World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

Check for updates

The role of AI in enhancing cybersecurity for smart farms

Adebunmi Okechukwu Adewusi [1, *], Njideka Rita Chiekezie [2] and Nsisong Louis Eyo-Udo [3]

[1] *Independent Researcher, Ohio, USA.*
[2] *Department of Agricultural Economics, Anambra State Polytechnic, Mgbakwu, Nigeria.*
[3] *Independent Researcher, Lagos Nigeria*

World Journal of Advanced Research and Reviews, 2022, 15(03), 501–512

Publication history: Received on 22 August 2022; revised on 24 September 2022; accepted on 28 September 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.15.3.0889

Abstract

The integration of advanced technologies into agriculture has given rise to smart farms, which leverage Internet of Things (IoT) devices, sensors, data management systems, and automation to optimize farming operations. However, the increasing digitization of agriculture introduces significant cybersecurity challenges, including vulnerabilities in IoT devices, data breaches, and threats to automated systems. Addressing these challenges is crucial to ensuring the security, efficiency, and sustainability of smart farms. Artificial Intelligence (AI) has emerged as a pivotal technology in enhancing cybersecurity measures for smart farms. By employing machine learning and predictive analytics, AI can provide real-time monitoring and threat detection, identifying unusual activities and predicting potential threats before they manifest. AI-driven anomaly detection systems enhance the ability to spot deviations from normal operations, enabling early intervention. Additionally, AI-powered threat intelligence systems gather and analyze data from various sources to provide actionable insights and fortify defenses against cyber-attacks. Securing IoT devices in smart farms is another critical application of AI. By implementing secure communication protocols and robust authentication mechanisms, AI can protect these devices from unauthorized access and control. Furthermore, AI technologies ensure data integrity and privacy through advanced encryption methods and AI-based access control systems, safeguarding sensitive information from breaches. Automated security management is a significant advantage of AI in smart farms. AI can streamline patch management and software updates, ensuring that systems are always protected against the latest threats. In the event of a security incident, AI-driven incident response mechanisms can quickly mitigate damage and facilitate recovery. Despite the clear benefits, the deployment of AI in smart farm cybersecurity faces challenges such as data quality, integration complexity, and cost considerations. Nevertheless, ongoing advancements in AI and machine learning, coupled with collaborative efforts and regulatory support, hold promise for overcoming these obstacles. AI's role in enhancing cybersecurity is vital to the future of smart agriculture, providing a robust foundation for secure and efficient farming operations.

Keywords: Artificial Intelligence; Cybersecurity; Smart farms; Review

1. Introduction

Smart farms represent a transformative approach to agriculture, integrating advanced technologies such as the Internet of Things (IoT), data analytics, automation, and artificial intelligence (AI) to enhance farming efficiency, productivity, and sustainability (Javaid *et al*., 2022; Dhanaraju *et al*., 2022). These farms leverage interconnected devices and systems to monitor and manage agricultural processes in real time. IoT sensors collect data on soil moisture, temperature, crop health, and livestock conditions, while automated machinery performs tasks like planting, watering, and harvesting. Data analytics and AI algorithms analyze this data to optimize operations, predict yields, and make informed decisions (Campbell *et al*., 2020). Smart farms exemplify the fusion of traditional farming practices with cutting-edge technology to meet the growing demands for food production in an efficient and sustainable manner (Sharma *et al*., 2022).

[*] Corresponding author: Adebunmi Okechukwu Adewusi

As smart farms become increasingly reliant on interconnected technologies, the importance of robust cybersecurity measures cannot be overstated (Sinha and Dhanalakshmi, 2022). The integration of IoT devices, data management systems, and automation introduces numerous vulnerabilities that can be exploited by malicious actors. Cybersecurity in smart agriculture is crucial for several reasons. Smart farms generate and store vast amounts of data, including proprietary agricultural information, financial records, and personal data of farmers (Anidu and Dara, 2021). Protecting this data from breaches and unauthorized access is vital to maintaining the confidentiality and integrity of farm operations. Cyber-attacks can disrupt the functioning of smart farm systems, leading to operational downtimes, loss of productivity, and potential damage to crops and livestock (Sujatha *et al*., 2022). Robust cybersecurity measures ensure that farm operations continue smoothly without interruptions. Cybersecurity breaches can result in significant financial losses due to theft, fraud, and damage to farm infrastructure. By implementing strong cybersecurity practices, smart farms can mitigate these risks and protect their investments (Demestichas *et al*., 2020). Smart farms play a critical role in the global food supply chain. Cyber-attacks targeting these farms can have far-reaching consequences, including disruptions in food production and distribution. Cybersecurity is essential to maintaining the integrity and security of the food supply (Syed *et al*., 2022).

Artificial intelligence has emerged as a powerful tool in enhancing cybersecurity for smart farms. AI technologies can bolster cybersecurity measures in several key ways. AI algorithms can continuously monitor network traffic and system activities, identifying anomalies and potential threats in real time (Garcia *et al*., 2021). By analyzing patterns and behaviors, AI can detect and respond to cyber-attacks more quickly and accurately than traditional methods. It can predict potential cybersecurity threats by analyzing historical data and identifying trends. This proactive approach allows smart farms to implement preventive measures before threats materialize, enhancing overall security (Verdouw *et al*., 2021). In the event of a cyber-attack, AI-driven systems can automatically respond to mitigate damage and prevent further breaches. Automated incident response reduces the time taken to address security incidents, minimizing their impact on farm operations. AI can enhance the security of IoT devices used in smart farms by implementing robust authentication protocols, detecting vulnerabilities, and ensuring secure communication between devices (Yazdinejad *et al*., 2021; Zaman *et al*., 2021).

This review aims to explore the role of AI in enhancing cybersecurity for smart farms, addressing the unique challenges posed by the integration of advanced technologies in agriculture. It will provide a comprehensive overview of smart farms and their cybersecurity needs, followed by an in-depth examination of AI technologies and their applications in securing these farms. The review will also discuss real-world case studies, highlighting successful implementations of AI-driven cybersecurity solutions in smart agriculture. Furthermore, it will identify the challenges and limitations associated with deploying AI for cybersecurity in smart farms and propose potential future trends and opportunities in this evolving field. The ultimate goal is to underscore the importance of AI in safeguarding smart farms, ensuring their resilience, and promoting sustainable agricultural practices in the digital age.

2. Understanding Smart Farms

The concept of smart farms represents the intersection of agriculture and advanced technology, aiming to revolutionize traditional farming practices by making them more efficient, productive, and sustainable (Duncan *et al*., 2021). Smart farms employ a variety of high-tech systems to monitor, manage, and optimize agricultural processes, ensuring that the growing demands for food production are met in an eco-friendly and economically viable manner.

