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)

An extensive survey of smart agriculture technologies: Current security posture

Martin Otieno *

School of Informatics and Innovative Systems, Jaramogi Oginga Odinga University of Science and Technology, Kenya.

World Journal of Advanced Research and Reviews, 2023, 18(03), 1207–1231

Publication history: Received on 15 May 2023; revised on 22 June 2023; accepted on 24 June 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.18.3.1241

Abstract

Smart agriculture, enabled by advanced technologies such as internet of things, artificial intelligence and data analytics, offers immense potential for optimizing farming practices and increasing agricultural productivity. However, as the adoption of smart agriculture systems continues to grow, it brings forth various security issues that need to be addressed to protect farming operations, data integrity, and privacy. This paper provides an overview of the security issues in smart agriculture, including vulnerabilities in internet of things devices, lack of standardized security protocols, limited security awareness among farmers, and challenges in securing data and communication networks. In addition, it highlights the need for robust security measures to mitigate risks such as unauthorized access, data breaches, and disruption of operations. Moreover, emphasis should be laid on the importance of collaborative efforts between technology providers, agricultural stakeholders, researchers, and policymakers to develop effective security solutions and standards that ensure the trustworthiness and resilience of smart agriculture systems.

Keywords: Smart Agriculture; Precision Agriculture; Attacks; Security; Threats; Vulnerabilities

1. Introduction

Smart farming, also known as precision agriculture, is an innovative approach to agricultural practices that leverages advanced technologies to optimize efficiency, productivity, and sustainability in farming operations [1]-[4]. As shown in Fig. 1, it involves the integration of various technologies, such as Internet of Things (IoT), artificial intelligence (AI), data analytics, robotics, and remote sensing, to make informed decisions and automate processes in agricultural systems. The primary goal of smart farming is to enhance crop production, minimize resource waste, reduce environmental impact, and improve overall profitability. By utilizing a network of interconnected devices and sensors [5], farmers can collect real-time data on various factors such as soil moisture levels, weather conditions, crop health, and pest infestations. This data is then analyzed to provide actionable insights, allowing farmers to make data-driven decisions and implement precise interventions [6]-[8].

One of the key components of smart farming is the use of IoT devices and sensors. These devices are deployed throughout the farmland to monitor and control different variables [8]-[11]. For instance, soil moisture sensors can provide information about the water requirements of crops, enabling farmers to apply water precisely where and when it is needed, reducing water wastage. Similarly, weather stations and satellite imagery can offer accurate and localized weather data, helping farmers optimize planting schedules and manage crop diseases.

According to [12], artificial intelligence plays a crucial role in smart farming by analyzing the collected data and providing intelligent recommendations. Machine learning algorithms can identify patterns and correlations in the data, enabling predictive models for crop growth, pest outbreaks, and yield estimation [13]-[16]. This information assists farmers in making informed decisions regarding the optimal use of fertilizers, pesticides, and other inputs, leading to improved resource management and reduced environmental impact. As explained in [17], robots and drones can be

---

*Corresponding author: Martin Otieno

utilized in smart farming to automate labor-intensive tasks. Robots can perform activities like seeding, weeding, and harvesting with precision and efficiency, reducing the need for manual labor and increasing productivity [18]-[20]. As shown in Fig.2, drones equipped with cameras and sensors [21] can gather high-resolution images and collect data over large areas, helping farmers monitor crop health, detect early signs of diseases or nutrient deficiencies, and identify areas requiring attention.

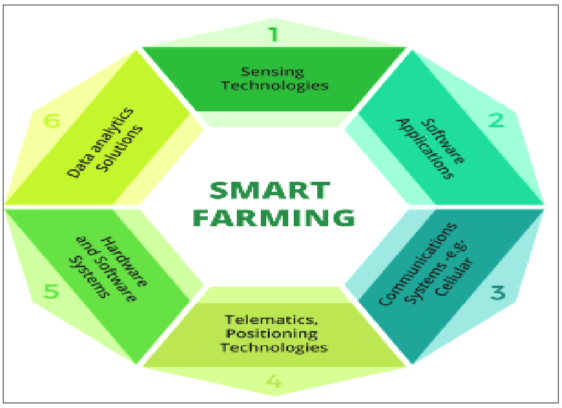

Figure 1 Typical smart agriculture scenario

Figure 2 Drones in smart agriculture

Researchers in [22] point out that smart agriculture relies on various sensors to collect real-time data about environmental conditions, crop health, soil characteristics, and livestock parameters. These sensors provide critical insights that enable farmers to make informed decisions and optimize farming practices. As shown in Fig. 3, examples of sensors commonly used in smart agriculture include weather sensors, soil moisture sensors, soil pH sensors, nutrient sensors, crop health sensors, light sensors, livestock monitoring sensors, water quality sensors, gas sensors and insect traps sensors. Here, weather sensors measure atmospheric conditions such as temperature, humidity, rainfall, wind speed, and solar radiation [23]–[26]. They help farmers understand weather patterns, predict storms, and optimize irrigation schedules based on evapo-transpiration rates. On the other hand, soil moisture sensors measure the water content in the soil, allowing farmers to monitor [27] soil moisture levels and determine irrigation needs. These sensors help prevent overwatering or underwatering, optimize water usage, and prevent water stress in crops. However, soil pH sensors measure the acidity or alkalinity of the soil. By monitoring soil pH, farmers can determine the soil's nutrient availability and adjust soil amendments accordingly [28]. Maintaining optimal pH levels is crucial for healthy plant growth and nutrient uptake. As explained in [29], nutrient sensors measure the concentration of essential nutrients in the soil, such as nitrogen, phosphorus, and potassium. These sensors provide valuable data for precise fertilizer application, ensuring that crops receive the right amount of nutrients for optimal growth and yield. On the other hand, crop health sensors detect indicators of plant stress, diseases, and pests [30]. They can measure parameters such as leaf temperature, chlorophyll content, and vegetation indices to assess crop health and detect early signs of disease or pest infestation. This data helps farmers take timely preventive measures and implement targeted pest management strategies. On their part, light sensors measure the intensity and quality of light in the crop canopy [31]. They provide information about photosynthetic activity, plant growth stages, and light requirements. This data helps optimize lighting conditions in controlled environment agriculture (CEA) systems, such as greenhouses or vertical farms. On the other hand, livestock monitoring sensors are used to track parameters related to animal health and well-being [32]. For example, temperature sensors [33] can monitor body temperature, activity sensors can track animal movement, and rumen pH sensors can assess digestive health in ruminant animals. Livestock sensors enable early detection of health issues and support proactive animal management.

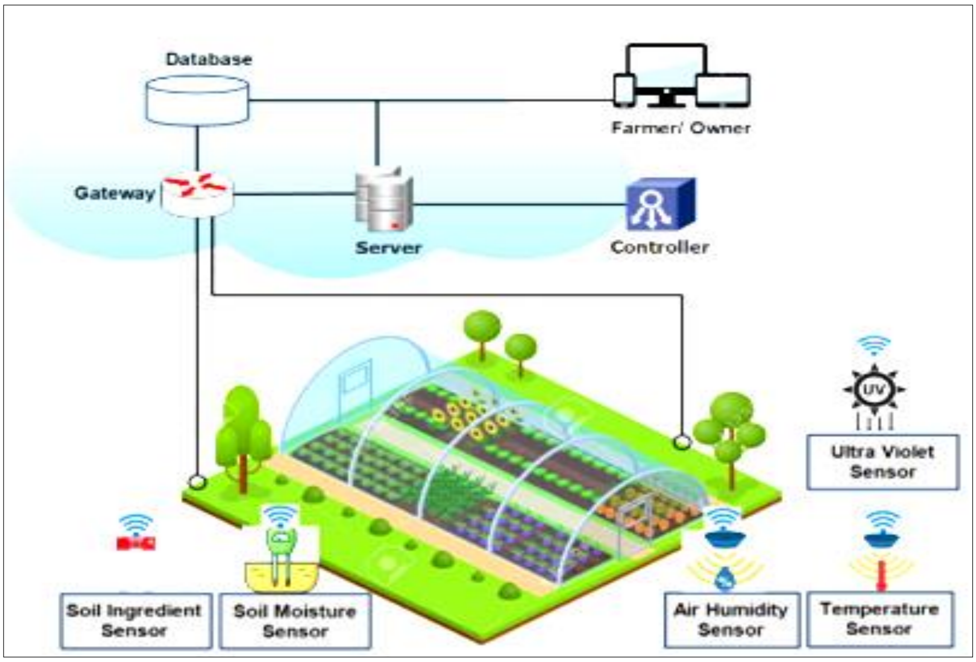

Figure 3 Smart agriculture

Water quality sensors measure parameters such as pH, dissolved oxygen, conductivity, and turbidity in irrigation water sources or aquaculture systems [34]. Monitoring water quality ensures that crops or aquatic organisms receive clean and suitable water, preventing adverse effects on plant health or aquatic ecosystems. However, gas sensors detect and measure the concentration of gases, such as carbon dioxide (CO2) or ethylene, which are important indicators of plant respiration and ripening processes [35]. Gas sensors can be used to optimize storage conditions and shelf life of harvested crops. On their part, insect traps equipped with sensors and lures capture and monitor insect populations [36]. These sensors help farmers assess pest infestation levels, identify specific pest species, and implement targeted pest management strategies. These sensors, among others, provide critical data points that enable farmers to monitor and manage agricultural systems effectively. Integrating sensor data with advanced analytics and decision support systems empowers farmers to optimize resource allocation, improve crop yields, and make informed decisions for sustainable and efficient farming practices.

In a nutshell, smart farming holds great promise for transforming agriculture into a more sustainable and productive industry. By harnessing the power of technology and data, farmers can optimize their operations, improve crop yields, conserve resources, minimize environmental impact, and contribute to global food security in a rapidly evolving world. In this paper, an extensive review of the current status of smart agriculture technologies and their security posture is given. Towards the end of this paper, some research gaps are identified which needs to be filled by future researches.

2. Need for smart agriculture

Smart agriculture, or precision agriculture, is increasingly becoming a necessity due to several pressing challenges and needs in the agricultural sector. Table 1 discusses some key reasons why smart agriculture is crucial.

Table 1 Necessity of smart agriculture

Necessity	**Discussion**
Resource Scarcity	Resources such as water, land, and energy are limited and face increasing pressure due to population growth and climate change [37]. Smart agriculture enables precise resource management, minimizing waste and maximizing the efficient [38] use of inputs like water, fertilizers, and energy.
Cost Optimization	Traditional farming practices often involve overuse or misuse of inputs, leading to higher costs [39]. Smart agriculture allows farmers to make data-driven decisions, optimizing the use of fertilizers, pesticides, and water, thereby reducing costs and increasing profitability [40].
Labor Efficiency and Safety	Farm labor shortages are a significant challenge in many regions. Smart agriculture introduces automation and robotics, reducing the reliance on manual labor for tasks such as planting, weeding, and harvesting. This not only improves efficiency [43] but also enhances worker safety by minimizing exposure to hazardous conditions.
Climate Change and Environmental Sustainability	Climate change impacts agriculture through extreme weather events, changing rainfall patterns, and the spread of pests and diseases. Smart agriculture helps farmers adapt to climate change by providing real-time data on weather conditions, enabling timely interventions, and reducing environmental impact through optimized resource usage [44], [45].
Traceability and Quality Assurance	Consumers are increasingly concerned about the origin and quality of the food they consume [46], [47]. Smart agriculture technologies enable improved traceability [48], allowing farmers to track the entire supply chain, ensure food safety, and provide transparent information to consumers.
Data-Driven Decision Making	Smart agriculture generates vast amounts of data through sensors, drones, and satellite imagery [49], [50]. Analyzing this data using AI and data analytics helps farmers gain valuable insights, make informed decisions, and optimize farming practices for better outcomes [51].
Population Growth and Food Demand	The global population is projected to reach 9.7 billion by 2050, which will significantly increase the demand for food. Smart agriculture offers a way to increase agricultural productivity and efficiency to meet this growing demand [52].
Crop Monitoring and Management	Smart agriculture technologies enable continuous monitoring [53] of crops, including factors like soil moisture, temperature, and nutrient levels. This data-driven approach helps farmers detect crop stress, diseases, and nutrient deficiencies early on, allowing timely interventions and reducing crop losses [54], [55].

