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)

Securing smart agriculture: Cybersecurity challenges and solutions in IoT-driven 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), 480–489

Publication history: Received on 21 August 2022; revised on 23 September 2022; accepted on 27 September 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.15.3.0887

Abstract

Smart agriculture, driven by the Internet of Things (IoT), has revolutionized modern farming, leading to enhanced efficiency, resource optimization, and improved crop yields. However, the integration of IoT devices and advanced technologies in agriculture also introduces significant cybersecurity challenges. This review explores the various cybersecurity threats faced by IoT-driven farms and proposes solutions to mitigate these risks. IoT devices in smart agriculture are often vulnerable due to a lack of standardization and weak authentication mechanisms, making them prime targets for cyber-attacks. Data security and privacy issues are also paramount, with risks of data breaches and unauthorized access threatening the integrity of agricultural data. Network security is another critical concern, with potential threats including man-in-the-middle attacks and Distributed Denial of Service (DDoS) attacks. Additionally, software and firmware vulnerabilities, such as outdated software and infrequent updates, further exacerbate the security risks. Physical security threats, including tampering with devices and theft of equipment, also pose significant challenges. To address these cybersecurity challenges, several solutions are proposed. Strengthening IoT device security through robust authentication and regular firmware updates is crucial. Ensuring data security and privacy can be achieved by encrypting data in transit and at rest, alongside implementing strict access control mechanisms. Network security can be bolstered through secure communication protocols, network segmentation, and the deployment of intrusion detection and prevention systems. Developing comprehensive cybersecurity policies, conducting regular security audits, and providing employee training and awareness programs are essential for maintaining a secure smart agriculture environment. Enhancing physical security through secure installation of IoT devices and employing surveillance and monitoring systems can also mitigate risks. The review includes case studies demonstrating successful cybersecurity implementations and lessons learned from past incidents. It also explores future trends, such as advances in IoT security technologies, blockchain integration, and the role of artificial intelligence in threat detection. This comprehensive analysis underscores the importance of a proactive approach to cybersecurity in smart agriculture, ensuring the resilience and sustainability of modern farming practices.

Keywords: Securing Smart Agriculture; Cybersecurity; IoT-Driven Farms; Review

1. Introduction

Smart agriculture, also known as precision agriculture or digital farming, refers to the application of modern information and communication technologies (ICT) to agricultural practices (El Bilali *et al*., 2020). This approach leverages advanced technologies such as IoT, big data analytics, artificial intelligence (AI), and machine learning to optimize the efficiency and productivity of farming operations (Misra *et al*., 2020). Smart agriculture aims to monitor and manage various agricultural processes, including crop cultivation, livestock management, soil health, and resource

* Corresponding author: Adebunmi Okechukwu Adewusi

utilization, with precision and accuracy. By utilizing sensors, drones, automated machinery, and connected devices, farmers can make data-driven decisions that enhance yield, reduce waste, and promote sustainable farming practices (Cheema and Khan, 2019).

The Internet of Things (IoT) plays a pivotal role in the evolution of modern farming. IoT encompasses a network of interconnected devices that collect and exchange data in real-time. In agriculture, IoT devices such as soil moisture sensors, weather stations, GPS-enabled tractors, and smart irrigation systems provide farmers with critical insights into their farming environment (Ayaz *et al*., 2019). These devices enable continuous monitoring of crops and livestock, facilitating timely interventions and optimizing resource allocation. For instance, IoT-based soil sensors can provide real-time data on soil moisture levels, allowing farmers to adjust irrigation schedules precisely, thereby conserving water and enhancing crop health. Similarly, IoT-enabled livestock monitoring systems can track animal health and behavior, ensuring timely medical attention and improving overall productivity (Akhigbe *et al*., 2021).

While the integration of IoT in agriculture offers numerous benefits, it also introduces significant cybersecurity challenges. The increasing reliance on connected devices and digital systems makes smart agriculture vulnerable to cyber threats (Demestichas *et al*., 2020). IoT devices often lack robust security features, making them susceptible to hacking, data breaches, and unauthorized access. Cybersecurity in smart agriculture encompasses measures to protect these devices, secure data transmission, and ensure the integrity and confidentiality of agricultural data (Gupta *et al*., 2020). Threats such as malware attacks, ransomware, and Distributed Denial of Service (DDoS) attacks can disrupt farming operations, leading to financial losses and compromised food security. Therefore, implementing comprehensive cybersecurity strategies is essential to safeguard the technological infrastructure of smart farms (Barreto and Amaral, 2018).

The primary purpose of this review is to explore the cybersecurity challenges associated with IoT-driven smart agriculture and propose effective solutions to mitigate these risks. The review aims to provide a detailed analysis of the vulnerabilities in IoT devices, data security and privacy concerns, network security threats, and software and firmware vulnerabilities. Additionally, it will address physical security threats that may affect IoT-enabled agricultural operations. The scope of the review includes a thorough examination of the current state of cybersecurity in smart agriculture, highlighting real-world case studies and examples of cybersecurity incidents in the agricultural sector. The review will also review existing cybersecurity measures and best practices that can be adopted by farmers and agricultural stakeholders to enhance the security of their IoT systems. Furthermore, it will explore emerging technologies and future trends in cybersecurity, such as blockchain integration and AI-driven threat detection, which hold the potential to revolutionize the security landscape of smart agriculture. By providing a comprehensive overview of the cybersecurity challenges and solutions in IoT-driven farms, this review aims to raise awareness among farmers, policymakers, and technology providers about the critical importance of cybersecurity in ensuring the resilience and sustainability of modern farming practices. The insights and recommendations presented in this review will contribute to the development of robust cybersecurity frameworks that can safeguard the technological advancements driving the future of agriculture.