Smart farms are composed of several integral components, each playing a crucial role in enhancing farm operations (Sharma *et al*., 2022). IoT devices and sensors are at the heart of smart farming. These devices are deployed throughout the farm to collect real-time data on various environmental parameters, including soil moisture, temperature, humidity, light intensity, and crop health. Sensors can also monitor livestock, tracking their movement, health, and feeding patterns. This continuous flow of data provides farmers with precise and actionable insights, enabling them to make informed decisions about planting, irrigation, pest control, and harvesting. The use of IoT devices minimizes guesswork and reduces the reliance on manual observations, leading to more accurate and efficient farm management (Akhigbe *et al*., 2021). The vast amounts of data generated by IoT devices and sensors need to be collected, stored, and analyzed efficiently. Data management systems in smart farms handle this task, providing a centralized platform for data integration and analysis. These systems employ advanced algorithms and machine learning models to process the data, identifying patterns and trends that can inform decision-making. For example, data on soil conditions can be analyzed to optimize irrigation schedules, while crop growth data can help predict yields. Effective data management systems also facilitate predictive analytics, allowing farmers to anticipate and mitigate potential issues before they arise (Fote *et al*., 2020). Automation and robotics play a pivotal role in smart farming by performing repetitive and labor-intensive tasks with precision and consistency. Automated machinery, such as drones, tractors, and harvesters, can carry out activities like planting, spraying, weeding, and harvesting with minimal human intervention. Robotics technology is also used in livestock management, with automated feeders and milking machines improving efficiency and animal welfare (Ali *et al*., 2020). The integration of robotics reduces the need for manual labor, lowers operational costs, and ensures tasks are performed with high accuracy and reliability. Furthermore, automated systems can operate continuously, increasing the overall productivity of the farm.

The implementation of smart farming technologies offers numerous benefits, transforming traditional agricultural practices into more efficient and sustainable operations (Mohamed *et al*., 2021). One of the most significant advantages of smart farms is the substantial increase in operational efficiency. IoT devices and sensors provide real-time data that helps farmers monitor and manage their crops and livestock more effectively. Automated systems streamline various agricultural processes, reducing the time and effort required for tasks such as irrigation, fertilization, and pest control (Kim *et al*., 2020). This increased efficiency not only lowers labor costs but also ensures that resources are utilized optimally, reducing waste and environmental impact. Smart farming technologies contribute to enhanced productivity by enabling precise and data-driven decision-making. The ability to monitor and control environmental conditions in real time allows farmers to create optimal growing conditions for their crops. Predictive analytics help anticipate issues like pest infestations or nutrient deficiencies, allowing for timely interventions that prevent crop loss. Additionally, automated machinery ensures that tasks are performed consistently and accurately, leading to higher yields and better-quality produce (Lyu *et al*., 2021). Overall, smart farms can produce more food on the same amount of land, meeting the increasing global demand for agricultural products. Resource optimization is a critical benefit of smart farms, addressing the challenges of limited natural resources and environmental sustainability (Idoje *et al*., 2021). IoT devices and sensors provide detailed insights into soil conditions, weather patterns, and crop health, enabling farmers to apply water, fertilizers, and pesticides more precisely. This targeted approach minimizes resource wastage and reduces the environmental footprint of farming activities. For instance, precision irrigation systems ensure that water is delivered exactly where and when it is needed, conserving water resources and reducing costs. Similarly, precision agriculture techniques optimize the use of fertilizers and pesticides, enhancing crop health while minimizing chemical runoff and soil degradation. Smart farms represent a significant advancement in agricultural practices, leveraging technology to improve efficiency, productivity, and sustainability. By integrating IoT devices, data management systems, and automation, smart farms provide farmers with the tools and insights needed to optimize their operations and meet the growing demands for food production. The benefits of smart farming, including increased efficiency, enhanced productivity, and resource optimization, highlight the potential of technology to transform agriculture and contribute to a more sustainable future (Maraseni *et al*., 2021).

3. Cybersecurity Challenges in Smart Farms

The adoption of smart farming technologies brings significant benefits to agricultural productivity and sustainability (Balafoutis *et al*., 2020). However, it also introduces a range of cybersecurity challenges that must be addressed to ensure the integrity, reliability, and security of smart farm operations. This review explores the primary cybersecurity challenges faced by smart farms, including vulnerabilities in IoT devices, data breaches and privacy concerns, threats to automation systems, and potential economic and operational impacts.

IoT devices are the cornerstone of smart farming, providing real-time data on various agricultural parameters. However, these devices are often vulnerable to cybersecurity threats due to several factors. Many IoT devices used in agriculture are designed with minimal security features, making them susceptible to attacks (Anand *et al*., 2020). Manufacturers often prioritize functionality and cost over security, resulting in devices that lack robust authentication, encryption, and access control mechanisms. IoT devices in smart farms are typically connected to local networks and the internet, exposing them to a wide range of potential cyber threats. Without proper network security measures, these devices can be easily accessed and manipulated by attackers. IoT devices often run on outdated software with known vulnerabilities. Manufacturers may not provide regular updates, or farmers may not have the expertise to install them, leaving devices exposed to cyber threats. In a farm setting, IoT devices are often deployed in remote and exposed locations, making them vulnerable to physical tampering (Rizvi *et al*., 2020). Attackers can easily access and compromise these devices, potentially gaining control over farm operations.

Smart farms generate and store vast amounts of data, including sensitive information about farm operations, financial records, and personal data of farmers. Protecting this data from breaches and unauthorized access is a critical cybersecurity challenge. Data collected by IoT devices includes detailed information about crop health, soil conditions, and livestock management (Singh *et al*., 2022). If this data is breached, it can be used for malicious purposes, such as sabotaging farm operations or stealing proprietary agricultural techniques. Farmers' personal data, including contact information, financial details, and business strategies, can be targeted by cybercriminals. Unauthorized access to this data can lead to identity theft, financial fraud, and other privacy violations. Data transmitted between IoT devices and central data management systems can be intercepted if not properly encrypted. Additionally, inadequate security measures for data storage systems can result in unauthorized access and data breaches. Smart farms often rely on third-party service providers for data analytics and cloud storage (Bapatla *et al.*, 2021). Ensuring these providers have robust cybersecurity measures in place is essential to protecting farm data from breaches.