Basically, the need for smart agriculture arises from the need to address challenges such as population growth, resource scarcity, climate change, cost optimization, and labor efficiency. By integrating advanced technologies, smart agriculture offers the potential to transform traditional farming practices into more sustainable, productive, and environmentally friendly systems.

2.1. Technologies driving smart agriculture

Smart agriculture is driven by various technologies that enable advanced monitoring, automation, and decision-making in agricultural practices. These technologies play a crucial role in optimizing resource management, improving crop yields, and enhancing overall efficiency in farming operations. Some of the prominent key driving technologies in smart agriculture are presented in Fig. 4 and are discussed in the sub-sections below.

2.1.1. Internet of Things (IoT)

IoT technology forms the backbone of smart agriculture by connecting physical devices and sensors to the internet, enabling data collection and remote monitoring [56]-[58]. IoT devices such as weather stations, soil moisture sensors, and crop health sensors provide real-time data on environmental conditions, plant growth, and livestock health. This data enables farmers to make data-driven decisions and optimize resource allocation [59].

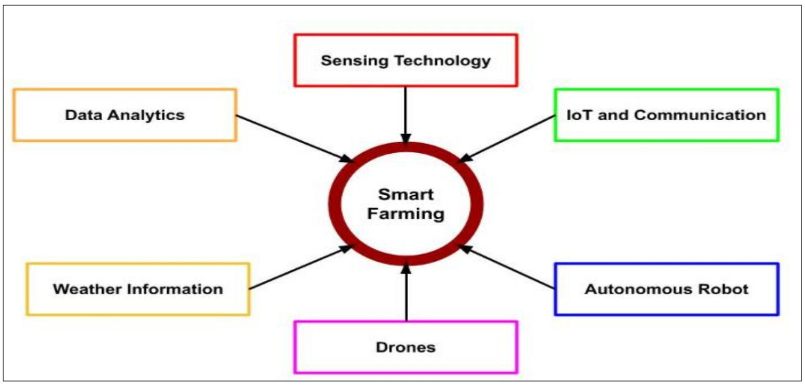

Figure 4 Key technological drivers for smart agriculture

2.1.2. Remote Sensing and Satellite Imaging

Remote sensing technologies, including satellite imaging and aerial drones, provide valuable insights into crop health, water stress, and pest infestation [60]-[62]. These technologies capture high-resolution images and multispectral data, allowing farmers to monitor large agricultural areas and detect anomalies or crop stress indicators. Remote sensing helps in early pest detection, disease prevention, and precision agriculture practices.

2.1.3. Big Data Analytics

The ability to process and analyze large volumes of data is vital in smart agriculture. Big data analytics techniques extract meaningful insights from various data sources, including weather data, soil data, sensor data, and historical crop records [63]-[67]. By analyzing this data, farmers can gain valuable insights into crop performance, predict yield outcomes, optimize irrigation and fertilization, and identify trends for better decision-making.

2.1.4. Artificial Intelligence (AI) and Machine Learning (ML)

AI and ML technologies are instrumental in smart agriculture applications. AI-powered algorithms and ML models can analyze vast amounts of data and generate predictive models for disease outbreak detection, crop yield forecasting, and pest management [68]-[71]. These technologies enable automated decision-making, real-time monitoring, and autonomous operations in smart agriculture systems.

2.1.5. Robotics and Automation

Robotics and automation technologies are transforming traditional farming practices [72]. Autonomous robots and drones equipped with sensors and cameras can perform tasks like seeding, spraying, and harvesting with precision and efficiency [73]-[76]. Robotic systems can also assist in weed detection and removal, reducing the need for manual labor and minimizing the use of chemical herbicides.

2.1.6. Precision Agriculture and Variable Rate Technology (VRT)

Precision agriculture utilizes technology to optimize resource application based on specific field conditions [77]. VRT systems analyze data from sensors [78] and mapping tools to precisely deliver inputs such as water, fertilizers, and pesticides. This technology ensures that resources are used efficiently, minimizing waste and environmental impact while maximizing crop productivity.

2.1.7. Cloud Computing and Edge Computing

Cloud computing enables the storage, processing, and analysis of agricultural data on remote servers, providing scalability and accessibility [79]-[83]. Edge computing, on the other hand, brings computing capabilities closer to the data source, reducing latency and enabling real-time decision-making at the field level. Both cloud and edge computing support the seamless integration of data from various sources and enable efficient data management and analysis in smart agriculture.

2.1.8. Agricultural Robotics and Sensing

Advanced robotic systems equipped with sophisticated sensors and actuators have the potential to revolutionize agricultural practices [84], [85]. These systems can perform tasks such as selective harvesting, precision spraying, and soil sampling with high accuracy and efficiency. Sensing technologies, including hyperspectral imaging and multispectral cameras, enable detailed crop analysis and monitoring.

It is important to note that these technologies are continuously evolving and becoming more sophisticated, enabling farmers to make data-driven decisions, optimize resource allocation, and improve overall agricultural productivity. As these technologies continue to advance, they hold immense potential to address the global challenges of food security, sustainable agriculture, and environmental conservation.

3. General challenges in smart agriculture

Although smart agriculture brings numerous benefits, there are several challenges that need to be addressed for its widespread adoption and successful implementation. Some of the general challenges in smart agriculture are described in the sub-sections below.

3.1.1. High Initial Investment

The upfront costs of implementing smart agriculture technologies can be a significant barrier for many farmers, especially small-scale and resource-constrained operations. The cost of purchasing and installing sensors, IoT devices, drones, robotics, and data management systems can be prohibitive [86], [87]. Governments, organizations, and stakeholders need to provide financial support, incentives, and subsidies to make these technologies more accessible.

3.1.2. Limited Technical Expertise

Smart agriculture requires a certain level of technical expertise in areas such as data analytics, AI, and IoT [88]-[91]. However, many farmers may lack the necessary knowledge and skills to effectively implement and utilize these technologies. Training programs, workshops, and educational initiatives are crucial to bridge this knowledge gap and empower farmers to leverage smart agriculture solutions effectively.

3.1.3. Connectivity and Infrastructure

Smart agriculture heavily relies on reliable and high-speed internet connectivity, especially in rural areas [92]. However, in some regions, internet infrastructure is inadequate or nonexistent. Poor connectivity can hinder real-time data collection, remote monitoring [93], and the seamless operation of IoT devices [94], [95]. Governments and private stakeholders must invest in improving rural connectivity to ensure widespread adoption of smart agriculture.

3.1.4. Data Privacy and Security

Smart agriculture involves the collection, storage, and analysis of vast amounts of data, including sensitive information about crops, farms, and farmers [96]-[99]. Ensuring data privacy and security is paramount to protect farmers' and consumers' interests. Strong data encryption, secure cloud storage, and robust cybersecurity measures must be implemented to prevent unauthorized access, data breaches, and misuse of information.

3.1.5. Data Interoperability and Integration

Smart agriculture systems often involve multiple technologies and platforms, which may use different data formats and protocols [100]-[104]. Ensuring seamless data interoperability and integration across various systems can be challenging. Standardization of data formats, open APIs (Application Programming Interfaces), and data-sharing protocols are essential for efficient data exchange and collaboration between different smart agriculture solutions.

3.1.6. Adoption and User Acceptance

Farmers may be resistant to change or skeptical about adopting new technologies. Lack of awareness, concerns about technology reliability, and the perceived complexity of smart agriculture solutions can hinder adoption rates [105]-[109]. Demonstrating the tangible benefits, providing training and support, and showcasing successful case studies are crucial to building trust and encouraging widespread adoption.

3.1.7. Data Management and Analysis

Smart agriculture generates large volumes of data, and effectively managing, analyzing, and interpreting this data can be overwhelming [110]-[114]. Farmers need user-friendly data management tools and analytics platforms that can process and present data in a meaningful way, providing actionable insights. Simplified data visualization, user-friendly interfaces, and user training can help farmers effectively utilize the data generated.

3.1.8. Regulatory and Policy Frameworks

As smart agriculture involves the use of new technologies, regulatory frameworks need to keep pace with these advancements. Issues related to data ownership, data sharing, privacy regulations, and standardization should be addressed through appropriate policies [115]-[117]. Governments need to establish clear guidelines and regulations to ensure ethical and responsible use of smart agriculture technologies.

By addressing these challenges, stakeholders can promote the adoption of smart agriculture and leverage its potential to revolutionize the agricultural sector, improve productivity, and achieve sustainable and efficient food production.

3.2. Security issues in smart agriculture

Smart agriculture, like any other technological system, is susceptible to various security issues that need to be addressed to ensure the integrity, confidentiality, and availability of data and operations [118], [119]. Fig. 5 shows the various layers of the smart agriculture environment.