2. Overview of Smart Agriculture

The evolution of agricultural technology has been a transformative journey from traditional methods to highly sophisticated systems (Dayıoğlu and Turker, 2021). In the early days, farming relied heavily on manual labor and simple tools. The advent of the Industrial Revolution brought about mechanization, introducing tractors and other machinery that significantly increased productivity. The Green Revolution in the mid-20th century further revolutionized agriculture with the development of high-yield crop varieties, chemical fertilizers, and advanced irrigation techniques (Fischer and Connor, 2018). In recent decades, the integration of information and communication technologies (ICT) has ushered in the era of smart agriculture. This shift has been characterized by the adoption of precision farming techniques, leveraging satellite imagery, GPS technology, and IoT devices to enhance accuracy and efficiency in farming practices. The continuous advancement in data analytics, artificial intelligence (AI), and machine learning has further propelled the capabilities of smart agriculture, enabling farmers to make data-driven decisions that optimize yields and reduce resource wastage (Chaterji *et al*., 2020; Mitra *et al*., 2022).

IoT devices and sensors are the backbone of smart agriculture, providing real-time data on various aspects of farming (Suciu *et al*., 2019). These devices include soil moisture sensors, weather stations, and GPS-enabled machinery. Soil sensors monitor parameters such as moisture levels, temperature, and nutrient content, allowing for precise irrigation and fertilization. Weather stations collect data on environmental conditions, helping farmers to anticipate weather patterns and make informed decisions. GPS technology enables precise mapping and navigation of agricultural machinery, enhancing the efficiency of planting, spraying, and harvesting operations (Raj *et al*., 2022). Data analytics

and AI are crucial for processing and interpreting the vast amounts of data generated by IoT devices. Advanced analytics techniques enable the identification of patterns and trends, providing insights that inform decision-making. AI algorithms can predict crop yields, detect diseases early, and recommend optimal planting times based on historical data and real-time inputs. Machine learning models continuously improve their accuracy over time, adapting to changing conditions and enhancing the overall effectiveness of smart agriculture systems (Shaikh *et al*., 2022). Automation and robotics play a significant role in modernizing agricultural practices. Automated systems such as drones and autonomous tractors perform tasks like planting, spraying, and monitoring crops with high precision. Drones equipped with multispectral cameras can assess crop health, identify pest infestations, and monitor field conditions from the air. Autonomous tractors and machinery reduce the need for manual labor, allowing for more efficient use of time and resources. Robotics also extend to livestock management, with automated feeders and milking systems improving animal care and productivity (Yiguang *et al*., 2019).

Smart agriculture significantly increases the efficiency of farming operations. Precision farming techniques reduce wastage of inputs such as water, fertilizers, and pesticides (Ahmad and Dar, 2020). For example, variable rate technology (VRT) allows farmers to apply inputs at varying rates across a field, ensuring that each area receives the optimal amount based on its specific needs. This targeted approach minimizes resource use while maximizing productivity. Automated machinery and robotics further enhance efficiency by performing repetitive tasks quickly and accurately, freeing up farmers to focus on more strategic activities. Resource optimization is a critical benefit of smart agriculture. By leveraging IoT devices and data analytics, farmers can monitor and manage resources more effectively. Precision irrigation systems, informed by soil moisture sensors, deliver water directly to the root zone of plants, reducing water wastage and improving crop health (Bwambale *et al*., 2022). Similarly, precise application of fertilizers and pesticides reduces environmental impact and enhances soil quality. Energy-efficient technologies and renewable energy sources, such as solar-powered sensors, contribute to sustainable farming practices and lower operational costs. The integration of smart agriculture technologies leads to improved crop yields and quality. Real-time monitoring and data-driven decision-making enable farmers to optimize planting schedules, irrigation, and fertilization, resulting in healthier crops and higher yields. Early detection of diseases and pests through IoT sensors and AI analysis allows for timely interventions, preventing significant damage and loss. Additionally, smart agriculture practices promote sustainable farming by reducing the reliance on chemical inputs, preserving soil health, and supporting biodiversity (Tahat *et al*., 2020). This holistic approach not only boosts productivity but also ensures the long-term viability of agricultural ecosystems. The evolution of agricultural technology has culminated in the advent of smart agriculture, characterized by the integration of IoT devices, data analytics, AI, and automation. These components collectively enhance the efficiency, resource optimization, and productivity of farming practices. As smart agriculture continues to evolve, it holds the promise of addressing global food security challenges, promoting sustainable farming, and improving the livelihoods of farmers worldwide (Das and Ansari, 2021).