Automation systems, including drones, automated tractors, and robotic harvesters, are integral to smart farms (Virk *et al.*, 2020). However, these systems are vulnerable to cyber-attacks that can disrupt their operations. Attackers can gain unauthorized access to automated machinery, potentially taking control of equipment and causing physical damage to crops and infrastructure. Such attacks can also pose safety risks to farm workers. Cyber-attacks can disrupt the normal functioning of automation systems, leading to delays in planting, watering, and harvesting activities. This can result in significant operational setbacks and reduced productivity. Automation systems run on complex software that may contain vulnerabilities. Attackers can exploit these vulnerabilities to introduce malware, disrupt communication between devices, and alter operational parameters. The components of automation systems often come from various suppliers. A breach in the supply chain can introduce compromised hardware or software into farm operations, leading to potential cyber threats (Gupta *et al.*, 2020).

The cybersecurity challenges faced by smart farms can have significant economic and operational impacts, affecting the overall sustainability and profitability of agricultural operations. Cyber-attacks can result in direct financial losses due to theft, fraud, and the cost of responding to security incidents (Lallie *et al.*, 2021). Additionally, disruptions to farm operations can lead to lost revenue and increased operational costs. Cyber-attacks that compromise IoT devices, data management systems, or automation equipment can cause operational downtime. This can delay critical farming activities, affecting crop yields and livestock health. Data breaches and security incidents can damage the reputation of smart farms, leading to loss of customer trust and potential business opportunities (Agarwal *et al.*, 2022). Rebuilding trust and reputation after a cyber incident can be a lengthy and costly process. Smart farms must comply with various regulations related to data protection and cybersecurity. Failure to meet these regulatory requirements can result in legal penalties, fines, and additional compliance costs. Persistent cybersecurity threats can undermine the long-term sustainability of smart farms. Investing in robust cybersecurity measures is essential to ensure the continued growth and resilience of smart agriculture. While smart farms offer numerous benefits in terms of efficiency, productivity, and sustainability, they also face significant cybersecurity challenges. Addressing vulnerabilities in IoT devices, protecting sensitive data, securing automation systems, and mitigating economic and operational impacts are critical to the success of smart farming (Quy *et al.*, 2022). As the agriculture sector continues to embrace digital transformation, prioritizing cybersecurity will be essential to safeguarding the future of smart farms.

4. AI Technologies in Cybersecurity

The integration of Artificial Intelligence (AI) in cybersecurity has revolutionized the way organizations protect their digital assets and respond to threats (Shah, 2021). AI technologies offer advanced capabilities that enhance the detection, analysis, and mitigation of cyber threats, providing a more proactive and efficient approach to cybersecurity. This review explores four key AI technologies in cybersecurity: machine learning and predictive analytics, anomaly detection systems, AI-driven threat intelligence, and automated incident response.

Machine learning (ML) and predictive analytics are foundational AI technologies that play a crucial role in modern cybersecurity. ML algorithms excel at recognizing patterns and anomalies in vast datasets (Avacharmal, 2021). By analyzing historical data on network traffic, user behavior, and system activities, ML models can identify unusual patterns that may indicate a cyber threat. This capability allows for the early detection of potential attacks before they can cause significant damage. Predictive analytics uses historical data to predict future events. In cybersecurity, this involves analyzing user behavior to establish baselines of normal activity. Deviations from these baselines can signal a potential security breach. For example, if a user's login activity suddenly spikes at unusual hours or from unfamiliar locations, predictive analytics can flag this as suspicious. ML models can analyze trends and patterns in past cyber-attacks to predict future threats. This proactive approach enables organizations to implement preventive measures and strengthen their defenses against anticipated attacks. Predictive analytics also helps in identifying vulnerabilities in systems and applications that need to be addressed to prevent exploitation (Hanif *et al.*, 2021).

Anomaly detection systems are AI-driven tools designed to identify deviations from normal behavior that may indicate a security threat (Agrawal, 2022). These systems continuously monitor network traffic, system logs, and user activities to detect anomalies. By establishing a baseline of normal behavior, anomaly detection systems can quickly identify deviations that may signify a security incident, such as unusual login attempts, unauthorized data access, or unexpected changes in system configurations. Advanced anomaly detection systems use contextual information to enhance their accuracy. For instance, they can differentiate between benign anomalies (such as an employee accessing a new application for the first time) and malicious activities (such as an external actor trying to gain unauthorized access).

This reduces false positives and ensures that security teams focus on genuine threats. Anomaly detection systems leverage ML algorithms to adapt to evolving threats (Bouchama and Kamal, 2021). They continuously learn from new data and adjust their detection models to account for changes in user behavior and network activity. This adaptability is crucial in an ever-changing threat landscape, where attackers constantly develop new tactics and techniques.

AI-driven threat intelligence involves the use of AI technologies to gather, analyze, and interpret data from various sources to provide actionable insights into cyber threats. AI-driven threat intelligence platforms aggregate data from multiple sources, including threat feeds, social media, dark web forums, and internal security logs. By consolidating this information, these platforms provide a comprehensive view of the threat landscape. AI technologies analyze vast amounts of threat data to identify patterns, trends, and correlations that human analysts might miss (Bécue *et al*., 2021). This automated analysis enables faster and more accurate identification of emerging threats, attack vectors, and indicators of compromise (IOCs). The primary goal of AI-driven threat intelligence is to provide actionable insights that can inform security strategies and responses. These insights help organizations prioritize their security efforts, allocate resources effectively, and implement targeted measures to mitigate identified threats.

Automated incident response leverages AI technologies to streamline and accelerate the process of responding to cybersecurity incidents. In the event of a security breach, automated incident response systems can take immediate action to contain and mitigate the threat (Mahima, 2021). For example, they can isolate compromised systems, block malicious IP addresses, and terminate suspicious processes, minimizing the potential damage. AI-driven incident response systems automate routine tasks, such as alert triage, log analysis, and threat investigation. This reduces the workload on security teams and allows them to focus on more complex and strategic aspects of incident response. Automated incident response platforms integrate with other security tools and systems, orchestrating a coordinated response to threats (Kinyua and Awuah, 2021). They can trigger predefined response playbooks, ensuring that appropriate actions are taken consistently and efficiently across the organization. These systems leverage ML algorithms to learn from each incident and improve their response strategies over time. By analyzing past incidents and outcomes, automated incident response platforms refine their detection and mitigation capabilities, enhancing overall security resilience. AI technologies have become indispensable in the realm of cybersecurity (Sarker *et al*., 2021). Machine learning and predictive analytics, anomaly detection systems, AI-driven threat intelligence, and automated incident response collectively provide a robust framework for defending against cyber threats. These AI-driven solutions enable organizations to proactively identify, analyze, and respond to threats, ensuring the security and integrity of their digital assets in an increasingly complex and dynamic threat landscape.