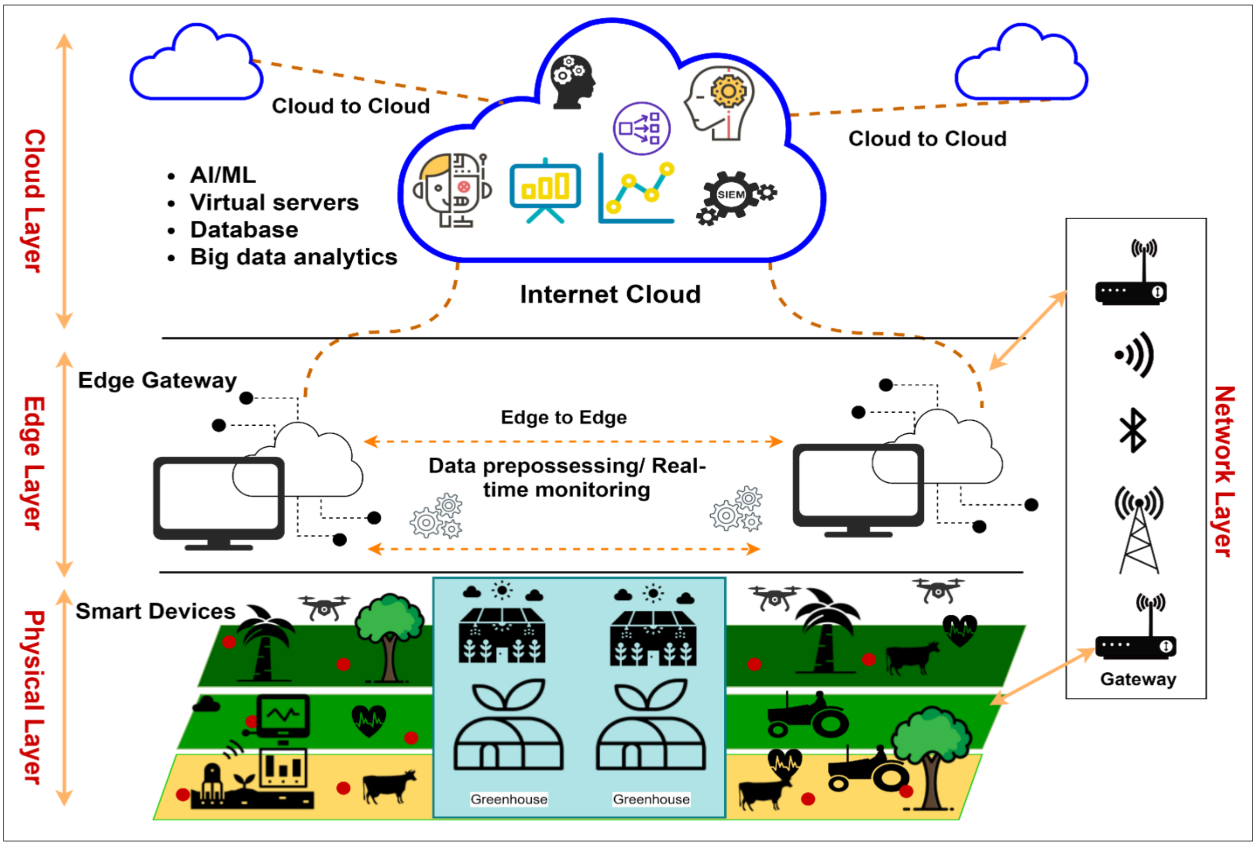

Figure 5 Smart agriculture environment layers

According to [120], some of these security issues specific to smart agriculture include unauthorized access, data privacy and confidentiality, data integrity, network security, device security, physical security, supply chain security, as well as awareness and training. Fig. 6 shows the layered depiction of these smart agriculture security challenges. Unauthorized individuals gaining access to smart agriculture systems can disrupt operations, manipulate data, or even cause physical damage [122]-[123]. It is crucial to implement strong access controls, such as secure authentication mechanisms, to prevent unauthorized access to devices, networks, and data [124]. On the other hand, authors in [125] explain that smart agriculture involves the collection and storage of sensitive data, including farm management information, crop yields, and farmer details. Ensuring data privacy and confidentiality is essential to protect farmers' and consumers' interests. Robust encryption techniques, secure storage, and proper data access controls should be implemented to safeguard sensitive information [126]-[129]. In addition, maintaining the integrity of data is crucial in smart agriculture systems. This is because any unauthorized modification, tampering, or corruption of data can lead to incorrect decisions and impact the overall farming operations. Implementing data validation mechanisms, digital signatures, and secure communication channels can help ensure data integrity [130]-[134]. As explained in [135], smart agriculture systems rely on networks and communication channels for data transmission. These networks are vulnerable to various threats such as eavesdropping, data interception, and denial-of-service (DoS) attacks [136]-[139]. Implementing secure network protocols, firewalls, intrusion detection systems, and regular network monitoring are essential to protect against network-based attacks.

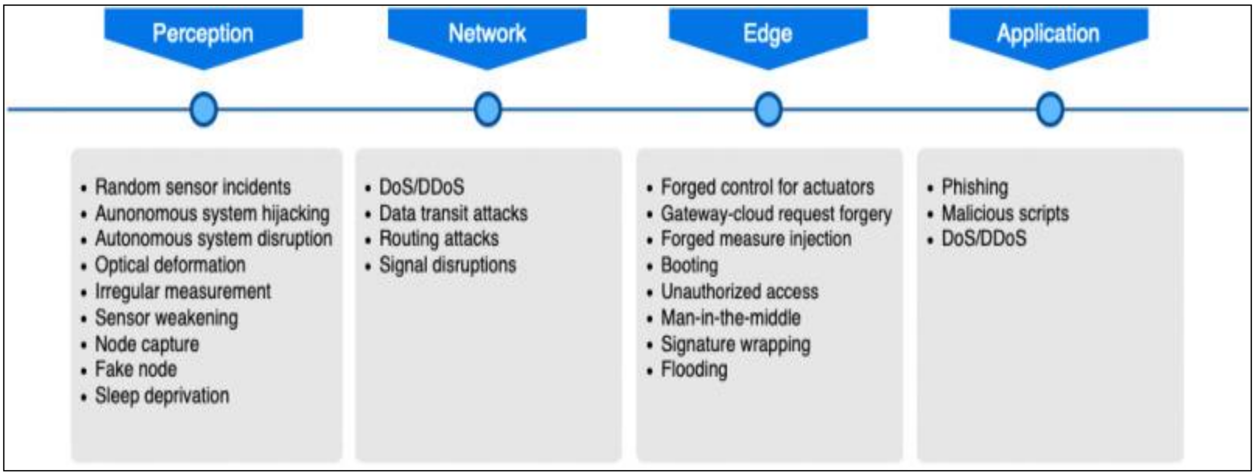

Figure 6 Layered security challenges in smart agriculture

IoT devices, sensors, and actuators play a significant role in smart agriculture [140]-[144]. However, these devices can be potential entry points for attackers. Ensuring the security of these devices through measures like strong authentication, regular firmware updates, and secure configurations is crucial to prevent unauthorized access and compromise of the entire system. Researchers in [145] discuss that smart agriculture systems may include physical infrastructure like weather stations, drones, and robots. Securing these physical assets from theft, vandalism, or physical tampering is vital. Implementing access controls, surveillance systems, and physical barriers can help protect the physical components of smart agriculture. On their part, the authors in [146] argue that smart agriculture systems rely on various vendors and suppliers for hardware, software, and services. Ensuring the security of the entire supply chain is crucial to prevent the introduction of compromised or malicious components [147], [148]. Conducting thorough vendor assessments, implementing secure development practices, and performing regular security audits are important for maintaining a secure supply chain. In addition, human error and lack of awareness can contribute to security vulnerabilities [149]. Farmers and operators should receive proper training and awareness programs to understand security best practices, identify potential threats, and respond to security incidents promptly.

Addressing these security issues requires a multi-layered approach that combines technical controls, policies, training, and regular security assessments. Collaboration between farmers, technology providers, and cybersecurity experts is crucial to identify and mitigate security risks, ensuring the safe and secure implementation of smart agriculture systems.

4. Ways of securing smart agriculture

Securing smart agriculture systems involves implementing various techniques and best practices to protect data, devices, and infrastructure. Table 2 describes some techniques for securing smart agriculture.

Table 2 Techniques for securing smart agriculture

Technique	**Description**
Strong Authentication and Access Controls	Implement robust authentication mechanisms, such as multi-factor authentication, to ensure that only authorized individuals can access the smart agriculture system [150]-[154]. Additionally, enforce strict access controls to limit privileges and restrict access to sensitive data and critical functionalities.
Regular Patching and Updates	Keep all software, firmware, and operating systems up to date with the latest security patches [155]-[158]. Regularly update IoT devices, sensors, and other components to address any known vulnerabilities [159] and ensure that they are running on the most secure versions.

Network Segmentation	Segment the smart agriculture network into different zones or subnets to separate critical components, such as IoT devices, sensors, and data storage systems [160]-[163]. This helps contain security breaches and limits unauthorized access to sensitive areas of the network.
Secure Communication Channels	Use secure protocols and encryption techniques (e.g., SSL/TLS) to ensure the confidentiality and integrity of data transmitted between devices, sensors, and the central system [164]-[168]. Secure communication channels prevent eavesdropping, data interception, and tampering during data transmission.
Physical Security Measures	Secure physical components of smart agriculture systems, including weather stations, drones, and robots, to prevent theft, tampering, or unauthorized access [169]. Implement physical barriers, surveillance systems, and access controls to protect physical assets [170]-[173].
Employee Training and Awareness	Provide comprehensive training programs to farmers, operators, and other stakeholders to raise awareness about security best practices, social engineering threats, and safe handling of data and devices. Educate users about potential risks and how to identify and report security incidents [174].
Security Monitoring and Incident Response	Implement robust monitoring tools and techniques to continuously monitor the smart agriculture system for potential security incidents [175]. Establish an incident response plan to handle security breaches, including procedures for investigation, containment, eradication, and recovery [176]-[178].
Intrusion Detection and Prevention Systems	Deploy intrusion detection and prevention systems (IDPS) to monitor network traffic, detect suspicious activities, and prevent potential attacks [179], [180]. IDPS can identify and respond to malicious behavior, such as unauthorized access [181] attempts or abnormal data patterns.
Data Encryption and Privacy	Implement strong encryption algorithms to protect sensitive data both at rest and in transit. Encrypt data stored on devices, databases, and cloud storage to prevent unauthorized access [182]-[186]. Also, ensure compliance with privacy regulations and establish clear policies on data handling and sharing.
Regular Security Assessments	Conduct regular security assessments, penetration testing, and vulnerability scanning to identify and address any potential weaknesses in the smart agriculture system [187]-[191]. Regular assessments help ensure that security measures are up to date and effective in protecting against emerging threats.

By implementing these techniques, smart agriculture systems can significantly enhance their security posture and protect against potential threats, ensuring the integrity, confidentiality, and availability of data and operations.

5. Issues with current smart agriculture protection techniques

There are several protection techniques available for securing smart agriculture systems. However, there are still some issues and challenges associated with their implementation. The following sub-sections discuss some common issues with current smart agriculture protection techniques.

5.1 Lack of Standardization

The smart agriculture industry lacks standardized security protocols and frameworks, making it challenging to ensure consistent and interoperable security measures across different systems and devices [192], [193]. The absence of widely accepted standards hinders seamless integration and can lead to compatibility issues when implementing security solutions.

5.2 Limited Security Awareness and Expertise

Many farmers and agricultural professionals may have limited knowledge and awareness of cybersecurity risks and best practices. The lack of security expertise among end-users can result in improper implementation of security measures, such as weak passwords, misconfigurations, or failure to update software/firmware promptly [194], [195].

5.3 Vulnerabilities in IoT Devices

IoT devices used in smart agriculture systems may have inherent security vulnerabilities [196]. These vulnerabilities can be exploited by attackers to gain unauthorized access, manipulate data, or disrupt operations [196]-[199]. The rapid proliferation of IoT devices and their diverse manufacturers make it challenging to ensure consistent security standards across all devices.

5.4 Complexity and Cost

Implementing comprehensive security measures can be complex and expensive for farmers, particularly small-scale operations with limited budgets. The costs associated with purchasing, deploying, and maintaining security solutions can be prohibitive, deterring widespread adoption of robust security measures [200], [201].

5.5 Legacy Systems and Infrastructure

Many agricultural systems still rely on legacy equipment and infrastructure that may not have built-in security features or support modern security protocols [202], [203]. Integrating security solutions with existing legacy systems can be challenging and may require additional investments in upgrading or replacing outdated components [204].

5.6 Lack of Security Updates and Support

Some smart agriculture solutions may lack regular security updates and ongoing support from vendors [205]-[207]. This can leave systems vulnerable to emerging threats, as security patches and updates are essential for addressing newly discovered vulnerabilities and ensuring the long-term security of the system.

5.7 Physical Security Risks

While digital security is crucial, physical security risks in smart agriculture systems cannot be overlooked [209], [210]. Components such as sensors, drones, or weather stations are vulnerable to physical tampering, theft, or damage. Ensuring adequate physical security measures, such as access controls and surveillance, is essential but can be challenging in remote or expansive farming environments.

5.8 Integration and Compatibility Challenges

Smart agriculture systems often involve the integration of various technologies, platforms, and third-party solutions. Ensuring seamless integration and compatibility between different components can be complex, as they may have different security requirements, protocols, or interfaces [211]-[214]. Incompatibility issues can create security gaps and increase the risk of vulnerabilities.

Addressing these issues requires collaborative efforts between technology providers, agricultural stakeholders, and policymakers. It involves promoting security standards and best practices, providing security training and awareness programs, encouraging security-by-design principles in IoT device manufacturing, and fostering partnerships to develop cost-effective security solutions tailored for the agricultural sector [215]-[219].