3. Cybersecurity Challenges in IoT-Driven Farms

One of the primary cybersecurity challenges in IoT-driven farms is the lack of standardization in IoT devices. The rapid development and deployment of various IoT devices by different manufacturers have led to a fragmented ecosystem with inconsistent security protocols (Gebremichael *et al*., 2020). Many devices lack uniform security standards, resulting in vulnerabilities that can be exploited by malicious actors. For instance, some devices may not encrypt data transmissions adequately or may use outdated encryption methods, making it easier for attackers to intercept and manipulate data. The absence of standardized security measures complicates the integration of multiple devices into a cohesive and secure smart agriculture system (Iqbal *et al*., 2020). Weak authentication mechanisms are another significant vulnerability in IoT devices used in smart agriculture. Many IoT devices rely on default or easily guessable passwords, making them susceptible to unauthorized access. Additionally, some devices may not support multi-factor authentication (MFA), which adds an extra layer of security. Attackers can exploit these weaknesses to gain control over the devices, access sensitive data, or disrupt agricultural operations (Rosline *et al*., 2022). For example, an attacker could potentially manipulate irrigation systems or livestock monitoring devices, leading to significant agricultural losses.

Data breaches pose a substantial risk to IoT-driven farms, as the vast amount of data collected by IoT devices can be highly valuable (Kumar *et al*., 2022). This data includes information on crop health, soil conditions, weather patterns, and farm management practices. If unauthorized individuals gain access to this data, it can lead to severe consequences, including financial losses, compromised competitive advantage, and damage to the farm's reputation. Data breaches can occur through various means, such as exploiting vulnerabilities in IoT devices, intercepting data transmissions, or hacking into cloud storage systems where the data is stored. Unauthorized access to IoT devices and data is another critical issue in smart agriculture. Attackers can exploit weak authentication mechanisms, software vulnerabilities, or unsecured network connections to gain access to IoT devices and the data they collect (Meneghello *et al*., 2019). Once inside the system, they can manipulate data, disrupt operations, or steal sensitive information. Unauthorized access can

also result in the misuse of data for malicious purposes, such as tampering with crop yield predictions or manipulating market information to influence prices.

Man-in-the-Middle (MitM) attacks are a significant threat to the network security of IoT-driven farms (Masud *et al*., 2022). In a MitM attack, an attacker intercepts and potentially alters the communication between IoT devices and their management systems. This type of attack can compromise the integrity and confidentiality of the data being transmitted. For instance, an attacker could intercept irrigation commands and alter them, leading to over- or under-watering of crops. MitM attacks can be challenging to detect, as they often go unnoticed until significant damage has been done. Distributed Denial of Service (DDoS) attacks can disrupt the network infrastructure of IoT-driven farms by overwhelming the network with excessive traffic (Kaushik and Gandhi, 2020). This can cause critical systems, such as irrigation controls, livestock monitoring, and data analytics platforms, to become unresponsive or unavailable. The impact of a DDoS attack on a smart farm can be severe, leading to operational disruptions, financial losses, and potential damage to crops and livestock. IoT devices with limited processing power and bandwidth are particularly vulnerable to DDoS attacks (Vishwakarma and Jain, 2020).

Outdated software is a common vulnerability in IoT devices used in smart agriculture. Many IoT devices run on embedded systems that may not receive regular software updates, leaving them exposed to known security vulnerabilities (Butun *et al*., 2019). Attackers can exploit these vulnerabilities to gain unauthorized access, disrupt operations, or steal data. The lack of automatic update mechanisms and the complexity of manually updating numerous devices further exacerbate this issue. The lack of regular updates for IoT devices' firmware is another significant security concern. Firmware updates are crucial for patching security vulnerabilities, improving device functionality, and maintaining overall system integrity (Mugarza *et al*., 2020). However, many IoT devices deployed in agricultural settings do not receive timely firmware updates, leaving them susceptible to attacks. This can be due to various factors, including limited manufacturer support, the logistical challenges of updating devices in remote locations, or the farmers' lack of technical expertise to perform updates.

Physical tampering with IoT devices is a critical security threat in smart agriculture. IoT devices installed in open fields or remote areas can be physically accessed and tampered with by malicious actors (Samaila *et al*., 2018). This can involve altering device settings, installing malware, or even replacing the device with a compromised one. Physical tampering can disrupt the normal functioning of the devices, leading to inaccurate data collection, compromised decision-making, and potential damage to crops or livestock. Theft of IoT equipment is another significant physical security threat. IoT devices, such as sensors, drones, and automated machinery, are valuable assets that can be targeted by thieves (Omolara *et al*., 2022). The loss of these devices can disrupt farming operations and result in substantial financial losses. Additionally, stolen devices may contain sensitive data that, if accessed by unauthorized individuals, can lead to further security breaches and privacy issues (Aswathy and Tyagi, 2022). Securing IoT-driven farms requires addressing various cybersecurity challenges, including vulnerabilities in IoT devices, data security and privacy issues, network security threats, software and firmware vulnerabilities, and physical security threats. By implementing robust security measures and adopting best practices, farmers can protect their smart agriculture systems from cyber threats and ensure the resilience and sustainability of modern farming practices.