5. AI Applications in Enhancing Cybersecurity for Smart Farms

The integration of Artificial Intelligence (AI) in smart farming not only boosts agricultural productivity but also significantly enhances cybersecurity measures (Shaikh *et al*., 2022). AI technologies provide advanced capabilities for real-time monitoring, threat detection, IoT device security, data integrity, and automated security management. This review delves into the specific AI applications in enhancing cybersecurity for smart farms.

AI technologies play a crucial role in the real-time monitoring and detection of potential cyber threats, ensuring that smart farm operations remain secure and uninterrupted. AI-driven systems excel at identifying unusual activities by continuously analyzing data from various sensors and devices (Ahmed *et al*., 2022). These systems establish a baseline of normal behavior and can quickly detect deviations that may indicate security threats. For instance, if an IoT sensor suddenly transmits data at an unusual frequency or from an unexpected location, the AI system can flag this as a potential security incident. By recognizing these anomalies in real-time, farmers can respond promptly to mitigate risks. Predictive analytics, powered by machine learning algorithms, enable AI systems to anticipate potential threats before they materialize. By analyzing historical data on network traffic, user behavior, and previous cyber-attacks, AI models can predict future vulnerabilities and attack patterns. This proactive approach allows farmers to implement preventive measures, such as strengthening network security or patching vulnerable devices, thereby reducing the likelihood of successful cyber-attacks (Yaacoub *et al*., 2022).

IoT devices are integral to smart farming, but they also present significant security challenges. AI technologies enhance the security of these devices through secure communication protocols and robust authentication mechanisms. AI can help develop and enforce secure communication protocols for IoT devices, ensuring that data transmitted between devices and central systems is encrypted and protected from interception (Attkan and Ranga, 2022). Machine learning algorithms can continuously monitor communication patterns, detecting any anomalies that may indicate a breach or tampering. By ensuring secure data transmission, AI helps safeguard sensitive information and maintain the integrity of farm operations. AI-based systems enhance the authentication and authorization processes for IoT devices. These systems use machine learning models to verify the identity of devices attempting to connect to the network, ensuring that only authorized devices can access critical resources. Additionally, AI can dynamically adjust access permissions based on the behavior and risk profile of each device, preventing unauthorized access and reducing the attack surface (Fragkos *et al*., 2022).

Protecting the integrity and privacy of data is paramount in smart farming. AI technologies offer robust solutions for encryption, secure data storage, and AI-based access control. AI enhances data encryption techniques, ensuring that data at rest and in transit is protected from unauthorized access. Machine learning algorithms can identify patterns in data usage and storage, optimizing encryption strategies to balance security and performance (Butt *et al*., 2020). Furthermore, AI systems can monitor data storage environments for signs of tampering or unauthorized access, providing an additional layer of security. AI-driven access control systems leverage machine learning to manage and enforce data access policies. These systems analyze user behavior and contextual information to determine appropriate access levels, dynamically adjusting permissions as needed. For instance, if a user's access patterns deviate from their usual behavior, the AI system can prompt for additional authentication or restrict access to sensitive data. This adaptive approach ensures that only authorized individuals can access critical information, protecting data privacy and reducing the risk of breaches.

AI technologies streamline and automate various aspects of security management, including patch management, updates, incident response, and recovery. AI-driven systems automate the process of identifying, testing, and deploying patches and updates for IoT devices and software applications. Machine learning algorithms can prioritize vulnerabilities based on their severity and potential impact, ensuring that critical patches are applied promptly (Le *et al*., 2022). This proactive approach minimizes the window of opportunity for attackers to exploit known vulnerabilities, enhancing the overall security posture of smart farms. In the event of a cyber-attack, AI technologies enable swift and effective incident response and recovery. Automated incident response systems use machine learning models to analyze security incidents in real-time, identifying the nature and scope of the attack. These systems can then trigger predefined response actions, such as isolating affected devices, blocking malicious IP addresses, and initiating data recovery procedures (Seshadri *et al*., 2020). By automating these processes, AI reduces the time and effort required for incident response, minimizing damage and ensuring a quick return to normal operations. AI applications significantly enhance the cybersecurity of smart farms by providing advanced capabilities for real-time monitoring, threat detection, IoT device security, data integrity, and automated security management. By leveraging AI technologies, smart farms can proactively identify and mitigate cyber threats, ensuring the security and resilience of their operations. As the adoption of smart farming continues to grow, the role of AI in cybersecurity will become increasingly critical in safeguarding the future of agriculture.

6. Case Studies and Real-World Applications

The integration of AI in enhancing cybersecurity for smart farms is not just theoretical but has practical, real-world applications that offer valuable insights. The Netherlands is a leader in agricultural technology, with many farms adopting AI-driven solutions to enhance their cybersecurity measures (Duncan *et al*., 2021). For example, some Dutch farms have integrated AI-powered anomaly detection systems that continuously monitor network traffic and IoT device activities. These systems identify unusual patterns, such as unexpected data transmissions or unauthorized access attempts, enabling farmers to respond swiftly to potential threats. In California, several vineyards have implemented AI-based security systems to protect their extensive IoT networks (Coppola *et al*., 2022). These vineyards use AI to secure communication protocols between sensors and central systems, ensuring that data related to soil moisture, weather conditions, and crop health remains confidential and tamper-proof. AI algorithms also help in authenticating and authorizing devices, preventing unauthorized access to critical information.

A smart farm in Australia reported a significant improvement in their incident response times after implementing AI-driven security systems (Chukkapalli *et al*., 2020). Previously, detecting and responding to security breaches could take hours or even days. With AI, the farm reduced response times to minutes, minimizing potential damage and operational disruption. The key lesson here is the importance of real-time monitoring and automated incident response in maintaining the security and efficiency of smart farming operations. A dairy farm in Denmark successfully enhanced its data security by employing AI-based encryption and access control systems. The farm managed to secure sensitive data related to animal health and production metrics, ensuring that only authorized personnel could access this information. This implementation not only protected the farm's intellectual property but also built trust with stakeholders by demonstrating a commitment to data privacy and security.