6. Future research scope

Based on the shortcomings of the current smart agriculture defense mechanisms, future research can explore several areas to enhance the protection of agricultural systems and address emerging challenges. Some potential research scopes include the following:

6.1 Threat Modeling and Risk Assessment

There is need to develop advanced threat modeling techniques specific to smart agriculture systems to identify potential vulnerabilities and attack vectors [220]-[225]. Conduct comprehensive risk assessments to understand the potential impact of security breaches and prioritize security measures accordingly.

6.2 Blockchain Technology

Investigate the applicability of blockchain technology in smart agriculture security. Explore how blockchain can enhance data integrity, traceability, and secure transactions in supply chains, ensuring transparency and trustworthiness in agricultural operations [226]-[231].

6.3 Secure Data Analytics

Develop secure and privacy-preserving data analytics techniques for smart agriculture [232]-[235]. Explore methods for secure aggregation, processing, and analysis of sensitive agricultural data while maintaining confidentiality and protecting against data leaks.

6.4 Intrusion Detection Systems for Agricultural Networks

Design and develop intrusion detection systems (IDS) specifically tailored for agricultural networks [236]-[239]. Create IDS algorithms and models capable of detecting and mitigating attacks targeting IoT devices, sensor networks, and communication channels in smart agriculture systems.

6.5 Machine Learning for Anomaly Detection

Explore the application of machine learning algorithms [240] for anomaly detection in smart agriculture systems. Develop intelligent models capable of detecting unusual patterns, behaviors, or deviations in sensor data, signaling potential security breaches or attacks [241]-[245].

6.6 Security-aware IoT Device Design

Investigate methods for designing and manufacturing IoT devices with built-in security features [246]-[248]. Develop secure firmware, authentication mechanisms, and communication protocols for IoT devices used in smart agriculture, ensuring resilience against common attack vectors [249], [250].

6.7 Security Information and Event Management (SIEM) for Agriculture

Adapt existing SIEM techniques to address the specific requirements and challenges of smart agriculture systems [251]-[253]. Design SIEM architectures capable of handling the large volume of heterogeneous data generated by agricultural sensors, devices, and networks.

6.8 Secure Communication Protocols

Develop and evaluate secure communication protocols [254] tailored for smart agriculture systems. Investigate lightweight and energy-efficient protocols suitable for resource-constrained IoT devices, ensuring secure and reliable communication in remote agricultural environments [255]-[259].

6.9 Privacy and Data Protection

Research privacy-preserving techniques for smart agriculture data, ensuring that personally identifiable information and sensitive farm data are protected [260]-[263]. Explore anonymization, differential privacy, and encryption techniques to balance data utility [264] with privacy requirements.

6.10 Security-aware Farm Management Systems

Investigate the integration of security features into farm management systems. Develop intelligent decision support systems that consider security risks and constraints while optimizing farming operations, resource allocation, and risk management [265], [266].

6.11 Social and Ethical Considerations

Study the social, ethical, and legal implications of smart agriculture security [267]. Investigate the impact of security breaches on farmers, consumers, and the environment [268]. Address ethical concerns related to data ownership, privacy, and responsible use of technology in agriculture.

These research scopes aim to advance the field of smart agriculture security, addressing the evolving security challenges and developing innovative solutions to protect agricultural systems, data, and stakeholders.

7 Conclusion

Security issues in smart agriculture pose significant challenges that need to be addressed to ensure the integrity, confidentiality, and availability of data and operations. The protection of smart agriculture systems is crucial to prevent unauthorized access, data breaches, tampering, and disruption of farming operations. This paper has highlighted several factors that contribute to the complexity and vulnerability of these systems. For example, lack of standardized security protocols and frameworks, limited security awareness and expertise among farmers, and vulnerabilities in IoT devices have been shown to be major concerns. Additionally, the complexity and cost associated with implementing comprehensive security measures, legacy systems and infrastructure, and the need for regular security updates and support pose additional challenges. Physical security risks and integration and compatibility issues further compound the security landscape of smart agriculture. To overcome these challenges, future research and development efforts should focus on threat modeling, risk assessment, blockchain technology, secure data analytics, intrusion detection systems, machine learning for anomaly detection, security-aware IoT device design, secure communication protocols, SIEM for agriculture, privacy and data protection, security-aware farm management systems, and social and ethical considerations. It has been shown that addressing security issues in smart agriculture requires collaborative efforts between technology providers, agricultural stakeholders, researchers, and policymakers. It is crucial to develop and implement robust security measures, promote security standards and best practices, provide security training and awareness programs, and foster partnerships to develop cost-effective security solutions tailored for the agricultural sector. By addressing these security issues comprehensively, we can ensure the trustworthiness, resilience, and sustainability of smart agriculture systems, thereby unlocking their full potential to revolutionize the agricultural industry, improve productivity, and contribute to global food security.

Compliance with ethical standards

Acknowledgments

All the efforts and help offered to me by my colleagues when I was developing this manuscript are highly appreciated.

References

[1] Shaikh TA, Rasool T, Lone FR. Towards leveraging the role of machine learning and artificial intelligence in precision agriculture and smart farming. Computers and Electronics in Agriculture. 2022 Jul 1;198:107119.

[2] Kwaghtyo DK, Eke CI. Smart farming prediction models for precision agriculture: a comprehensive survey. Artificial Intelligence Review. 2023 Jun;56(6):5729-72.

[3] Boursianis AD, Papadopoulou MS, Diamantoulakis P, Liopa-Tsakalidi A, Barouchas P, Salahas G, Karagiannidis G, Wan S, Goudos SK. Internet of things (IoT) and agricultural unmanned aerial vehicles (UAVs) in smart farming: a comprehensive review. Internet of Things. 2022 May 1;18:100187.

[4] Javaid M, Haleem A, Singh RP, Suman R. Enhancing smart farming through the applications of Agriculture 4.0 technologies. International Journal of Intelligent Networks. 2022 Jan 1;3:150-64.

[5] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[6] Bacco M, Barsocchi P, Ferro E, Gotta A, Ruggeri M. The digitisation of agriculture: a survey of research activities on smart farming. Array. 2019 Sep 1;3:100009.

[7] Wolfert S, Ge L, Verdouw C, Bogaardt MJ. Big data in smart farming–a review. Agricultural systems. 2017 May 1;153:69-80.

[8] Bucci G, Bentivoglio D, Finco A. Precision agriculture as a driver for sustainable farming systems: state of art in litterature and research. Calitatea. 2018 Mar 1;19(S1):114-21.

[9] Encinas C, Ruiz E, Cortez J, Espinoza A. Design and implementation of a distributed IoT system for the monitoring of water quality in aquaculture. In2017 Wireless telecommunications symposium (WTS) 2017 Apr 26 (pp. 1-7). IEEE.

[10] Ting L, Khan M, Sharma A, Ansari MD. A secure framework for IoT-based smart climate agriculture system: Toward blockchain and edge computing. Journal of Intelligent Systems. 2022 Jan 1;31(1):221-36.

[11] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[12] Akkem Y, Biswas SK, Varanasi A. Smart farming using artificial intelligence: A review. Engineering Applications of Artificial Intelligence. 2023 Apr 1;120:105899.

[13] Williams MJ, Sikder MN, Wang P, Gorentala N, Gurrapu S, Batarseh FA. The application of artificial intelligence assurance in precision farming and agricultural economics. InAI Assurance 2023 Jan 1 (pp. 501-529). Academic Press.

[14] Foster L, Szilagyi K, Wairegi A, Oguamanam C, de Beer J. Smart farming and artificial intelligence in East Africa: Addressing indigeneity, plants, and gender. Smart Agricultural Technology. 2023 Feb 1;3:100132.

[15] Thorat T, Patle BK, Kashyap SK. Intelligent insecticide and fertilizer recommendation system based on TPF-CNN for smart farming. Smart Agricultural Technology. 2023 Feb 1;3:100114.

[16] Ghrabat MJ, Hussien ZA, Khalefa MS, Abduljabba ZA, Nyangaresi VO, Al Sibahee MA, Abood EW. Fully automated model on breast cancer classification using deep learning classifiers. Indonesian Journal of Electrical Engineering and Computer Science. 2022 Oct;28(1):183-91.

[17] Prajapati JB, Barad R, Patel MB, Saini K, Prajapati D, Engineer P. Smart Farming Ingredients: IoT Sensors, Software, Connectivity, Data Analytics, Robots, Drones, GIS-GPS. InApplying Drone Technologies and Robotics for Agricultural Sustainability 2023 (pp. 31-49). IGI Global.

[18] Pal D, Joshi S. AI, IoT and Robotics in Smart Farming: Current Applications and Future Potentials. In2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS) 2023 Mar 23 (pp. 1096-1101). IEEE.

[19] Güven B, Baz İ, Kocaoğlu B, Toprak E, Erol Barkana D, Soğutmaz Özdemir B. Smart Farming Technologies for Sustainable Agriculture: From Food to Energy. InA Sustainable Green Future 2023 (pp. 481-506). Springer, Cham.

[20] Sajid J, Hayawi K, Malik AW, Anwar Z, Trabelsi Z. A Fog Computing Framework for Intrusion Detection of Energy-Based Attacks on UAV-Assisted Smart Farming. Applied Sciences. 2023 Mar 17;13(6):3857.

[21] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[22] Priya PL, Harshith NS, Ramesh NV. Smart agriculture monitoring system using IoT. Int. J. Eng. Technol.(UAE). 2018;7:308-11.

[23] Kapoor P, Barbhuiya FA. Cloud based weather station using IoT devices. InTENCON 2019-2019 IEEE Region 10 Conference (TENCON) 2019 Oct 17 (pp. 2357-2362). IEEE.

[24] Wang Y, Zhang X, Ning W, Lazzara MA, Ding M, Reijmer CH, Smeets PC, Grigioni P, Heil P, Thomas ER, Mikolajczyk D. The AntAWS dataset: a compilation of Antarctic automatic weather station observations. Earth System Science Data. 2023 Jan 24;15(1):411-29.

[25] Muñoz LE, Campozano LV, Guevara DC, Parra R, Tonato D, Suntaxi A, Maisincho L, Páez C, Villacís M, Córdova J, Valencia N. Comparison of Radiosonde Measurements of Meteorological Variables with Drone, Satellite Products, and WRF Simulations in the Tropical Andes: The Case of Quito, Ecuador. Atmosphere. 2023 Jan 28;14(2):264.

[26] Li ZL, Wu H, Duan SB, Zhao W, Ren H, Liu X, Leng P, Tang R, Ye X, Zhu J, Sun Y. Satellite remote sensing of global land surface temperature: definition, methods, products, and applications. Reviews of Geophysics. 2023 Mar;61(1):e2022RG000777.

[27] Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Khalefa MS, Honi DG. MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. InFuture Access Enablers for Ubiquitous and Intelligent Infrastructures: 6th EAI International Conference, FABULOUS 2022, Virtual Event, May 4, 2022, Proceedings 2022 Sep 18 (pp. 16-36). Cham: Springer International Publishing.

[28] Siddiqui MS, Aslam M. Highly Stable and Reusable 3D Graphene-Quinizarin Voltammetric pH Sensor. Journal of The Electrochemical Society. 2023 Apr 24;170(4):047511.

[29] Belgiu M, Marshall M, Boschetti M, Pepe M, Stein A, Nelson A. PRISMA and Sentinel-2 spectral response to the nutrient composition of grains. Remote Sensing of Environment. 2023 Jul 1;292:113567.

[30] He J, Chen K, Pan X, Zhai J, Lin X. Advanced biosensing technologies for monitoring of agriculture pests and diseases: A review. Journal of Semiconductors. 2023 Feb 1;44(2):023104.

[31] Schipper R, Van der Meer M, De Visser PH, Heuvelink E, Marcelis LF. Consequences of intra-canopy and top LED lighting for uniformity of light distribution in a tomato crop. Frontiers in plant science. 2023;14.