4. Solutions for Enhancing Cybersecurity in Smart Agriculture

To bolster the security of IoT devices in smart agriculture, it is crucial to implement robust authentication and authorization mechanisms (Sylla *et al*., 2021). Strong authentication methods, such as multi-factor authentication (MFA), should be employed to ensure that only authorized users can access IoT devices and systems (Mohammed and Yassin, 2019). This can significantly reduce the risk of unauthorized access and tampering. Additionally, role-based access control (RBAC) should be established to define user permissions based on their roles within the agricultural operation, limiting access to sensitive functions and data to only those who require it. Regular firmware and software updates are essential for maintaining the security of IoT devices. Manufacturers and farmers should ensure that all IoT devices receive timely updates to patch known vulnerabilities and improve functionality. Automatic update mechanisms can simplify this process, ensuring that devices are always running the latest secure versions (El Jaouhari and Bouvet, 2022). Regular updates help protect against emerging threats and enhance the overall resilience of smart agriculture systems.

Encryption is a fundamental measure for ensuring data security and privacy in smart agriculture (Song *et al*., 2020). Data should be encrypted both in transit and at rest to protect it from unauthorized access and interception. Secure communication protocols, such as Transport Layer Security (TLS), should be used to encrypt data transmitted between IoT devices, gateways, and cloud platforms (Li *et al*., 2020). Similarly, data stored on devices, servers, and storage systems should be encrypted using robust encryption algorithms to safeguard against data breaches and unauthorized

access. Access control mechanisms are vital for protecting sensitive agricultural data. Implementing fine-grained access control policies ensures that only authorized users and systems can access specific data sets and functionalities. Access controls should be based on the principle of least privilege, granting users the minimum level of access necessary to perform their tasks (Qiu *et al*., 2020). Additionally, continuous monitoring and auditing of access logs can help detect and respond to unauthorized access attempts promptly.

Secure communication protocols are essential for protecting data exchanged between IoT devices and networks in smart agriculture. Protocols such as MQTT (Message Queuing Telemetry Transport) with TLS encryption, HTTPS (Hypertext Transfer Protocol Secure), and CoAP (Constrained Application Protocol) with DTLS (Datagram Transport Layer Security) should be utilized to ensure secure and reliable data transmission (Sanaa *et al*., 2020). These protocols provide encryption, integrity, and authentication, preventing eavesdropping, data tampering, and spoofing attacks. Network segmentation is a powerful strategy for enhancing the security of IoT-driven farms. By dividing the network into smaller, isolated segments, farmers can limit the spread of cyber-attacks and contain potential breaches. Critical systems and devices should be placed in separate network segments, with strict access controls and firewalls governing communication between segments (Wichary *et al*., 2022). This approach reduces the attack surface and helps prevent lateral movement by attackers within the network. Intrusion Detection and Prevention Systems (IDPS) are essential for monitoring network traffic and detecting malicious activities. These systems can identify and block suspicious behavior, such as unauthorized access attempts, malware infections, and network anomalies. Implementing IDPS with real-time alerting and automated response capabilities can help farmers promptly address security incidents and minimize potential damage (Avtar *et al*., 2021).

Regular security audits are crucial for identifying and addressing vulnerabilities in smart agriculture systems. Farmers and agricultural stakeholders should conduct comprehensive security assessments to evaluate the effectiveness of existing security measures and identify areas for improvement. Security audits should include vulnerability scanning, penetration testing, and compliance checks to ensure that IoT devices, networks, and data storage systems meet industry security standards and best practices (Bicaku *et al*., 2020). Employee training and awareness programs are vital components of a robust cybersecurity strategy. Farmers and agricultural workers should be educated about common cybersecurity threats, such as phishing attacks, social engineering, and password security. Regular training sessions can help employees recognize and respond to potential security incidents, reducing the risk of human error and enhancing the overall security posture of smart agriculture operations (Benos *et al*., 2020; Hazrati *et al*., 2022).

Physical security measures are essential to protect IoT devices from tampering and theft. IoT devices should be securely installed in locations that are difficult for unauthorized individuals to access (Tawalbeh *et al*., 2020). This may include using tamper-proof enclosures, securing devices to fixed structures, and employing physical locks and seals. Additionally, access to critical IoT devices should be restricted to authorized personnel only, with strict access controls and monitoring in place. Surveillance and monitoring systems are critical for enhancing the physical security of IoT-driven farms. Installing cameras, motion detectors, and other surveillance equipment can help deter potential intruders and provide real-time monitoring of agricultural operations. Surveillance systems should be integrated with automated alerting mechanisms to notify farmers and security personnel of suspicious activities promptly (George *et al*., 2021). Regular monitoring and maintenance of these systems are necessary to ensure their effectiveness and reliability. Enhancing cybersecurity in smart agriculture requires a multi-faceted approach that addresses IoT device security, data security and privacy, network security measures, robust cybersecurity policies, and physical security enhancements (Yazdinejad *et al*., 2021). By implementing these solutions, farmers can protect their IoT-driven farms from cyber threats, ensuring the resilience and sustainability of modern agricultural practices.