In a notable incident, a smart greenhouse in Japan experienced a ransomware attack that targeted its IoT network. The attackers encrypted the greenhouse's control systems, demanding a ransom to restore access. However, the farm had previously integrated AI-driven security solutions capable of detecting and mitigating such threats. The AI system identified the anomaly immediately and initiated a pre-programmed response that isolated the affected systems, preventing the spread of the ransomware (Neupane *et al*., 2019). This incident highlights the critical role of AI in providing swift, automated responses to mitigate cyber-attacks effectively. A smart dairy farm in Canada faced a data breach where sensitive information, including production data and animal health records, was compromised. The farm's AI-based anomaly detection system identified unusual data access patterns and flagged the incident. Despite the breach, the farm's AI systems enabled a quick response, securing the network and preventing further unauthorized access. The incident underscored the importance of continuous monitoring and AI-based threat detection in safeguarding sensitive information in smart farms. An orchard in Spain encountered an incident where hackers attempted to hijack IoT devices to gain control over irrigation systems. The AI-powered security solution detected the unauthorized access attempts through anomaly detection and immediately restricted access to the compromised devices (Gudala *et al*., 2019). The system also alerted the farm management, allowing them to take corrective actions swiftly. This case demonstrated the effectiveness of AI in detecting and responding to IoT device vulnerabilities, ensuring the continuity of critical farm operations. The implementation of AI technologies in smart farming for cybersecurity purposes is proving to be highly effective. Real-world examples and case studies illustrate the significant benefits of AI, including improved incident response times, enhanced data security, and robust defenses against various cyber threats. These success stories and lessons learned highlight the importance of adopting AI-driven solutions to protect the integrity, confidentiality, and availability of smart farm operations. As the agricultural sector continues to embrace digital transformation, the role of AI in enhancing cybersecurity will become increasingly vital, ensuring the resilience and sustainability of smart farming practices (Mitra *et al*., 2022).

7. Challenges and Limitations of AI in Smart Farm Cybersecurity

Artificial Intelligence (AI) offers significant advancements in enhancing cybersecurity for smart farms, its implementation is not without challenges and limitations. Addressing these issues is crucial to maximizing the effectiveness of AI-driven security solutions. This review explores four key challenges: data quality and availability, complexity and integration issues, AI model interpretability and trust, and cost and resource considerations.

AI systems rely heavily on data for training and operation. In the context of smart farms, this data includes information from various IoT devices, sensors, and network logs. The accuracy and reliability of AI models depend on the quality of this data. However, data collected from agricultural IoT devices can be noisy or incomplete, leading to potential inaccuracies in threat detection and prediction. Poor data quality can result in false positives or missed threats, undermining the effectiveness of AI-based security measures (Brundage *et al*., 2018). The availability of comprehensive and representative datasets is another challenge. Smart farms may face difficulties in accessing diverse and extensive datasets required to train robust AI models. Limited data can hinder the development of effective security solutions, as AI models may not have enough information to recognize and respond to a wide range of threats. Furthermore, privacy concerns and data protection regulations can restrict the sharing and availability of critical security data.

The deployment of AI-driven cybersecurity solutions in smart farms involves integrating various technologies, including IoT devices, data management systems, and security platforms. The complexity of these systems can pose significant challenges in ensuring seamless operation and coordination. Integrating AI technologies with existing farm infrastructure may require substantial adjustments and customization, which can be technically demanding and time-consuming (Redhu *et al*., 2022). Ensuring interoperability between different AI systems and farm technologies is a crucial challenge. Smart farms often use a mix of devices and platforms from various vendors, each with its own standards and protocols. Integrating AI solutions with these diverse systems can be problematic, leading to issues such as data incompatibility, communication barriers, and reduced effectiveness of security measures. As smart farms grow and evolve, scaling AI-driven security solutions to accommodate increased data volume and complexity can be challenging. Ensuring that AI systems can handle the expanding scope of farm operations without compromising performance or accuracy requires careful planning and adaptation.

One of the significant challenges in AI applications is the interpretability of AI models. Many advanced AI techniques, such as deep learning, operate as "black boxes," making it difficult to understand how decisions are made. In the context of cybersecurity, this lack of transparency can hinder the ability of security professionals to interpret and validate AI-generated alerts and responses. Without clear insights into how AI models reach their conclusions, it can be challenging to trust and act upon their recommendations. Building trust in AI systems is essential for their effective adoption. If stakeholders lack confidence in the reliability and accuracy of AI-driven security measures, they may be hesitant to fully implement and rely on these solutions (Lockey *et al*., 2021). Ensuring that AI models are thoroughly tested, validated, and explainable is crucial for fostering trust and promoting their use in smart farm cybersecurity.

The initial costs associated with implementing AI-driven cybersecurity solutions can be substantial. These costs include investments in AI technology, infrastructure upgrades, and training for personnel. For many smart farms, especially smaller operations, these financial requirements may pose a barrier to adopting advanced AI security measures. Effective AI implementation requires dedicated resources, including skilled personnel and computational power (Shaw *et al*., 2019). Developing, maintaining, and updating AI models involves ongoing resource allocation, which can strain the financial and human resources of smart farms. Ensuring that the benefits of AI outweigh the costs and that resources are allocated efficiently is a critical consideration for successful deployment. AI systems require regular maintenance and updates to remain effective against evolving cyber threats. The need for continuous monitoring, retraining of models, and system updates can add to the long-term costs and resource requirements. Farms must balance these ongoing demands with other operational priorities to ensure sustainable AI deployment (Grieve *et al*., 2019). While AI technologies hold great promise for enhancing cybersecurity in smart farms, they also face several challenges and limitations. Addressing issues related to data quality and availability, system complexity and integration, model interpretability and trust, and cost and resource considerations is essential for maximizing the effectiveness and sustainability of AI-driven security solutions. By tackling these challenges, smart farms can better leverage AI to safeguard their operations and ensure the resilience of their cybersecurity measures.

8. Future Trends and Opportunities in Smart Farm Cybersecurity

As smart farms increasingly integrate advanced technologies to optimize agricultural practices, the future of cybersecurity in this sector is poised for significant evolution. Advances in AI and machine learning, emerging cybersecurity technologies, collaborative efforts and industry standards, and policy and regulatory developments will shape the landscape of smart farm cybersecurity (Shackelford, 2019). This review explores these future trends and opportunities, highlighting their potential impact on enhancing security measures in smart agriculture.

Future advancements in AI and machine learning are expected to further improve threat detection and response capabilities. Next-generation AI algorithms will leverage larger and more diverse datasets, enabling more accurate identification of subtle anomalies and sophisticated attack patterns. Enhanced machine learning models will also facilitate real-time analysis of vast amounts of data, leading to quicker and more precise responses to emerging threats (Sun and Scanlon, 2019). The development of autonomous AI-driven security systems will become more prevalent. These systems will be capable of independently detecting, analyzing, and responding to cyber threats without human intervention. By utilizing advanced machine learning techniques, such as reinforcement learning, these systems will continuously adapt to new threats and optimize their security measures, providing smarter and more resilient protection for smart farms. The integration of AI at the edge where data is processed locally on IoT devices will offer enhanced security capabilities. Edge AI will enable real-time threat detection and response directly on IoT devices, reducing latency and dependence on centralized systems (Chang *et al*., 2021). This approach will enhance the overall security posture by minimizing the risk of data breaches and ensuring prompt action against detected threats.