[32] Mancuso D, Castagnolo G, Porto SM. Cow Behavioural Activities in Extensive Farms: Challenges of Adopting Automatic Monitoring Systems. Sensors. 2023 Apr 8;23(8):3828.

[33] Nyangaresi VO, Ogundoyin SO. Certificate based authentication scheme for smart homes. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[34] Jamroen C, Yonsiri N, Odthon T, Wisitthiwong N, Janreung S. A standalone photovoltaic/battery energy-powered water quality monitoring system based on narrowband internet of things for aquaculture: Design and implementation. Smart Agricultural Technology. 2023 Feb 1;3:100072.

[35] Wu Y, Li J, Lv M, Zhang X, Gao R, Guo C, Cheng X, Zhou X, Xu Y, Gao S, Major Z. Selective detection of trace carbon monoxide at room temperature based on CuO nanosheets exposed to (111) crystal facets. Journal of Hazardous Materials. 2023 Jan 15;442:130041.

[36] Guo Q, Wang C, Xiao D, Huang Q. Automatic monitoring of flying vegetable insect pests using an RGB camera and YOLO-SIP detector. Precision Agriculture. 2023 Apr;24(2):436-57.

[37] Race D, Gentle P, Mathew S. Living on the margins: Climate change impacts and adaptation by remote communities living in the Pacific Islands, the Himalaya and desert Australia. Climate Risk Management. 2023 Jan 1;40:100503.

[38] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[39] Thakur N, Nigam M, Mann NA, Gupta S, Hussain CM, Shukla SK, Shah AA, Casini R, Elansary HO, Khan SA. Host-mediated gene engineering and microbiome-based technology optimization for sustainable agriculture and environment. Functional & Integrative Genomics. 2023 Mar;23(1):57.

[40] Linaza MT, Posada J, Bund J, Eisert P, Quartulli M, Döllner J, Pagani A, G. Olaizola I, Barriguinha A, Moysiadis T, Lucat L. Data-driven artificial intelligence applications for sustainable precision agriculture. Agronomy. 2021 Jun 17;11(6):1227.

[41] Botta A, Cavallone P, Baglieri L, Colucci G, Tagliavini L, Quaglia G. A review of robots, perception, and tasks in precision agriculture. Applied Mechanics. 2022 Jul 5;3(3):830-54.

[42] Sparrow R, Howard M. Robots in agriculture: prospects, impacts, ethics, and policy. precision agriculture. 2021 Jun;22:818-33.

[43] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan 25;4(1):10-9.

[44] Adamides G, Kalatzis N, Stylianou A, Marianos N, Chatzipapadopoulos F, Giannakopoulou M, Papadavid G, Vassiliou V, Neocleous D. Smart farming techniques for climate change adaptation in Cyprus. Atmosphere. 2020 May 27;11(6):557.

[45] Mohamed ES, Belal AA, Abd-Elmabod SK, El-Shirbeny MA, Gad A, Zahran MB. Smart farming for improving agricultural management. The Egyptian Journal of Remote Sensing and Space Science. 2021 Dec 1;24(3):971-81.

[46] Zhang A, Mankad A, Ariyawardana A. Establishing confidence in food safety: is traceability a solution in consumers' eyes?. Journal of Consumer Protection and Food Safety. 2020 Jun;15(2):99-107.

[47] Mesías FJ, Martín A, Hernández A. Consumers' growing appetite for natural foods: Perceptions towards the use of natural preservatives in fresh fruit. Food Research International. 2021 Dec 1;150:110749.

[48] Omollo VN, Musyoki S. Global Positioning System Based Routing Algorithm for Adaptive Delay Tolerant Mobile Adhoc Networks. International Journal of Computer and Communication System Engineering. 2015 May 11; 2(3): 399-406.

[49] Goel RK, Yadav CS, Vishnoi S, Rastogi R. Smart agriculture–Urgent need of the day in developing countries. Sustainable Computing: Informatics and Systems. 2021 Jun 1;30:100512.

[50] Huuskonen J, Oksanen T. Soil sampling with drones and augmented reality in precision agriculture. Computers and electronics in agriculture. 2018 Nov 1;154:25-35.

[51] Atitallah SB, Driss M, Boulila W, Ghézala HB. Leveraging Deep Learning and IoT big data analytics to support the smart cities development: Review and future directions. Computer Science Review. 2020 Nov 1;38:100303.

[52] Saiz-Rubio V, Rovira-Más F. From smart farming towards agriculture 5.0: A review on crop data management. Agronomy. 2020 Feb 3;10(2):207.

[53] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[54] Paul K, Chatterjee SS, Pai P, Varshney A, Juikar S, Prasad V, Bhadra B, Dasgupta S. Viable smart sensors and their application in data driven agriculture. Computers and Electronics in Agriculture. 2022 Jul 1;198:107096.

[55] van Etten J, de Sousa K, Cairns JE, Dell'Acqua M, Fadda C, Guereña D, Heerwaarden JV, Assefa T, Manners R, Müller A, Enrico Pè M. Data-driven approaches can harness crop diversity to address heterogeneous needs for breeding products. Proceedings of the National Academy of Sciences. 2023 Apr 4;120(14):e2205771120.

[56] Tripathy PK, Tripathy AK, Agarwal A, Mohanty SP. MyGreen: An IoT-enabled smart greenhouse for sustainable agriculture. IEEE Consumer Electronics Magazine. 2021 Feb 1;10(4):57-62.

[57] Ray PP. Internet of things for smart agriculture: Technologies, practices and future direction. Journal of Ambient Intelligence and Smart Environments. 2017 Jan 1;9(4):395-420.

[58] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan;13(2):691.

[59] Raja L, Vyas S. The study of technological development in the field of smart farming. InSmart Farming Technologies for Sustainable Agricultural Development 2019 (pp. 1-24). IGI Global.

[60] Easterday K, Kislik C, Dawson TE, Hogan S, Kelly M. Remotely sensed water limitation in vegetation: Insights from an experiment with unmanned aerial vehicles (UAVs). Remote Sensing. 2019 Aug 9;11(16):1853.

[61] Singh P, Pandey PC, Petropoulos GP, Pavlides A, Srivastava PK, Koutsias N, Deng KA, Bao Y. Hyperspectral remote sensing in precision agriculture: Present status, challenges, and future trends. InHyperspectral remote sensing 2020 Jan 1 (pp. 121-146). Elsevier.

[62] Yang G, Liu J, Zhao C, Li Z, Huang Y, Yu H, Xu B, Yang X, Zhu D, Zhang X, Zhang R. Unmanned aerial vehicle remote sensing for field-based crop phenotyping: current status and perspectives. Frontiers in plant science. 2017 Jun 30;8:1111.

[63] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[64] Chergui N, Kechadi MT. Data analytics for crop management: a big data view. Journal of Big Data. 2022 Dec;9(1):1-37.

[65] Saggi MK, Jain S. A survey towards an integration of big data analytics to big insights for value-creation. Information Processing & Management. 2018 Sep 1;54(5):758-90.

[66] Van Evert FK, Fountas S, Jakovetic D, Crnojevic V, Travlos I, Kempenaar C. Big data for weed control and crop protection. Weed Research. 2017 Aug;57(4):218-33.

[67] Kamilaris A, Kartakoullis A, Prenafeta-Boldú FX. A review on the practice of big data analysis in agriculture. Computers and Electronics in Agriculture. 2017 Dec 1;143:23-37.

[68] Honi DG, Ali AH, Abduljabbar ZA, Ma J, Nyangaresi VO, Mutlaq KA, Umran SM. Towards Fast Edge Detection Approach for Industrial Products. In2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS) 2022 Dec 19 (pp. 239-244). IEEE.

[69] Arumugam K, Swathi Y, Sanchez DT, Mustafa M, Phoemchalard C, Phasinam K, Okoronkwo E. Towards applicability of machine learning techniques in agriculture and energy sector. Materials Today: Proceedings. 2022 Jan 1;51:2260-3.

[70] Jerhamre E, Carlberg CJ, van Zoest V. Exploring the susceptibility of smart farming: Identified opportunities and challenges. Smart Agricultural Technology. 2022 Dec 1;2:100026.

[71] Nabi F, Jamwal S, Padmanbh K. Wireless sensor network in precision farming for forecasting and monitoring of apple disease: a survey. International Journal of Information Technology. 2022 Mar;14(2):769-80.

[72] Fountas S, Espejo-Garcia B, Kasimati A, Mylonas N, Darra N. The future of digital agriculture: technologies and opportunities. IT professional. 2020 Feb 11;22(1):24-8.

[73] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[74] Maddikunta PK, Hakak S, Alazab M, Bhattacharya S, Gadekallu TR, Khan WZ, Pham QV. Unmanned aerial vehicles in smart agriculture: Applications, requirements, and challenges. IEEE Sensors Journal. 2021 Jan 6;21(16):17608-19.

[75] Roldán JJ, del Cerro J, Garzón-Ramos D, Garcia-Aunon P, Garzón M, De León J, Barrientos A. Robots in agriculture: State of art and practical experiences. Service robots. 2018 Jan 4:67-90.

[76] Aslan MF, Durdu A, Sabanci K, Ropelewska E, Gültekin SS. A comprehensive survey of the recent studies with UAV for precision agriculture in open fields and greenhouses. Applied Sciences. 2022 Jan 20;12(3):1047.

[77] Sanjeevi P, Prasanna S, Siva Kumar B, Gunasekaran G, Alagiri I, Vijay Anand R. Precision agriculture and farming using Internet of Things based on wireless sensor network. Transactions on Emerging Telecommunications Technologies. 2020 Dec;31(12):e3978.

[78] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[79] Emmi L, Fernández R, Gonzalez-de-Santos P, Francia M, Golfarelli M, Vitali G, Sandmann H, Hustedt M, Wollweber M. Exploiting the Internet Resources for Autonomous Robots in Agriculture. Agriculture. 2023 May 2;13(5):1005.

[80] Motalo K, Nojeem L, Ewani J, Opuiyo A, Browndi I. Algebraic Multigrid and Cloud Computing: Enhancing Scalability and Performance. International Journal of Technology and Scientific Research. 2023 Mar;12:342-8.

[81] Saban M, Bekkour M, Amdaouch I, El Gueri J, Ait Ahmed B, Chaari MZ, Ruiz-Alzola J, Rosado-Muñoz A, Aghzout O. A Smart Agricultural System Based on PLC and a Cloud Computing Web Application Using LoRa and LoRaWan. Sensors. 2023 Mar 2;23(5):2725.

[82] Hazra A, Rana P, Adhikari M, Amgoth T. Fog computing for next-generation internet of things: fundamental, state-of-the-art and research challenges. Computer Science Review. 2023 May 1;48:100549.

[83] Nyangaresi VO, Abood EW, Abduljabbar ZA, Al Sibahe MA. Energy Efficient WSN Sink-Cloud Server Authentication Protocol. In2021 5th International Conference on Information Systems and Computer Networks (ISCON) 2021 Oct 22 (pp. 1-6).

[84] Mehta CR, Chandel NS, Dubey K. Smart Agricultural Mechanization in India—Status and Way Forward. InSmart Agriculture for Developing Nations: Status, Perspectives and Challenges 2023 Mar 9 (pp. 1-14). Singapore: Springer Nature Singapore.

[85] Mesías-Ruiz GA, Pérez-Ortiz M, Dorado J, de Castro AI, Peña JM. Boosting precision crop protection towards agriculture 5.0 via machine learning and emerging technologies: A contextual review. Frontiers in Plant Science. 2023;14.

[86] Dutta PK, Mitra S. Application of agricultural drones and IoT to understand food supply chain during post COVID-19. Agricultural Informatics: Automation Using the IoT and Machine Learning. 2021 Mar 19:67-87.