5. Case Studies and Applications in Cybersecurity for Smart Agriculture

Several case studies highlight the successful implementation of cybersecurity measures in smart agriculture, demonstrating effective strategies to protect IoT-driven farms. One notable example is the deployment of a comprehensive cybersecurity framework by a large-scale agricultural operation in the United States. This farm integrated robust authentication mechanisms, including multi-factor authentication (MFA), to secure access to its IoT devices and control systems. The implementation of secure communication protocols, such as Transport Layer Security (TLS), ensured that data transmitted between sensors, drones, and central management systems remained encrypted and protected from interception (Allouch *et al*., 2021). Additionally, the farm adopted regular firmware updates and vulnerability assessments to address potential security gaps. The proactive measures led to a significant reduction in security incidents and enhanced the overall resilience of the farm's technological infrastructure. Another example involves a European agricultural cooperative that successfully implemented network segmentation and intrusion detection systems (IDPS) to protect its IoT ecosystem. By segmenting its network into isolated zones, the cooperative minimized the risk of lateral movement by attackers and contained potential breaches. The IDPS provided real-time

monitoring and alerts, enabling rapid response to suspicious activities. These measures effectively safeguarded the cooperative's sensitive data and operational systems, reducing the risk of cyber-attacks and ensuring the continuity of agricultural operations.

Analyzing cybersecurity incidents in smart agriculture provides valuable insights into the challenges and vulnerabilities associated with IoT-driven farms (Rudrakar and Rughani, 2022). One prominent case is the 2019 cyber-attack on a smart irrigation system used by a major agricultural enterprise in Australia. The attack exploited weak authentication mechanisms and outdated firmware, leading to unauthorized access and disruption of irrigation controls. The incident resulted in significant financial losses due to crop damage and operational downtime. Key lessons from this incident include the importance of implementing strong authentication measures, regularly updating firmware, and conducting thorough security audits to identify and address vulnerabilities before they can be exploited. Another instructive case is the 2021 ransomware attack on a livestock monitoring system in the UK. Attackers gained access to the system through a compromised network connection and encrypted critical data, demanding a ransom for decryption. The attack disrupted livestock management operations and highlighted the need for robust backup solutions and encryption of data both in transit and at rest. The incident underscored the necessity of having a well-defined incident response plan and regularly testing backup and recovery processes to mitigate the impact of ransomware attacks.

A comparative analysis of different cybersecurity approaches in smart agriculture reveals varied effectiveness in addressing IoT-related threats (Khalil *et al*., 2022). For instance, the adoption of multi-layered security strategies, such as those implemented by the aforementioned U.S. farm and European cooperative, demonstrates a comprehensive approach to protecting IoT systems. The combination of strong authentication, secure communication, network segmentation, and real-time monitoring provides a robust defense against a wide range of cyber threats. This multi-faceted approach is generally more effective in mitigating risks compared to single-layer solutions. In contrast, some smaller agricultural operations may rely on more basic cybersecurity measures due to limited resources. For example, a small farm might implement basic password protection and periodic firmware updates without additional security layers. While these measures can provide a baseline level of protection, they may not be sufficient to address advanced cyber threats or sophisticated attacks. The comparative analysis highlights the importance of scaling cybersecurity measures based on the size and complexity of the agricultural operation, as well as the potential impact of security breaches (Ferrag *et al*., 2021). Successful implementation of cybersecurity measures in smart agriculture involves integrating multiple strategies to protect IoT systems effectively. Lessons learned from cybersecurity incidents emphasize the need for strong authentication, regular updates, and robust incident response plans. Comparative analysis of different approaches underscores the value of adopting comprehensive, multi-layered security strategies to address diverse threats and ensure the resilience of smart agriculture systems. These insights contribute to the ongoing development of effective cybersecurity practices that can safeguard the technological advancements driving modern agriculture.

6. Future Trends and Emerging Technologies in Cybersecurity for Smart Agriculture

The field of IoT security is rapidly evolving to address the increasing complexity and scale of smart agriculture systems. One of the key advancements is the development of hardware-based security solutions, such as Trusted Platform Modules (TPMs) and Hardware Security Modules (HSMs) (Michailidis and Vouyioukas, 2022). These devices provide secure storage of cryptographic keys and protect against physical tampering, enhancing the security of IoT devices at the hardware level. Additionally, the integration of Secure Elements (SEs) in IoT devices ensures that sensitive data and cryptographic operations are isolated from potentially compromised software environments. Another significant advancement is the use of advanced encryption algorithms and protocols tailored for resource-constrained IoT devices. For instance, lightweight encryption methods, such as Elliptic Curve Cryptography (ECC), offer robust security while minimizing computational overhead. These advancements enable IoT devices to maintain high security standards without sacrificing performance. Furthermore, the implementation of secure boot mechanisms ensures that only authorized firmware is executed, preventing unauthorized modifications and ensuring the integrity of the IoT devices (Yao and Zimmer, 2020).

Blockchain technology is emerging as a transformative solution for enhancing data integrity and security in smart agriculture. Blockchain provides a decentralized and immutable ledger that can record and verify transactions transparently (Aggarwal and Kumar, 2021). By leveraging blockchain, agricultural stakeholders can ensure the integrity of data collected from IoT devices, such as soil moisture levels, crop health metrics, and weather conditions. Each data entry is timestamped and linked to previous entries, creating an unalterable chain of records that is resistant to tampering and fraud. Smart contracts, a feature of blockchain technology, can automate and enforce security policies and operational rules. For example, smart contracts can facilitate secure and transparent transactions between farmers, suppliers, and buyers, ensuring that data such as crop yields and quality metrics are accurately recorded and verified.

Blockchain's decentralized nature also enhances resilience against single points of failure and reduces the risk of data breaches, providing a robust framework for securing agricultural data (Bhat *et al*., 2021).