Quantum computing holds the potential to revolutionize cybersecurity by providing unprecedented computational power. While this technology poses a threat to traditional encryption methods, it also offers new opportunities for developing quantum-resistant cryptographic algorithms. Future advancements in quantum-safe cryptography will enhance the security of smart farm data against potential quantum-based attacks. Blockchain technology is emerging as a promising solution for enhancing cybersecurity in smart farms (Firouzi *et al*., 2022). Its decentralized and immutable nature can be leveraged to secure data transactions and ensure the integrity of information. Blockchain-based systems can provide secure authentication, traceability, and auditability for IoT devices and communication protocols, reducing the risk of tampering and unauthorized access. The evolution of threat intelligence platforms will provide more sophisticated tools for identifying and mitigating cyber threats. AI-powered threat intelligence platforms will integrate data from various sources, including social media, dark web forums, and security feeds, to offer comprehensive and actionable insights. These platforms will enable smart farms to anticipate and prepare for emerging threats more effectively.

Collaborative efforts between technology providers, cybersecurity experts, and agricultural stakeholders will be crucial for advancing smart farm cybersecurity (Jerhamre *et al*., 2022). Industry partnerships and collaborative research initiatives will drive the development of innovative security solutions and best practices. Sharing threat intelligence, security frameworks, and incident response strategies will enhance the collective ability to address cybersecurity challenges. The development of industry standards and frameworks specific to smart farm cybersecurity will help ensure consistency and effectiveness in security practices. Standards organizations and industry associations will play a key role in defining security requirements, guidelines, and best practices. Adoption of these standards will facilitate interoperability, enhance security measures, and promote a unified approach to addressing cybersecurity challenges.

As the use of smart technologies in agriculture grows, policymakers and regulators will need to adapt existing regulations and create new ones to address emerging cybersecurity threats. Future regulatory developments will focus on establishing comprehensive guidelines for data protection, privacy, and security in smart farming. These regulations will help ensure that cybersecurity measures are implemented effectively and that farms comply with legal requirements. Cybersecurity is a global issue, and international cooperation will be essential for addressing cross-border threats and challenges. Collaborative efforts between governments, international organizations, and industry stakeholders will drive the development of global cybersecurity standards and protocols (Fischer-Hübner *et al*., 2021). Such cooperation will help create a unified approach to securing smart farms and protect against global cyber threats. Policy and regulatory frameworks will need to support innovation in cybersecurity technologies while ensuring adequate protection. Governments and regulatory bodies can incentivize research and development in cybersecurity by providing funding, grants, and tax incentives. Supporting innovation will foster the development of cutting-edge solutions and ensure that smart farms remain resilient against evolving threats. The future of cybersecurity in smart farms will be shaped by advances in AI and machine learning, emerging technologies, collaborative industry efforts, and evolving policy and regulatory frameworks. By embracing these trends and opportunities, smart farms can enhance their cybersecurity measures, address emerging threats, and ensure the resilience and security of their operations. As technology continues to advance, the ongoing development and implementation of innovative security solutions will be crucial in safeguarding the future of smart agriculture.

9. Conclusion

In summary, the integration of Artificial Intelligence (AI) in smart farm cybersecurity addresses numerous challenges and opportunities within modern agricultural systems. Key points discussed include the transformative role of AI in enhancing real-time monitoring, threat detection, and automated responses, which collectively strengthen the security posture of smart farms. AI technologies, such as machine learning, anomaly detection, and predictive analytics, are instrumental in identifying and mitigating potential cyber threats, securing IoT devices, and protecting data integrity.

The importance of AI in securing smart agriculture cannot be overstated. As smart farms increasingly rely on interconnected technologies and data-driven solutions, the risk of cyber threats grows concurrently. AI provides advanced capabilities that not only detect and respond to threats more effectively but also adapt to evolving attack vectors. The use of AI enhances the ability of smart farms to maintain operational continuity, safeguard sensitive data, and ensure the security of their technological infrastructure.

Looking ahead, the future outlook for AI-driven cybersecurity in smart farms is promising yet challenging. Advances in AI and emerging technologies will likely bring new opportunities for more robust and adaptive security measures. However, addressing challenges such as data quality, system complexity, and regulatory frameworks will be crucial. The continued evolution of AI technologies, coupled with collaborative efforts across the industry and regulatory support, will be essential in shaping the future of cybersecurity for smart agriculture. By leveraging these advancements, smart farms can enhance their resilience against cyber threats, ensuring a secure and sustainable future for agricultural innovation.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Agarwal, S., Rashid, A. and Gardiner, J., 2022, August. Old MacDonald had a smart farm: Building a testbed to study cybersecurity in smart dairy farming. In *Proceedings of the 15th Workshop on Cyber Security Experimentation and Test* (pp. 1-9).

[2] Agrawal, S., 2022. Enhancing payment security through AI-Driven anomaly detection and predictive analytics. *International Journal of Sustainable Infrastructure for Cities and Societies*, *7*(2), pp.1-14.

[3] Ahmed, A., Aziz, S., Abd-Alrazaq, A., Farooq, F. and Sheikh, J., 2022. Overview of artificial intelligence–driven wearable devices for diabetes: scoping review. *Journal of Medical Internet Research*, *24*(8), p.e36010.

[4] Akhigbe, B.I., Munir, K., Akinade, O., Akanbi, L. and Oyedele, L.O., 2021. IoT technologies for livestock management: a review of present status, opportunities, and future trends. *Big data and cognitive computing*, *5*(1), p.10.

[5] Ali, W., Ali, M., Ahmad, M., Dilawar, S., Firdous, A. and Afzal, A., 2020. Application of modern techniques in animal production sector for human and animal welfare. *Turkish Journal of Agriculture-Food Science and Technology*, *8*(2), pp.457-463.

[6] Anand, P., Singh, Y., Selwal, A., Alazab, M., Tanwar, S. and Kumar, N., 2020. IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges. *IEEE Access*, *8*, pp.168825-168853.

[7] Anidu, A. and Dara, R., 2021, October. A review of data governance challenges in smart farming and potential solutions. In *2021 IEEE International Symposium on Technology and Society (ISTAS)* (pp. 1-8). IEEE.

[8] Attkan, A. and Ranga, V., 2022. Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. *Complex & Intelligent Systems*, *8*(4), pp.3559-3591.