[87] Wajs J, Trybała P, Górniak-Zimroz J, Krupa-Kurzynowska J, Kasza D. Modern solution for fast and accurate inventorization of open-pit mines by the active remote sensing technique—case study of mikoszów granite mine (lower silesia, sw poland). Energies. 2021 Oct 19;14(20):6853.

[88] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19;11(3):55.

[89] Ouafiq EM, Saadane R, Chehri A. Data Management and Integration of Low Power Consumption Embedded Devices IoT for Transforming Smart Agriculture into Actionable Knowledge. Agriculture. 2022 Feb 24;12(3):329.

[90] Lin J, Shen Z, Zhang A, Chai Y. Blockchain and IoT based food traceability for smart agriculture. InProceedings of the 3rd international conference on crowd science and engineering 2018 Jul 28 (pp. 1-6).

[91] Ferrández-Pastor FJ, García-Chamizo JM, Nieto-Hidalgo M, Mora-Martínez J. Precision agriculture design method using a distributed computing architecture on internet of things context. Sensors. 2018 May 28;18(6):1731.

[92] Math RK, Dharwadkar NV. IoT Based low-cost weather station and monitoring system for precision agriculture in India. In2018 2nd international conference on I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC) I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC), 2018 2nd international conference on 2018 Aug 30 (pp. 81-86). IEEE.

[93] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[94] Mekala MS, Viswanathan P. A novel technology for smart agriculture based on IoT with cloud computing. In2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) 2017 Feb 10 (pp. 75-82). IEEE.

[95] Islam N, Rashid MM, Pasandideh F, Ray B, Moore S, Kadel R. A review of applications and communication technologies for internet of things (Iot) and unmanned aerial vehicle (uav) based sustainable smart farming. Sustainability. 2021 Feb 8;13(4):1821.

[96] Almalki FA, Soufiene BO, Alsamhi SH, Sakli H. A low-cost platform for environmental smart farming monitoring system based on IoT and UAVs. Sustainability. 2021 May 24;13(11):5908.

[97] Farooq MS, Riaz S, Abid A, Abid K, Naeem MA. A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. Ieee Access. 2019 Oct 25;7:156237-71.

[98] Kalyani Y, Collier R. A systematic survey on the role of cloud, fog, and edge computing combination in smart agriculture. Sensors. 2021 Sep 3;21(17):5922.

[99] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[100] Roussaki I, Doolin K, Skarmeta A, Routis G, Lopez-Morales JA, Claffey E, Mora M, Martinez JA. Building an interoperable space for smart agriculture. Digital Communications and Networks. 2023 Feb 1;9(1):183-93.

[101] Carolan M. Publicising food: big data, precision agriculture, and co-experimental techniques of addition. Sociologia Ruralis. 2017 Apr;57(2):135-54.

[102] Shafi U, Mumtaz R, García-Nieto J, Hassan SA, Zaidi SA, Iqbal N. Precision agriculture techniques and practices: From considerations to applications. Sensors. 2019 Sep 2;19(17):3796.

[103] Rao NH. Big data and climate smart agriculture-status and implications for agricultural research and innovation in India. InProc. Indian Natl. Sci. Acad 2018 Sep 1 (Vol. 84, No. 3, pp. 625-640).

[104] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[105] Long TB, Blok V, Coninx I. Barriers to the adoption and diffusion of technological innovations for climate-smart agriculture in Europe: evidence from the Netherlands, France, Switzerland and Italy. Journal of cleaner production. 2016 Jan 20;112:9-21.

[106] Kernecker M, Knierim A, Wurbs A, Kraus T, Borges F. Experience versus expectation: Farmers' perceptions of smart farming technologies for cropping systems across Europe. Precision Agriculture. 2020 Feb;21:34-50.

[107] Giua C, Materia VC, Camanzi L. Smart farming technologies adoption: Which factors play a role in the digital transition?. Technology in Society. 2022 Feb 1;68:101869.

[108] Annosi MC, Brunetta F, Monti A, Nati F. Is the trend your friend? An analysis of technology 4.0 investment decisions in agricultural SMEs. Computers in Industry. 2019 Aug 1;109:59-71.

[109] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[110] Issad HA, Aoudjit R, Rodrigues JJ. A comprehensive review of Data Mining techniques in smart agriculture. Engineering in Agriculture, Environment and Food. 2019 Oct 1;12(4):511-25.

[111] Rahman MU, Baiardi F, Ricci L. Blockchain smart contract for scalable data sharing in IoT: a case study of smart agriculture. In2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT) 2020 Dec 12 (pp. 1-7). IEEE.

[112] Lee K, Silva BN, Han K. Deep learning entrusted to fog nodes (DLEFN) based smart agriculture. Applied sciences. 2020 Feb 24;10(4):1544.

[113] Pathan M, Patel N, Yagnik H, Shah M. Artificial cognition for applications in smart agriculture: A comprehensive review. Artificial Intelligence in Agriculture. 2020 Jan 1;4:81-95.

[114] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InIoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings 2022 Jul 8 (pp. 3-18). Cham: Springer International Publishing.

[115] Kamilaris A, Gao F, Prenafeta-Boldu FX, Ali MI. Agri-IoT: A semantic framework for Internet of Things-enabled smart farming applications. In2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) 2016 Dec 12 (pp. 442-447). IEEE.

[116] Radoglou-Grammatikis P, Sarigiannidis P, Lagkas T, Moscholios I. A compilation of UAV applications for precision agriculture. Computer Networks. 2020 May 8;172:107148.

[117] Taylor M. Climate-smart agriculture: what is it good for?. The Journal of Peasant Studies. 2018 Jan 2;45(1):89-107.

[118] Kumar R, Bhatia MP. A Systematic review of the security in cloud computing: Data integrity, confidentiality and availability. In2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON) 2020 Oct 2 (pp. 334-337). IEEE.

[119] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[120] Demestichas K, Peppes N, Alexakis T. Survey on security threats in agricultural IoT and smart farming. Sensors. 2020 Nov 12;20(22):6458.

[121] Basharat A, Mohamad MM. Security Challenges and Solutions for Internet of Things based Smart Agriculture: A Review. In2022 4th International Conference on Smart Sensors and Application (ICSSA) 2022 Jul 26 (pp. 102-107). IEEE.

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

[123] de Araujo Zanella AR, da Silva E, Albini LC. Security challenges to smart agriculture: Current state, key issues, and future directions. Array. 2020 Dec 1;8:100048.

[124] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. Journal of Sensor and Actuator Networks. 2022 Dec;11(4):66.

[125] Lopez ID, Grass JF, Figueroa A, Corrales JC. A proposal for a multi-domain data fusion strategy in a climate-smart agriculture context. International Transactions in Operational Research. 2023 Jul;30(4):2049-70.

[126] Kumar PR, Raj PH, Jelciana P. Exploring data security issues and solutions in cloud computing. Procedia Computer Science. 2018 Jan 1;125:691-7.

[127] Mahajan HB, Rashid AS, Junnarkar AA, Uke N, Deshpande SD, Futane PR, Alkhayyat A, Alhayani B. Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. Applied Nanoscience. 2022 Feb 4:1-4.

[128] Achar S. Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape. International Journal of Computer and Systems Engineering. 2022 Sep 13;16(9):379-84.

[129] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[130] Li X, Wei L, Wang L, Ma Y, Zhang C, Sohail M. A blockchain-based privacy-preserving authentication system for ensuring multimedia content integrity. International Journal of Intelligent Systems. 2022 May;37(5):3050-71.

[131] Gupta DS, Karati A, Saad W, da Costa DB. Quantum-defended blockchain-assisted data authentication protocol for internet of vehicles. IEEE Transactions on Vehicular Technology. 2022 Jan 25;71(3):3255-66.

[132] Das S, Namasudra S. A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure. Computers and Electrical Engineering. 2022 Jul 1;101:107991.

[133] Chen CL, Yang J, Tsaur WJ, Weng W, Wu CM, Wei X. Enterprise data sharing with privacy-preserved based on hyperledger fabric blockchain in IIOT's application. Sensors. 2022 Feb 2;22(3):1146.

[134] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11;10:26257-70.

[135] Dhruva AD, Prasad B, Kamepalli S, Kunisetti S. An efficient mechanism using IoT and wireless communication for smart farming. Materials Today: Proceedings. 2023 Jan 1;80:3691-6.

[136] Sontowski S, Gupta M, Chukkapalli SS, Abdelsalam M, Mittal S, Joshi A, Sandhu R. Cyber attacks on smart farming infrastructure. In2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC) 2020 Dec 1 (pp. 135-143). IEEE.

[137] Alahari HP, Yelavarthi SB. Performance analysis of denial of service dos and distributed dos attack of application and network layer of iot. In2019 Third International Conference on Inventive Systems and Control (ICISC) 2019 Jan 10 (pp. 72-81). IEEE.

[138] Al-issa AI, Al-Akhras M, ALsahli MS, Alawairdhi M. Using machine learning to detect DoS attacks in wireless sensor networks. In2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT) 2019 Apr 9 (pp. 107-112). IEEE.

[139] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[140] Prathibha SR, Hongal A, Jyothi MP. IoT based monitoring system in smart agriculture. In2017 international conference on recent advances in electronics and communication technology (ICRAECT) 2017 Mar 16 (pp. 81-84). IEEE.

[141] Gupta B, Madan G, Md AQ. A smart agriculture framework for IoT based plant decay detection using smart croft algorithm. Materials Today: Proceedings. 2022 Jan 1;62:4758-63.

[142] Jaiswal SP, Bhadoria VS, Agrawal A, Ahuja H. Internet of Things (IoT) for smart agriculture and farming in developing nations. International Journal of Scientific & Technology Research. 2019;8(12):1049-56.

[143] Lakhwani K, Gianey H, Agarwal N, Gupta S. Development of IoT for smart agriculture a review. InEmerging Trends in Expert Applications and Security: Proceedings of ICETEAS 2018 2019 (pp. 425-432). Springer Singapore.

[144] Nyakomitta PS, Nyangaresi VO, Ogara SO. Efficient authentication algorithm for secure remote access in wireless sensor networks. Journal of Computer Science Research. 2021 Aug;3(4):43-50.

[145] Charania I, Li X. Smart farming: Agriculture's shift from a labor intensive to technology native industry. Internet of Things. 2020 Mar 1;9:100142.

[146] McFadden J, Njuki E, Griffin T. Precision Agriculture in the Digital Era: Recent Adoption on US Farms.

[147] Rünzel MA, Hassler EE, Rogers RE, Formato G, Cazier JA. Designing a smart honey supply chain for sustainable development. IEEE Consumer Electronics Magazine. 2021 Feb 17;10(4):69-78.

[148] Musa SF, Basir KH. Smart farming: towards a sustainable agri-food system. British Food Journal. 2021 Aug 13;123(9):3085-99.

[149] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[150] Ahmad MO, Tripathi G, Siddiqui F, Alam MA, Ahad MA, Akhtar MM, Casalino G. BAuth-ZKP—A Blockchain-Based Multi-Factor Authentication Mechanism for Securing Smart Cities. Sensors. 2023 Mar 2;23(5):2757.

[151] Otta SP, Panda S, Gupta M, Hota C. A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure. Future Internet. 2023 Apr 10;15(4):146.

[152] Carrillo-Torres D, Pérez-Díaz JA, Cantoral-Ceballos JA, Vargas-Rosales C. A Novel Multi-Factor Authentication Algorithm Based on Image Recognition and User Established Relations. Applied Sciences. 2023 Jan 20;13(3):1374.

[153] Marasco E, Albanese M, Patibandla VV, Vurity A, Sriram SS. Biometric multi-factor authentication: On the usability of the FingerPIN scheme. Security and Privacy. 2023 Jan;6(1):e261.