Artificial Intelligence (AI) plays a critical role in advancing cybersecurity for smart agriculture by enhancing threat detection and mitigation capabilities (Zeadally *et al*., 2020). Machine learning algorithms can analyze vast amounts of data from IoT devices and network traffic to identify patterns indicative of potential cyber threats. AI-driven systems can detect anomalies, such as unusual access patterns or unexpected changes in device behavior, which may signal a security breach or attack. Deep learning models are particularly effective in detecting sophisticated attacks, including zero-day threats and advanced persistent threats (APTs) (Khaleefa and Abdulah, 2022). These models can continuously learn from new data and adapt to evolving threat landscapes, improving their ability to identify and respond to emerging threats. AI-powered threat intelligence platforms can also provide actionable insights and recommendations for mitigating identified risks, enabling more effective and timely responses to cybersecurity incidents.

Predictive analytics is becoming an essential tool for proactive cybersecurity in smart agriculture (Sinha and Dhanalakshmi, 2022). By leveraging historical data and advanced analytics techniques, predictive models can forecast potential security threats and vulnerabilities before they materialize. For example, predictive analytics can analyze trends in network traffic, device behavior, and known vulnerabilities to identify potential attack vectors and prioritize security measures accordingly. The application of predictive analytics enables organizations to adopt a proactive approach to cybersecurity, focusing on preventive measures rather than reactive responses. This includes implementing early warning systems, enhancing threat detection capabilities, and optimizing resource allocation for security initiatives. Predictive analytics also supports risk management by providing insights into the likelihood and potential impact of various threats, helping organizations to develop targeted and effective security strategies (Pandey *et al*., 2020; Ullah *et al*., 2021). The future of cybersecurity in smart agriculture is shaped by advancements in IoT security technologies, the integration of blockchain for data integrity, the role of AI in threat detection, and the application of predictive analytics. These emerging technologies and trends offer promising solutions for addressing the evolving cybersecurity challenges in smart agriculture, enhancing the resilience and security of IoT-driven farming systems. As these technologies continue to advance, they will play a crucial role in safeguarding the technological innovations that drive modern agricultural practices

7. Conclusion

In conclusion, cybersecurity is a critical aspect of managing smart agriculture systems, which integrate advanced technologies such as IoT devices, data analytics, and automation to enhance farming practices. The key points discussed highlight the multifaceted nature of cybersecurity challenges and solutions in this context. We have explored vulnerabilities in IoT devices, including issues with authentication and outdated software; data security concerns, such as breaches and unauthorized access; and network threats, including DDoS attacks and MitM attacks. Addressing these challenges involves implementing strong security measures, such as robust authentication, regular updates, and encryption, as well as adopting advanced technologies like AI and blockchain.

The importance of cybersecurity in smart agriculture cannot be overstated. As farming practices increasingly rely on interconnected systems and data-driven decision-making, the potential impact of cyber threats grows. Effective cybersecurity measures are essential not only for protecting sensitive data but also for ensuring the continuity and efficiency of agricultural operations. Security breaches can lead to significant financial losses, operational disruptions, and damage to both the technology and the reputation of the agricultural enterprise.

Looking ahead, the future of cybersecurity in smart agriculture will be shaped by ongoing advancements in technology and evolving threat landscapes. Recommendations for enhancing cybersecurity include adopting comprehensive, multi-layered security strategies that integrate IoT security technologies, blockchain for data integrity, and AI for threat detection. Additionally, investing in predictive analytics will enable proactive risk management and early threat detection. As smart agriculture continues to advance, staying ahead of emerging threats and continuously evolving security practices will be crucial for maintaining the integrity and resilience of agricultural systems.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Aggarwal, S. and Kumar, N., 2021. Basics of blockchain. In *Advances in computers* (Vol. 121, pp. 129-146). Elsevier.

[2] Ahmad, S.F. and Dar, A.H., 2020. Precision farming for resource use efficiency. *Resources Use Efficiency in Agriculture*, pp.109-135.

[3] 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.

[4] Allouch, A., Cheikhrouhou, O., Koubâa, A., Toumi, K., Khalgui, M. and Nguyen Gia, T., 2021. Utm-chain: blockchain-based secure unmanned traffic management for internet of drones. *Sensors*, *21*(9), p.3049.

[5] Aswathy, S.U. and Tyagi, A.K., 2022. Privacy Breaches through Cyber Vulnerabilities: Critical Issues, Open Challenges, and Possible Countermeasures for the Future. In *Security and Privacy-Preserving Techniques in Wireless Robotics* (pp. 163-210). CRC Press.

[6] Avtar, R., Kouser, A., Kumar, A., Singh, D., Misra, P., Gupta, A., Yunus, A.P., Kumar, P., Johnson, B.A., Dasgupta, R. and Sahu, N., 2021. Remote sensing for international peace and security: Its role and implications. *Remote Sensing*, *13*(3), p.439.

[7] Ayaz, M., Ammad-Uddin, M., Sharif, Z., Mansour, A. and Aggoune, E.H.M., 2019. Internet-of-Things (IoT)-based smart agriculture: Toward making the fields talk. *IEEE access*, *7*, pp.129551-129583.

[8] Barreto, L. and Amaral, A., 2018, September. Smart farming: Cyber security challenges. In *2018 International Conference on Intelligent Systems (IS)* (pp. 870-876). IEEE.