[9] Avacharmal, R., 2021. Leveraging Supervised Machine Learning Algorithms for Enhanced Anomaly Detection in Anti-Money Laundering (AML) Transaction Monitoring Systems: A Comparative Analysis of Performance and Explainability. *African Journal of Artificial Intelligence and Sustainable Development*, *1*(2), pp.68-85.

[10] Balafoutis, A.T., Evert, F.K.V. and Fountas, S., 2020. Smart farming technology trends: economic and environmental effects, labor impact, and adoption readiness. *Agronomy*, *10*(5), p.743.

[11] Bapatla, A.K., Mohanty, S.P. and Kougianos, E., 2021, November. sFarm: A distributed ledger based remote crop monitoring system for smart farming. In *IFIP International Internet of Things Conference* (pp. 13-31). Cham: Springer International Publishing.

[12] Bécue, A., Praça, I. and Gama, J., 2021. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review*, *54*(5), pp.3849-3886.

[13] Bouchama, F. and Kamal, M., 2021. Enhancing cyber threat detection through machine learning-based behavioral modeling of network traffic patterns. *International Journal of Business Intelligence and Big Data Analytics*, *4*(9), pp.1-9.

[14] Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B. and Anderson, H., 2018. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.

[15] Butt, U.A., Mehmood, M., Shah, S.B.H., Amin, R., Shaukat, M.W., Raza, S.M., Suh, D.Y. and Piran, M.J., 2020. A review of machine learning algorithms for cloud computing security. *Electronics*, *9*(9), p.1379.

[16] Campbell, C., Sands, S., Ferraro, C., Tsao, H.Y.J. and Mavrommatis, A., 2020. From data to action: How marketers can leverage AI. *Business horizons*, *63*(2), pp.227-243.

[17] Chang, Z., Liu, S., Xiong, X., Cai, Z. and Tu, G., 2021. A survey of recent advances in edge-computing-powered artificial intelligence of things. *IEEE Internet of Things Journal*, *8*(18), pp.13849-13875.

[18] Chukkapalli, S.S.L., Mittal, S., Gupta, M., Abdelsalam, M., Joshi, A., Sandhu, R. and Joshi, K., 2020. Ontologies and artificial intelligence systems for the cooperative smart farming ecosystem. *Ieee Access*, *8*, pp.164045-164064.

[19] Coppola, M., Noaille, L., Pierlot, C., de Oliveira, R.O., Gaveau, N., Rondeau, M., Mohimont, L., Steffenel, L.A., Sindaco, S. and Salmon, T., 2022. Innovative Vineyards Environmental Monitoring System Using Deep Edge AI. In *Artificial Intelligence for Digitising Industry–Applications* (pp. 261-278). River Publishers.

[20] Demestichas, K., Peppes, N. and Alexakis, T., 2020. Survey on security threats in agricultural IoT and smart farming. *Sensors*, *20*(22), p.6458.

[21] Dhanaraju, M., Chenniappan, P., Ramalingam, K., Pazhanivelan, S. and Kaliaperumal, R., 2022. Smart farming: Internet of Things (IoT)-based sustainable agriculture. *Agriculture*, *12*(10), p.1745.

[22] Duncan, E., Abdulai, A.R. and Fraser, E.D., 2021. Modernizing agriculture through digital technologies: Prospects and challenges. *Handbook on the human impact of agriculture*, pp.138-161.

[23] Duncan, E., Glaros, A., Ross, D.Z. and Nost, E., 2021. New but for whom? Discourses of innovation in precision agriculture. *Agriculture and Human Values*, *38*, pp.1181-1199.

[24] Firouzi, F., Farahani, B. and Marinšek, A., 2022. The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT). *Information Systems*, *107*, p.101840.

[25] Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., Islami, L. and Akil, M., 2021. Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of information security and applications*, *61*, p.102916.

[26] Fote, F.N., Mahmoudi, S., Roukh, A. and Mahmoudi, S.A., 2020, November. Big data storage and analysis for smart farming. In *2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech)* (pp. 1-8). IEEE.

[27] Fragkos, G., Johnson, J. and Tsiropoulou, E.E., 2022. Dynamic role-based access control policy for smart grid applications: an offline deep reinforcement learning approach. *IEEE Transactions on Human-Machine Systems*, *52*(4), pp.761-773.

[28] Garcia, N., Alcaniz, T., González-Vidal, A., Bernabe, J.B., Rivera, D. and Skarmeta, A., 2021. Distributed real-time SlowDoS attacks detection over encrypted traffic using Artificial Intelligence. *Journal of Network and Computer Applications*, *173*, p.102871.

[29] Grieve, B.D., Duckett, T., Collison, M., Boyd, L., West, J., Yin, H., Arvin, F. and Pearson, S., 2019. The challenges posed by global broadacre crops in delivering smart agri-robotic solutions: A fundamental rethink is required. *Global Food Security*, *23*, pp.116-124.

[30] Gudala, L., Shaik, M., Venkataramanan, S. and Sadhu, A.K.R., 2019. Leveraging Artificial Intelligence for Enhanced Threat Detection, Response, and Anomaly Identification in Resource-Constrained IoT Networks. *Distributed Learning and Broad Applications in Scientific Research*, *5*, pp.23-54.

[31] Gupta, M., Abdelsalam, M., Khorsandroo, S. and Mittal, S., 2020. Security and privacy in smart farming: Challenges and opportunities. *IEEE access*, *8*, pp.34564-34584.

[32] Hanif, H., Nasir, M.H.N.M., Ab Razak, M.F., Firdaus, A. and Anuar, N.B., 2021. The rise of software vulnerability: Taxonomy of software vulnerabilities detection and machine learning approaches. *Journal of Network and Computer Applications*, *179*, p.103009.

[33] Idoje, G., Dagiuklas, T. and Iqbal, M., 2021. Survey for smart farming technologies: Challenges and issues. *Computers & Electrical Engineering*, *92*, p.107104.

[34] Javaid, M., Haleem, A., Singh, R.P. and Suman, R., 2022. Enhancing smart farming through the applications of Agriculture 4.0 technologies. *International Journal of Intelligent Networks*, *3*, pp.150-164.

[35] Jerhamre, E., Carlberg, C.J.C. and van Zoest, V., 2022. Exploring the susceptibility of smart farming: Identified opportunities and challenges. *Smart Agricultural Technology*, *2*, p.100026.

[36] Kim, W.S., Lee, W.S. and Kim, Y.J., 2020. A review of the applications of the internet of things (IoT) for agricultural automation. *Journal of Biosystems Engineering*, *45*, pp.385-400.