[154] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1;11(1):185-94.

[155] Bauwens J, Ruckebusch P, Giannoulis S, Moerman I, De Poorter E. Over-the-air software updates in the internet of things: An overview of key principles. IEEE Communications Magazine. 2020 Feb 14;58(2):35-41.

[156] Hu JW, Yeh LY, Liao SW, Yang CS. Autonomous and malware-proof blockchain-based firmware update platform with efficient batch verification for Internet of Things devices. Computers & Security. 2019 Sep 1;86:238-52.

[157] Ruge J, Classen J, Gringoli F, Hollick M. Frankenstein: Advanced wireless fuzzing to exploit new bluetooth escalation targets. InProceedings of the 29th USENIX Conference on Security Symposium 2020 Aug 12 (pp. 19-36).

[158] Mantz D, Classen J, Schulz M, Hollick M. InternalBlue-Bluetooth binary patching and experimentation framework. InProceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services 2019 Jun 12 (pp. 79-90).

[159] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[160] Sapra L, Mathani A, Bhatnagar G. A thorough Analysis of Blockchain's Potential for Internet of Things Applications in Precision Agricultural Networks. Mathematical Statistician and Engineering Applications. 2022 Sep 28;71(4):4141-59.

[161] Bodkhe U, Tanwar S, Bhattacharya P, Kumar N. Blockchain for precision irrigation: Opportunities and challenges. Transactions on Emerging Telecommunications Technologies. 2022 Oct;33(10):e4059.

[162] Rayes A, Salam S. Internet of things from hype to reality. Cham: Springer International Publishing; 2019.

[163] Mehmood MY, Oad A, Abrar M, Munir HM, Hasan SF, Muqeet HA, Golilarz NA. Edge computing for IoT-enabled smart grid. Security and Communication Networks. 2021 Jul 13;2021:1-6.

[164] Hussain MA, Hussien ZA, Abduljabbar ZA, Ma J, Al Sibahee MA, Hussain SA, Nyangaresi VO, Jiao X. Provably throttling SQLI using an enciphering query and secure matching. Egyptian Informatics Journal. 2022 Dec 1; 23(4):145-62.

[165] Dinculeană D, Cheng X. Vulnerabilities and limitations of MQTT protocol used between IoT devices. Applied Sciences. 2019 Feb 27;9(5):848.

[166] Gupta S, Garg R, Gupta N, Alnumay WS, Ghosh U, Sharma PK. Energy-efficient dynamic homomorphic security scheme for fog computing in IoT networks. Journal of Information Security and Applications. 2021 May 1;58:102768.

[167] Mrabet H, Belguith S, Alhomoud A, Jemai A. A survey of IoT security based on a layered architecture of sensing and data analysis. Sensors. 2020 Jun 28;20(13):3625.

[168] Hatzivasilis G, Soultatos O, Ioannidis S, Verikoukis C, Demetriou G, Tsatsoulis C. Review of security and privacy for the Internet of Medical Things (IoMT). In2019 15th international conference on distributed computing in sensor systems (DCOSS) 2019 May 29 (pp. 457-464). IEEE.

[169] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[170] Salih FI, Abas HB, Azizan A, Daud SM. Enhancement of Physical Security Control for Data Centre and Perimeter in Banking: A Case Study of Central Bank of Sudan (CBOS). Open International Journal of Informatics (OIJI). 2018 Nov 27:67-84.

[171] Silva MA. Security Measures: Physical Security. InStrategic Security Management 2019 Sep 5 (pp. 123-153). CRC Press.

[172] Al-Fedaghi S, Alsumait O. Towards a conceptual foundation for physical security: Case study of an it department. International Journal of Safety and Security Engineering. 2019 Jun 30;9(2):137-56.

[173] Al Zaabi SH, Zamri R, Yassin SW. Developing a Conceptual Model for Integrating FRT in Oil and Gas Company Physical Security: A Comparative Study of Security Models. resmilitaris. 2023 Mar 2;13(2):4528-46.

[174] Alshaikh M, Naseer H, Ahmad A, Maynard SB. Toward sustainable behaviour change: an approach for cyber security education training and awareness.

[175] Sinha BB, Dhanalakshmi R. Recent advancements and challenges of Internet of Things in smart agriculture: A survey. Future Generation Computer Systems. 2022 Jan 1;126:169-84.

[176] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec;39(10):e13126.

[177] Hazrati M, Dara R, Kaur J. On-farm data security: practical recommendations for securing farm data. Front. Sustain. Food Syst. 6: 884187. doi: 10.3389/fsufs. 2022 Jun 21.

[178] Sharma V, Tripathi AK, Mittal H. Technological revolutions in smart farming: Current trends, challenges & future directions. Computers and Electronics in Agriculture. 2022 Aug 13:107217.

[179] Birkinshaw C, Rouka E, Vassilakis VG. Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks. Journal of Network and Computer Applications. 2019 Jun 15;136:71-85.

[180] Thapa S, Mailewa A. The role of intrusion detection/prevention systems in modern computer networks: A review. InConference: Midwest Instruction and Computing Symposium (MICS) 2020 Apr 28 (Vol. 53, pp. 1-14).

[181] Al Sibahee MA, Abdulsada AI, Abduljabbar ZA, Ma J, Nyangaresi VO, Umran SM. Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences. 2021 Jan;11(24):12040.

[182] Saxena UR, Alam T. Role-based access using partial homomorphic encryption for securing cloud data. International Journal of System Assurance Engineering and Management. 2023 Mar 30:1-7.

[183] Abd-El-Atty B, ElAffendi M, El-Latif AA. A novel image cryptosystem using Gray code, quantum walks, and Henon map for cloud applications. Complex & Intelligent Systems. 2023 Feb;9(1):609-24.

[184] Deepak S, Abimanyu NK, Kumar H. Review On Prevention of Data Leakage in Cloud Server by Utilizing Watermarking and Double Encryption Techniques. In2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS) 2023 Mar 17 (Vol. 1, pp. 1619-1625). IEEE.

[185] Lin H, Xue Q, Feng J, Bai D. Internet of things intrusion detection model and algorithm based on cloud computing and multi-feature extraction extreme learning machine. Digital Communications and Networks. 2023 Feb 1;9(1):111-24.

[186] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[187] Anand P, Singh Y, Selwal A, Alazab M, Tanwar S, Kumar N. IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges. IEEE Access. 2020 Sep 9;8:168825-53.

[188] West J. A prediction model framework for cyber-attacks to precision agriculture technologies. Journal of Agricultural & Food Information. 2018 Oct 2;19(4):307-30.

[189] Yaacoub JP, Salman O, Noura HN, Kaaniche N, Chehab A, Malli M. Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and microsystems. 2020 Sep 1;77:103201.

[190] Watkins L, Ramos J, Snow G, Vallejo J, Robinson WH, Rubin AD, Ciocco J, Jedrzejewski F, Liu J, Li C. Exploiting multi-vendor vulnerabilities as back-doors to counter the threat of rogue small unmanned aerial systems. InProceedings of the 1st ACM MobiHoc workshop on mobile IoT sensing, security, and privacy 2018 Jun 26 (pp. 1-6).

[191] Abood EW, Hussien ZA, Kawi HA, Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Kalafy A, Ahmad S. Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical & Computer Engineering (2088-8708). 2023 Feb 1;13(1).

[192] Senoo EE, Akansah E, Mendonça I, Aritsugi M. Monitoring and Control Framework for IoT, Implemented for Smart Agriculture. Sensors. 2023 Mar 1;23(5):2714.

[193] Glaroudis D, Iossifides A, Chatzimisios P. Survey, comparison and research challenges of IoT application protocols for smart farming. Computer Networks. 2020 Feb 26;168:107037.

[194] Aljedaani B, Ahmad A, Zahedi M, Babar MA. End-users' knowledge and perception about security of clinical mobile health apps: A case study with two Saudi Arabian mHealth providers. Journal of Systems and Software. 2023 Jan 1;195:111519.

[195] Qin ZZ, Barrett R, del Mar Castro M, Zaidi S, Codlin AJ, Creswell J, Denkinger CM. Early user experience and lessons learned using ultra-portable digital X-ray with computer-aided detection (DXR-CAD) products: A qualitative study from the perspective of healthcare providers. Plos one. 2023 Feb 24;18(2):e0277843.

[196] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9;3(5):364.

[197] Telo J. Smart City Security Threats and Countermeasures in the Context of Emerging Technologies. International Journal of Intelligent Automation and Computing. 2023 Feb 27;6(1):31-45.

[198] Islam SN, Baig Z, Zeadally S. Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures. IEEE Transactions on Industrial Informatics. 2019 Jul 26;15(12):6522-30.

[199] Sayed MA, Atallah R, Assi C, Debbabi M. Electric vehicle attack impact on power grid operation. International Journal of Electrical Power & Energy Systems. 2022 May 1;137:107784.

[200] Javaid M, Haleem A, Khan IH, Suman R. Understanding the potential applications of Artificial Intelligence in Agriculture Sector. Advanced Agrochem. 2023 Mar 1;2(1):15-30.

[201] Juncal MJ, Masino P, Bertone E, Stewart RA. Towards nutrient neutrality: A review of agricultural runoff mitigation strategies and the development of a decision-making framework. Science of The Total Environment. 2023 May 20;874:162408.

[202] Kitchin R, Dodge M. The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. Journal of urban technology. 2019 Apr 3;26(2):47-65.

[203] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[204] Gill SS, Xu M, Ottaviani C, Patros P, Bahsoon R, Shaghaghi A, Golec M, Stankovski V, Wu H, Abraham A, Singh M. AI for next generation computing: Emerging trends and future directions. Internet of Things. 2022 Aug 1;19:100514.

[205] Jakku E, Taylor B, Fleming A, Mason C, Fielke S, Sounness C, Thorburn P. “If they don’t tell us what they do with it, why would we trust them?” Trust, transparency and benefit-sharing in Smart Farming. NJAS-Wageningen Journal of Life Sciences. 2019 Dec 1;90:100285.

[206] Gayatri MK, Jayasakthi J, Mala GA. Providing Smart Agricultural solutions to farmers for better yielding using IoT. In2015 IEEE Technological Innovation in ICT for Agriculture and Rural Development (TIAR) 2015 Jul 10 (pp. 40-43). IEEE.

[207] Khanna A, Kaur S. Evolution of Internet of Things (IoT) and its significant impact in the field of Precision Agriculture. Computers and electronics in agriculture. 2019 Feb 1;157:218-31.

[208] Mitra A, Vangipuram SL, Bapatla AK, Bathalapalli VK, Mohanty SP, Kougianos E, Ray C. Everything you wanted to know about smart agriculture. arXiv preprint arXiv:2201.04754. 2022 Jan 13.

[209] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[210] Heideker A, Ottolini D, Zyrianoff I, Neto AT, Cinotti TS, Kamienski C. IoT-based measurement for smart agriculture. In2020 IEEE International Workshop on Metrology for Agriculture and Forestry (MetroAgriFor) 2020 Nov 4 (pp. 68-72). IEEE.

[211] Popović T, Latinović N, Pešić A, Zečević Ž, Krstajić B, Djukanović S. Architecting an IoT-enabled platform for precision agriculture and ecological monitoring: A case study. Computers and electronics in agriculture. 2017 Aug 1;140:255-65.

[212] Pranto TH, Noman AA, Mahmud A, Haque AB. Blockchain and smart contract for IoT enabled smart agriculture. PeerJ Computer Science. 2021 Mar 31;7:e407.

[213] Jayaraman PP, Yavari A, Georgakopoulos D, Morshed A, Zaslavsky A. Internet of things platform for smart farming: Experiences and lessons learnt. Sensors. 2016 Nov 9;16(11):1884.