[9] Benos, L., Bechar, A. and Bochtis, D., 2020. Safety and ergonomics in human-robot interactive agricultural operations. *Biosystems Engineering*, *200*, pp.55-72.

[10] Bhat, S.A., Huang, N.F., Sofi, I.B. and Sultan, M., 2021. Agriculture-food supply chain management based on blockchain and IoT: a narrative on enterprise blockchain interoperability. *Agriculture*, *12*(1), p.40.

[11] Bicaku, A., Tauber, M. and Delsing, J., 2020. Security standard compliance and continuous verification for Industrial Internet of Things. *International Journal of Distributed Sensor Networks*, *16*(6), p.1550147720922731.

[12] Butun, I., Österberg, P. and Song, H., 2019. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials*, *22*(1), pp.616-644.

[13] Bwambale, E., Abagale, F.K. and Anornu, G.K., 2022. Smart irrigation monitoring and control strategies for improving water use efficiency in precision agriculture: A review. *Agricultural Water Management*, *260*, p.107324.

[14] Chaterji, S., DeLay, N., Evans, J., Mosier, N., Engel, B., Buckmaster, D. and Chandra, R., 2020. Artificial intelligence for digital agriculture at scale: Techniques, policies, and challenges. *arXiv preprint arXiv:2001.09786*.

[15] Cheema, M.J.M. and Khan, M.A., 2019. Information technology for sustainable agriculture. *Innovations in sustainable agriculture*, pp.585-597.

[16] Das, U. and Ansari, M.A., 2021. The nexus of climate change, sustainable agriculture and farm livelihood: contextualizing climate smart agriculture. *Climate Research*, *84*, pp.23-40.

[17] Dayıoğlu, M.A. and Turker, U., 2021. Digital transformation for sustainable future-agriculture 4.0: A review. *Journal of Agricultural Sciences*, *27*(4), pp.373-399.

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

[19] El Bilali, H., Bottalico, F., Ottomano Palmisano, G. and Capone, R., 2020. Information and communication technologies for smart and sustainable agriculture. In *30th Scientific-Experts Conference of Agriculture and Food Industry: Answers for Forthcoming Challenges in Modern Agriculture* (pp. 321-334). Springer International Publishing.

[20] El Jaouhari, S. and Bouvet, E., 2022. Secure firmware Over-The-Air updates for IoT: Survey, challenges, and discussions. *Internet of Things*, *18*, p.100508.

[21] Ferrag, M.A., Shu, L., Friha, O. and Yang, X., 2021. Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions. *IEEE/CAA Journal of Automatica Sinica*, *9*(3), pp.407-436.

[22] Fischer, R.A. and Connor, D.J., 2018. Issues for cropping and agricultural science in the next 20 years. *Field Crops Research*, *222*, pp.121-142.

[23] Gebremichael, T., Ledwaba, L.P., Eldefrawy, M.H., Hancke, G.P., Pereira, N., Gidlund, M. and Akerberg, J., 2020. Security and privacy in the industrial internet of things: Current standards and future challenges. *IEEE Access*, *8*, pp.152351-152366.

[24] George, J., Häsler, B., Komba, E., Sindato, C., Rweyemamu, M. and Mlangwa, J., 2021. Towards an integrated animal health surveillance system in Tanzania: making better use of existing and potential data sources for early warning surveillance. *BMC veterinary research*, *17*, pp.1-18.

[25] 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.

[26] Hazrati, M., Dara, R. and Kaur, J., 2022. On-farm data security: practical recommendations for securing farm data. *Frontiers in Sustainable Food Systems*, *6*, p.884187.

[27] Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B. and Bangash, Y.A., 2020. An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. *IEEE Internet of Things Journal*, *7*(10), pp.10250-10276.

[28] Kaushik, S. and Gandhi, C., 2020. Security and Privacy Issues in Fog/Edge/Pervasive Computing. *Fog, Edge, and Pervasive Computing in Intelligent IoT Driven Applications*, pp.369-387.

[29] Khaleefa, E.J. and Abdulah, D.A., 2022. Concept and difficulties of advanced persistent threats (APT): Survey. *International Journal of Nonlinear Analysis and Applications*, *13*(1), pp.4037-4052.

[30] Khalil, U., Malik, O.A., Uddin, M. and Chen, C.L., 2022. A comparative analysis on blockchain versus centralized authentication architectures for IoT-enabled smart devices in smart cities: a comprehensive review, recent advances, and future research directions. *Sensors*, *22*(14), p.5168.

[31] Kumar, R., Sinwar, D., Pandey, A., Tadele, T., Singh, V. and Raghuwanshi, G., 2022. IoT enabled technologies in smart farming and challenges for adoption. *Internet of Things and Analytics for Agriculture, Volume 3*, pp.141-164.

[32] Li, P., Su, J. and Wang, X., 2020. iTLS: Lightweight transport-layer security protocol for IoT with minimal latency and perfect forward secrecy. *IEEE Internet of Things Journal*, *7*(8), pp.6828-6841.

[33] M. Tahat, M., M. Alananbeh, K., A. Othman, Y. and I. Leskovar, D., 2020. Soil health and sustainable agriculture. *Sustainability*, *12*(12), p.4859.

[34] Masud, M., Gaba, G.S., Kumar, P. and Gurtov, A., 2022. A user-centric privacy-preserving authentication protocol for IoT-AmI environments. *Computer Communications*, *196*, pp.45-54.