[37] Kinyua, J. and Awuah, L., 2021. AI/ML in Security Orchestration, Automation and Response: Future Research Directions. *Intelligent Automation & Soft Computing*, *28*(2).

[38] Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X., 2021. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & security*, *105*, p.102248.

[39] Le, T.H., Chen, H. and Babar, M.A., 2022. A survey on data-driven software vulnerability assessment and prioritization. *ACM Computing Surveys*, *55*(5), pp.1-39.

[40] Lockey, S., Gillespie, N., Holm, D. and Someh, I.A., 2021. A review of trust in artificial intelligence: Challenges, vulnerabilities and future directions.

[41] Lyu, J., Chen, P.S. and Huang, W.T., 2021. Combining an automatic material handling system with lean production to improve outgoing quality assurance in a semiconductor foundry. *Production Planning & Control*, *32*(10), pp.829-844.

[42] Mahima, D., 2021, February. Cyber threat in public sector: Modeling an incident response framework. In *2021 International Conference on Innovative Practices in Technology and Management (ICIPTM)* (pp. 55-60). IEEE.

[43] Maraseni, T., An-Vo, D.A., Mushtaq, S. and Reardon-Smith, K., 2021. Carbon smart agriculture: An integrated regional approach offers significant potential to increase profit and resource use efficiency, and reduce emissions. *Journal of Cleaner Production*, *282*, p.124555.

[44] Mitra, A., Vangipuram, S.L., Bapatla, A.K., Bathalapalli, V.K., Mohanty, S.P., Kougianos, E. and Ray, C., 2022. Everything you wanted to know about smart agriculture. *arXiv preprint arXiv:2201.04754*.

[45] Mohamed, E.S., Belal, A.A., Abd-Elmabod, S.K., El-Shirbeny, M.A., Gad, A. and Zahran, M.B., 2021. Smart farming for improving agricultural management. *The Egyptian Journal of Remote Sensing and Space Science*, *24*(3), pp.971-981.

[46] Neupane, R.L., Neely, T., Calyam, P., Chettri, N., Vassell, M. and Durairajan, R., 2019. Intelligent defense using pretense against targeted attacks in cloud platforms. *Future Generation Computer Systems*, *93*, pp.609-626.

[47] Quy, V.K., Hau, N.V., Anh, D.V., Quy, N.M., Ban, N.T., Lanza, S., Randazzo, G. and Muzirafuti, A., 2022. IoT-enabled smart agriculture: architecture, applications, and challenges. *Applied Sciences*, *12*(7), p.3396.

[48] Redhu, N.S., Thakur, Z., Yashveer, S. and Mor, P., 2022. Artificial intelligence: a way forward for agricultural sciences. In *Bioinformatics in Agriculture* (pp. 641-668). Academic Press.

[49] Rizvi, S., Pipetti, R., McIntyre, N., Todd, J. and Williams, I., 2020. Threat model for securing internet of things (IoT) network at device-level. *Internet of Things*, *11*, p.100240.

[50] Sarker, I.H., Furhad, M.H. and Nowrozy, R., 2021. Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, *2*(3), p.173.

[51] Seshadri, S.S., Rodriguez, D., Subedi, M., Choo, K.K.R., Ahmed, S., Chen, Q. and Lee, J., 2020. IoTCop: A blockchain-based monitoring framework for detection and isolation of malicious devices in Internet-of-Things systems. *IEEE Internet of Things Journal*, *8*(5), pp.3346-3359.

[52] Shackelford, S.J., 2019. Smart factories, dumb policy? Managing cybersecurity and data privacy risks in the industrial internet of things. *Minn. JL Sci. & Tech.*, *21*, p.1.

[53] Shah, V., 2021. Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. *Revista Espanola de Documentacion Cientifica*, *15*(4), pp.42-66.

[54] Shaikh, T.A., Rasool, T. and Lone, F.R., 2022. Towards leveraging the role of machine learning and artificial intelligence in precision agriculture and smart farming. *Computers and Electronics in Agriculture*, *198*, p.107119.

[55] Sharma, V., Tripathi, A.K. and Mittal, H., 2022. Technological revolutions in smart farming: Current trends, challenges & future directions. *Computers and Electronics in Agriculture*, *201*, p.107217.

[56] Shaw, J., Rudzicz, F., Jamieson, T. and Goldfarb, A., 2019. Artificial intelligence and the implementation challenge. *Journal of medical Internet research*, *21*(7), p.e13659.

[57] Singh, D.K., Sobti, R., Jain, A., Malik, P.K. and Le, D.N., 2022. LoRa based intelligent soil and weather condition monitoring with internet of things for precision agriculture in smart cities. *IET communications*, *16*(5), pp.604-618.

[58] Sinha, B.B. and Dhanalakshmi, R., 2022. Recent advancements and challenges of Internet of Things in smart agriculture: A survey. *Future Generation Computer Systems*, *126*, pp.169-184.

[59] Sujatha, R., Prakash, G. and Jhanjhi, N.Z. eds., 2022. *Cyber Security Applications for Industry 4.0*. CRC Press.

[60] Sun, A.Y. and Scanlon, B.R., 2019. How can Big Data and machine learning benefit environment and water management: a survey of methods, applications, and future directions. *Environmental Research Letters*, *14*(7), p.073001.

[61] Syed, N.F., Shah, S.W., Trujillo-Rasua, R. and Doss, R., 2022. Traceability in supply chains: A Cyber security analysis. *Computers & Security*, *112*, p.102536.

[62] Verdouw, C., Tekinerdogan, B., Beulens, A. and Wolfert, S., 2021. Digital twins in smart farming. *Agricultural Systems*, *189*, p.103046.

[63] Virk, A.L., Noor, M.A., Fiaz, S., Hussain, S., Hussain, H.A., Rehman, M., Ahsan, M. and Ma, W., 2020. Smart farming: an overview. *Smart village technology: concepts and developments*, pp.191-201.

[64] Yaacoub, J.P.A., Noura, H.N., Salman, O. and Chehab, A., 2022. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, *21*(1), pp.115-158.

[65] Yazdinejad, A., Zolfaghari, B., Azmoodeh, A., Dehghantanha, A., Karimipour, H., Fraser, E., Green, A.G., Russell, C. and Duncan, E., 2021. A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures. *Applied Sciences*, *11*(16), p.7518.

[66] Zaman, S., Alhazmi, K., Aseeri, M.A., Ahmed, M.R., Khan, R.T., Kaiser, M.S. and Mahmud, M., 2021. Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. *Ieee Access*, *9*, pp.94668-94690.