[214] Qiu Z, Ma J, Zhang H, Al Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Concurrent pipeline rendering scheme based on GPU multi-queue and partitioning images. InInternational Conference on Optics and Machine Vision (ICOMV 2023) 2023 Apr 14 (Vol. 12634, pp. 143-149). SPIE.

[215] Bazzana D, Foltz J, Zhang Y. Impact of climate smart agriculture on food security: an agent-based analysis. Food Policy. 2022 Aug 1;111:102304.

[216] Amiri-Zarandi M, Hazrati Fard M, Yousefinaghani S, Kaviani M, Dara R. A platform approach to smart farm information processing. Agriculture. 2022 Jun 10;12(6):838.

[217] Shaaban AM, Chlup S, El-Araby N, Schmittner C. Towards Optimized Security Attributes for IoT Devices in Smart Agriculture Based on the IEC 62443 Security Standard. Applied Sciences. 2022 Jun 2;12(11):5653.

[218] Riaz AR, Gilani SM, Naseer S, Alshmrany S, Shafiq M, Choi JG. Applying Adaptive Security Techniques for Risk Analysis of Internet of Things (IoT)-Based Smart Agriculture. Sustainability. 2022 Sep 2;14(17):10964.

[219] Nyangaresi VO. Provably secure protocol for 5G HetNets. In2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[220] Al Asif MR, Hasan KF, Islam MZ, Khondoker R. STRIDE-based cyber security threat modeling for IoT-enabled precision agriculture systems. In2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI) 2021 Dec 18 (pp. 1-6). IEEE.

[221] Cho SH, Kang DS, Kang MS, Kim HS, Bae JW, Lee CI, Ji HB, Won YH, Hong HK, Kim K. A study on threat modeling in smart greenhouses.

[222] Catalano C, Paiano L, Calabrese F, Cataldo M, Mancarella L, Tommasi F. Anomaly detection in smart agriculture systems. Computers in Industry. 2022 Dec 1;143:103750.

[223] Valenza F, Karafili E, Steiner RV, Lupu EC. A hybrid threat model for smart systems. IEEE Transactions on Dependable and Secure Computing. 2022 Oct 11.

[224] Rodríguez JP, Montoya-Munoz AI, Rodriguez-Pabon C, Hoyos J, Corrales JC. IoT-Agro: A smart farming system to Colombian coffee farms. Computers and Electronics in Agriculture. 2021 Nov 1;190:106442.

[225] Nyangaresi VO. ECC based authentication scheme for smart homes. In2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[226] Liu W, Shao XF, Wu CH, Qiao P. A systematic literature review on applications of information and communication technologies and blockchain technologies for precision agriculture development. Journal of Cleaner Production. 2021 May 20;298:126763.

[227] Chaganti R, Varadarajan V, Gorantla VS, Gadekallu TR, Ravi V. Blockchain-based cloud-enabled security monitoring using Internet of Things in smart agriculture. Future Internet. 2022 Aug 24;14(9):250.

[228] Shyamala Devi M, Suguna R, Joshi AS, Bagate RA. Design of IoT blockchain based smart agriculture for enlightening safety and security. InEmerging Technologies in Computer Engineering: Microservices in Big Data Analytics: Second International Conference, ICETCE 2019, Jaipur, India, February 1–2, 2019, Revised Selected Papers 2 2019 (pp. 7-19). Springer Singapore.

[229] Sajja GS, Rane KP, Phasinam K, Kassanuk T, Okoronkwo E, Prabhu P. Towards applicability of blockchain in agriculture sector. Materials Today: Proceedings. 2023 Jan 1;80:3705-8.

[230] Xiong H, Dalhaus T, Wang P, Huang J. Blockchain technology for agriculture: applications and rationale. frontiers in Blockchain. 2020 Feb 21;3:7.

[231] Nyangaresi VO, Abd-Elnaby M, Eid MM, Nabih Zaki Rashed A. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. 2022 Sep;33(9):e4528.

[232] Kumar R, Kumar P, Tripathi R, Gupta GP, Gadekallu TR, Srivastava G. SP2F: A secured privacy-preserving framework for smart agricultural Unmanned Aerial Vehicles. Computer Networks. 2021 Mar 14;187:107819.

[233] Song J, Zhong Q, Wang W, Su C, Tan Z, Liu Y. FPDP: Flexible privacy-preserving data publishing scheme for smart agriculture. IEEE Sensors Journal. 2020 Aug 18;21(16):17430-8.

[234] Yang X, Shu L, Chen J, Ferrag MA, Wu J, Nurellari E, Huang K. A survey on smart agriculture: Development modes, technologies, and security and privacy challenges. IEEE/CAA Journal of Automatica Sinica. 2021;8(2):273-302.

[235] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014;16(5):137-44.

[236] Friha O, Ferrag MA, Shu L, Maglaras L, Choo KK, Nafaa M. FELIDS: Federated learning-based intrusion detection system for agricultural Internet of Things. Journal of Parallel and Distributed Computing. 2022 Jul 1;165:17-31.

[237] El-Ghamry A, Darwish A, Hassanien AE. An optimized CNN-based intrusion detection system for reducing risks in smart farming. Internet of Things. 2023 Jul 1;22:100709.

[238] Saba T, Rehman A, Sadad T, Kolivand H, Bahaj SA. Anomaly-based intrusion detection system for IoT networks through deep learning model. Computers and Electrical Engineering. 2022 Apr 1;99:107810.

[239] Kheddar H, Himeur Y, Awad AI. Deep Transfer Learning Applications in Intrusion Detection Systems: A Comprehensive Review. arXiv preprint arXiv:2304.10550. 2023 Apr 19.

[240] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[241] Wang M, Yang N, Weng N. Securing a Smart Home with a Transformer-Based IoT Intrusion Detection System. Electronics. 2023 May 4;12(9):2100.

[242] Martins I, Resende JS, Sousa PR, Silva S, Antunes L, Gama J. Host-based IDS: A review and open issues of an anomaly detection system in IoT. Future Generation Computer Systems. 2022 Mar 15.

[243] Fernandes G, Rodrigues JJ, Carvalho LF, Al-Muhtadi JF, Proença ML. A comprehensive survey on network anomaly detection. Telecommunication Systems. 2019 Mar 15;70:447-89.

[244] Bécue A, Praça I, Gama J. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. Artificial Intelligence Review. 2021 Jun;54(5):3849-86.

[245] Nyangaresi VO, Abduljabbar ZA, Ma J, Al Sibahee MA. Verifiable Security and Privacy Provisioning Protocol for High Reliability in Smart Healthcare Communication Environment. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 569-574). IEEE.

[246] Escobedo P, Ramos-Lorente CE, Ejaz A, Erenas MM, Martínez-Olmos A, Carvajal MA, García-Núñez C, de Orbe-Payá I, Capitán-Vallvey LF, Palma AJ. QRsens: Dual-purpose Quick Response code with built-in colorimetric sensors. Sensors and Actuators B: Chemical. 2023 Feb 1;376:133001.

[247] Shrivastava A, Krishna KM, Rinawa ML, Soni M, Ramkumar G, Jaiswal S. Inclusion of IoT, ML, and blockchain technologies in next generation industry 4.0 environment. Materials Today: Proceedings. 2023 Jan 1;80:3471-5.

[248] Dehlaghi-Ghadim A, Balador A, Moghadam MH, Hansson H, Conti M. ICSSIM—A framework for building industrial control systems security testbeds. Computers in Industry. 2023 Jun 1;148:103906.

[249] Nandy T, Idris MY, Noor RM, Kiah LM, Lun LS, Juma'at NB, Ahmedy I, Ghani NA, Bhattacharyya S. Review on security of internet of things authentication mechanism. IEEE Access. 2019 Oct 16;7:151054-89.

[250] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[251] Radoglou-Grammatikis P, Sarigiannidis P, Iturbe E, Rios E, Martinez S, Sarigiannidis A, Eftathopoulos G, Spyridis Y, Sesis A, Vakakis N, Tzovaras D. Spear siem: A security information and event management system for the smart grid. Computer Networks. 2021 Jul 5;193:108008.

[252] Morufu O, Juliana N, Abdulhamid SI, Odey P. Performance Analysis of Security Information and Event Management Solutions Detecting Web-Based Attacks. Proceedings of the Cyber Secure Nigeria 2019 Conference, CBN International Training Institute, Maitama, Abuja, Nigeria.

[253] Miloslavskaya N, Tolstoy A. IoTBlockSIEM for information security incident management in the internet of things ecosystem. Cluster Computing. 2020 Sep;23:1911-25.

[254] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22;6(7):154.

[255] Noguchi T, Nakagawa M, Yoshida M, Ramonet AG. A Secure Secret Key-Sharing System for Resource-Constrained IoT Devices using MQTT. In2022 24th International Conference on Advanced Communication Technology (ICACT) 2022 Feb 13 (pp. 147-153). IEEE.

[256] Singh P, Acharya B, Chaurasiya RK. Lightweight cryptographic algorithms for resource-constrained IoT devices and sensor networks. InSecurity and Privacy Issues in IoT Devices and Sensor Networks 2021 Jan 1 (pp. 153-185). Academic Press.

[257] Suárez-Albela M, Fraga-Lamas P, Castedo L, Fernández-Caramés TM. Clock frequency impact on the performance of high-security cryptographic cipher suites for energy-efficient resource-constrained IoT devices. Sensors. 2018 Dec 20;19(1):15.

[258] Thakor VA, Razzaque MA, Khandaker MR. Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access. 2021 Jan 19;9:28177-93.

[259] Nyangaresi VO, Ibrahim A, Abduljabbar ZA, Hussain MA, Al Sibahee MA, Hussien ZA, Ghrabat MJ. Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges. In2021 International Conference on Electrical, Computer and Energy Technologies (ICECET) 2021 Dec 9 (pp. 1-6). IEEE.

[260] Chukkapalli SS, Ranade P, Mittal S, Joshi A. A Privacy Preserving Anomaly Detection Framework for Cooperative Smart Farming Ecosystem. In2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA) 2021 Dec 13 (pp. 340-347). IEEE.

[261] Yan Q, Lou J, Vuran MC, Irmak S. Scalable Privacy-preserving Geo-distance Evaluation for Precision Agriculture IoT Systems. ACM Transactions on Sensor Networks (TOSN). 2021 Jul 22;17(4):1-30.

[262] Huning L, Bauer J, Aschenbruck N. A privacy preserving mobile crowdsensing architecture for a smart farming application. InProceedings of the First ACM Workshop on Mobile Crowdsensing Systems and Applications 2017 Nov 6 (pp. 62-67).

[263] Zhou M, Zheng Y, Guan Y, Peng L, Lu R. Efficient and privacy-preserving range-max query in fog-based agricultural IoT. Peer-to-Peer Networking and Applications. 2021 Jul;14(4):2156-70.

[264] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[265] Tiwari S, Jain A, Sapra V, Koundal D, Alenezi F, Polat K, Alhudhaif A, Nour M. A smart decision support system to diagnose arrhythymia using ensembled ConvNet and ConvNet-LSTM model. Expert Systems with Applications. 2023 Mar 1;213:118933.

[266] Wuni IY, Mazher KM. Ending the suitability quantification dilemma: intelligent decision support system for modular integrated construction in a high-density metropolis. Construction Innovation. 2023 Jan 11(ahead-of-print).

[267] Gardezi M, Stock R. Growing algorithmic governmentality: Interrogating the social construction of trust in precision agriculture. Journal of Rural Studies. 2021 May 1;84:1-1.

[268] Ofori M, El-Gayar O. Drivers and challenges of precision agriculture: a social media perspective. Precision Agriculture. 2021 Jun;22:1019-44.