R. C. de, & Silva, R. D. de S. e. (2023). Artificial Intelligence in Agriculture: Benefits, Challenges, and Trends. *Applied Sciences (Switzerland)*, *13*(13). https://doi.org/10.3390/app13137405

Raturi, A., Thompson, J. J., Ackroyd, V., Chase, C. A., Davis, B. W., Myers, R., Poncet, A., Ramos-Giraldo, P., Reberg-Horton, C., Rejesus, R., Robertson, A., Ruark, M. D., Seehaver-Eagen, S., & Mirsky, S. (2022). Cultivating trust in technology-mediated sustainable agricultural research. *Agronomy Journal*, *114*(5), 2669–2680. https://doi.org/10.1002/agj2.20974

Rondelli, V., Franceschetti, B., & Mengoli, D. (2022). A Review of Current and Historical Research Contributions to the Development of Ground Autonomous Vehicles for Agriculture. *Sustainability (Switzerland)*, *14*(15). https://doi.org/10.3390/su14159221

Shepherd, M., Turner, J. A., Small, B., & Wheeler, D. (2020). Priorities for science to overcome hurdles thwarting the full promise of the 'digital agriculture' revolution. *Journal of the Science of Food and Agriculture*, *100*(14), 5083–5092. https://doi.org/10.1002/jsfa.9346

Simone Stephen, Alexander, K., Potter, L., & Palmer, X.-L. (2023). Implications of Cyberbiosecurity in Advanced Agriculture. *International Conference on Cyber Warfare and Security*, *18*(1), 387–393. https://doi.org/10.34190/iccws.18.1.995

Son, K. H., Sim, H. S., Lee, J. K., & Lee, J. (2023). Precise Sensing of Leaf Temperatures for Smart Farm Applications. *Horticulturae*, *9*(4), 1–16. https://doi.org/10.3390/horticulturae9040518

Song, H., Ge, W., Gao, P., & Xu, W. (2023). A Novel Blockchain-Enabled Supply-Chain Management Framework for Xinjiang Jujube: Research on Optimized Blockchain Considering Private Transactions. *Foods*, *12*(3). https://doi.org/10.3390/foods12030587

Trnka, M., Abdelfattah, A. S., Shrestha, A., Coffey, M., & Cerny, T. (2022). Systematic Review of Authentication and Authorization Advancements for the Internet of Things. *Sensors*, *22*(4), 1–24. https://doi.org/10.3390/s22041361

Wei, Y., Han, C., & Yu, Z. (2023). An environment safety monitoring system for agricultural production based on artificial intelligence, cloud computing and big data networks. *Journal of Cloud Computing*, *12*(1), 1–17. https://doi.org/10.1186/s13677-023-00463-1.