[35] Meneghello, F., Calore, M., Zucchetto, D., Polese, M. and Zanella, A., 2019. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal*, *6*(5), pp.8182-8201.

[36] Michailidis, E.T. and Vouyioukas, D., 2022. A review on software-based and hardware-based authentication mechanisms for the internet of drones. *Drones*, *6*(2), p.41.

[37] Misra, N.N., Dixit, Y., Al-Mallahi, A., Bhullar, M.S., Upadhyay, R. and Martynenko, A., 2020. IoT, big data, and artificial intelligence in agriculture and food industry. *IEEE Internet of things Journal*, *9*(9), pp.6305-6324.

[38] 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*.

[39] Mohammed, A.J. and Yassin, A.A., 2019. Efficient and flexible multi-factor authentication protocol based on fuzzy extractor of administrator's fingerprint and smart mobile device. *Cryptography*, *3*(3), p.24.

[40] Mugarza, I., Flores, J.L. and Montero, J.L., 2020. Security issues and software updates management in the industrial internet of things (iiot) era. *Sensors*, *20*(24), p.7160.

[41] Omolara, A.E., Alabdulatif, A., Abiodun, O.I., Alawida, M., Alabdulatif, A. and Arshad, H., 2022. The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*, p.102494.

[42] Pandey, S., Singh, R.K., Gunasekaran, A. and Kaushik, A., 2020. Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), pp.103-128.

[43] Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S. and Fang, B., 2020. A survey on access control in the age of internet of things. *IEEE Internet of Things Journal*, *7*(6), pp.4682-4696.

[44] Raj, E.F.I., Appadurai, M. and Athiappan, K., 2022. Precision farming in modern agriculture. In Smart agriculture automation using advanced technologies: Data analytics and machine learning, cloud architecture, automation and IoT (pp. 61-87). Singapore: Springer Singapore.

[45] Rosline, G.J., Rani, P. and Gnana Rajesh, D., 2022. Comprehensive analysis on security threats prevalent in IoT-based smart farming systems. In *Ubiquitous Intelligent Systems: Proceedings of ICUIS 2021* (pp. 185-194). Springer Singapore.

[46] Rudrakar, S. and Rughani, P., 2022. IoT based Agriculture (IoTA): Architecture, Cyber Attack, Cyber Crime and Digital Forensics Challenges.

[47] Samaila, M.G., Neto, M., Fernandes, D.A., Freire, M.M. and Inácio, P.R., 2018. Challenges of securing Internet of Things devices: A survey. *Security and Privacy*, *1*(2), p.e20.

[48] Sanaa, E.L., Bajit, A., Barodi, A., Chaoui, H. and Tamtaoui, A., 2020, December. An optimized security vehicular Internet of Things-IoT-application layer protocols MQTT and COAP based on cryptographic elliptic-curve. In *2020 IEEE 2nd International Conference on Electronics, Control, Optimization and Computer Science (ICECOCS)* (pp. 1-6). IEEE.

[49] 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.

[50] 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.

[51] Song, J., Zhong, Q., Wang, W., Su, C., Tan, Z. and Liu, Y., 2020. FPDP: Flexible privacy-preserving data publishing scheme for smart agriculture. *IEEE Sensors Journal*, *21*(16), pp.17430-17438.

[52] Suciu, G., Ijaz, H., Zatreanu, I. and Drăgulinescu, A.M., 2019. Real time analysis of weather parameters and smart agriculture using IoT. In *Future Access Enablers for Ubiquitous and Intelligent Infrastructures: 4th EAI International Conference, FABULOUS 2019, Sofia, Bulgaria, March 28-29, 2019, Proceedings 283* (pp. 181-194). Springer International Publishing.

[53] Sylla, T., Mendiboure, L., Chalouf, M.A. and Krief, F., 2021. Blockchain-based context-aware authorization management as a service in iot. *Sensors*, *21*(22), p.7656.

[54] Tawalbeh, L.A., Muheidat, F., Tawalbeh, M. and Quwaider, M., 2020. IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), p.4102.

[55] Ullah, F., Qayyum, S., Thaheem, M.J., Al-Turjman, F. and Sepasgozar, S.M., 2021. Risk management in sustainable smart cities governance: A TOE framework. *Technological Forecasting and Social Change*, *167*, p.120743.

[56] Vishwakarma, R. and Jain, A.K., 2020. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommunication systems*, *73*(1), pp.3-25.

[57] Wichary, T., Mongay Batalla, J., Mavromoustakis, C.X., Żurek, J. and Mastorakis, G., 2022. Network slicing security controls and assurance for verticals. *Electronics*, *11*(2), p.222.

[58] Yao, J. and Zimmer, V., 2020. Building secure firmware. *Apress: New York, NY, USA*, pp.18-48.

[59] 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.

[60] Yiguang, Z., Liang, Y., Shanshan, Z. and Benhai, X., 2019. Advances in the development and applications of intelligent equipment and feeding technology for livestock production. *Smart agriculture*, *1*(1), p.20.

[61] Zeadally, S., Adi, E., Baig, Z. and Khan, I.A., 2020. Harnessing artificial intelligence capabilities to improve cybersecurity. *Ieee Access*, *8*, pp.23817-23837